[HTB] Bashed

10.10.10.68

Phase #1: Enumeration

80/tcp

gobuster scan reveals /dev directory

/dev has 2 php files: phpbash.min.php and phpbash.php

phpbash is a webshell

Phase #2: Exploit

Execute a python reverse shell

netcat (www-data)

Phase #3: Privilege Escalation

sudo -l: www-data can run any command as scriptmanager

switch to user scriptmanager

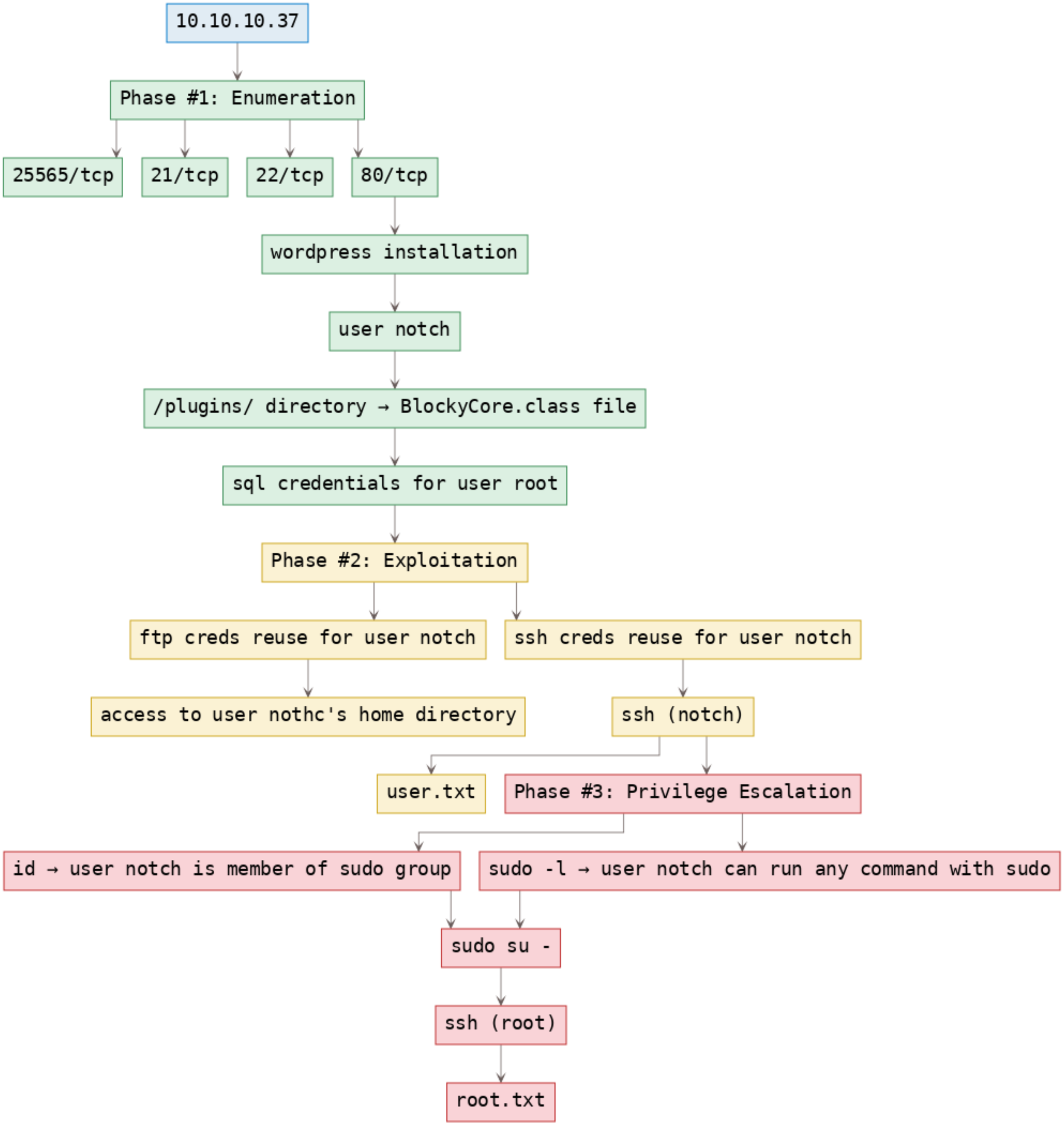
cronjob running a python script as root but owned by scriptmanager

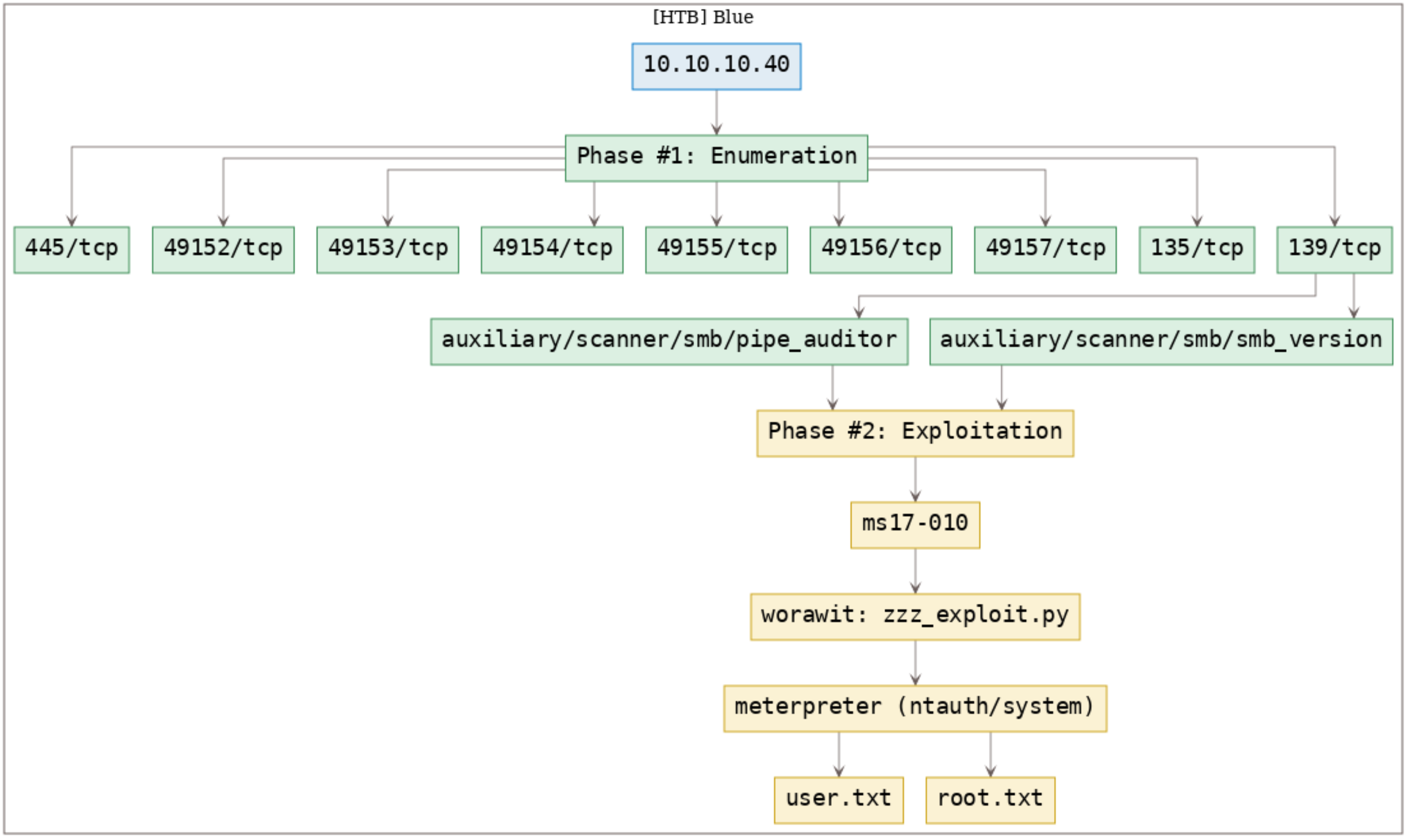
edit script to execute a python reverse shell

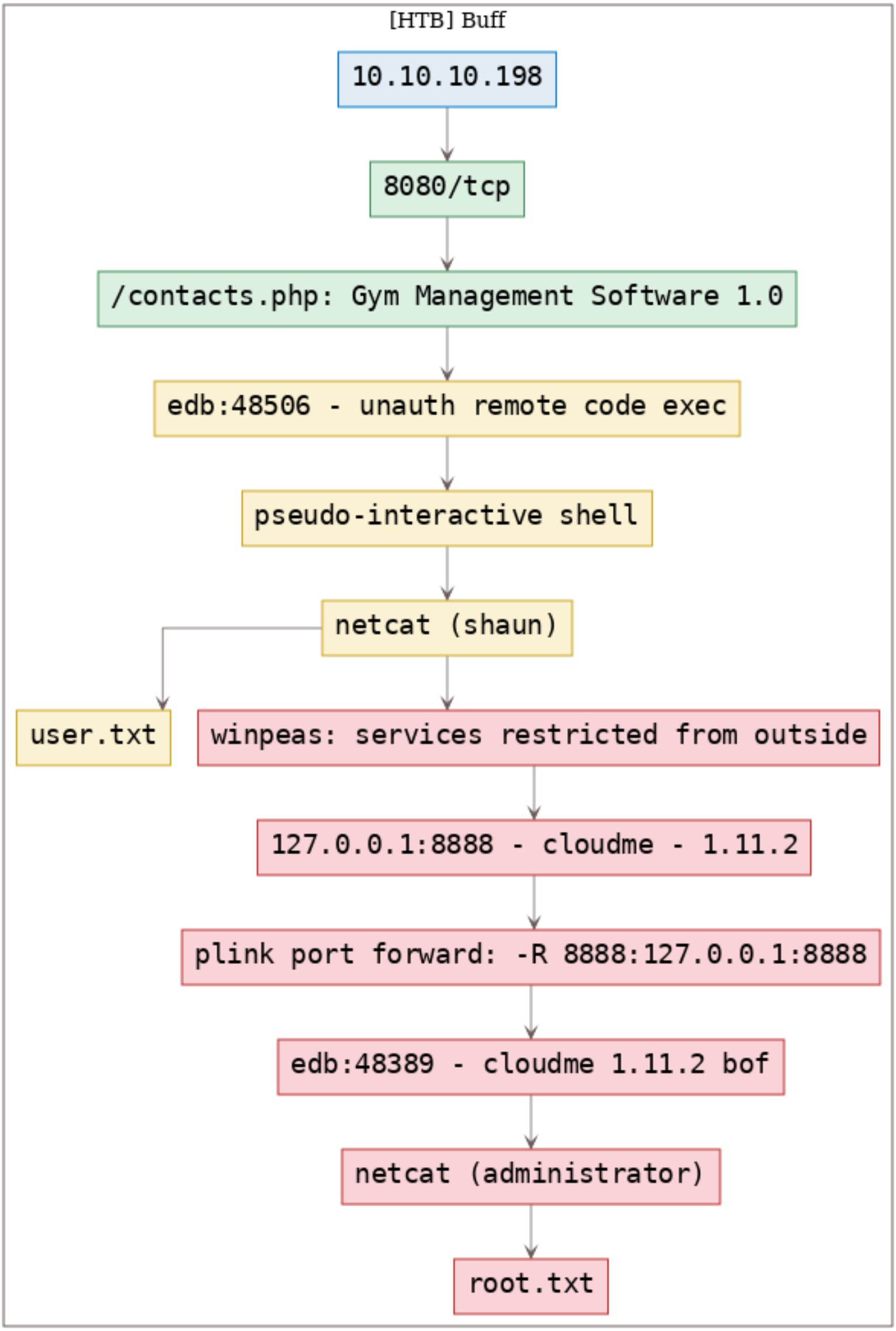
netcat (root)

root.txt

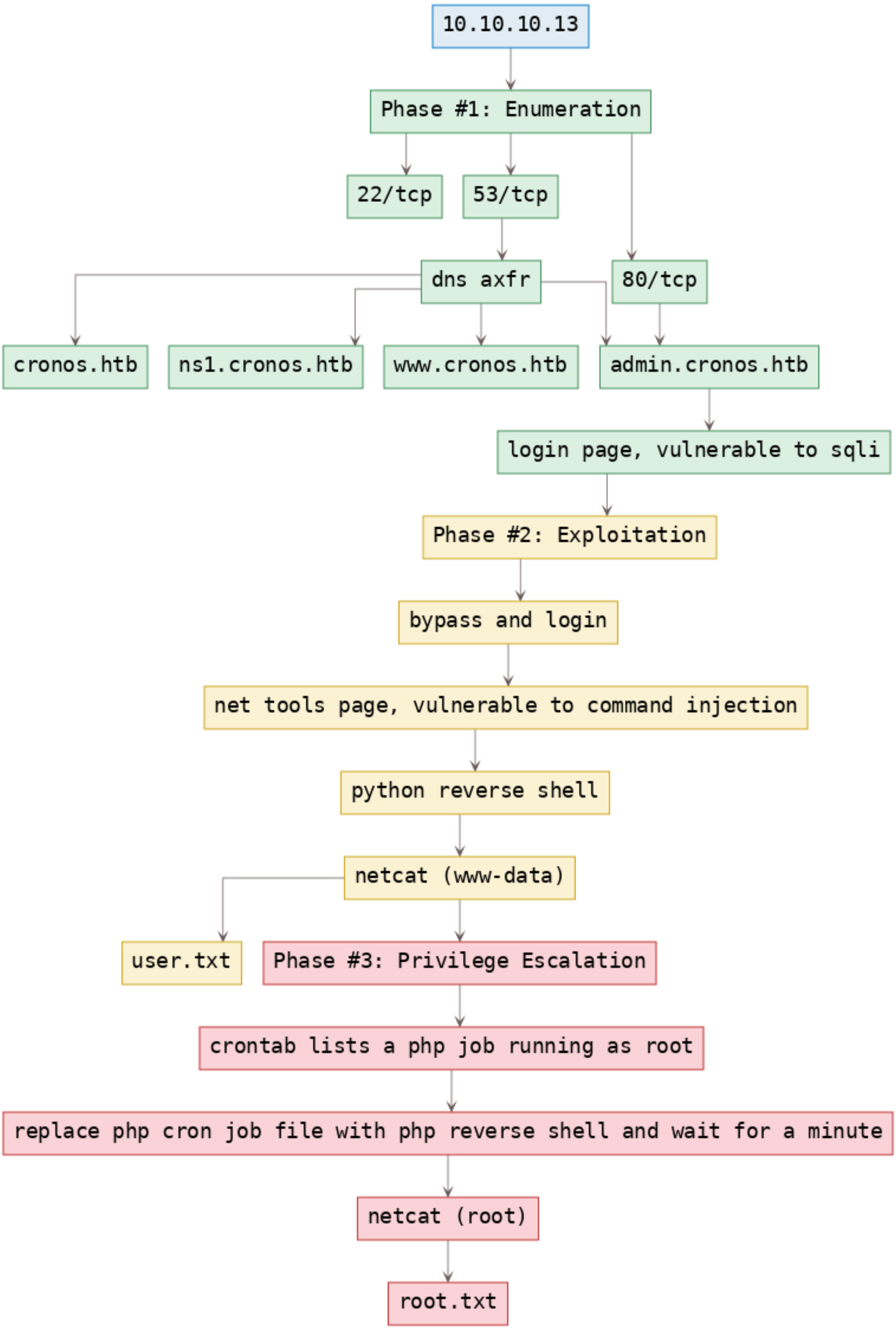
[HTB] Blocky

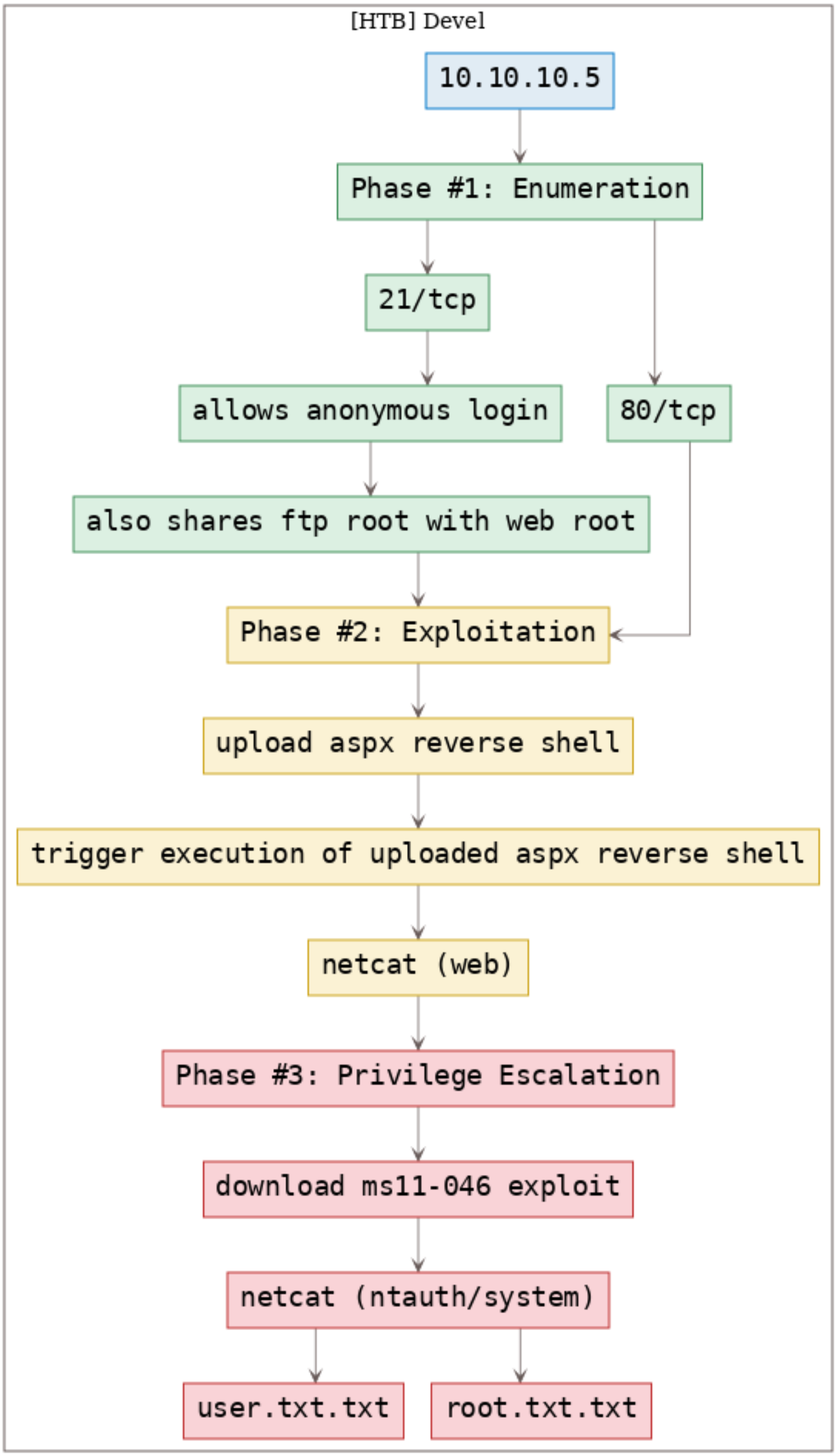

10.10.10.37
Phase #1: Enumeration
25565/tcp
21/tcp
22/tcp
80/tcp
wordpress installation
user notch
/plugins/ directory → BlockyCore.class file
sql credentials for user root
Phase #2: Exploitation
ftp creds reuse for user notch
ssh creds reuse for user notch
access to user nothc's home directory
ssh (notch)
user.txt
Phase #3: Privilege Escalation
id → user notch is member of sudo group
sudo -l → user notch can run any command with sudo
sudo su -
ssh (root)
root.txt

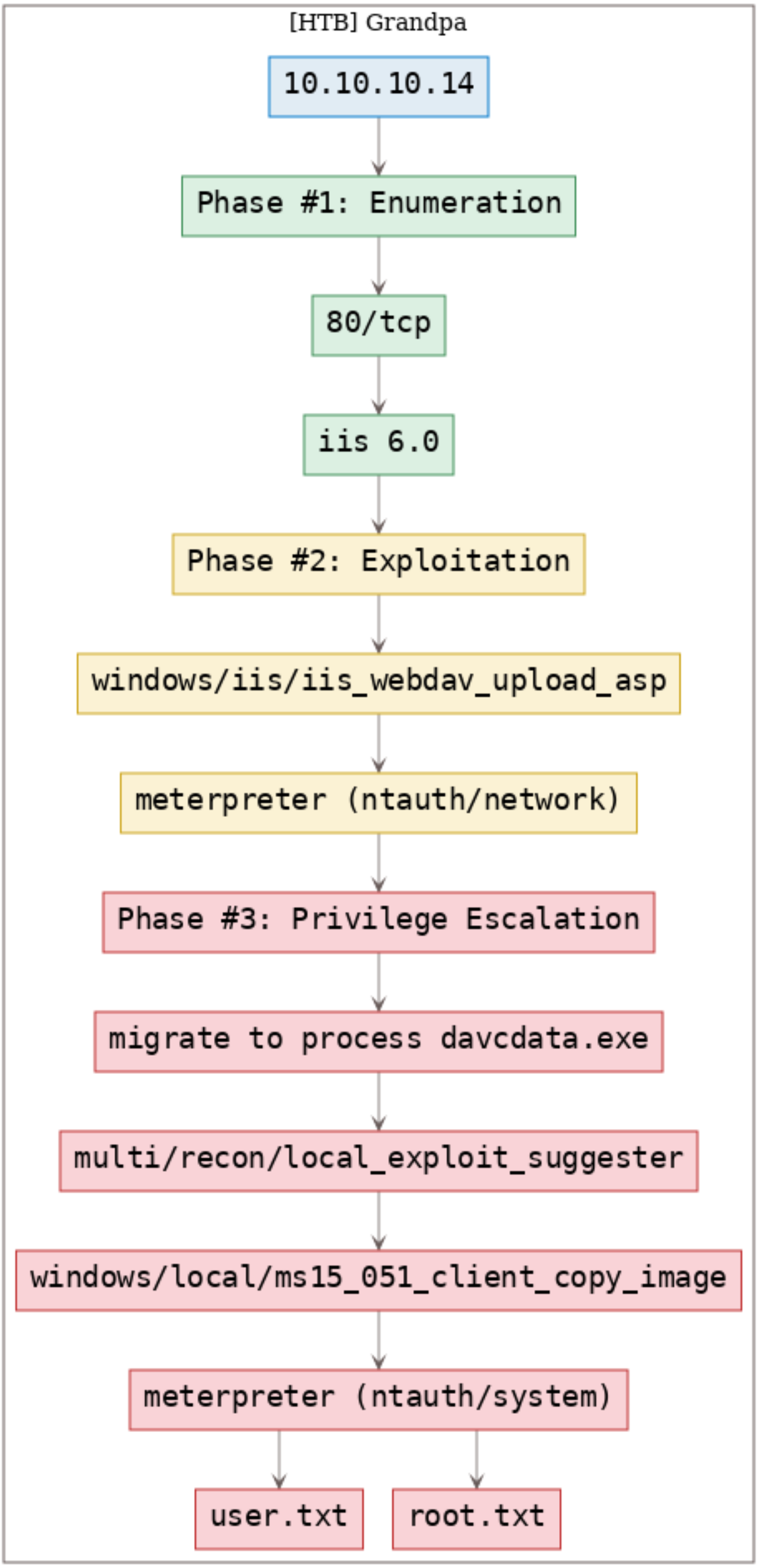

[HTB] Blue
10.10.10.40
Phase #1: Enumeration
445/tcp
49152/tcp
49153/tcp
49154/tcp
49155/tcp
49156/tcp
49157/tcp
135/tcp
139/tcp
auxiliary/scanner/smb/pipe_auditor
auxiliary/scanner/smb/smb_version
Phase #2: Exploitation
ms17-010
worawit: zzz_exploit.py
meterpreter (ntauth/system)
user.txt
root.txt

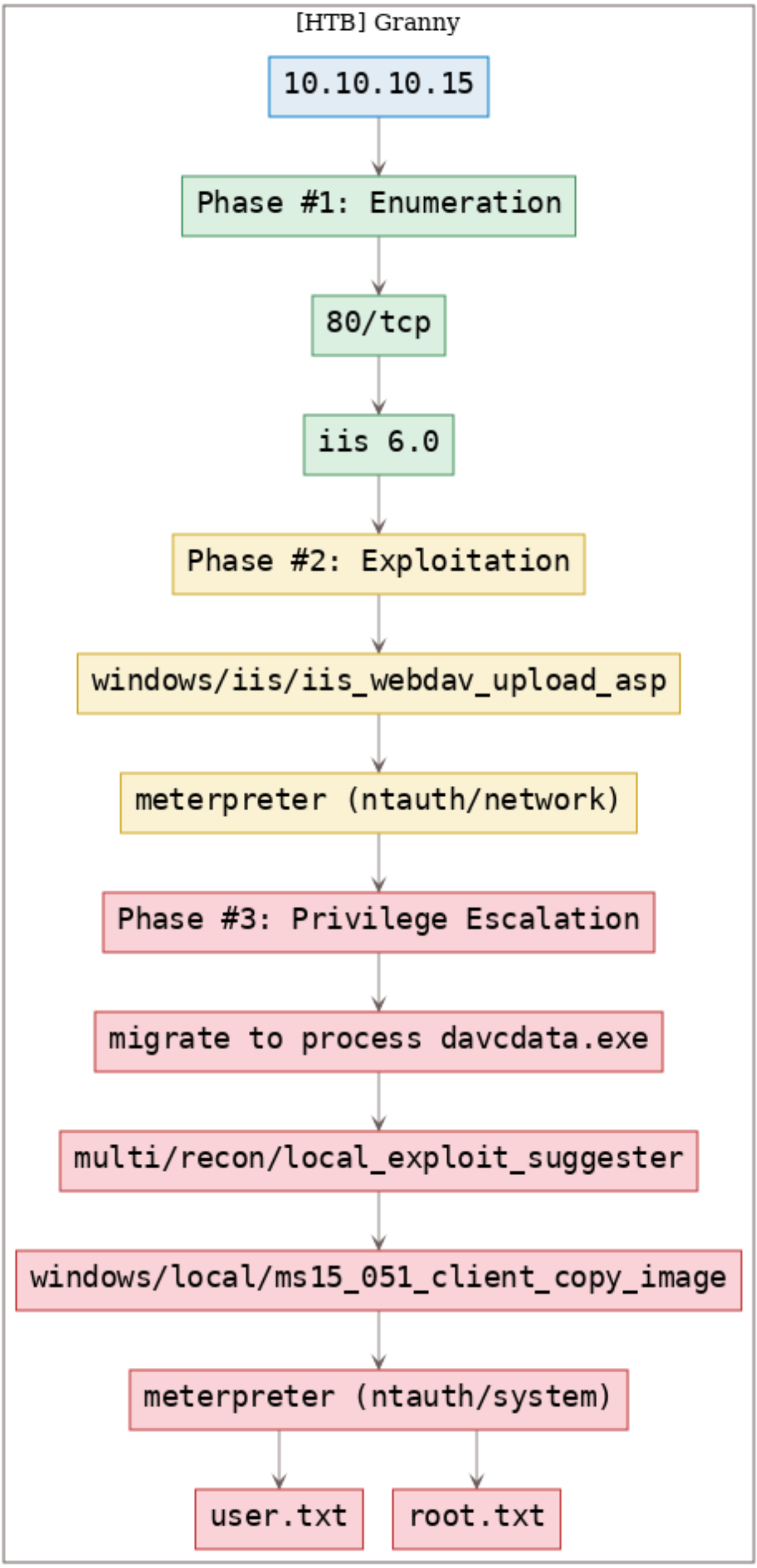

[HTB] Buff
10.10.10.198
8080/tcp
/contacts.php: Gym Management Software 1.0
edb:48506 - unauth remote code exec
pseudo-interactive shell
netcat (shaun)
user.txt
winpeas: services restricted from outside
127.0.0.1:8888 - cloudme - 1.11.2
plink port forward: -R 8888:127.0.0.1:8888
edb:48389 - cloudme 1.11.2 bof
netcat (administrator)
root.txt

[HTB] Cronos


10.10.10.13
Phase #1: Enumeration
22/tcp
53/tcp
dns axfr
80/tcp
cronos.htb
ns1.cronos.htb
www.cronos.htb
admin.cronos.htb
login page, vulnerable to sqli
Phase #2: Exploitation
bypass and login
net tools page, vulnerable to command injection
python reverse shell
netcat (www-data)
user.txt
Phase #3: Privilege Escalation
crontab lists a php job running as root
replace php cron job file with php reverse shell and wait for a minute
netcat (root)
root.txt

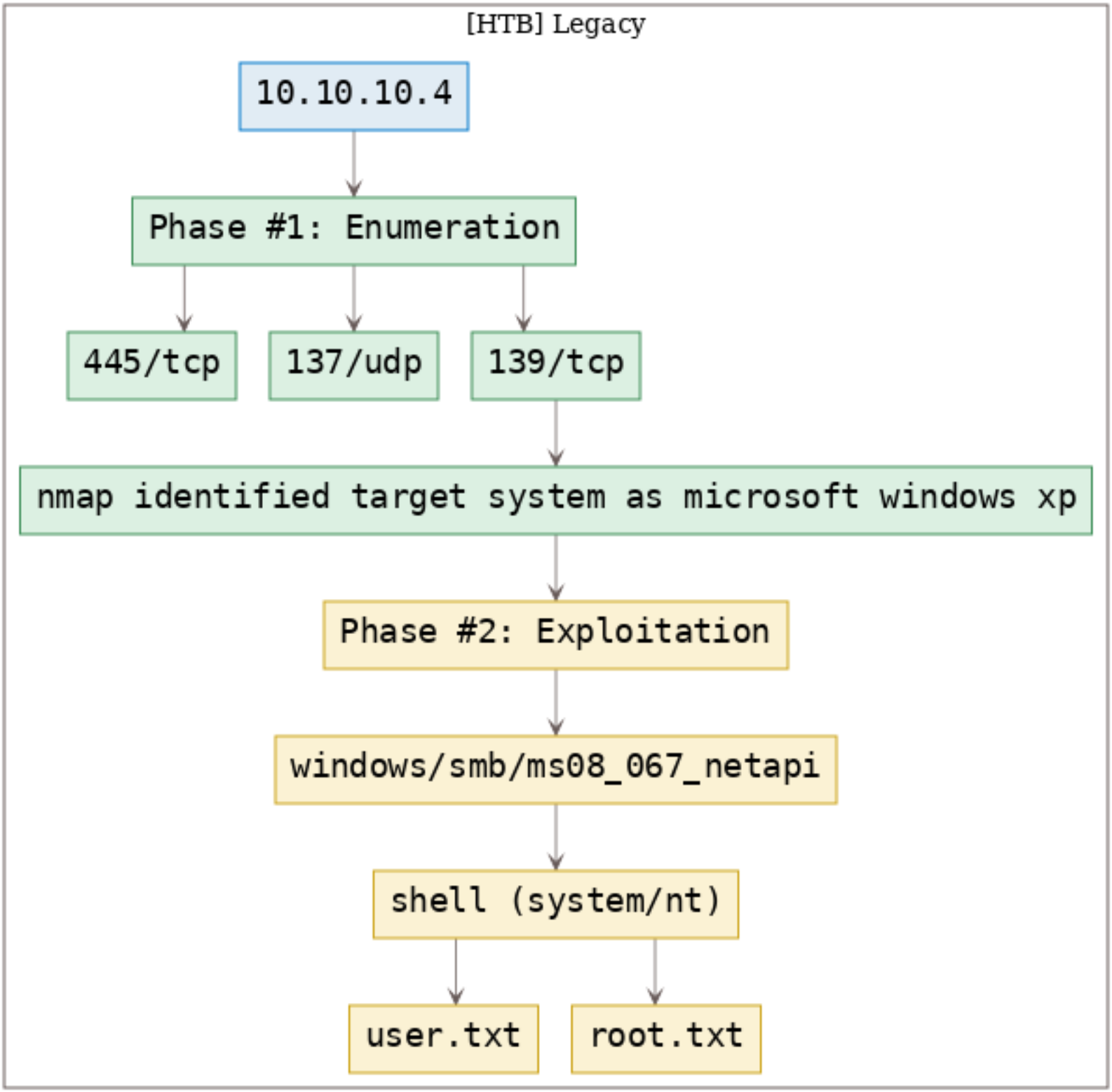

[HTB] Devel
10.10.10.5
Phase #1: Enumeration
21/tcp
allows anonymous login
also shares ftp root with web root
80/tcp
Phase #2: Exploitation
upload aspx reverse shell
trigger execution of uploaded aspx reverse shell
netcat (web)
Phase #3: Privilege Escalation
download ms11-046 exploit
netcat (ntauth/system)
user.txt.txt
root.txt.txt


[HTB] Grandpa
10.10.10.14
Phase #1: Enumeration
80/tcp
iis 6.0
Phase #2: Exploitation
windows/iis/iis_webdav_upload_asp
meterpreter (ntauth/network)
Phase #3: Privilege Escalation
migrate to process davcdata.exe
multi/recon/local_exploit_suggester
windows/local/ms15_051_client_copy_image
meterpreter (ntauth/system)
user.txt
root.txt

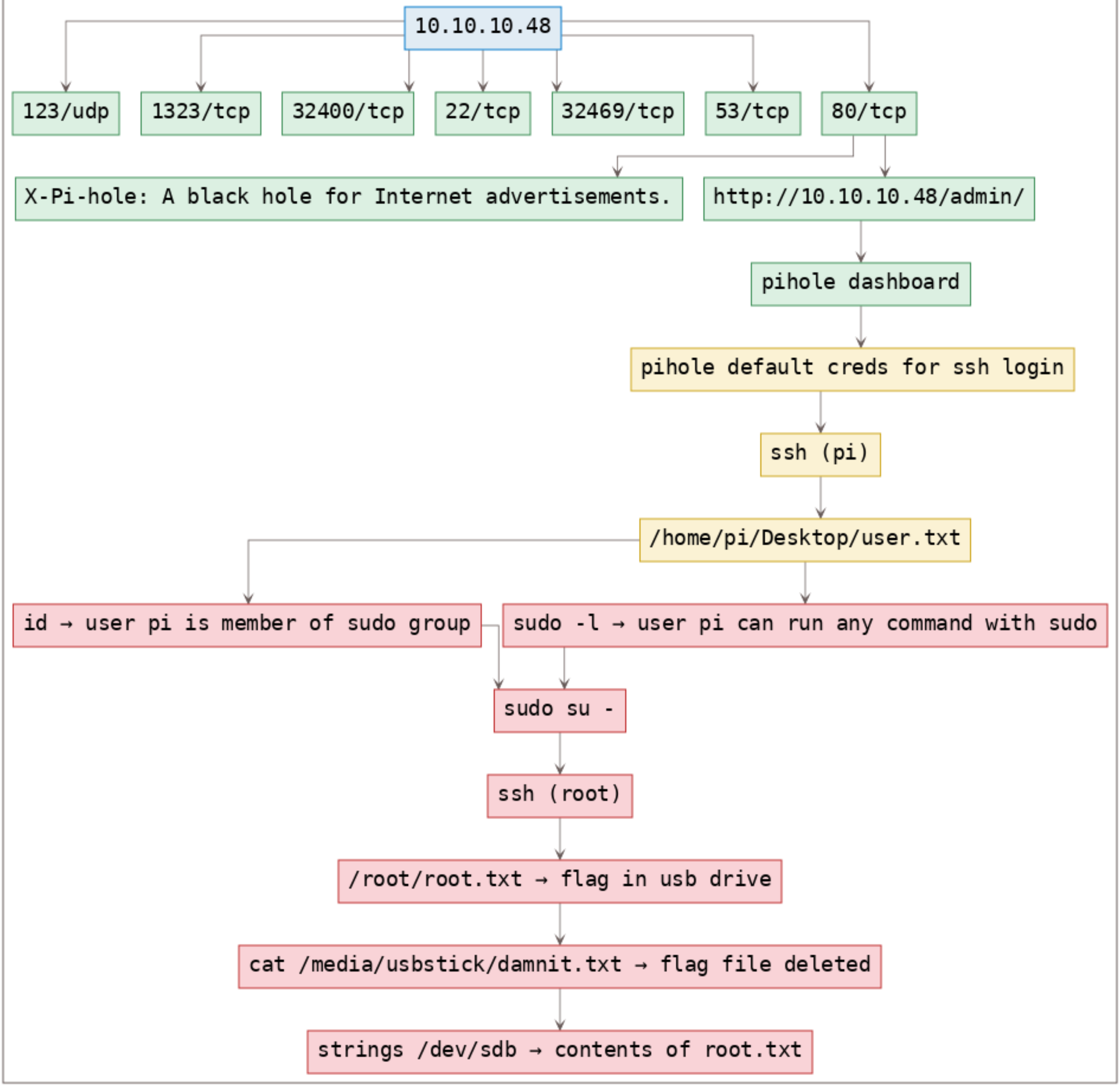

[HTB] Granny
10.10.10.15
Phase #1: Enumeration
80/tcp
iis 6.0
Phase #2: Exploitation
windows/iis/iis_webdav_upload_asp
meterpreter (ntauth/network)
Phase #3: Privilege Escalation
migrate to process davcdata.exe
multi/recon/local_exploit_suggester
windows/local/ms15_051_client_copy_image
meterpreter (ntauth/system)
user.txt
root.txt

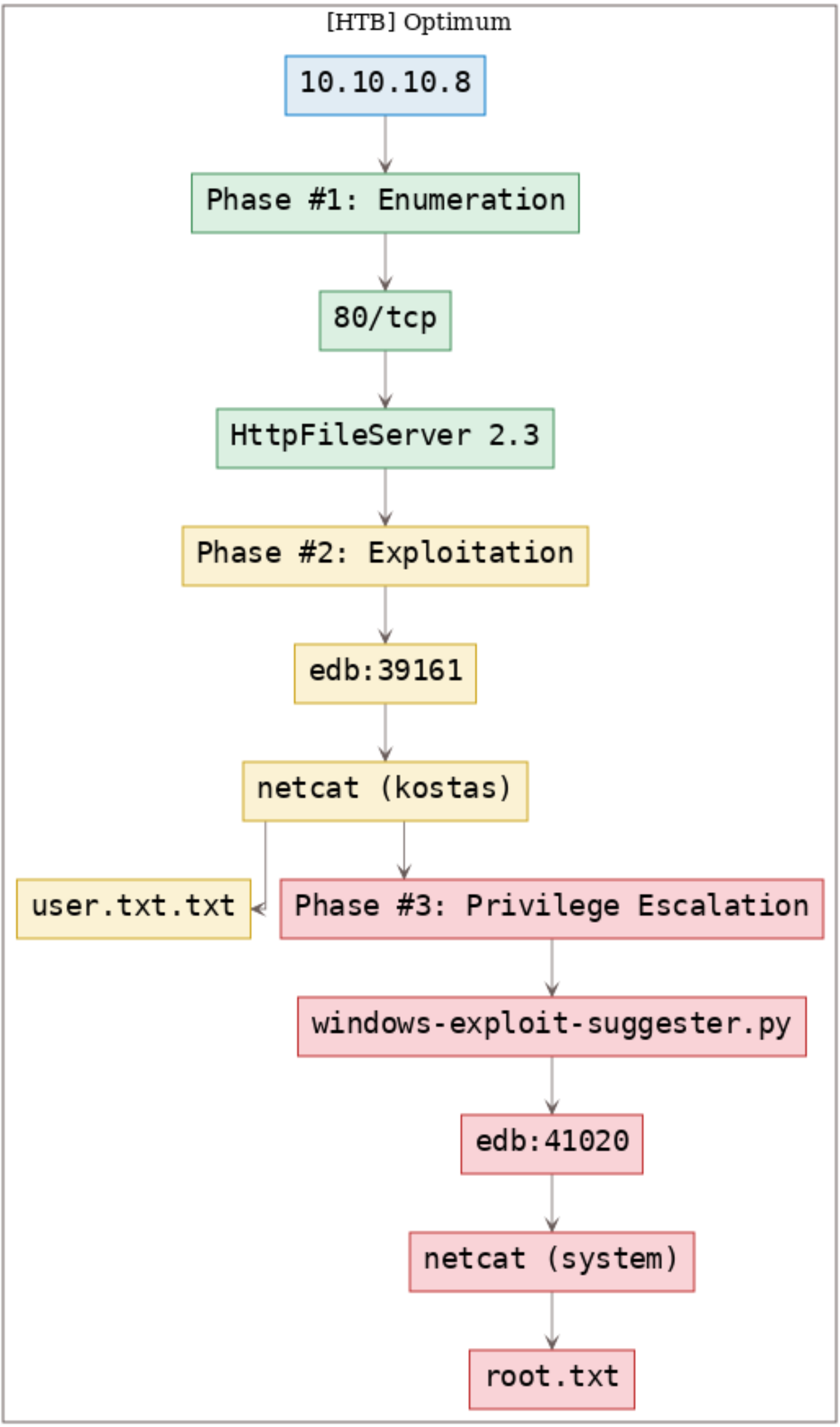
[HTB] Lame

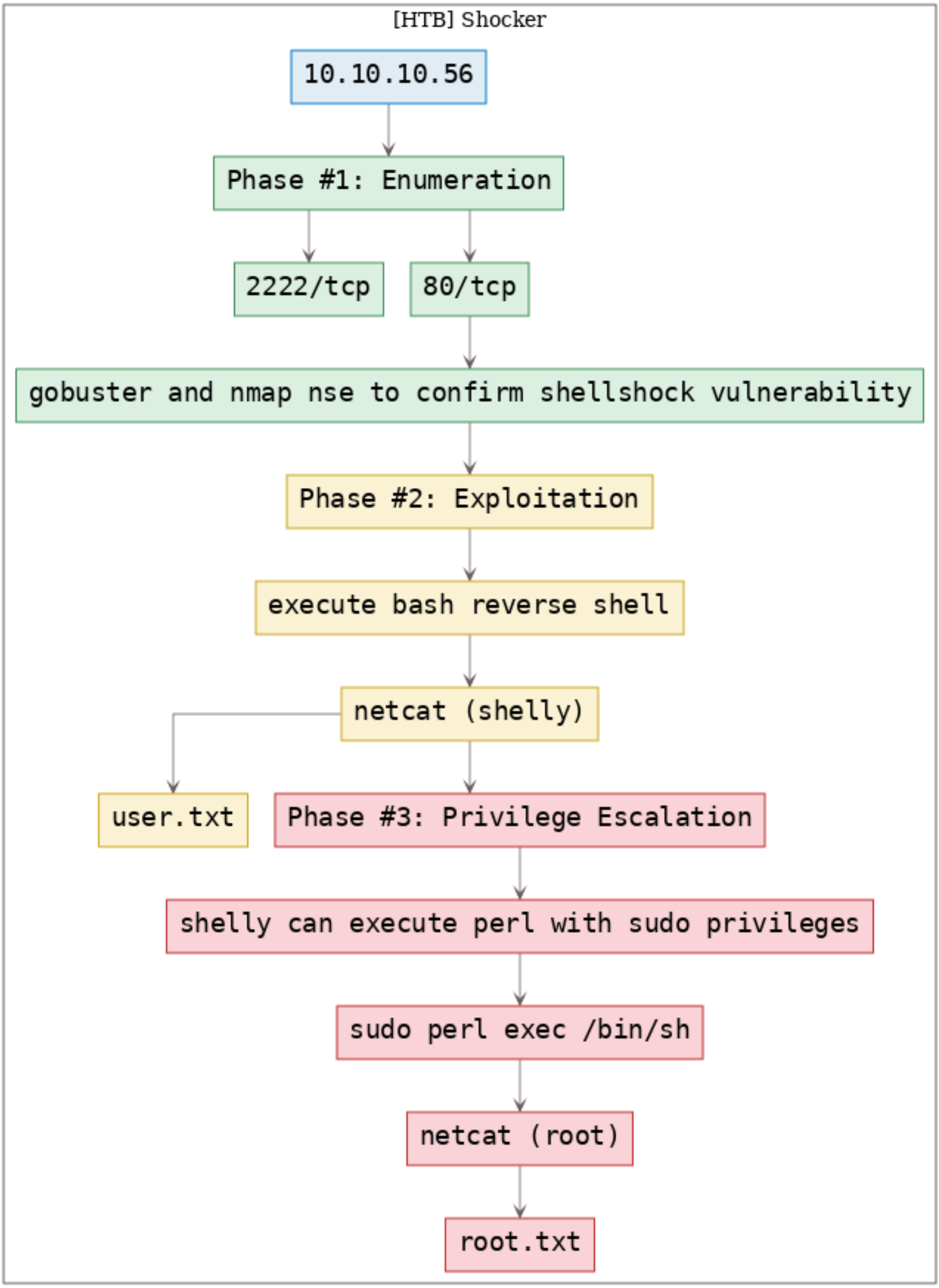
- 10.10.10.3
  - Phase #1: Enumeration
    - 139/tcp
      - tmp: read+write share with anonymous access
        - nothing interesting, no way to leverage uploaded files
      - samba 3.0.20-Debian
        - Phase #2: Exploitation
          - cve-2007-2447
            - smb usermap_script exploit
              - nc (root)
                - user.txt
                - root.txt
    - 445/tcp
    - 21/tcp
      - vsftpd 2.3.4
        - Phase #2: Exploitation
          - exploit/unix/ftp/vsftpd_234_backdoor
            - no session
      - anonymous login allowed
        - nothing interesting here
    - 22/tcp


[HTB] Legacy
10.10.10.4
Phase #1: Enumeration
445/tcp
137/udp
139/tcp
nmap identified target system as microsoft windows xp
Phase #2: Exploitation
windows/smb/ms08_067_netapi
shell (system/nt)
user.txt
root.txt

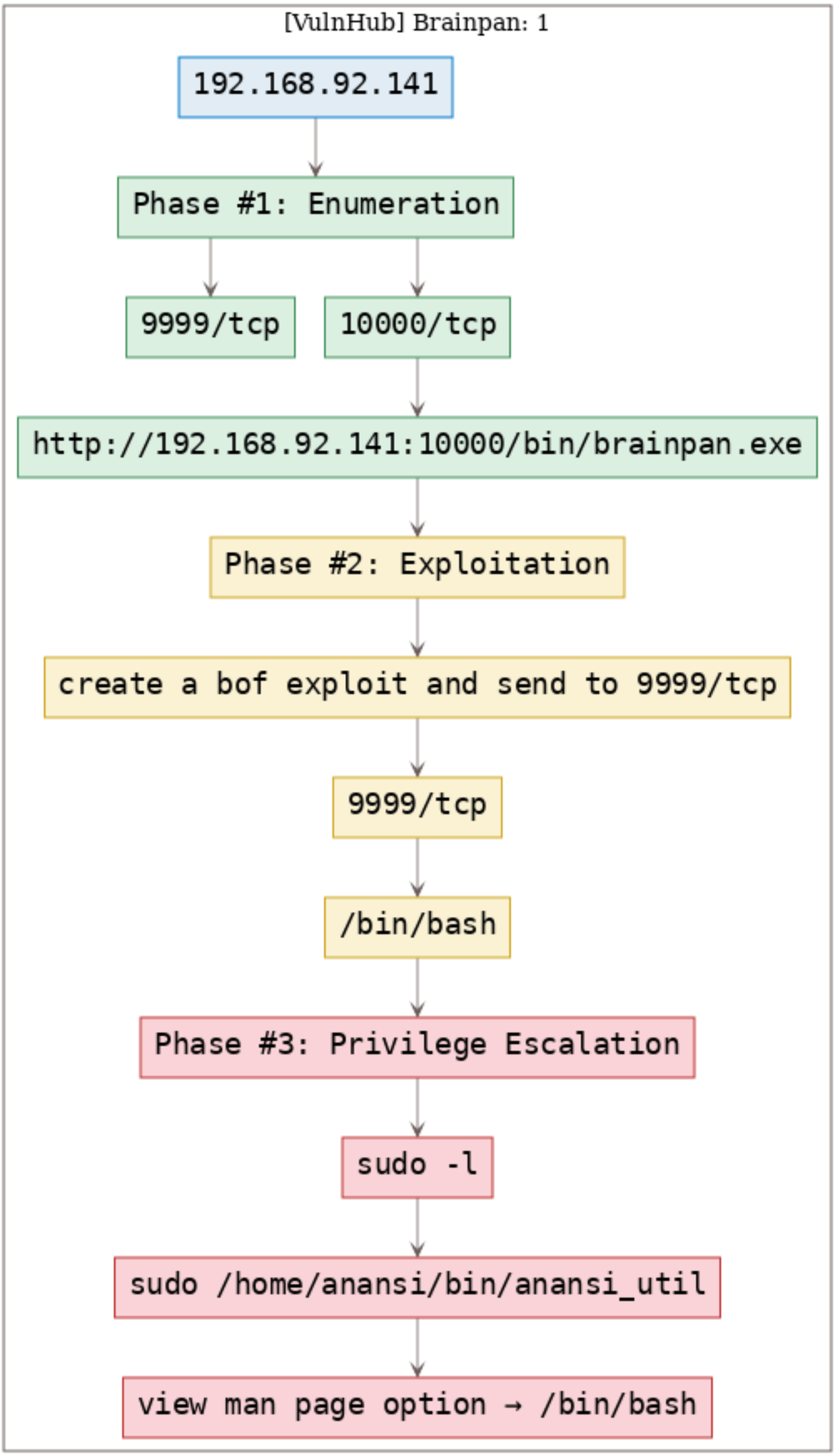
[HTB] Mirai


10.10.10.48
123/udp
1323/tcp
32400/tcp
22/tcp
32469/tcp
53/tcp
80/tcp
X-Pi-hole: A black hole for Internet advertisements.
http://10.10.10.48/admin/
pihole dashboard
pihole default creds for ssh login
ssh (pi)
/home/pi/Desktop/user.txt
id → user pi is member of sudo group
sudo -l → user pi can run any command with sudo
sudo su -
ssh (root)
/root/root.txt → flag in usb drive
cat /media/usbstick/damnit.txt → flag file deleted
strings /dev/sdb → contents of root.txt

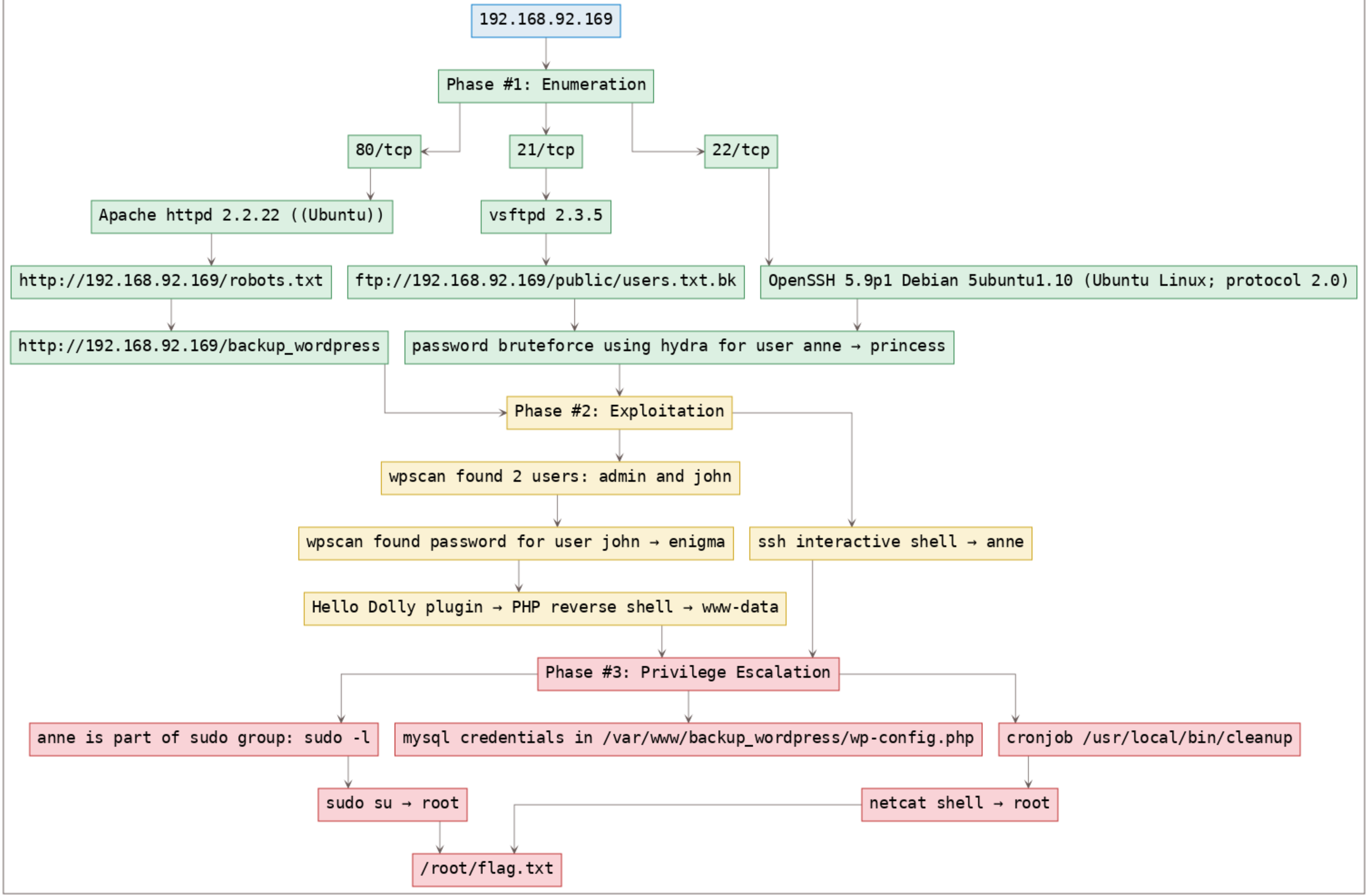

[HTB] Optimum
10.10.10.8
Phase #1: Enumeration
80/tcp
HttpFileServer 2.3
Phase #2: Exploitation
edb:39161
netcat (kostas)
user.txt.txt
Phase #3: Privilege Escalation
windows-exploit-suggester.py
edb:41020
netcat (system)
root.txt


[HTB] Shocker
10.10.10.56
Phase #1: Enumeration
2222/tcp
80/tcp
gobuster and nmap nse to confirm shellshock vulnerability
Phase #2: Exploitation
execute bash reverse shell
netcat (shelly)
user.txt
Phase #3: Privilege Escalation
shelly can execute perl with sudo privileges
sudo perl exec /bin/sh
netcat (root)
root.txt

[VulnHub] Billy Madison: 1.1


[VulnHub] Brainpan: 1
192.168.92.141
Phase #1: Enumeration
9999/tcp
10000/tcp
http://192.168.92.141:10000/bin/brainpan.exe
Phase #2: Exploitation
create a bof exploit and send to 9999/tcp
9999/tcp
/bin/bash
Phase #3: Privilege Escalation
sudo -l
sudo /home/anansi/bin/anansi_util
view man page option → /bin/bash

[VulnHub] BSides Vancouver: 2018 (Workshop)



[VulnHub] DC: 6

192.168.92.170

Phase #1: Enumeration

22/tcp

80/tcp

wordpress

hydra: mark/helpdesk01

wpscan: mark/helpdesk01

Phase #2: Exploitation

wordpress: activity monitor plugin

edb:45274

netcat: www-data

Phase #3: Privilege Escalation

/var/www/html/wp-config.php

/home/mark/stuff/things-to-do.txt

mysql: wpdbuser/meErKatZ

ssh: graham/GSo7isUM1D4

mysql

shell: graham

select user_login, user_pass from wp_users;

/home/jens/backups.sh

sudo -u jens /home/jens/backups.sh

shell: jens

echo os.execute('/bin/bash') >nse && sudo nmap --script=nse

shell: root

/root/theflag.txt

[VulnHub] Escalate_Linux: 1

192.168.92.173

Phase #1: Enumeration

111/tcp

137/udp

139/tcp

445/tcp

2049/tcp

39393/tcp

43937/tcp

55567/tcp

59061/tcp

80/tcp

dirb

http://192.168.92.173:80/shell.php

Phase #2: Exploitation

python reverse shell

user6@osboxes

Phase #3: Privilege Escalation

setuid files: /home/user3/shell

linenum.sh

echo 'bash -p' >>./.script.sh; chmod +x ./.script.sh; /home/user3/shell

mysql default credentials (root/root)

root@osboxes

mysql user credentials (mysql/mysql@12345)

[VulnHub] FristiLeaks: 1.3

192.168.92.133

Phase #1: Enumeration

80/tcp

http://192.168.92.133/robots.txt

http://192.168.92.133/cola

http://192.168.92.133/sisi

http://192.168.92.133/beer

http://192.168.92.133/fristi

rabbithole

#fristileaks admin portal

Phase #2: Exploitation

credentials from html source → eezeepz/keKkeKKeKKeKkEkkEk

upload php file with gif header and extension

netcat listener → php reverse shell → apache

Phase #3: Privilege Escalation

/var/www/notes.txt

/home/eezeepz/notes.txt

/tmp/runthis

/bin/bash → admin

/home/admin/cryptpass.py

su - fristigod

/home/fristigod/.secret_admin_stuff/doCom

/bin/bash → root

/root/fristileaks_secrets

[VulnHub] hackme: 1

192.168.92.180

Phase #1: Enumeration

80/tcp

http://192.168.92.180:80/index.php

http://192.168.92.180:80/login.php

http://192.168.92.180:80/register.php

foobar/foobar

http://192.168.92.180:80/login.php (foobar)

online book catalog

Phase 2: Exploitation

sqlmap: mysql dump

users: superadmin/Uncrackable

http://192.168.92.180:80/login.php (superadmin)

file upload: php reverse shell

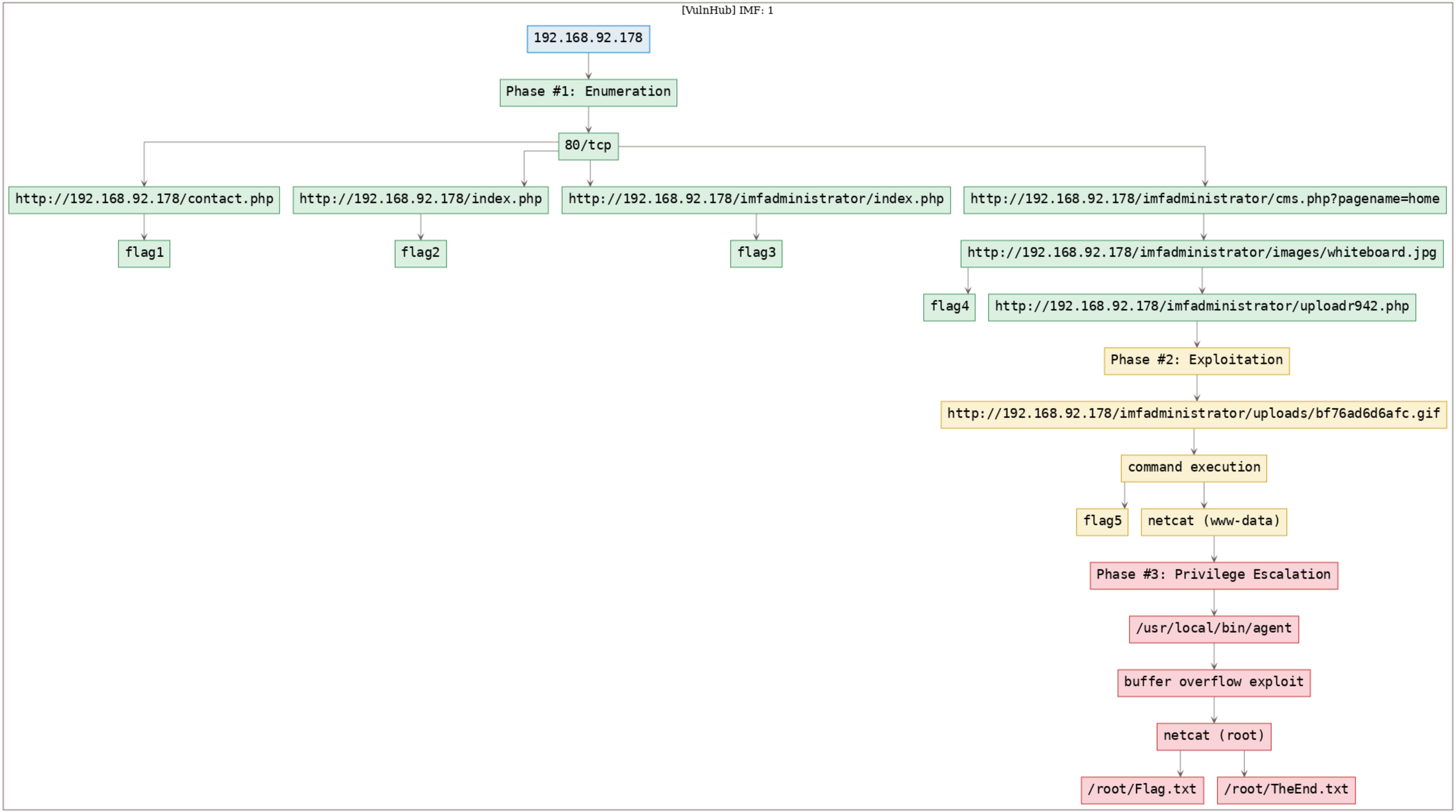
netcat (www-data)

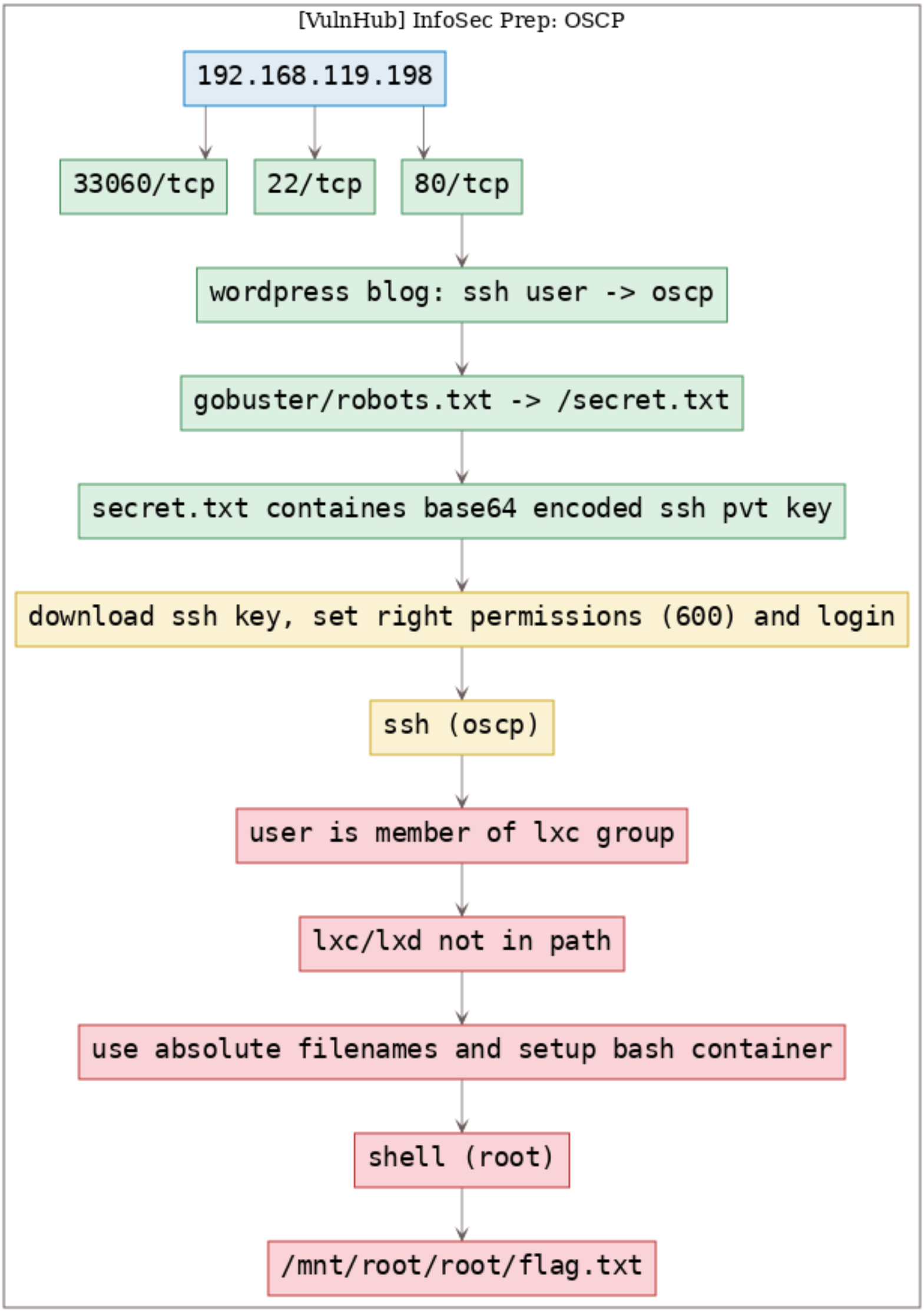
Phase #3: Privilege Escalation

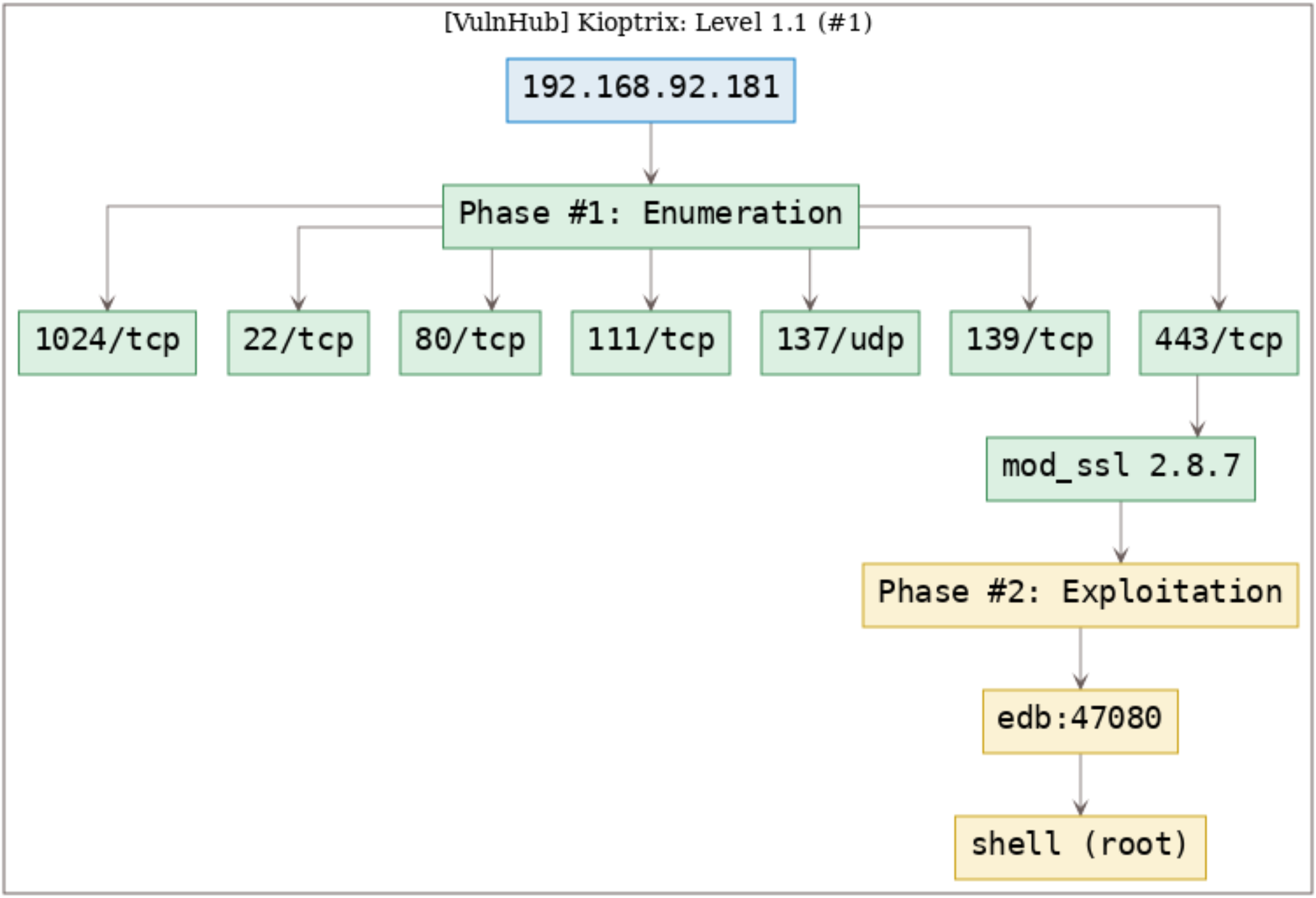
find setuid files

/home/legacy/touchmenot

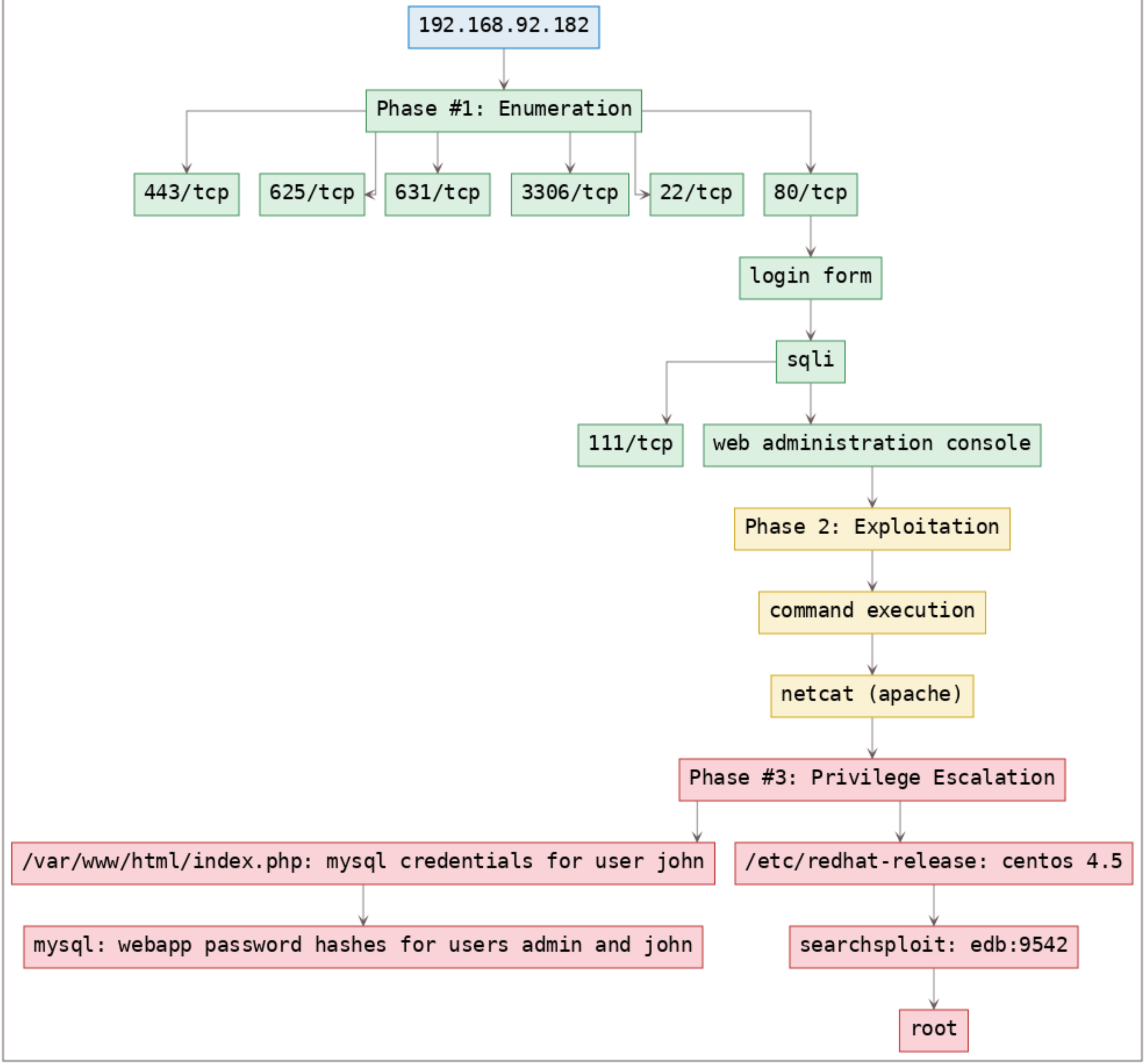
netcat (root)


[VulnHub] IMF: 1
192.168.92.178
Phase #1: Enumeration
80/tcp
http://192.168.92.178/contact.php
flag1
http://192.168.92.178/index.php
flag2
http://192.168.92.178/imfadministrator/index.php
flag3
http://192.168.92.178/imfadministrator/cms.php?pagename=home
http://192.168.92.178/imfadministrator/images/whiteboard.jpg
flag4
http://192.168.92.178/imfadministrator/uploadr942.php
Phase #2: Exploitation
http://192.168.92.178/imfadministrator/uploads/bf76ad6d6afc.gif
command execution
flag5
netcat (www-data)
Phase #3: Privilege Escalation
/usr/local/bin/agent
buffer overflow exploit
netcat (root)
/root/Flag.txt
/root/TheEnd.txt

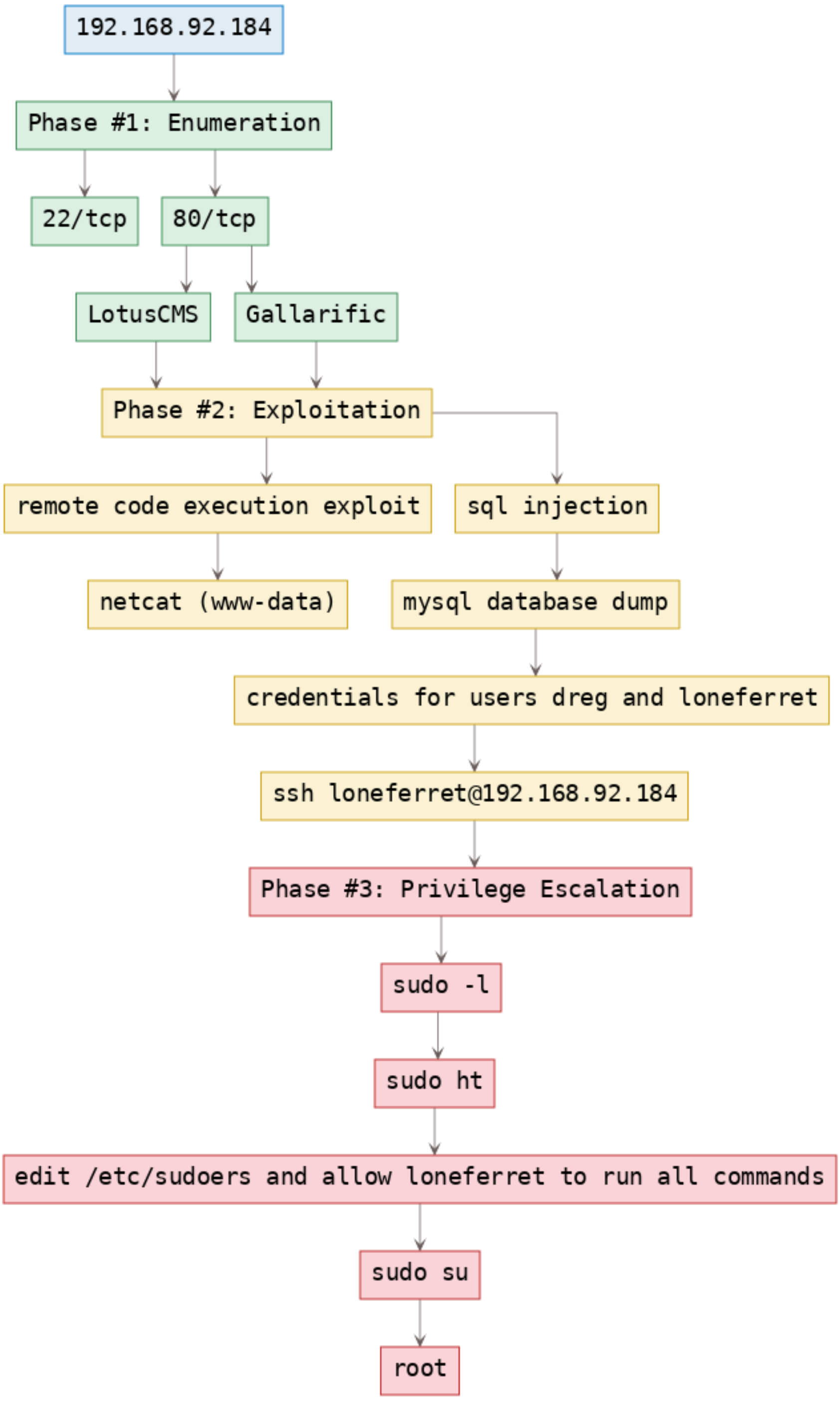

[VulnHub] InfoSec Prep: OSCP
192.168.119.198
33060/tcp
22/tcp
80/tcp
wordpress blog: ssh user -> oscp
gobuster/robots.txt -> /secret.txt
secret.txt containes base64 encoded ssh pvt key
download ssh key, set right permissions (600) and login
ssh (oscp)
user is member of lxc group
lxc/lxd not in path
use absolute filenames and setup bash container
shell (root)
/mnt/root/root/flag.txt


[VulnHub] Kioptrix: Level 1.1 (#1)
192.168.92.181
Phase #1: Enumeration
1024/tcp
22/tcp
80/tcp
111/tcp
137/udp
139/tcp
443/tcp
mod_ssl 2.8.7
Phase #2: Exploitation
edb:47080
shell (root)

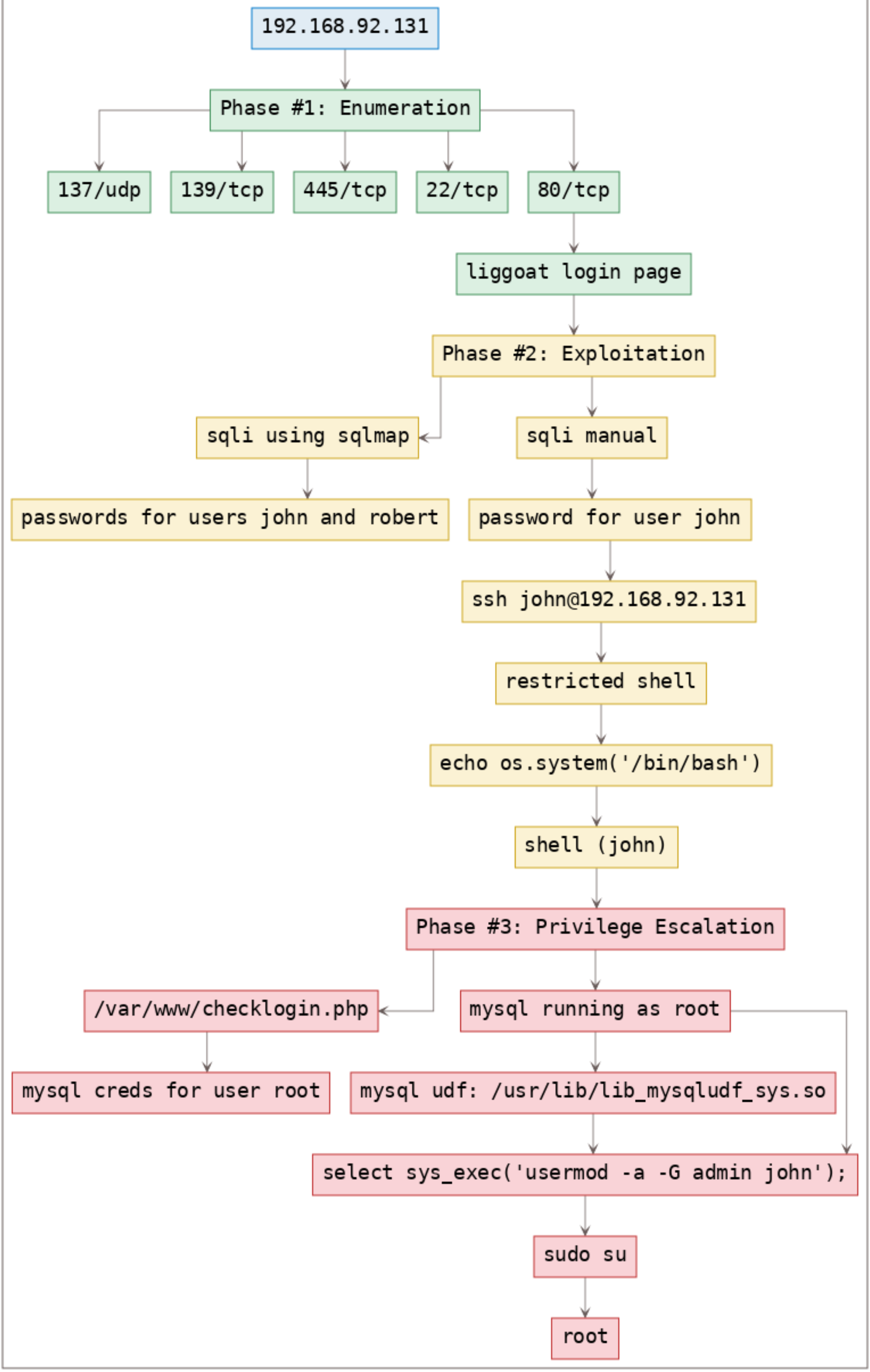
[VulnHub] Kioptrix: Level 1.1 (#2)



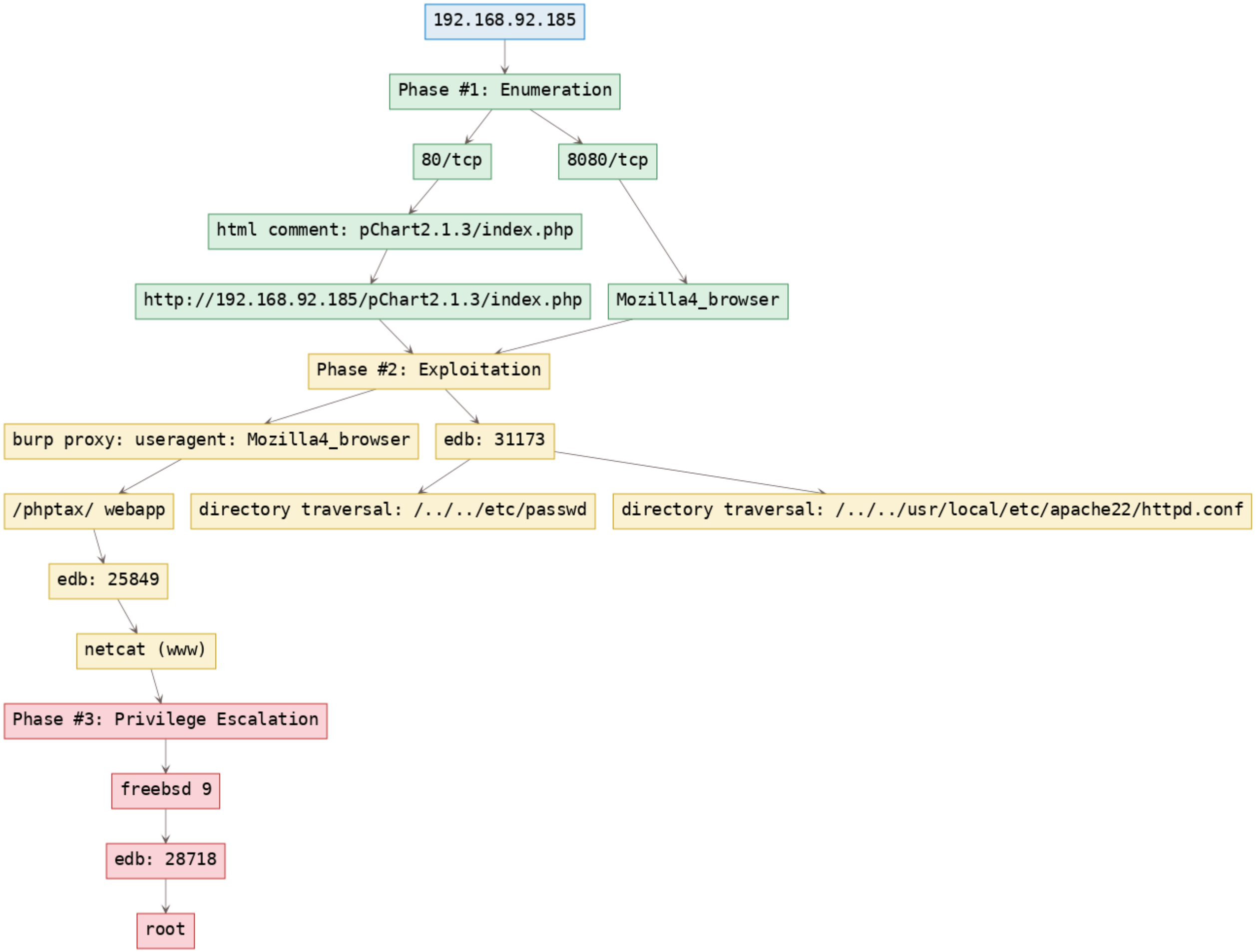
[VulnHub] Kioptrix: Level 1.2 (#3)

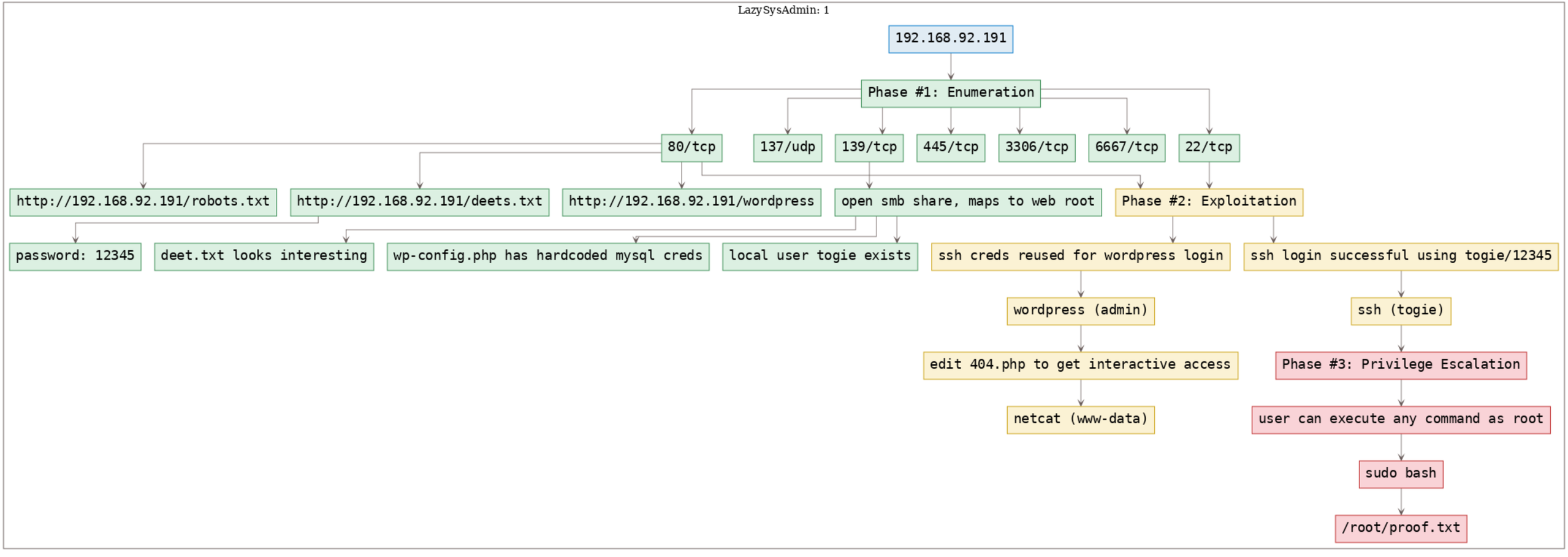


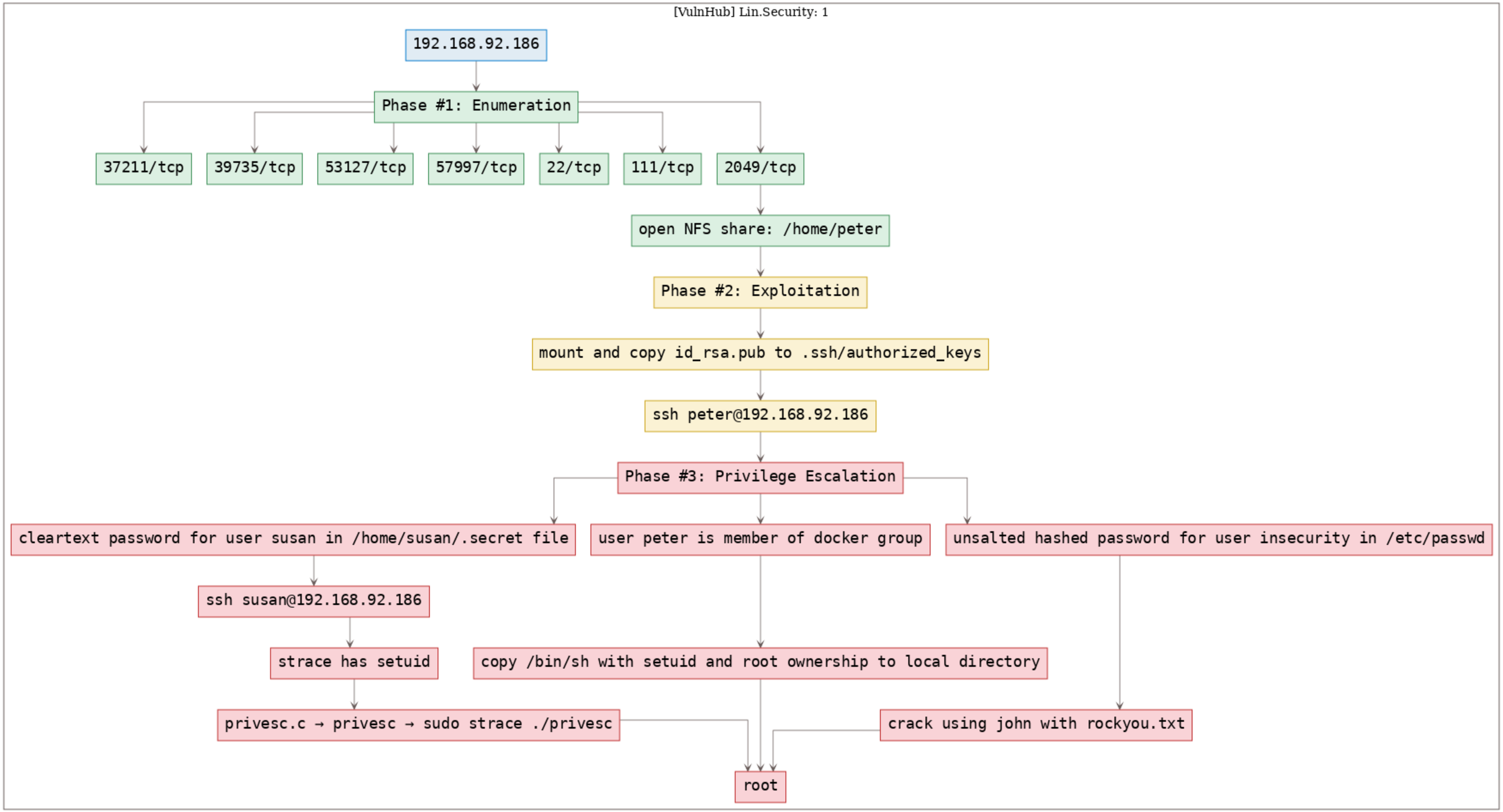
[VulnHub] Kioptrix: Level 1.3 (#4)



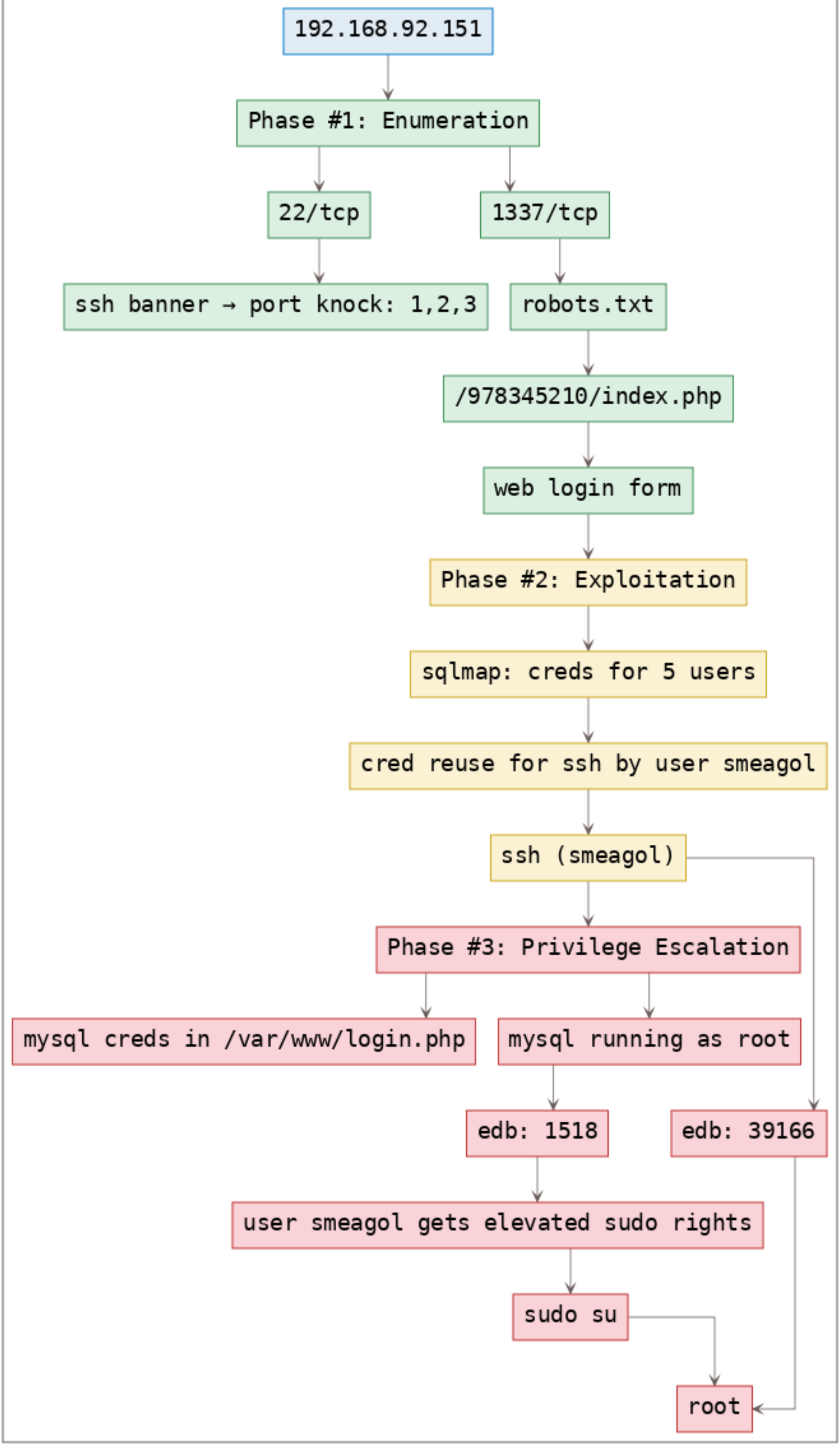
[VulnHub] Kioptrix: 2014 (#5)

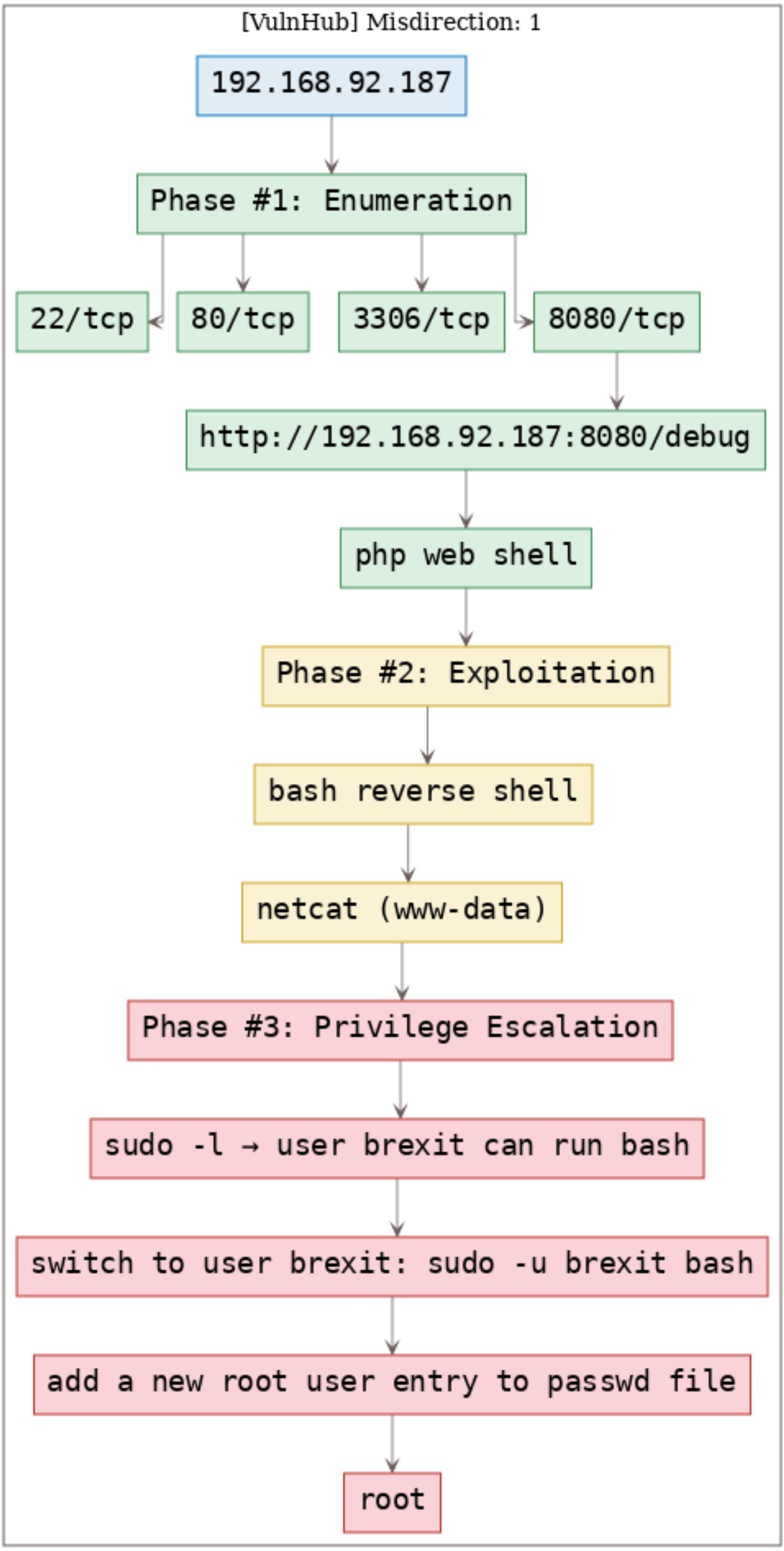



LazySysAdmin: 1
192.168.92.191
Phase #1: Enumeration
80/tcp
137/udp
139/tcp
445/tcp
3306/tcp
6667/tcp
22/tcp
http://192.168.92.191/robots.txt
http://192.168.92.191/deets.txt
http://192.168.92.191/wordpress
open smb share, maps to web root
Phase #2: Exploitation
password: 12345
deet.txt looks interesting
wp-config.php has hardcoded mysql creds
local user togie exists
ssh creds reused for wordpress login
ssh login successful using togie/12345
wordpress (admin)
ssh (togie)
edit 404.php to get interactive access
Phase #3: Privilege Escalation
netcat (www-data)
user can execute any command as root
sudo bash
/root/proof.txt

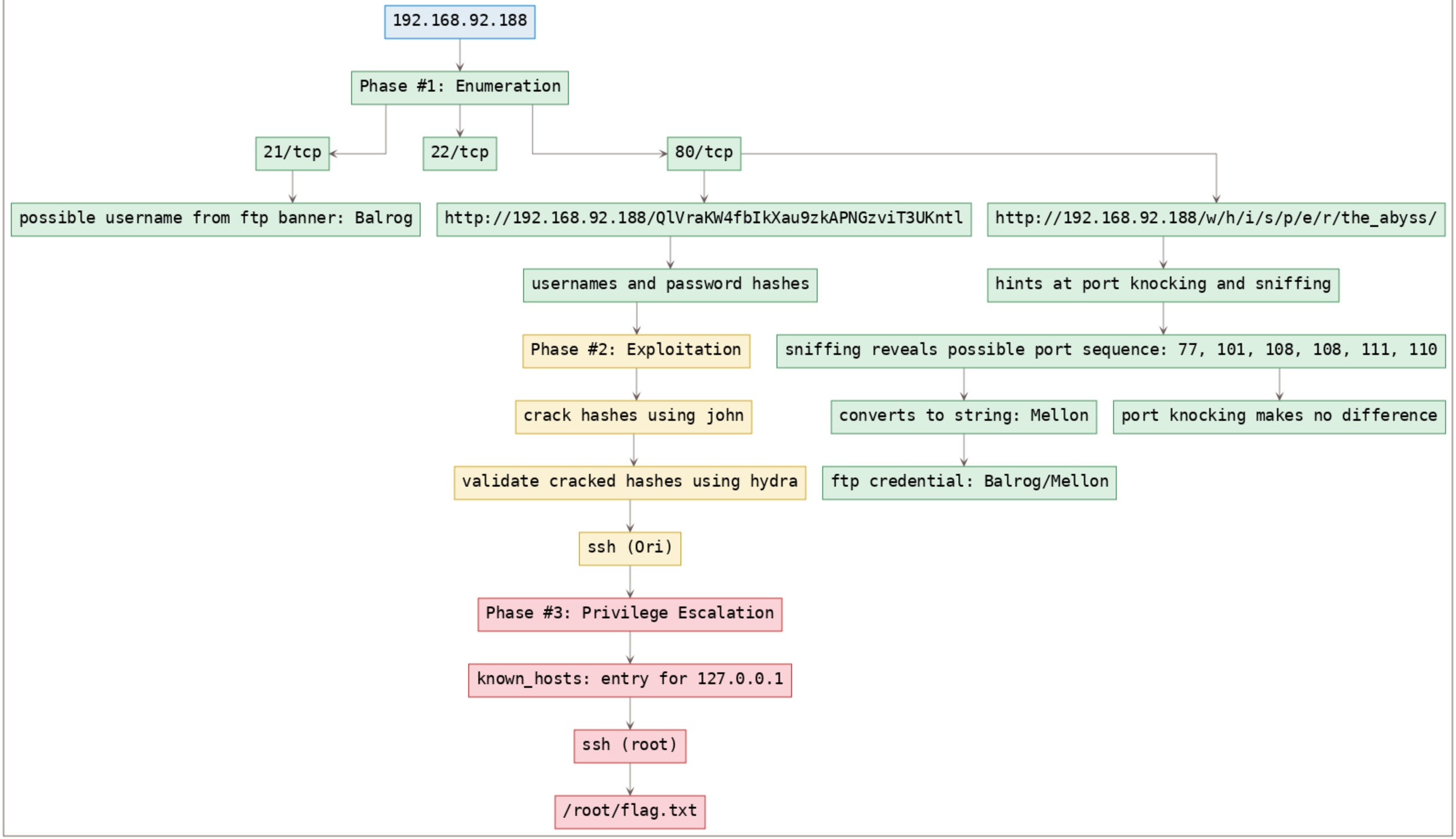

[VulnHub] Lin.Security: 1
192.168.92.186
Phase #1: Enumeration
37211/tcp
39735/tcp
53127/tcp
57997/tcp
22/tcp
111/tcp
2049/tcp
open NFS share: /home/peter
Phase #2: Exploitation
mount and copy id_rsa.pub to .ssh/authorized_keys
ssh peter@192.168.92.186
Phase #3: Privilege Escalation
cleartext password for user susan in /home/susan/.secret file
user peter is member of docker group
unsalted hashed password for user insecurity in /etc/passwd
ssh susan@192.168.92.186
strace has setuid
copy /bin/sh with setuid and root ownership to local directory
privesc.c → privesc → sudo strace ./privesc
crack using john with rockyou.txt
root

Lord Of The Root: 1.0.1

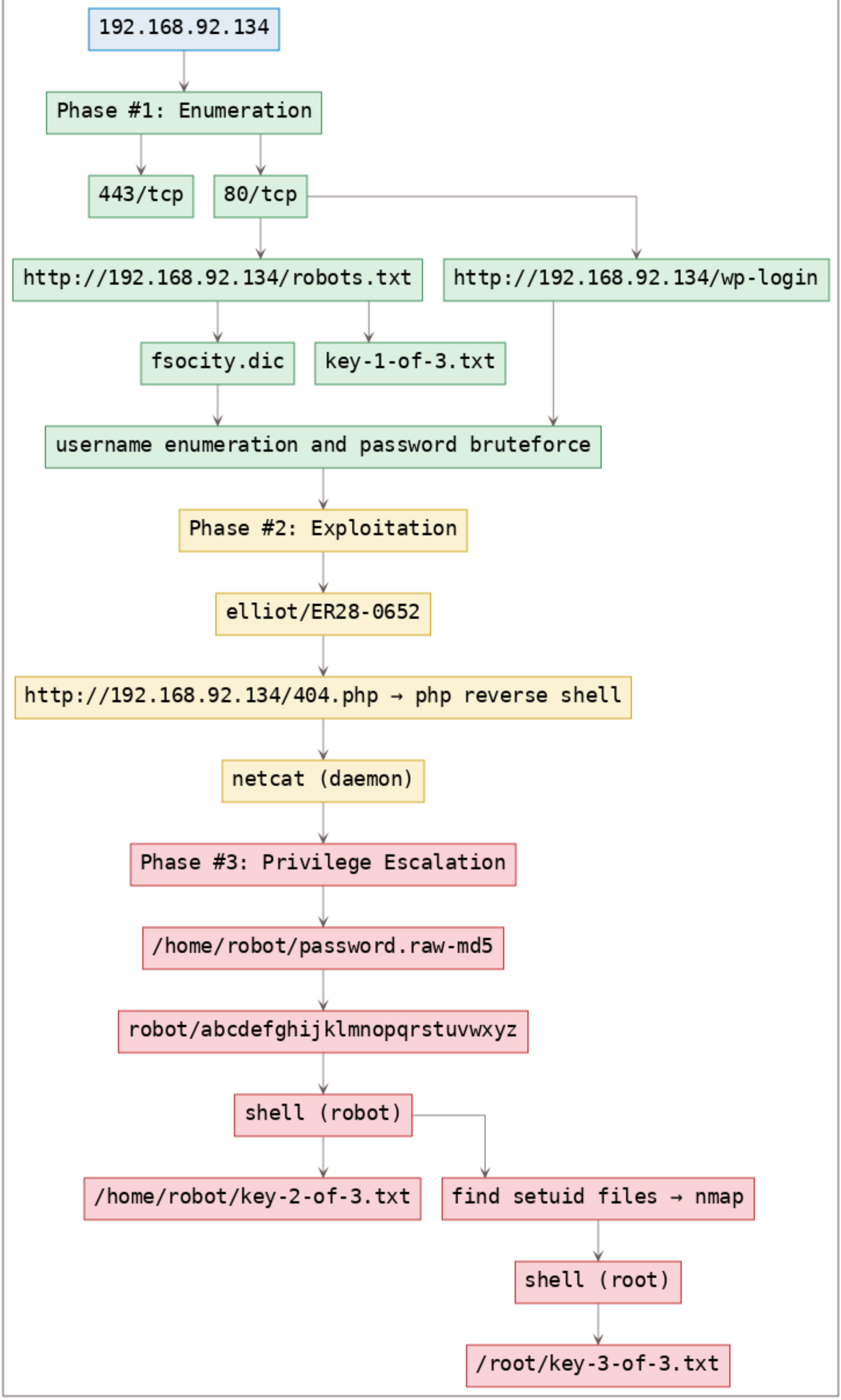



[VulnHub] Misdirection: 1
192.168.92.187
Phase #1: Enumeration
22/tcp
80/tcp
3306/tcp
8080/tcp
http://192.168.92.187:8080/debug
php web shell
Phase #2: Exploitation
bash reverse shell
netcat (www-data)
Phase #3: Privilege Escalation
sudo -l → user brexit can run bash
switch to user brexit: sudo -u brexit bash
add a new root user entry to passwd file
root

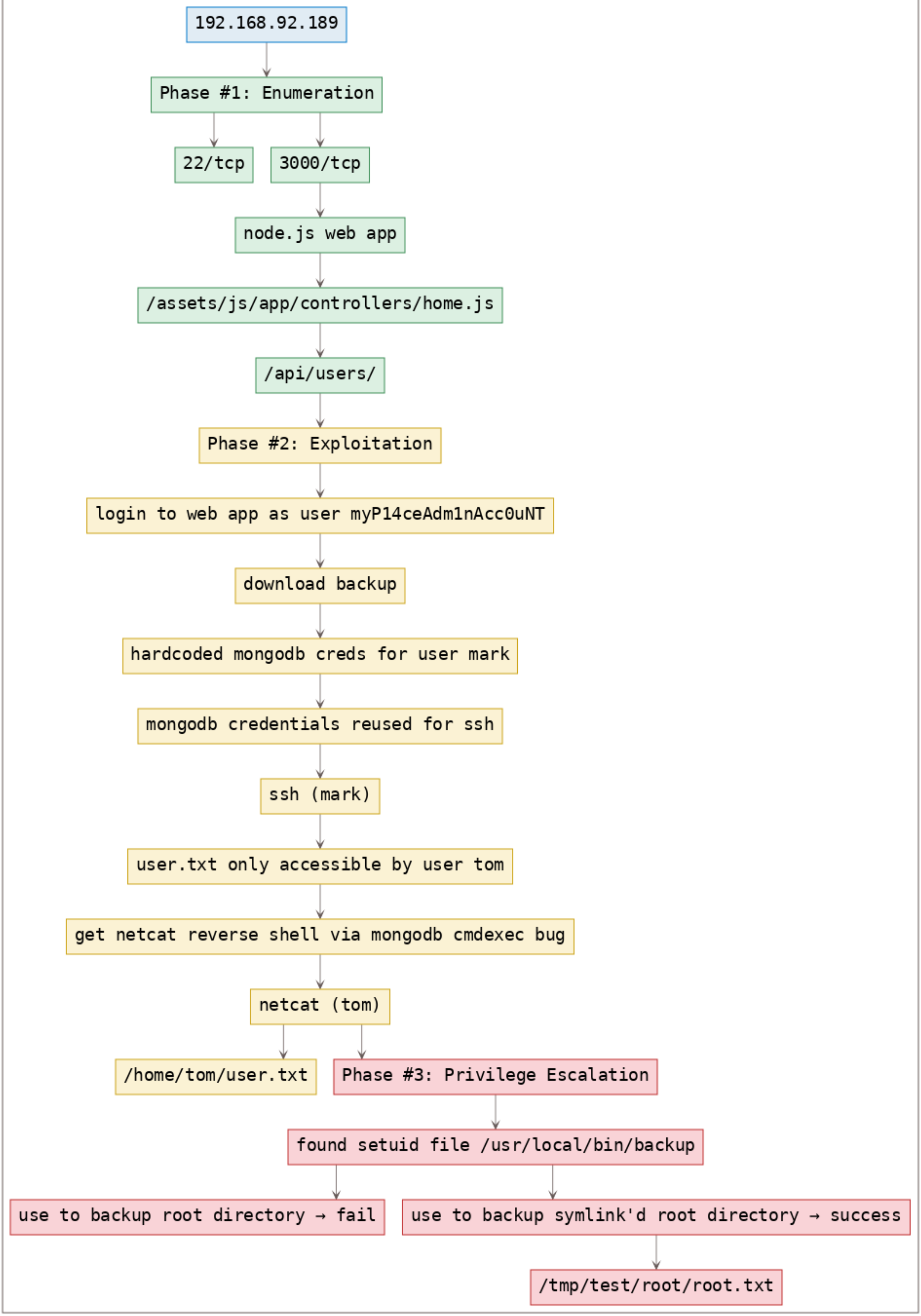
[VulnHub] Moria: 1.1



[VulnHub] Mr-Robot: 1



[VulnHub] Node: 1



[VulnHub] hackfest2016: Quaoar

192.168.92.175

Phase #1: Enumeration

110/tcp

137/udp

139/tcp

143/tcp

445/tcp

993/tcp

995/tcp

22/tcp

53/tcp

80/tcp

http://192.168.92.175/robots.txt

http://192.168.92.175/wordpress/

wpscan → admin,wpuser

Phase #2: Exploitation

default credentials → admin/admin

wordpress Hello Dolly plugin

edit, add PHP reverse shell and activate

netcat (www-data)

/home/wpadmin/flag.txt

Phase #3: Privilege Escalation

/var/www/wordpress/wp-config.php

mysql credentials for user root

credentials reused for root account

shell (root)

/root/flag.txt

[VulnHub] hackfest2016: Sedna

192.168.92.176

Phase #1: Enumeration

110/tcp
111/tcp
137/udp
139/tcp
143/tcp
445/tcp
993/tcp
995/tcp
8080/tcp
40176/tcp
22/tcp
53/tcp
80/tcp

nikto

http://192.168.92.176/license.txt

Copyright (c) 2012 - 2015 BuilderEngine / Radian Enterprise Systems Limited.

Phase #2: Exploitation

searchsploit → edb:40390

php reverse shell file upload

netcat (www-data)

Phase #3: Privilege Escalation

/var/www/flag.txt

/etc/chkrootkit/chkrootkit

searchsploit → edb:33899

cronjob → /tmp/update

netcat (root)

/root/flag.txt

/etc/tomcat7/tomcat-users.xml

[VulnHub] HackLAB: Vulnix