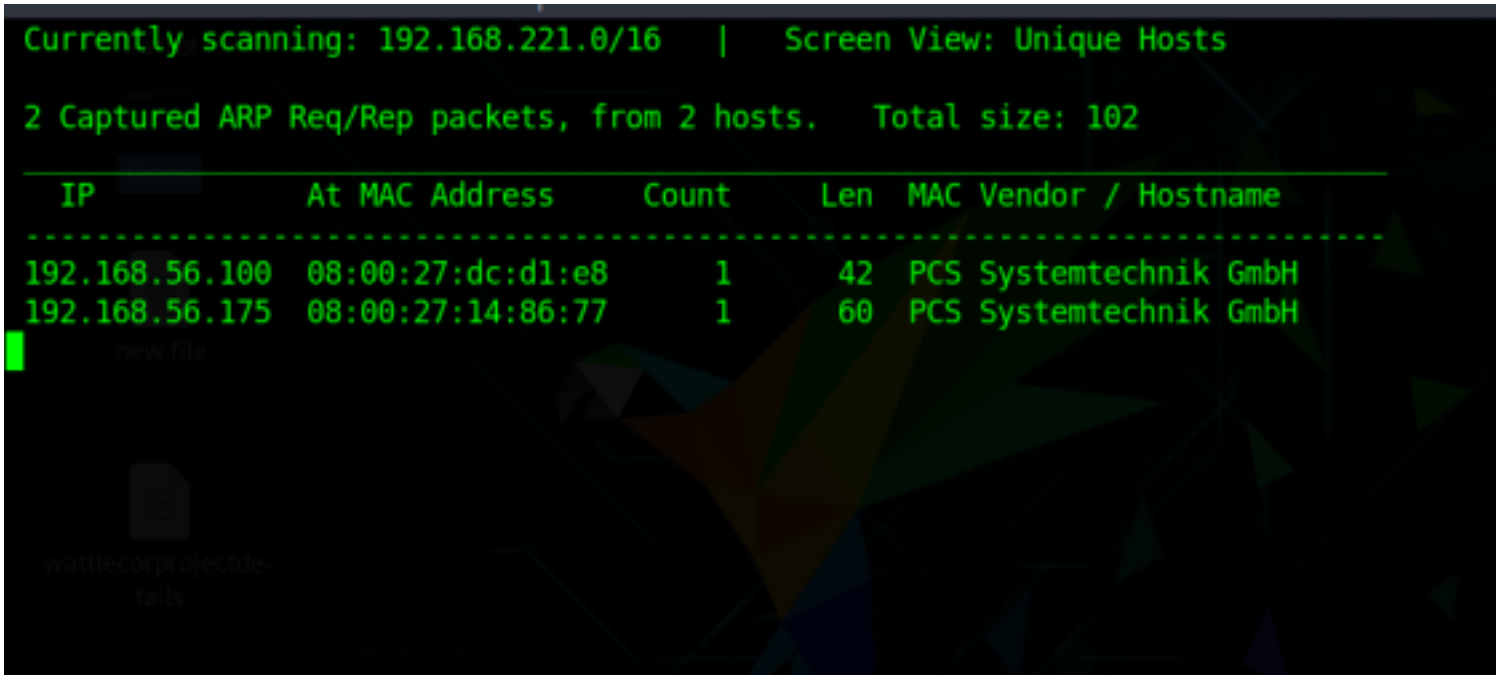
Cybersploit2

Boot to Root
Your target is gain the Root access
There is no any flag in this VMs
today we are going to solve another boot2root challenge vulnerable VM machine called “CyberSploit: 2“. This machine is made by Cyberspace which is an easy level lab. There is no flag in this challenge, just us to gain the root access of VM machine.today we are going to solve another boot2root challenge vulnerable VM machine called “CyberSploit: 2“. This machine is made by Cyberspace which is an easy level lab. There is no flag in this challenge, just us to gain the root access of VM machine.

Link to Download: https://www.vulnhub.com/entry/cybersploit-2,511/

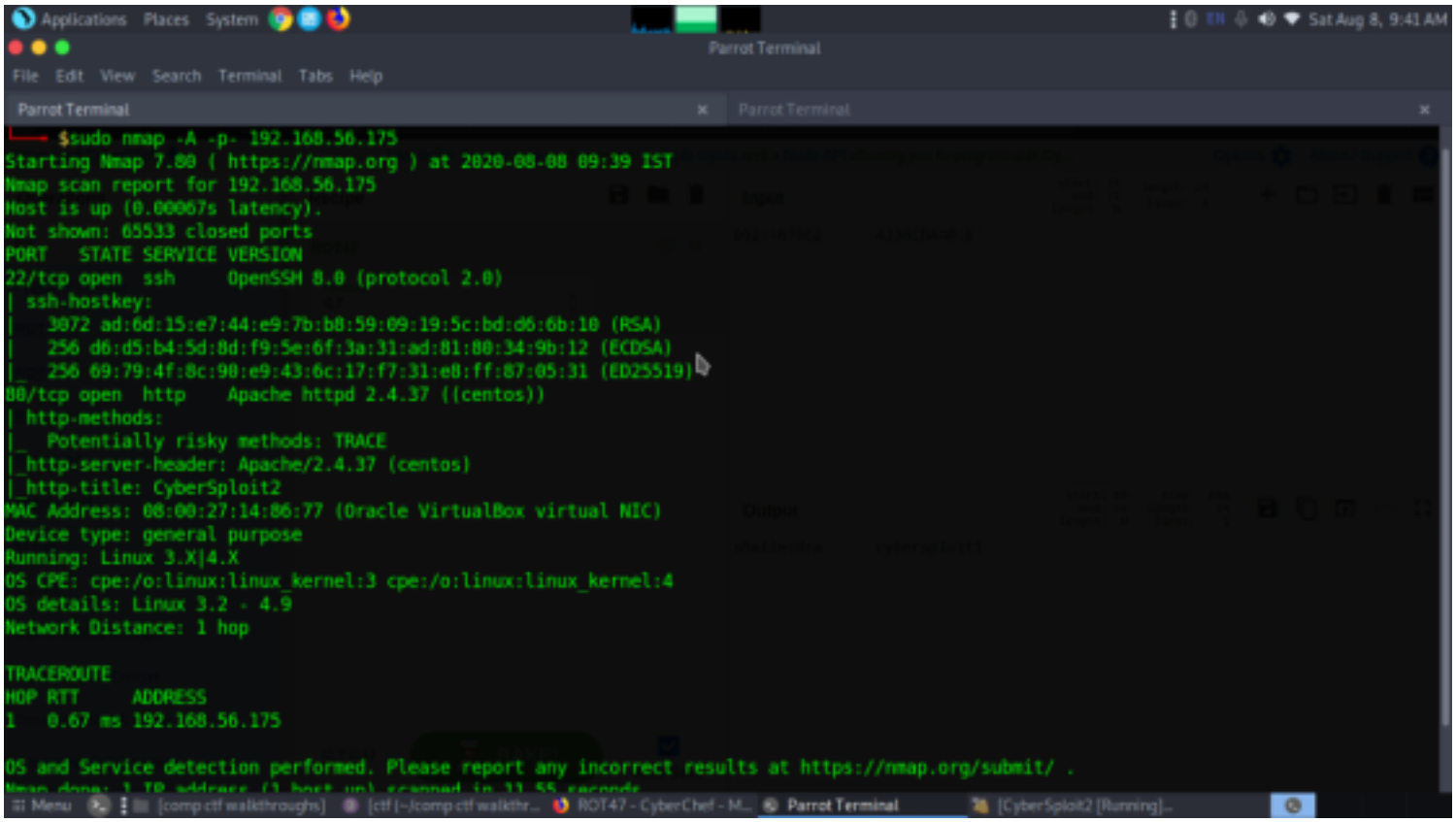
Reconnaisance

Let's start off by identifying our target IP
sudo netdiscover -i vboxnet0



Target IP- 192.168.56.175

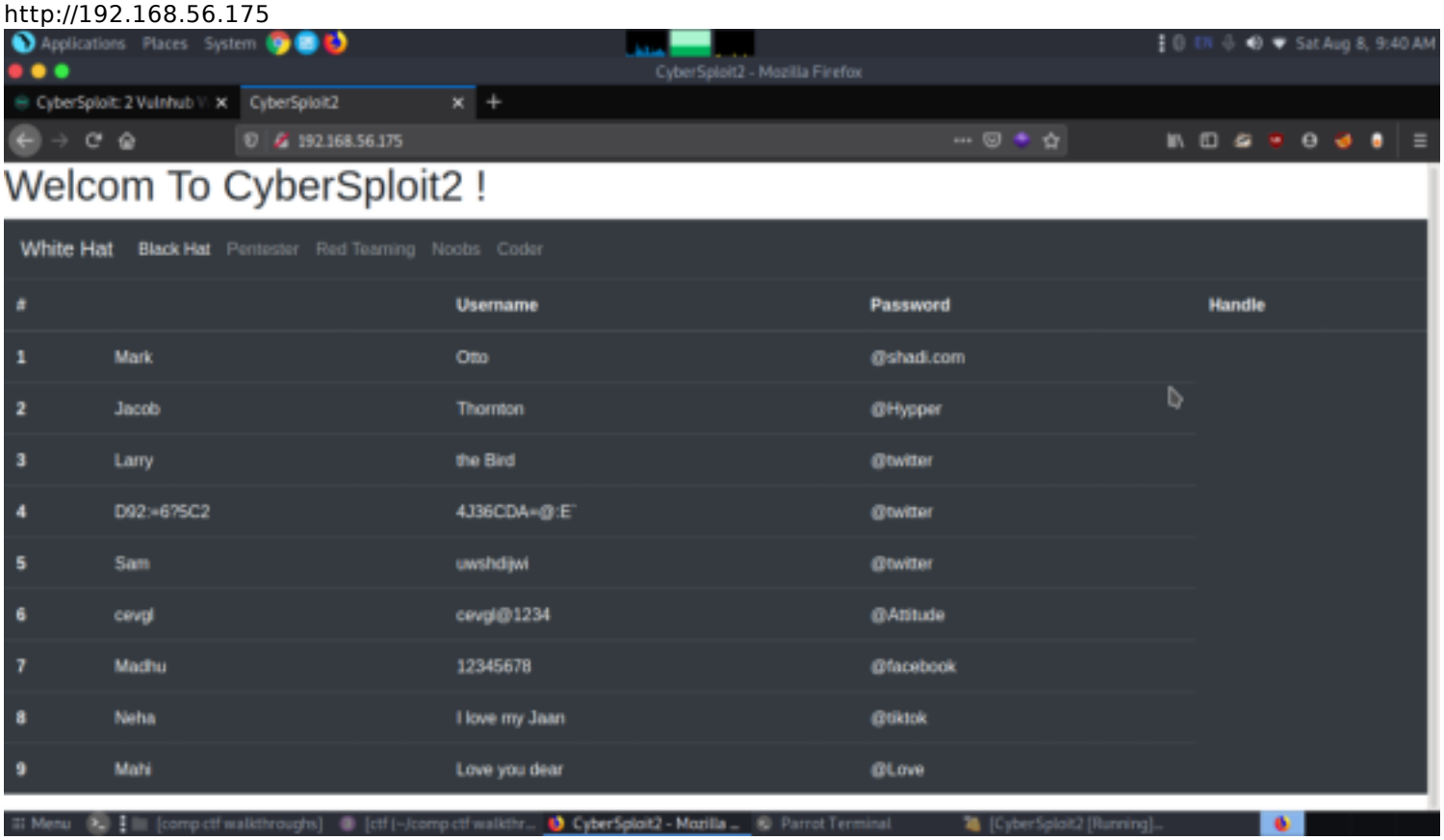
Now we have our target. Let's identify open ports,services,versions that are running using nmap
sudo nmap -A -p- 192.168.56.175



Great we got to know there is only two open ports running port22 (ssh) and port80 (http)

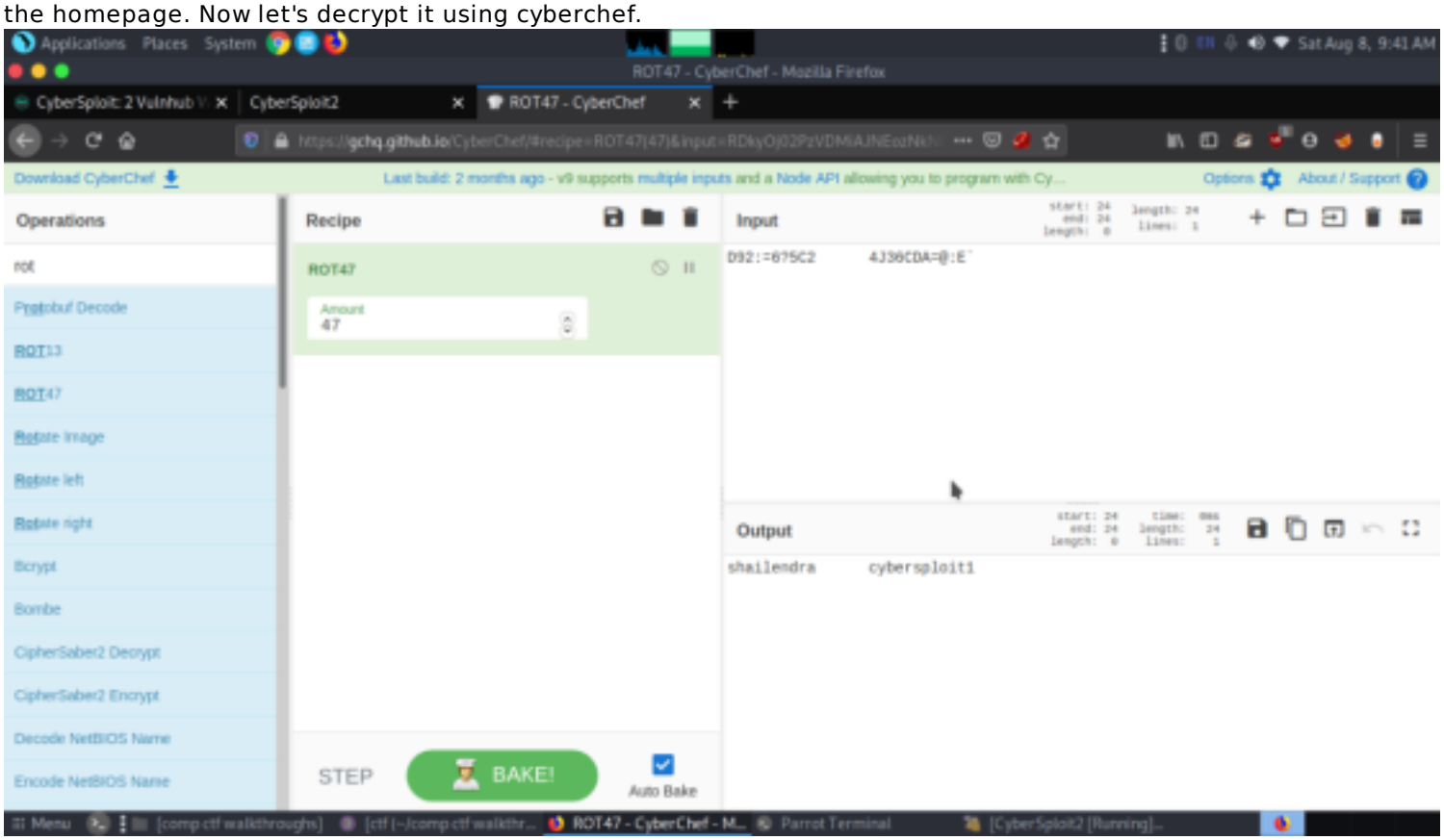
Enumeration

Since the port80 is running let's explore the webpage.
http://192.168.56.175



Great we have a proper looking webpage and it looks like a table of some security enthusiasts. but there is one name which is decrypted might be useful. Let's check the source code

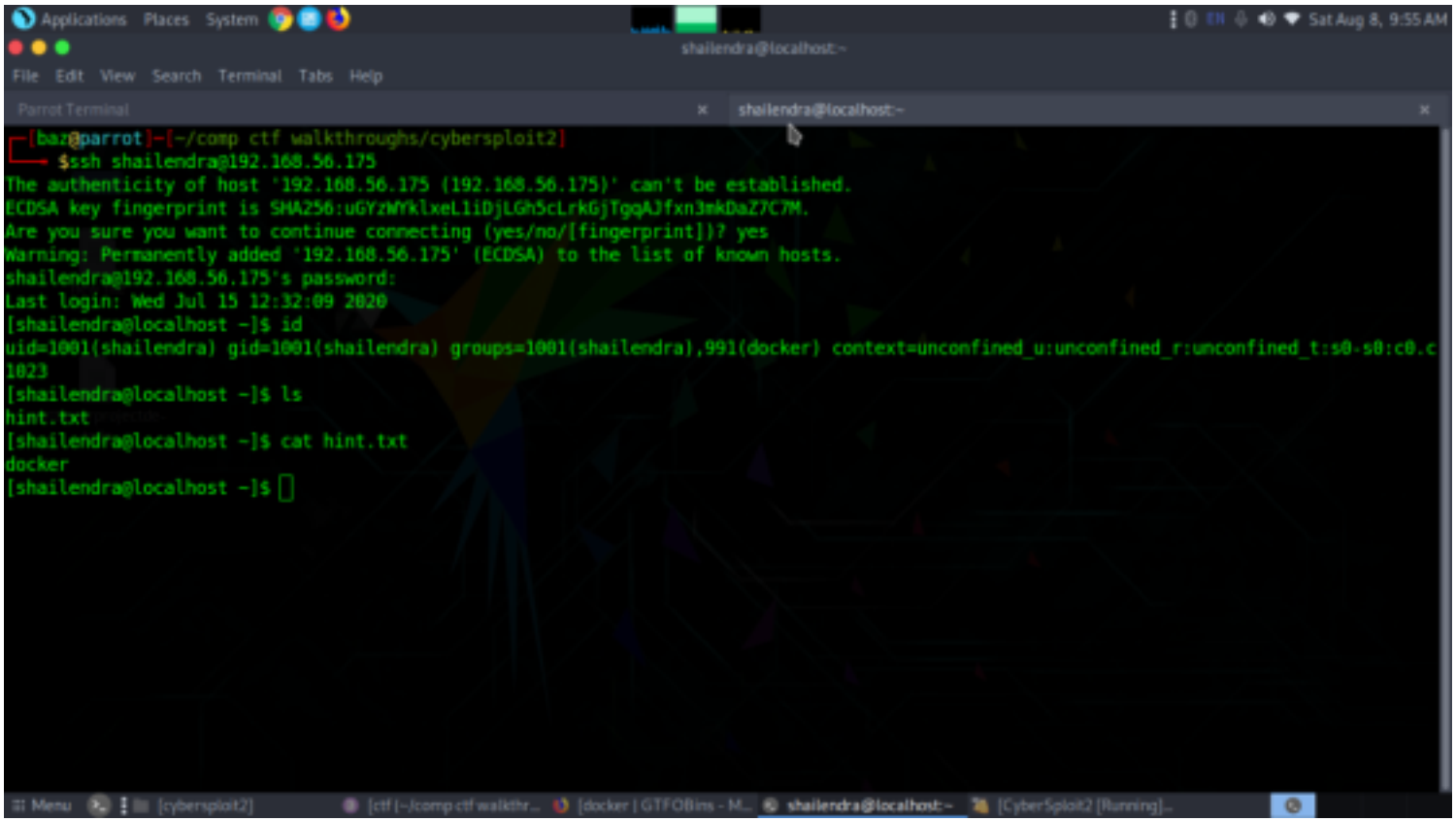
Great from the source code they were referring to rot47. It might be the encryption used for the user we seen in the homepage. Now let's decrypt it using cyberchef.



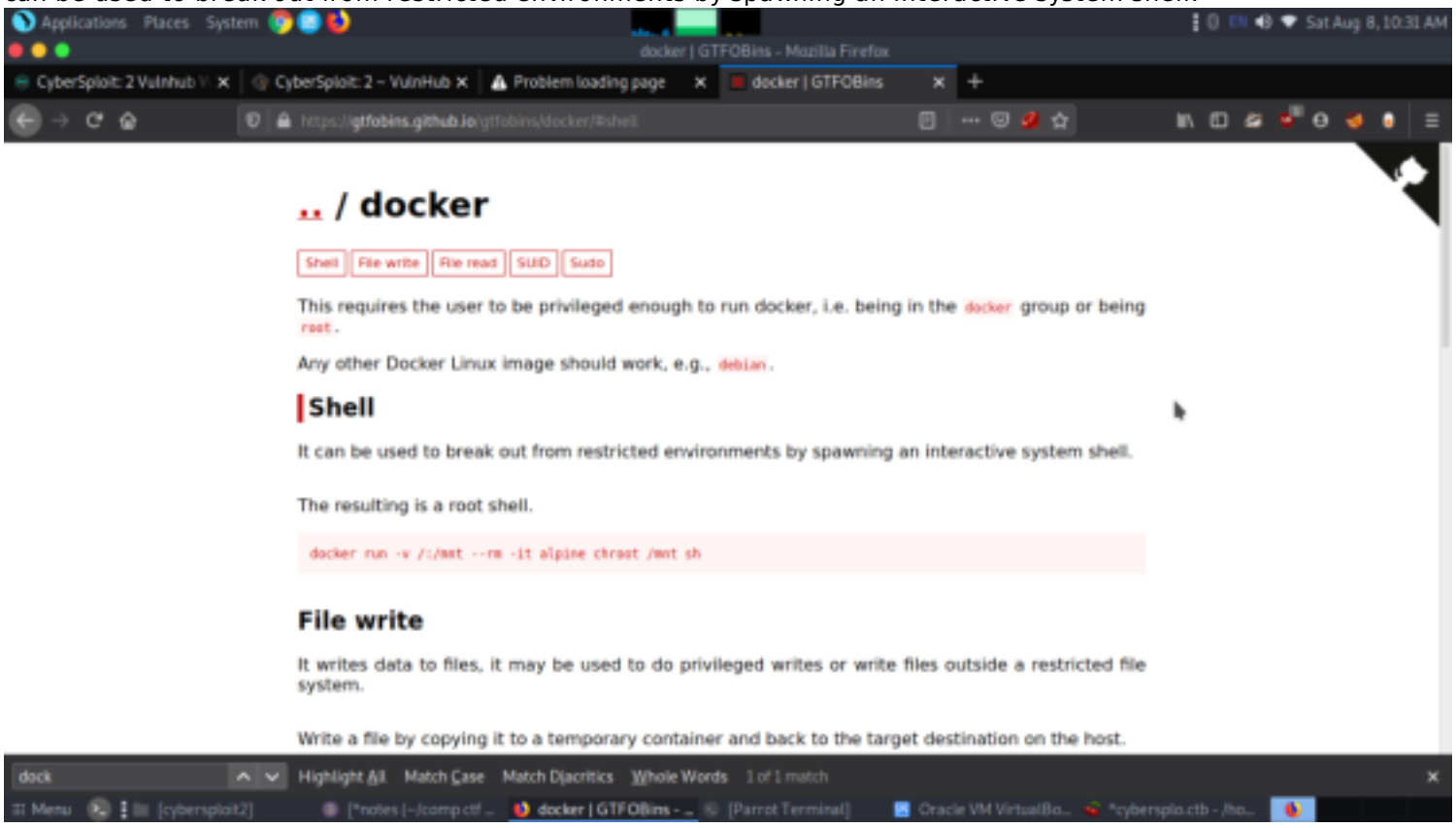
After decrypting there was two words. It might be the ssh credentials.

Exploitation

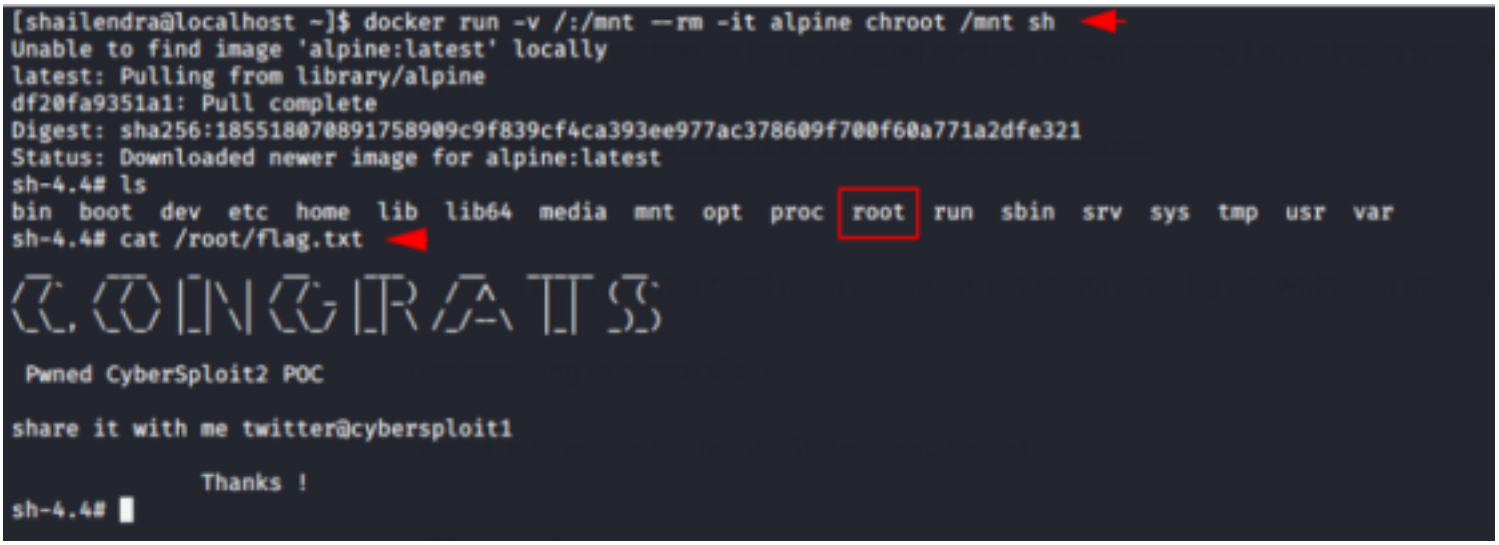
Let's login to the ssh server using this credentials we got from cyberchef.
We access the ssh service with the obtained username and password.
ssh shailendra@192.168.56.175
pass- cybersploit1



After login we got another text file like a hint refering of a docker.
Then from gtfobins we got a docker escalating script. After search we found a docker shell on gfobins website that can be used to break out from restricted environments by spawning an interactive system shell.



After executing this we get final flag in the root directory
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
id
cat /root/flag.txt



Walkthrough by Basil

.....HappyHacking.....