**Contents**

Task - 1 Reconnaissance

Arp Scan

Nmap Scan

Analysing Nmap Report

Nmap Scan for Scanning Open Ports

Analysing Nmap Report

Searching The Bruteforce Script

Bruteforce Wordlist and its Usage

Task - 2 Gain Access

Starting the Metasploit Framework

Select the Payload to Exploit

Details and Options required for the Payload

Set the necessary details

Checking the Details Correctly Set in the Payload

Starting the Exploit

Successful Exploit

Task - 3 Cracking

Checking the Commands available in Meterpreter

Successfully cracked the Password

Saving the Hash Password to .txt file for Bruteforce

Checking the Password correctly saved

Task - 5 Brute-Forcing

Cracking the Password with John the Ripper

Changing the Format of Hash Password

Successfully cracked the Password

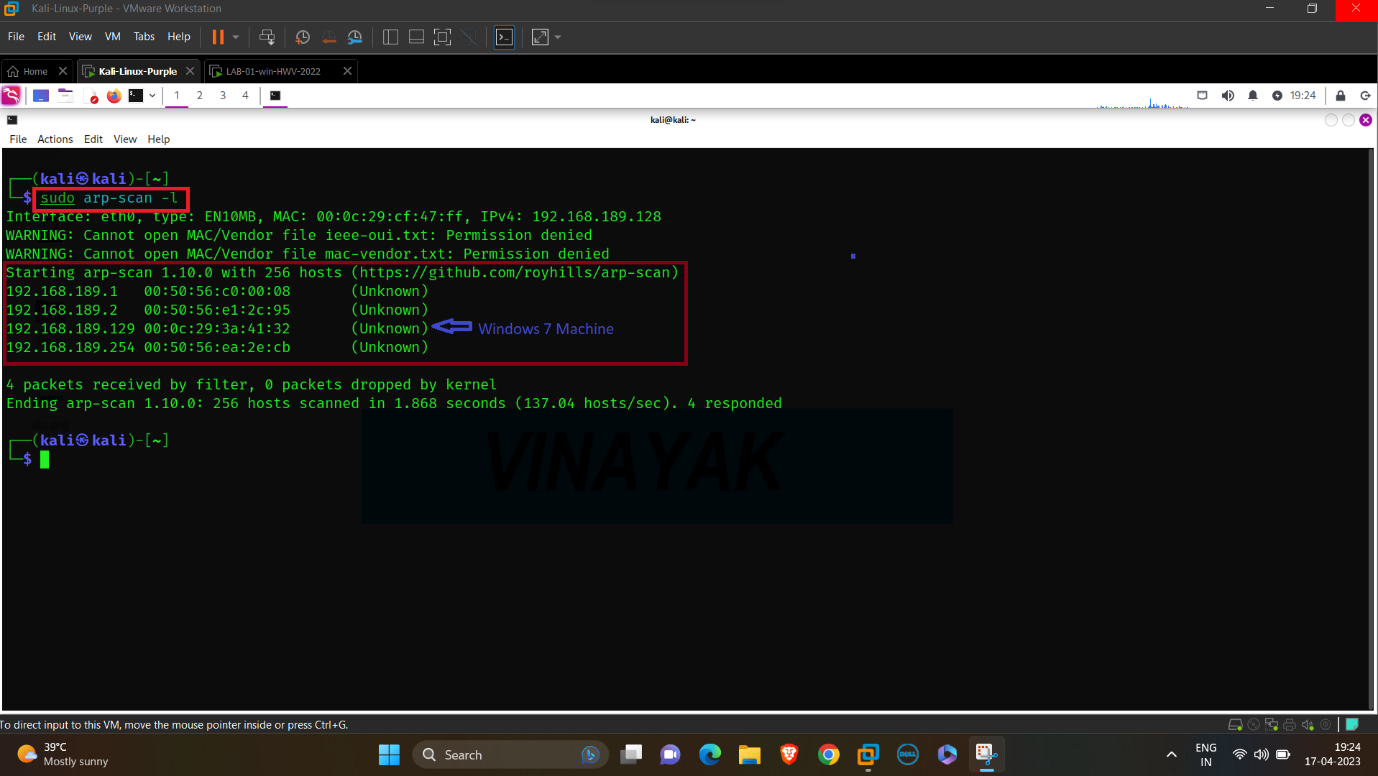
Task - 6 Login to Machine

Log-in into the Windows 7 Machine Successfully Logged-in into the Windows 7 Machine

PROCEDURE

**Starts an Arp Scan on the given box:**

arp-scan -l



arp-scan -l is used to scan and obtain the IP Address.

After scanning we got 4 IP Address:

192.168.189.1 NAT Adapter

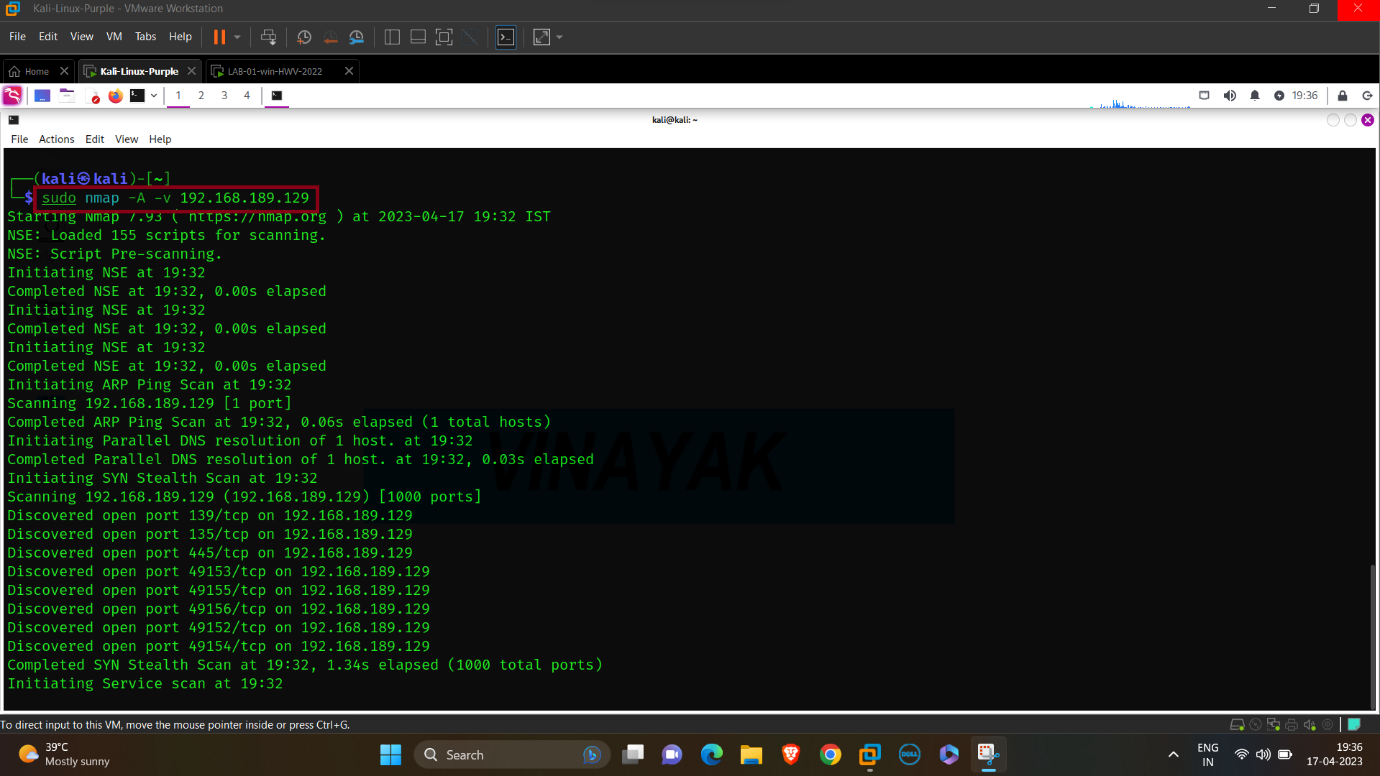
192.168.189.2 VMware

192.168.189.129 Windows 7 Machine

192.168.163.254 Our Machine

**Start a Nmap scan on the given box:**

nmap -A -v 192.168.189.129



nmap is a tool to scan the IP Address.

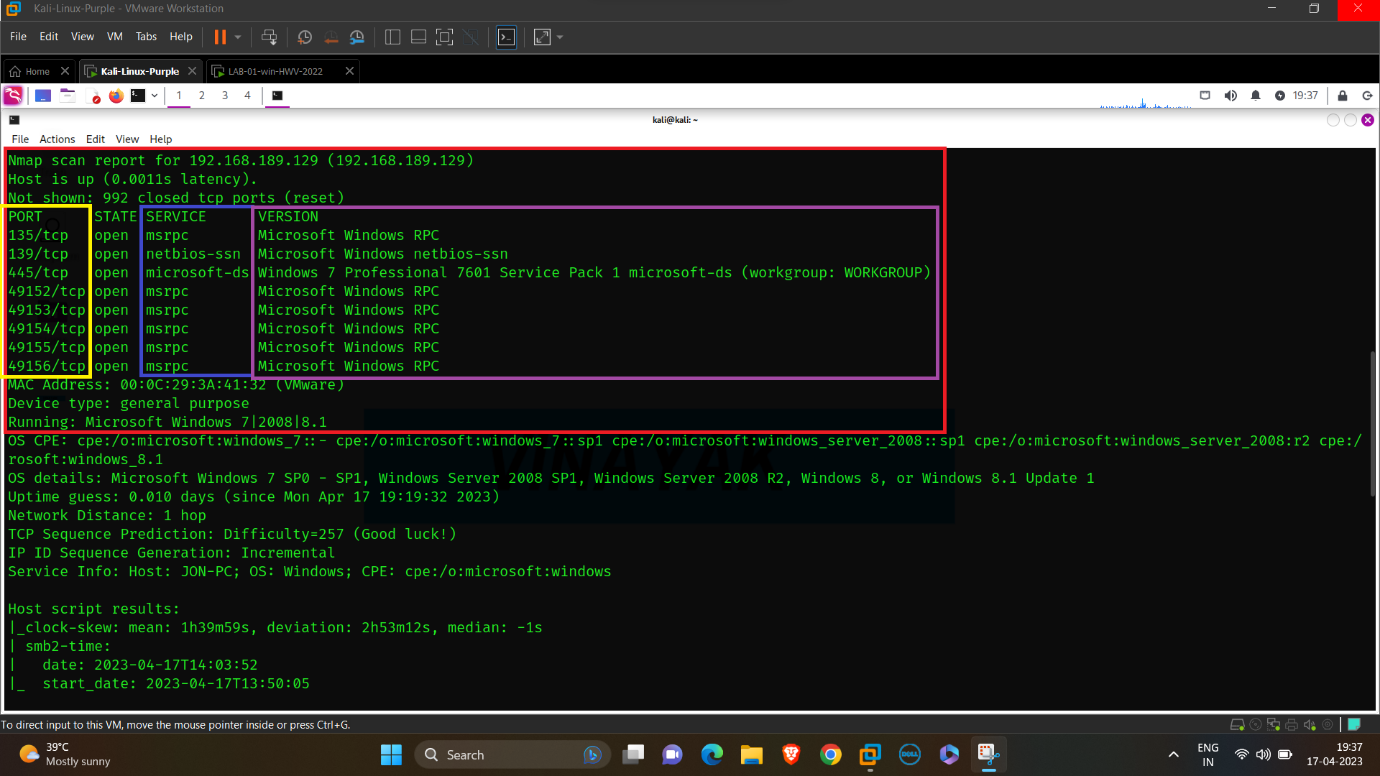
-A is used for OS Detection, Version Detection, Script Scanning and Traceroute.

-v (Verbosity) is used for a detail report of scanning the IP Address.

It is used to get information and a detail report about The Target’s IP Address.

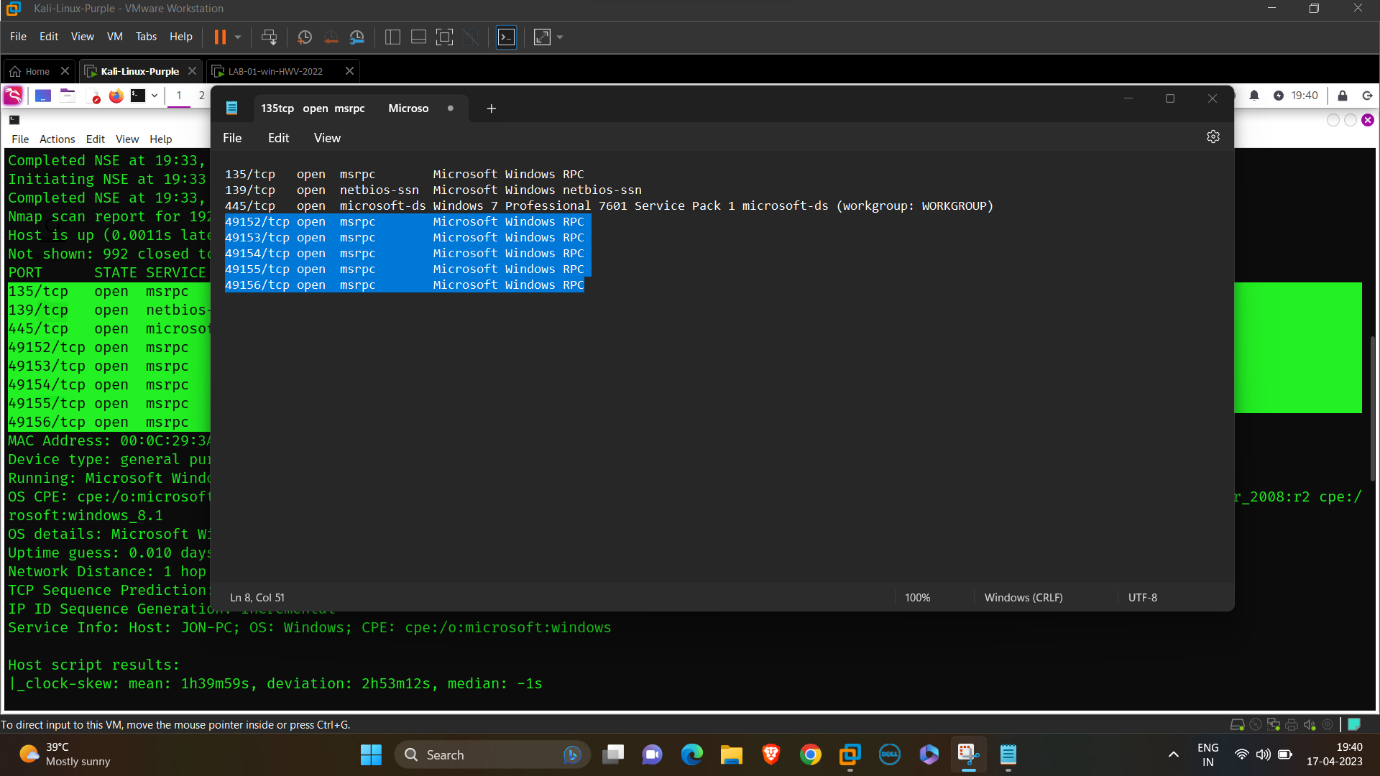
After scanning we find the open ports available in the machine.

**Analysing Nmap Report:**



We discovered 8 Ports are Open and 992 Ports are Closed Out of 1000 Ports

After Segrigating the useful information:



We can see that 3 Ports are Open and using different services:

Port Service Version

135/tcp msrpc Microsoft Windows RPC

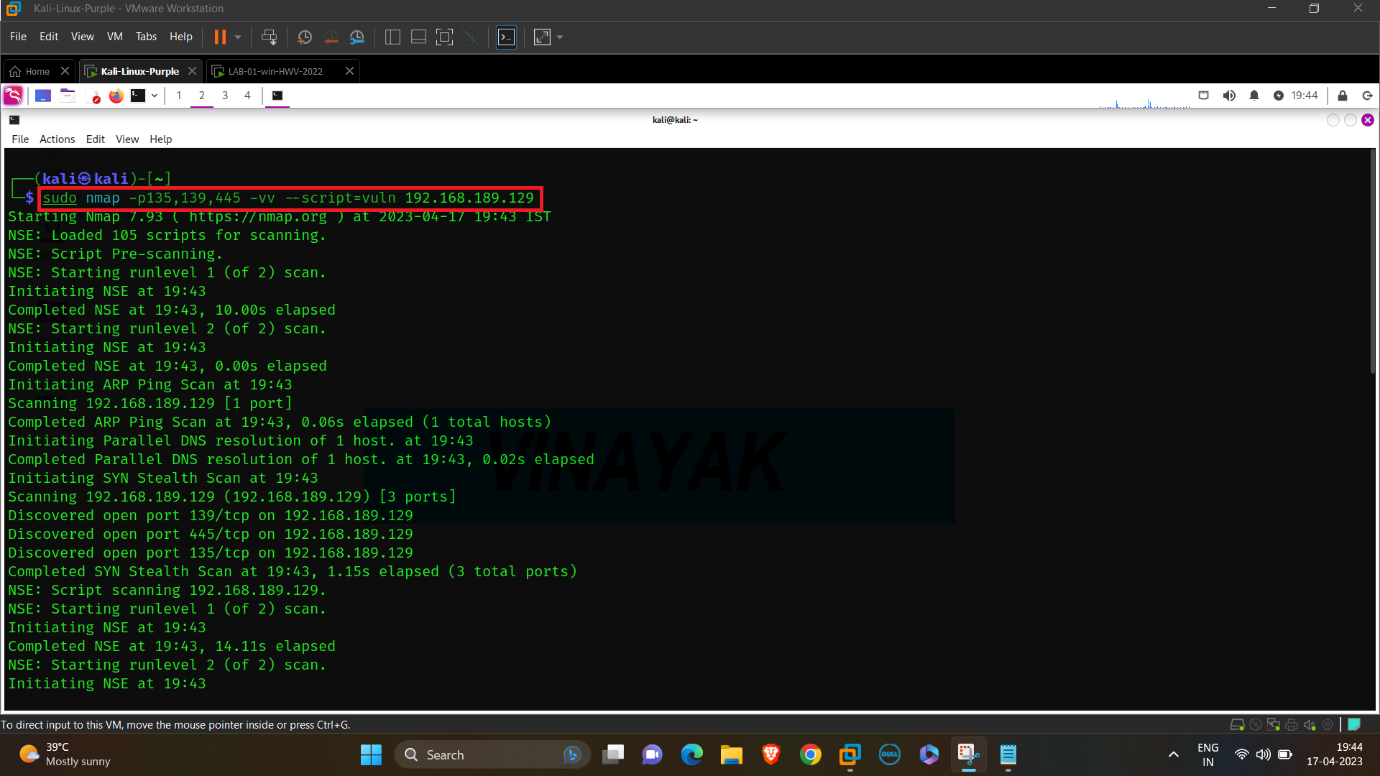
139/tcp netbios-ssn Microsoft Windows netbios-ssn

445/tcp microsoft-ds Windows 7 Professional 7601 Service

Pack 1 microsoft-ds (workgroup: WORKGROUP)

**Start an Nmap scan for Scanning Open Port:**

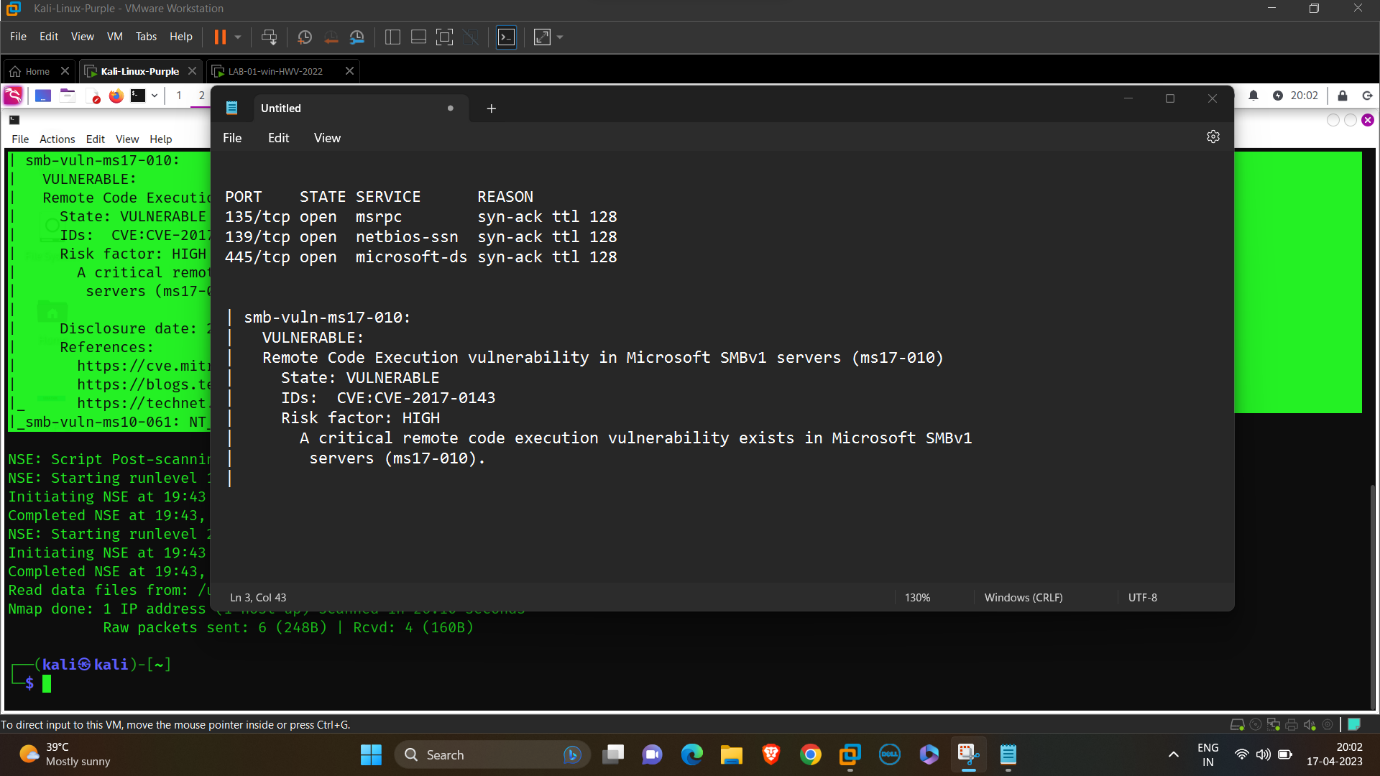
nmap -p135,139,445 -vv –script=vuln 192.168.189.129



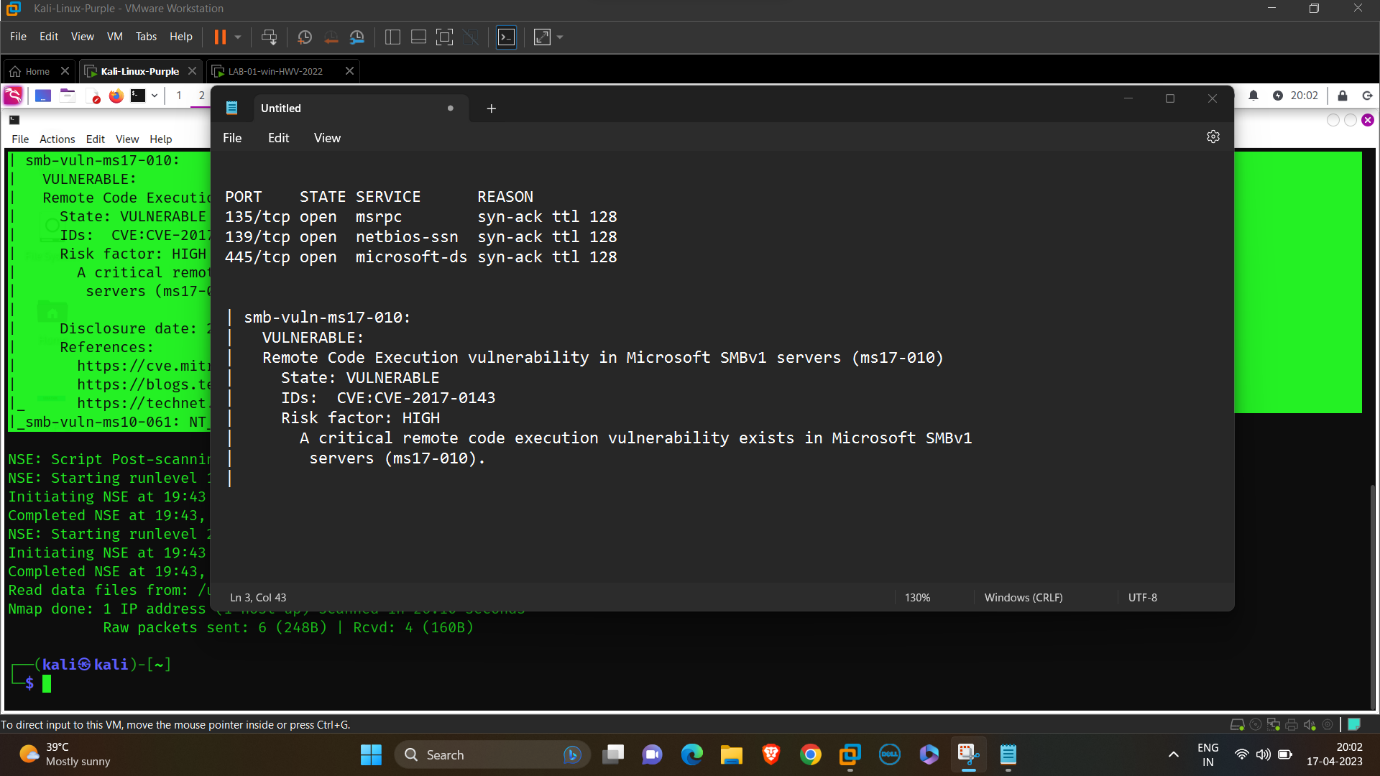
-p is used to scan a port or ports

--script=vuln is used to access the script which contains (vuln) factor

**Analysing Nmap Report:**



After Segrigating the useful information with the help of notepad:



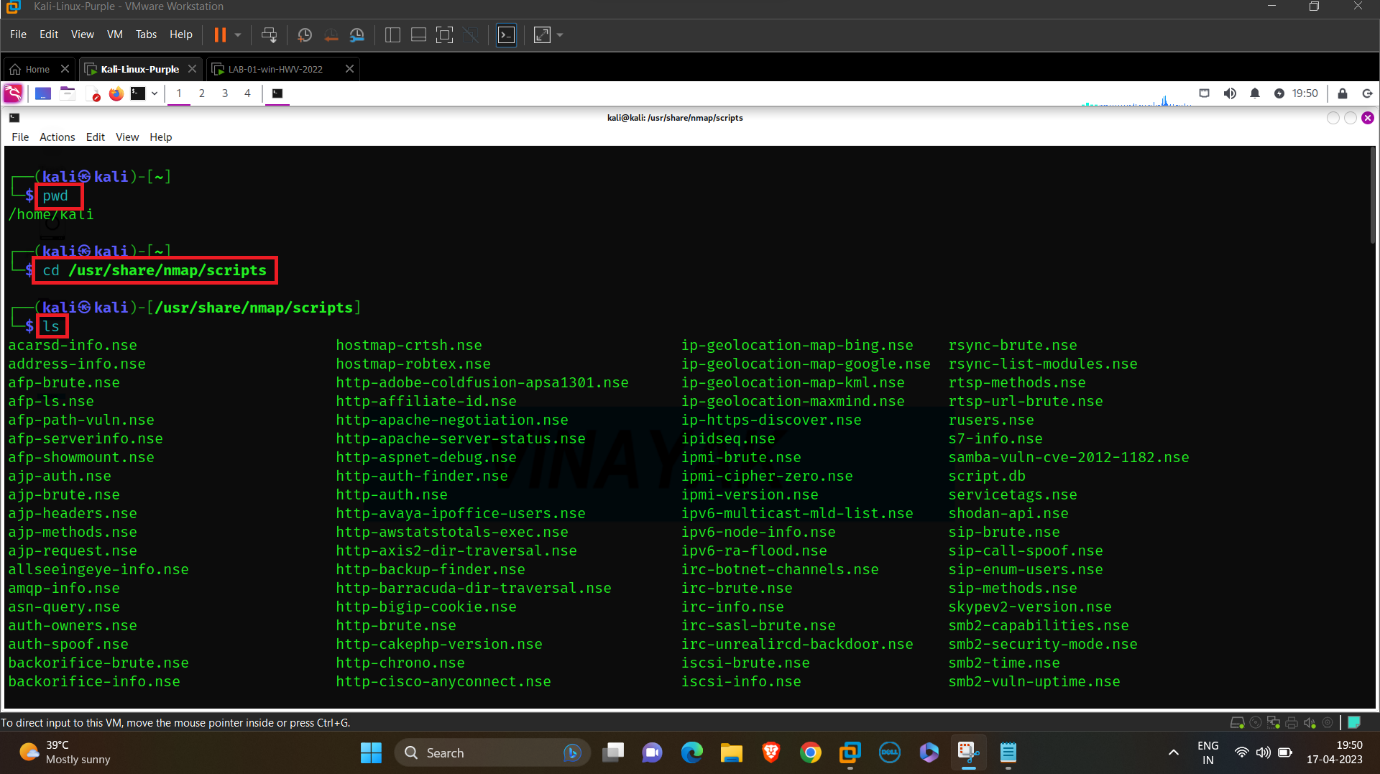
We discovered that a critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010)

**Searching the Bruteforce Script:**

pwd

cd /usr/share/nmap/scripts

ls



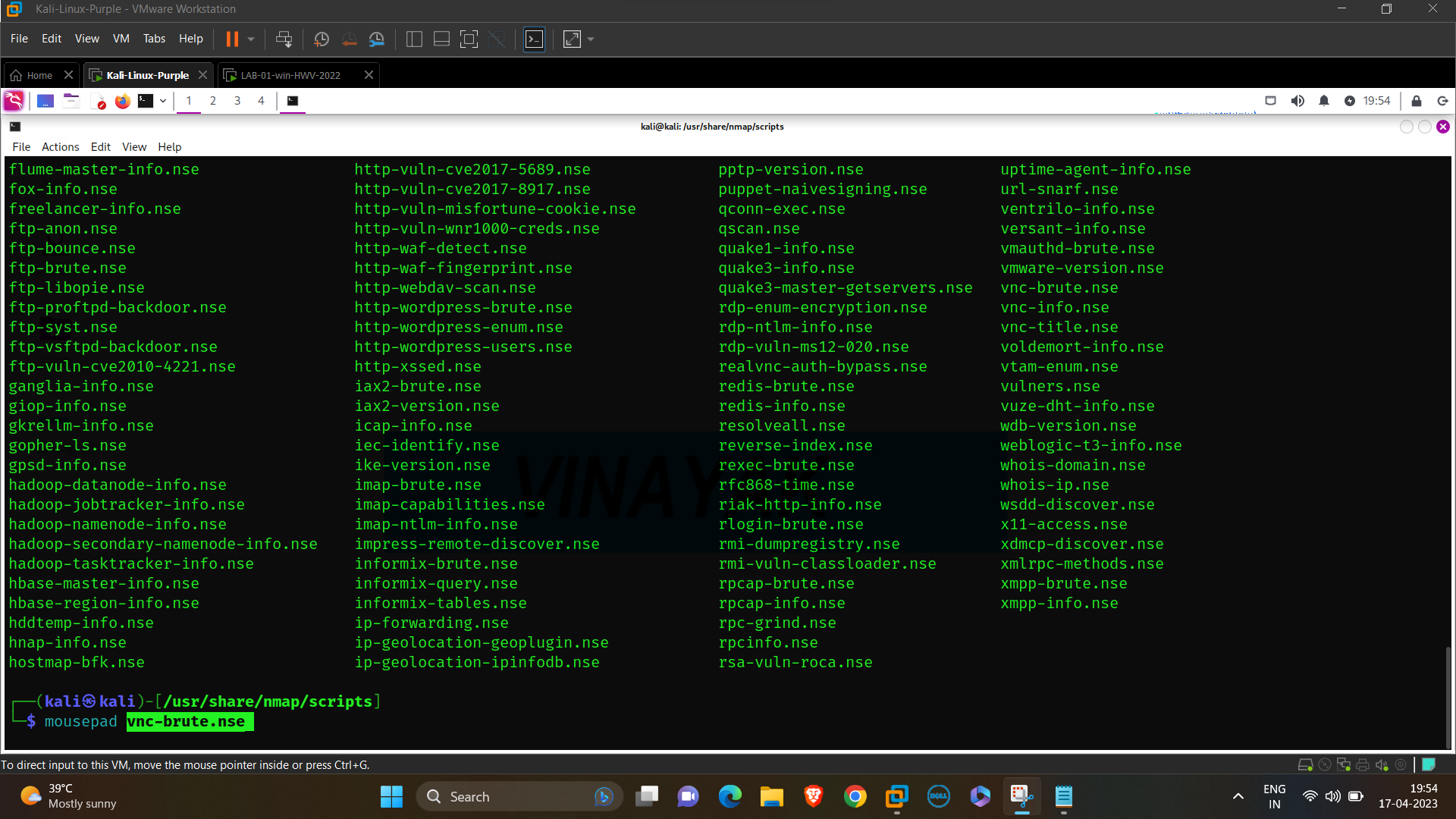
We have to search for a particular script in the list called vnc-brute.nse

vnc-brute.nse is a script specially designed for testing a vnc for a Bruteforce attack.

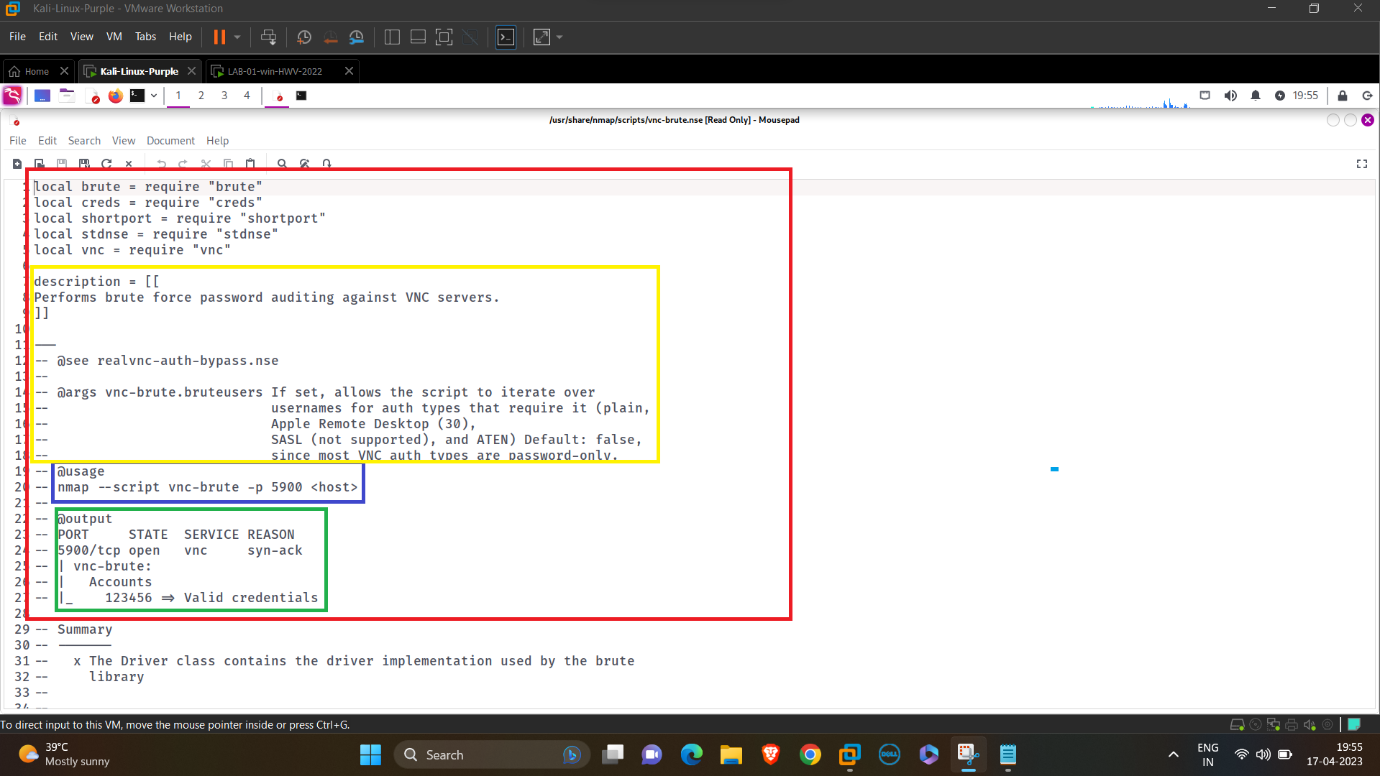
We can open and see the script in detail and check the usage of the script with the help of Mousepad.

**Bruteforce Wordlist and its Usage:**

mousepad vnc-brute.nse



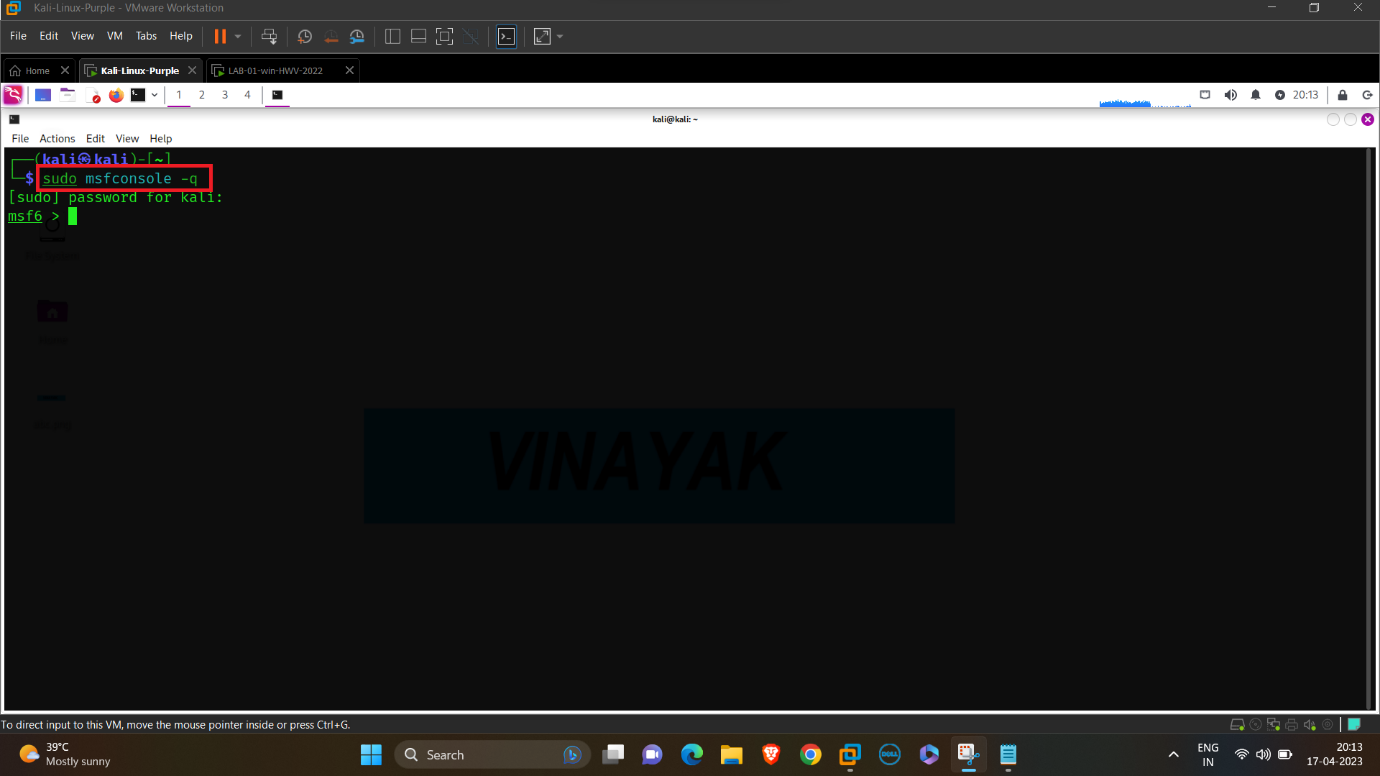
mousepad is a tool used to open and edit text files



Now we can check the usage of the script for Bruteforce attack.

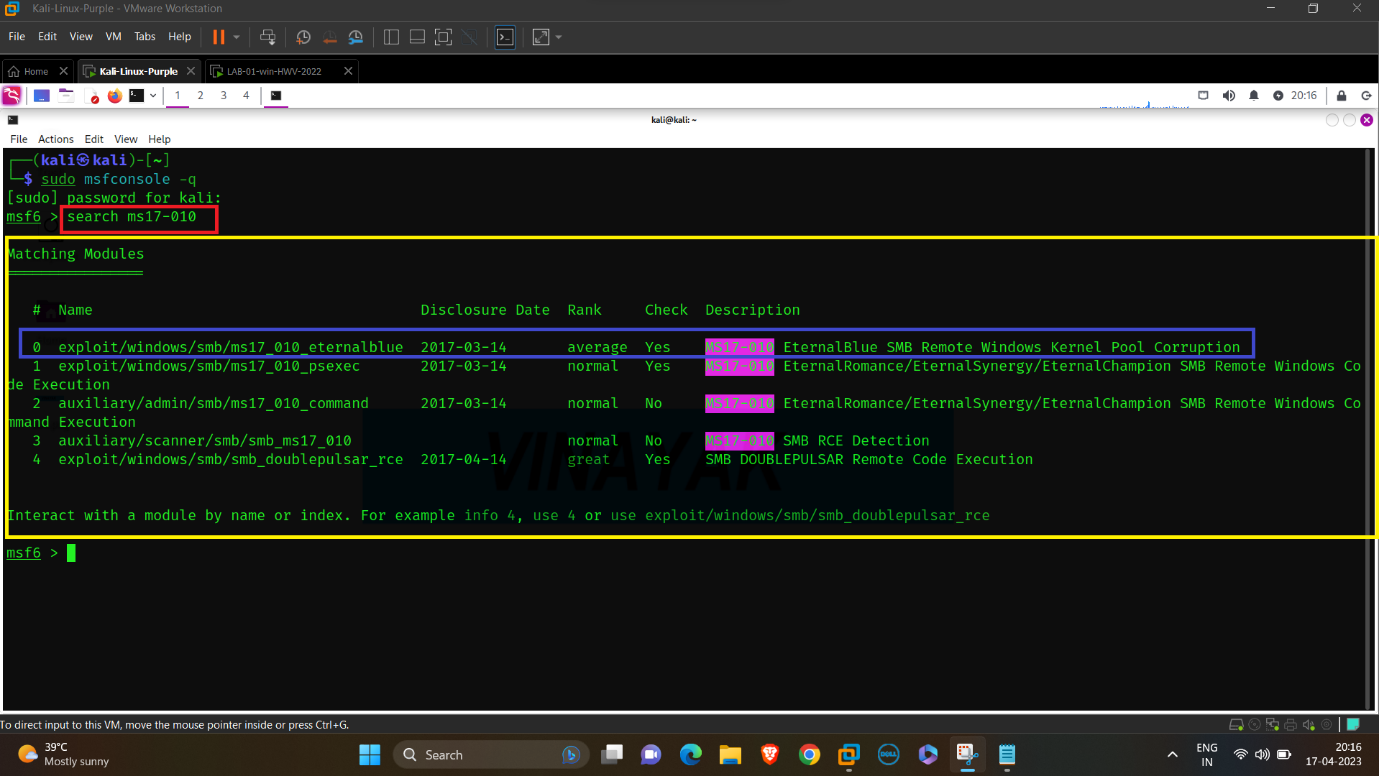
**Starting the Metasploit Framework for attack:**

msfconsole -q



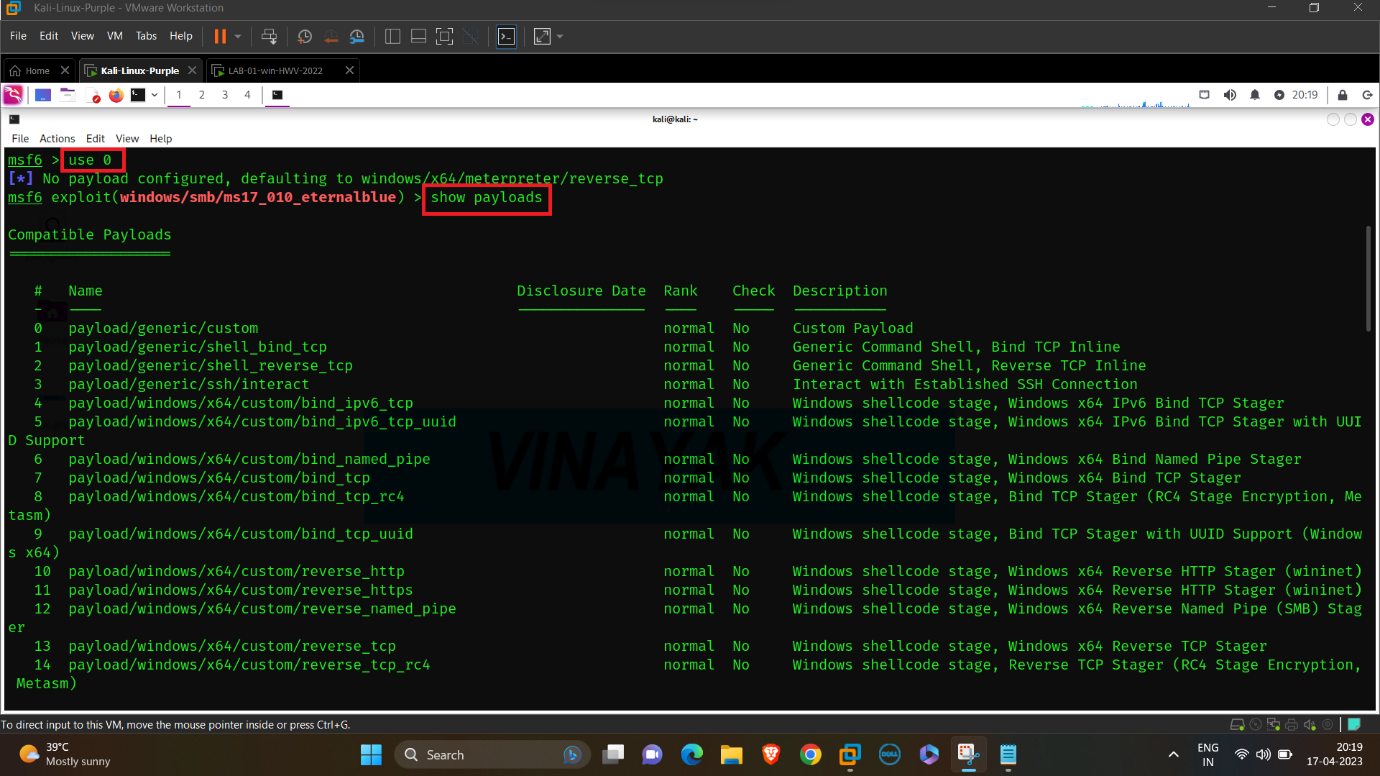
msfconsoleis the most commonly used shell which allows to access all the features of Metasploit.

-q is used to do not print the banner on startup.

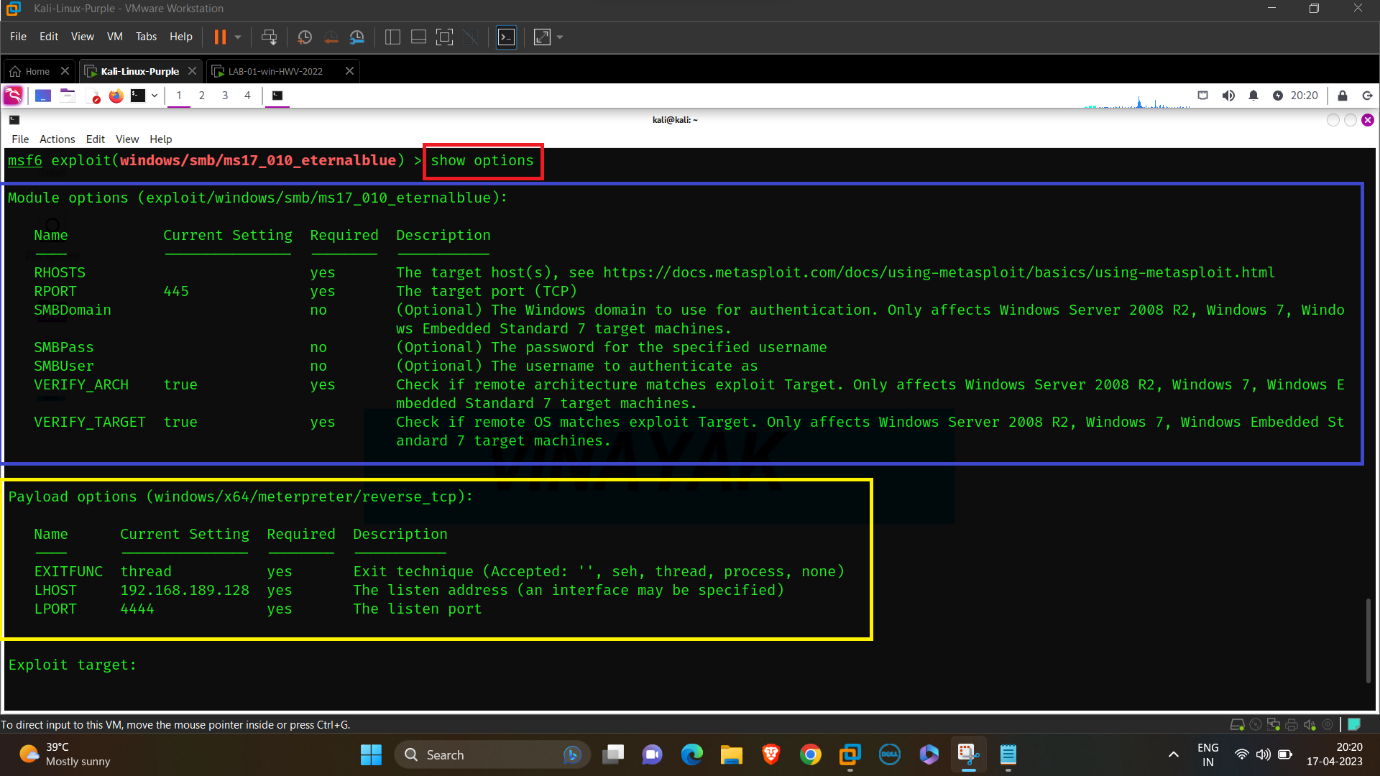


Search in Metasploit is used for searching the Exploit available for given version of the Service.

After that choose the Exploit with the help of use 0 or use (Exploit name).



**Details and Options required for the payload:**

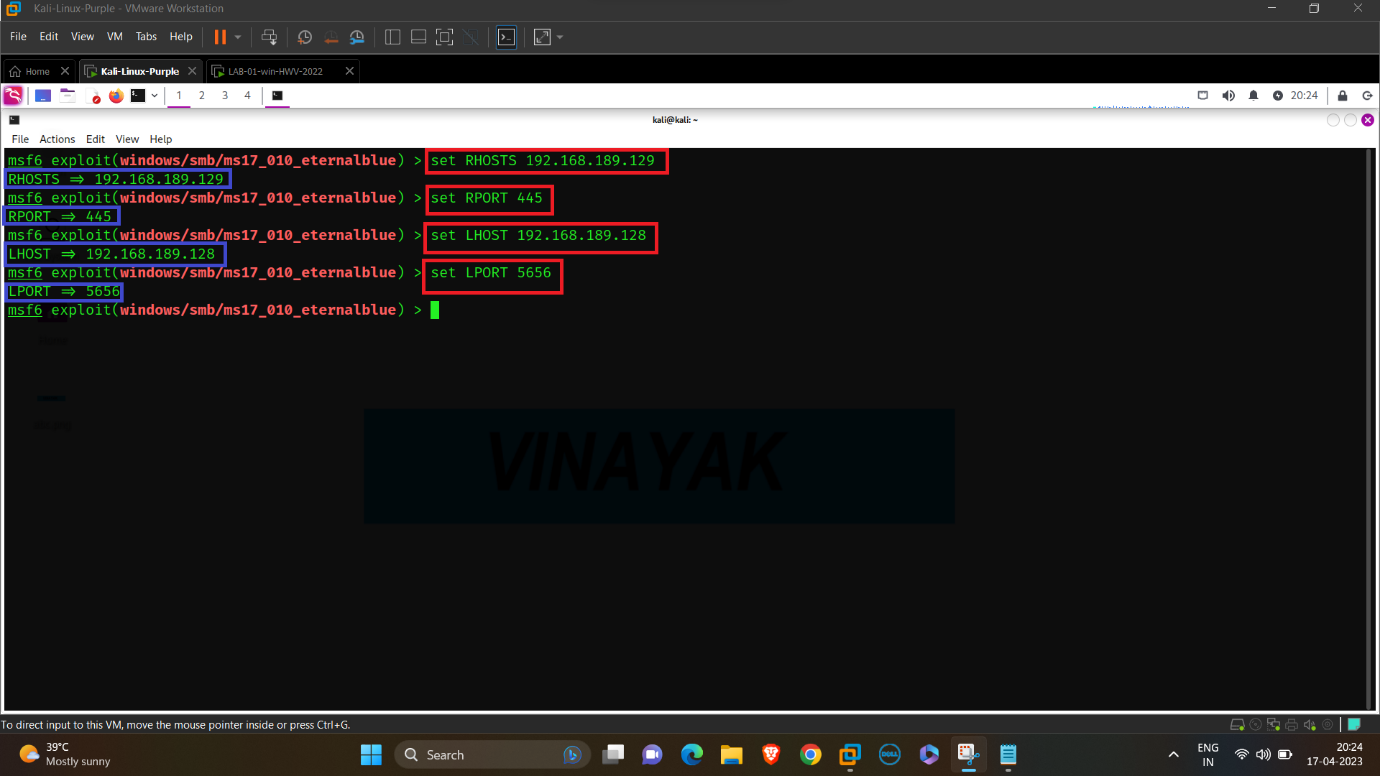
show options

Options for the details required for payload like:

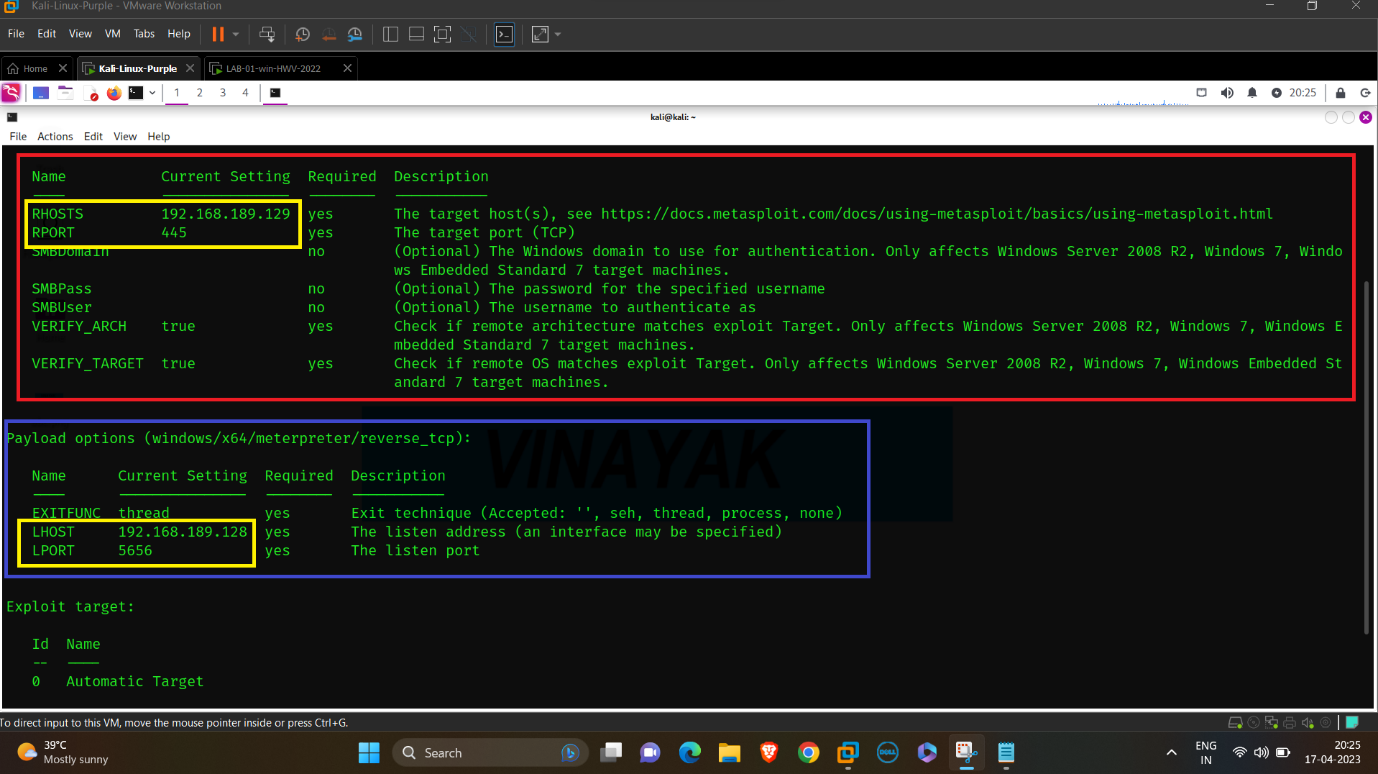
1. RHOSTS & RPORT are the IP Address and Port number of the Victim.
2. LHOST & LPORT are the IP Address and Port Number of User or Hacker.

**Set the necessary details:**

set RHOSTS, RPORT, LHOST, LPORT

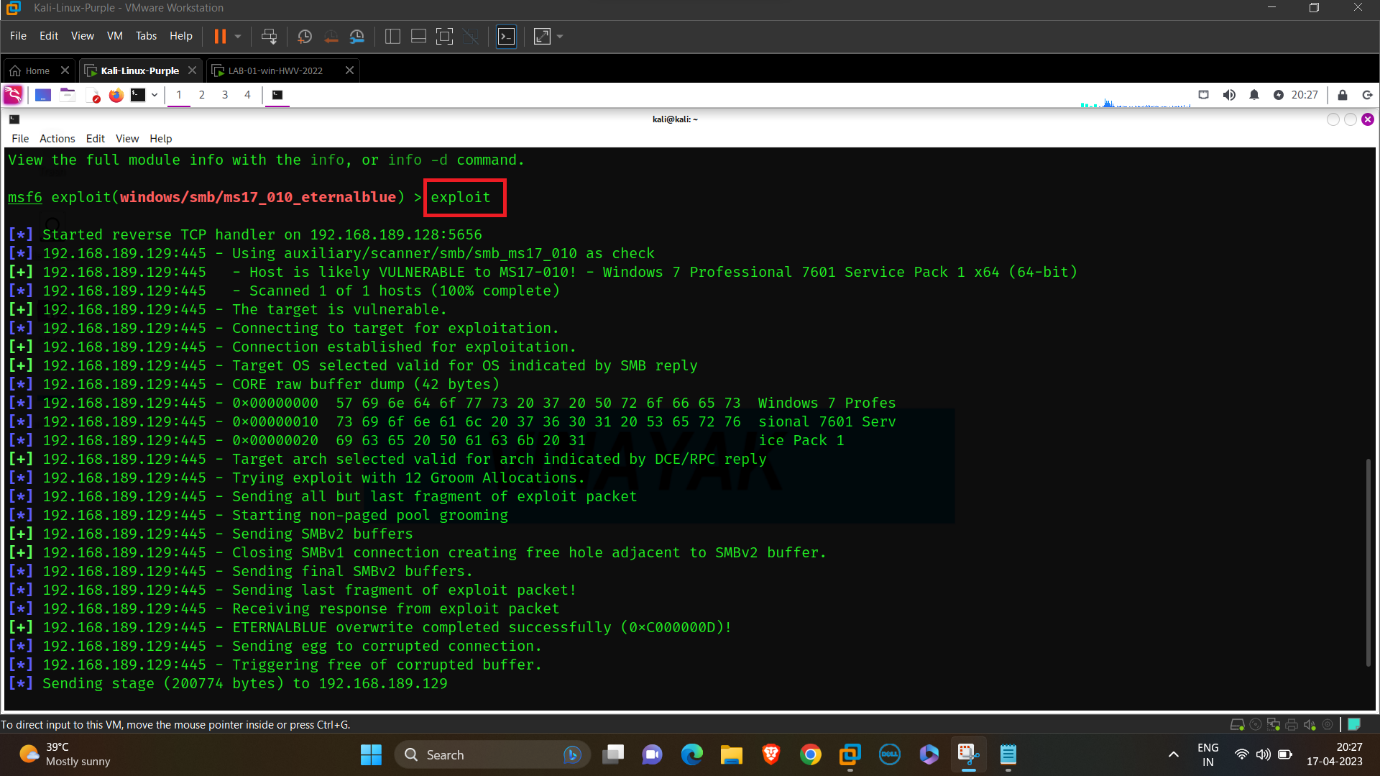


After that we have to check that all details are saved correctly by show options.



**Starting the Exploit:**

exploit

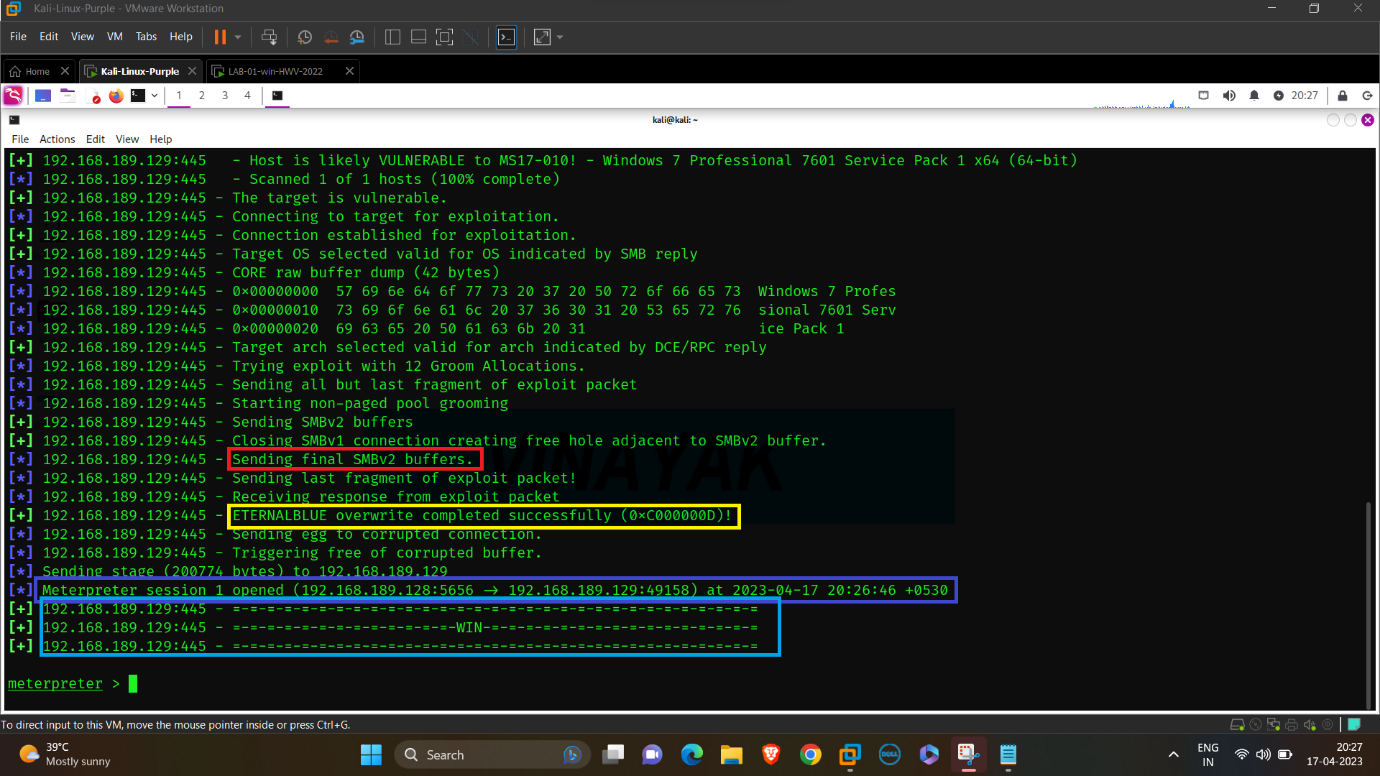


After starting the exploit, a Session will be opened like -

(LHOST:LPORT -> RHOSTS:RPORT)

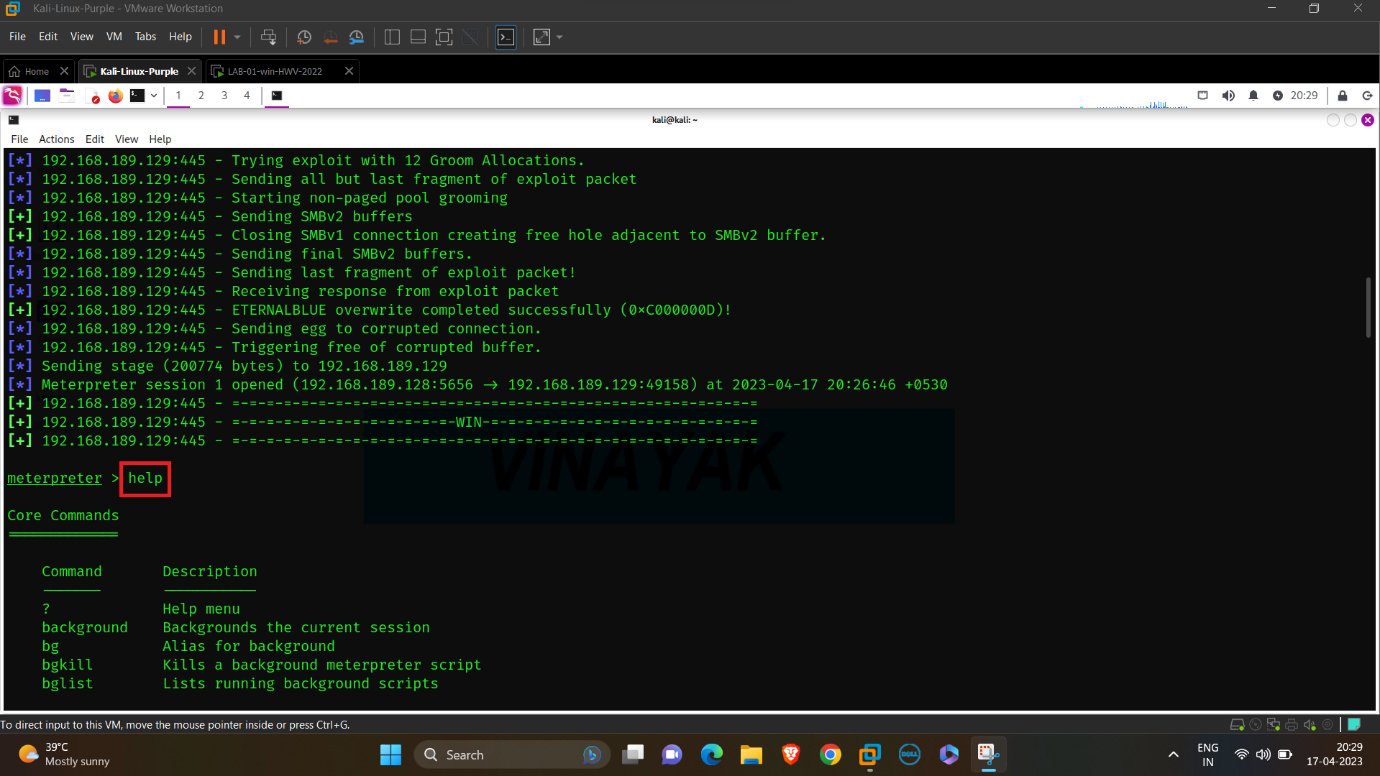
192.168.189.128:5656 ->192.168.189.129:49158

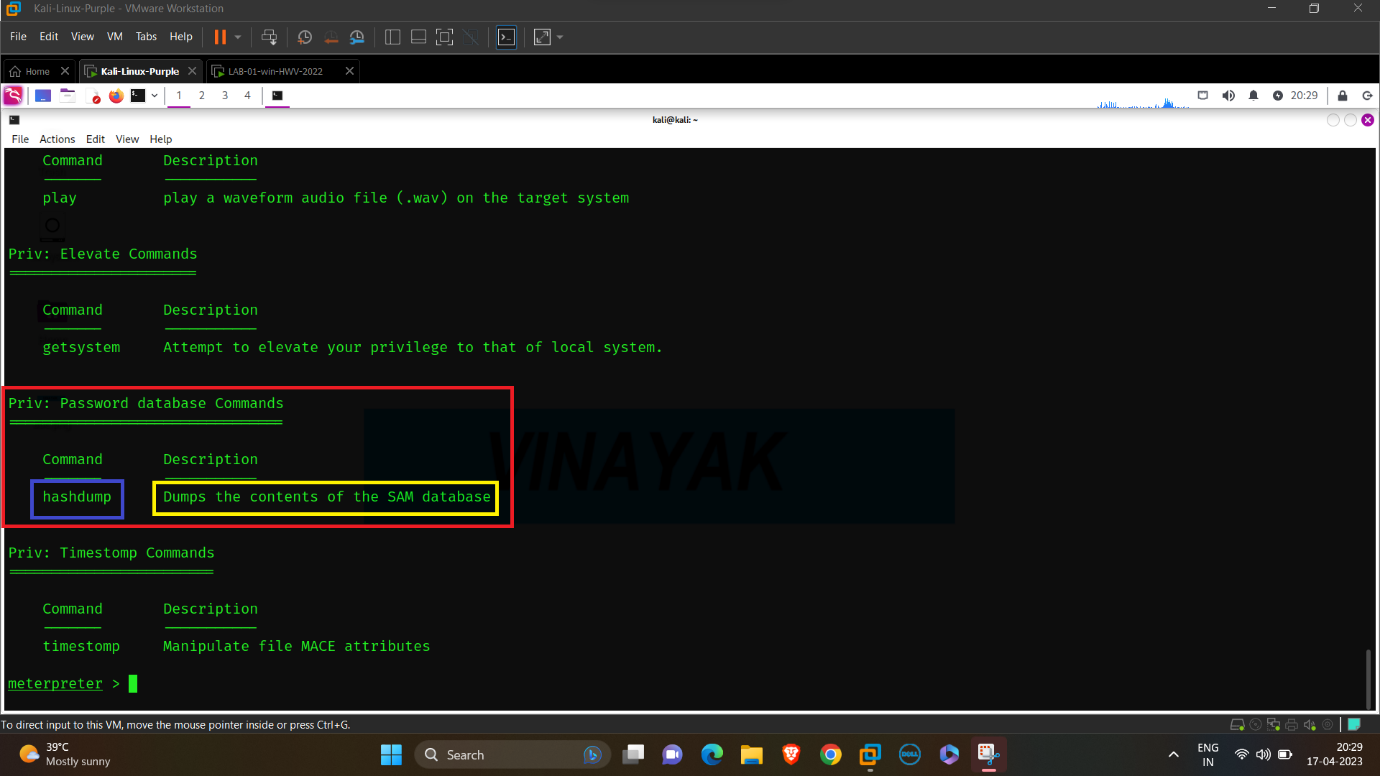
**Successful Exploit:**



**Checking the Commands available in Meterpreter:**

help



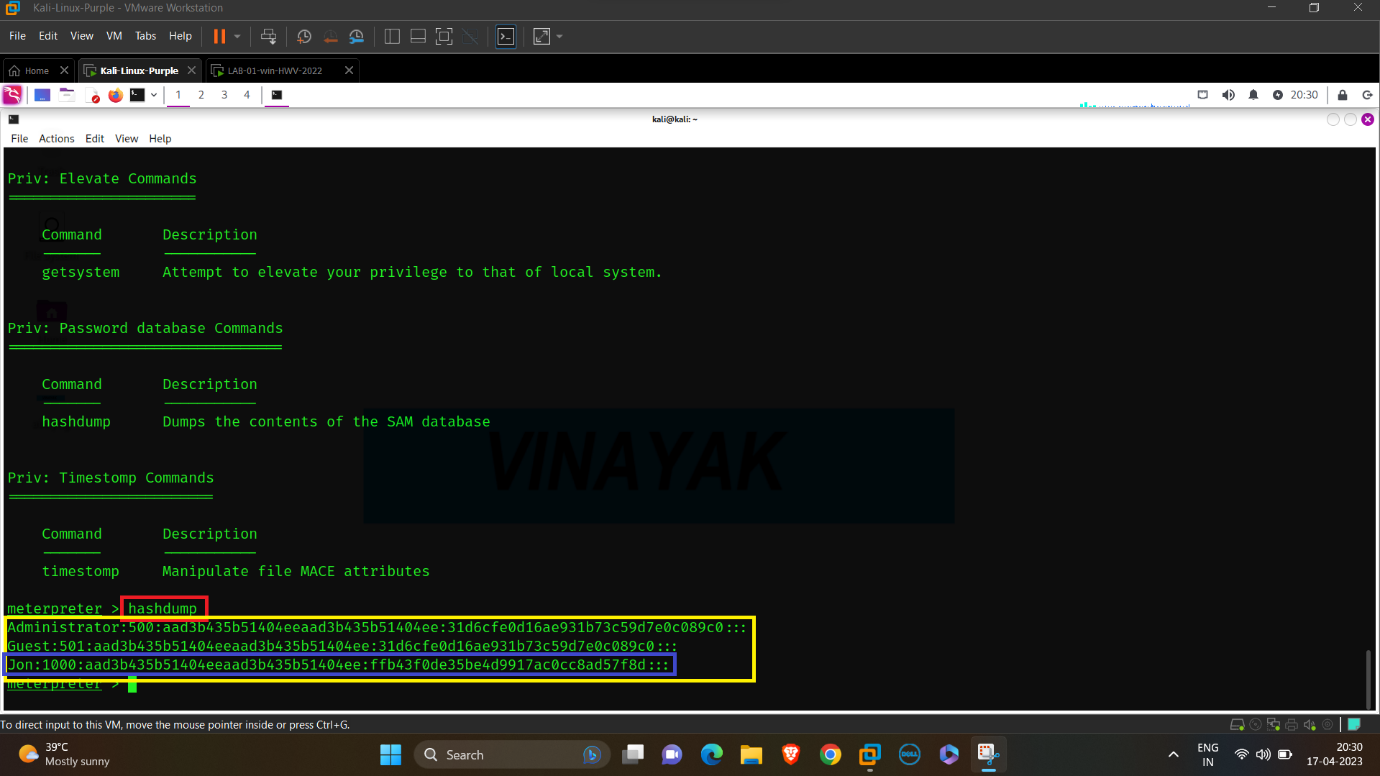


The Metasploit Meterpreter has supported the "hashdump" command. The "hashdump" command is an in-memory version of the pwdump tool, but instead of loading a DLL into LSASS.exe, it allocates memory inside the process, injects raw assembly code, executes its via CreateRemoteThread, and then reads the captured hashes back out of memory. This avoids writing files to the drive and by the same token avoids being flagged by antivirus (AV) and intrusion prevention (HIPS) products.

Over the last few years, many AV and HIPS products have added hooks to detect this behaviour and block it at the API level. Unfortunately, the hooks are often implemented in a way that causes LSASS.exe to crash, which forces the entire system to either halt or reboot. This has made the "hashdump" command (along with pwdump and its friends) somewhat risky to use during a penetration test.

**Successfully cracked the Password:**

hashdump



We have successfully got the Username and Password.

Username = Jon

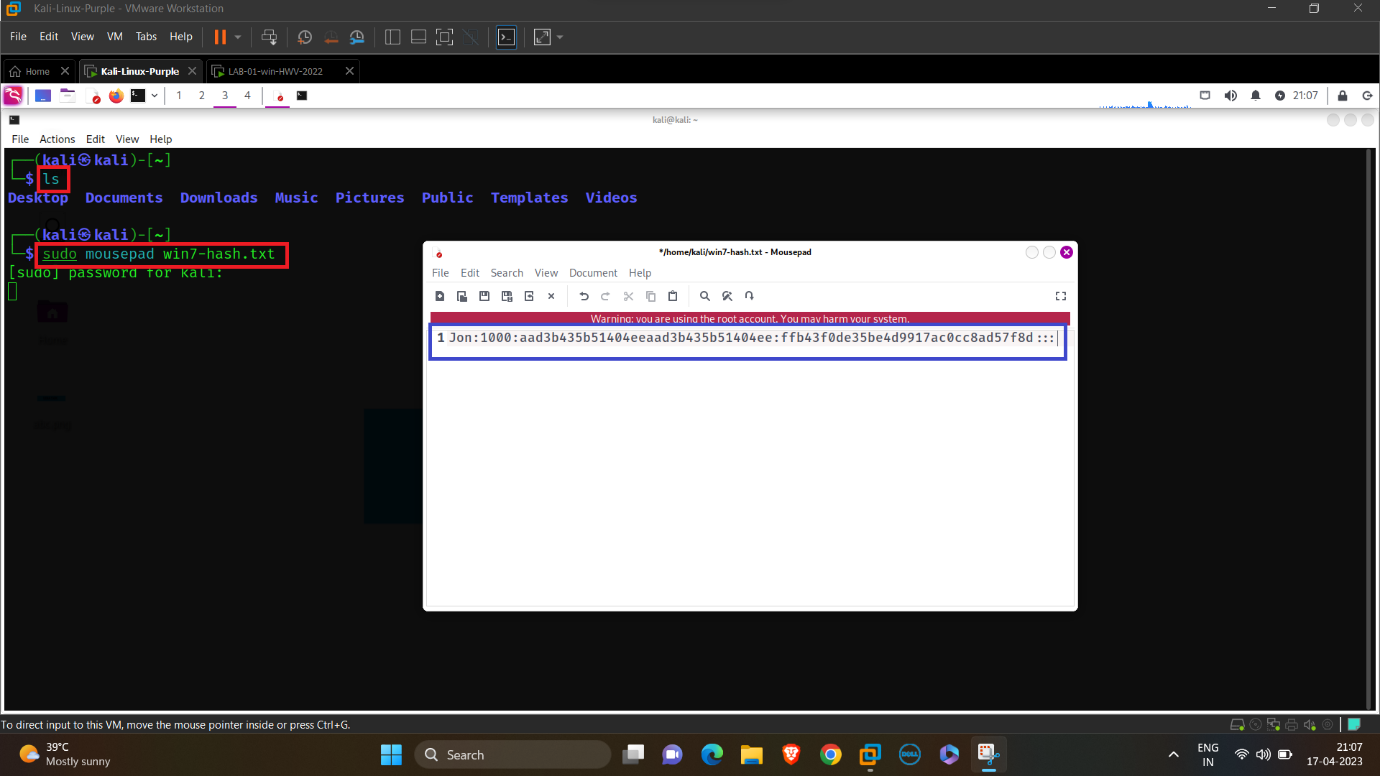
Password = Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

Then we have to save the Hash Password or Encrypted Password for Bruteforce attack to crack the Original Password.

**Saving the Hash Password in Text File:**

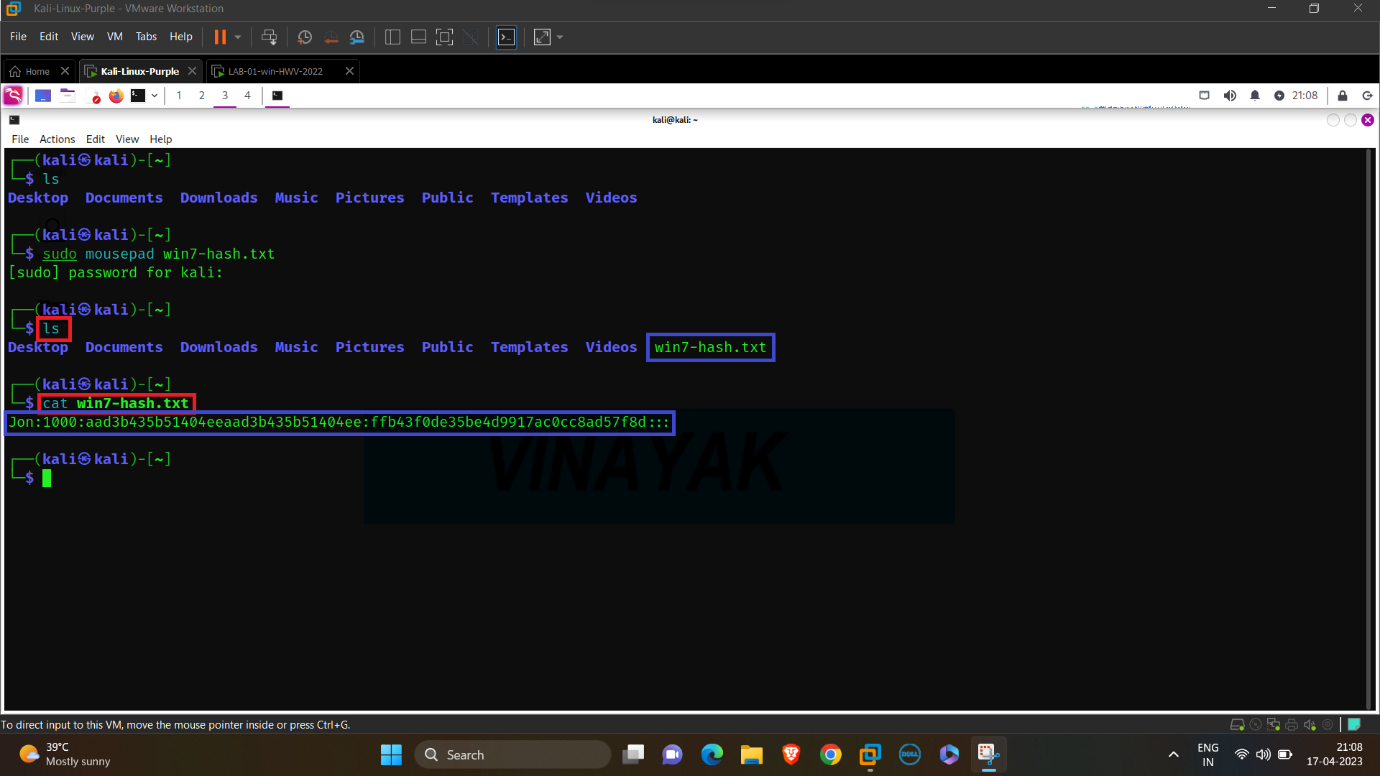
ls

mousepad win7-hash.txt



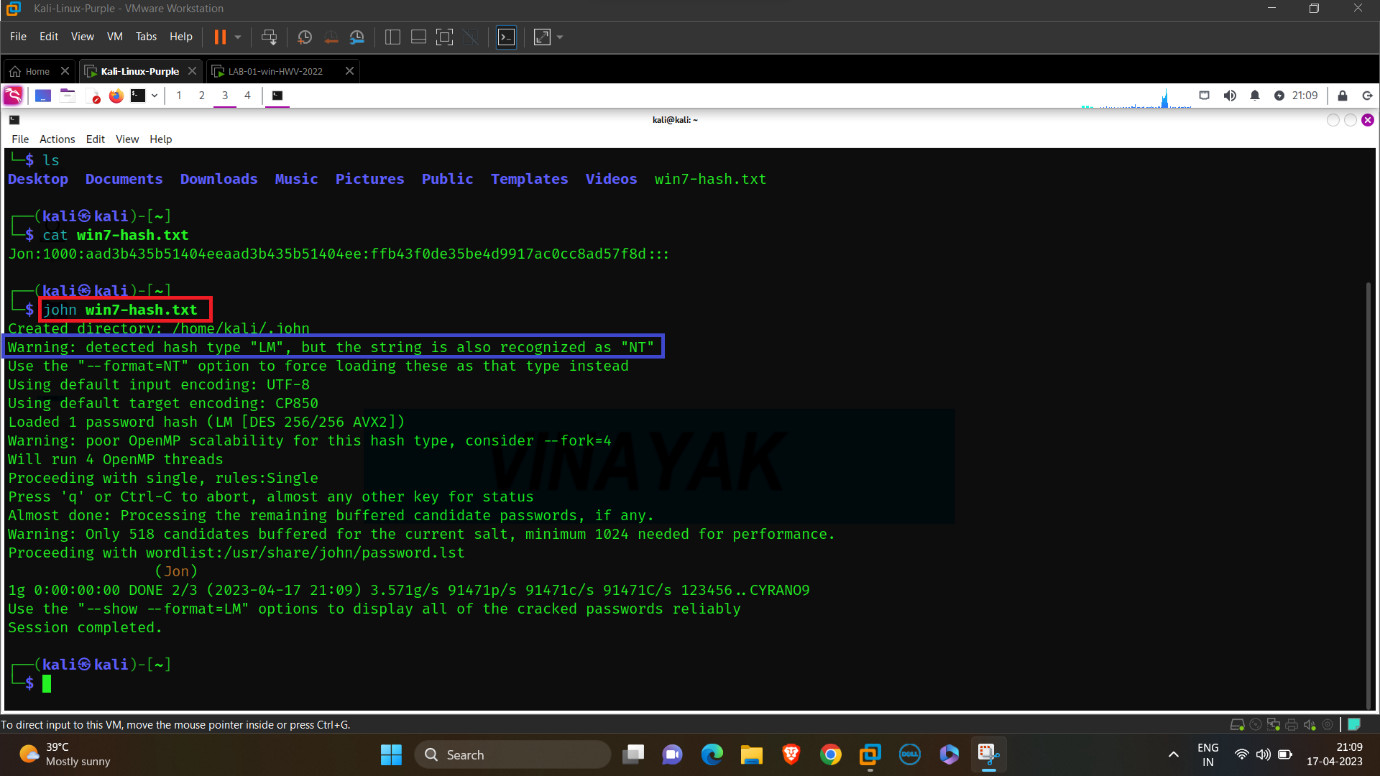
**Checking the Password correctly saved:**

cat win7-hash.txt

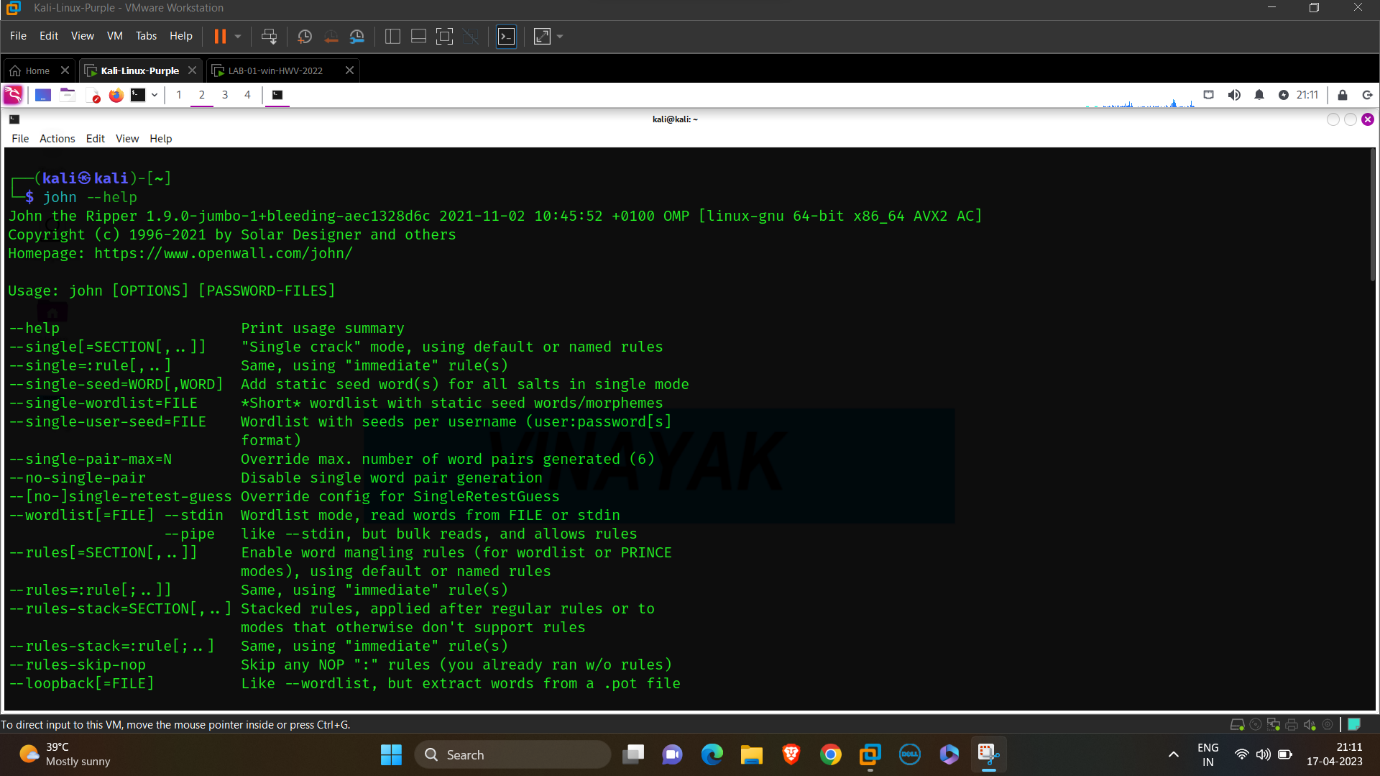


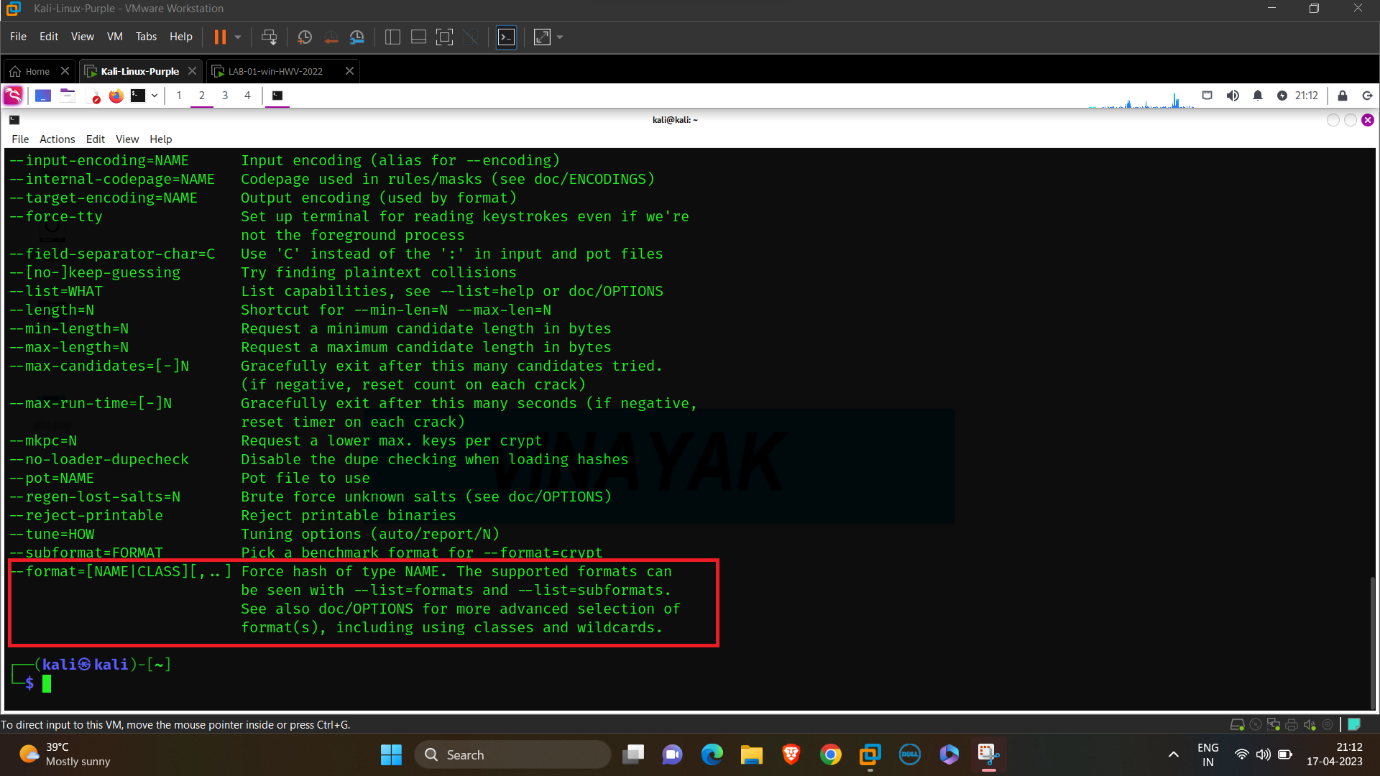
**Cracking the Password with John the Ripper:**

john win7-hash.txt



We have got an error regarding the format of the Hash Password. The Hash Password we saved is in the LM format, but the required format for John the Ripper is NT.

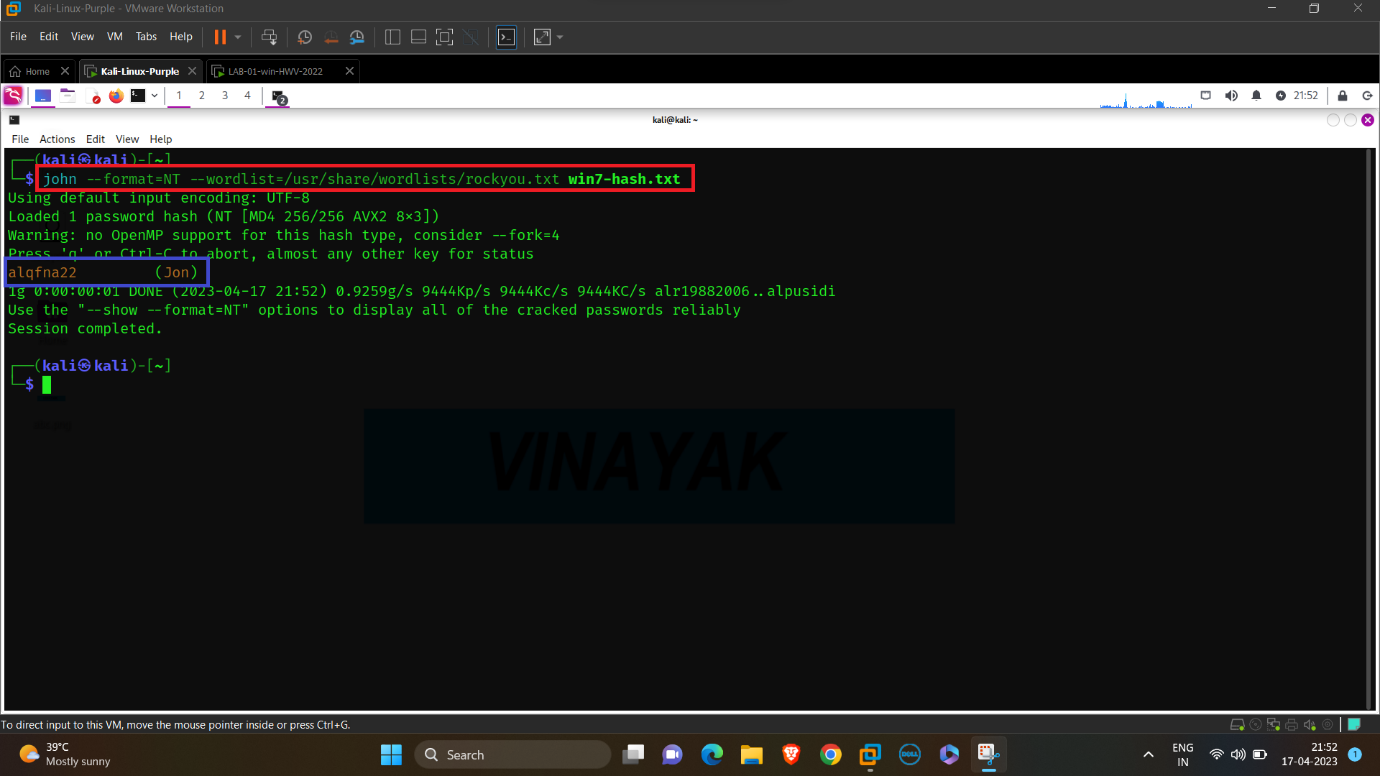
**Changing the Format of Hash Password:** 



We have found the command to change the format.

**Successfully cracked the Password:**

john --format=NT –wordlist=/usr/share/wordlists/rockyou.txt win7-hash.txt

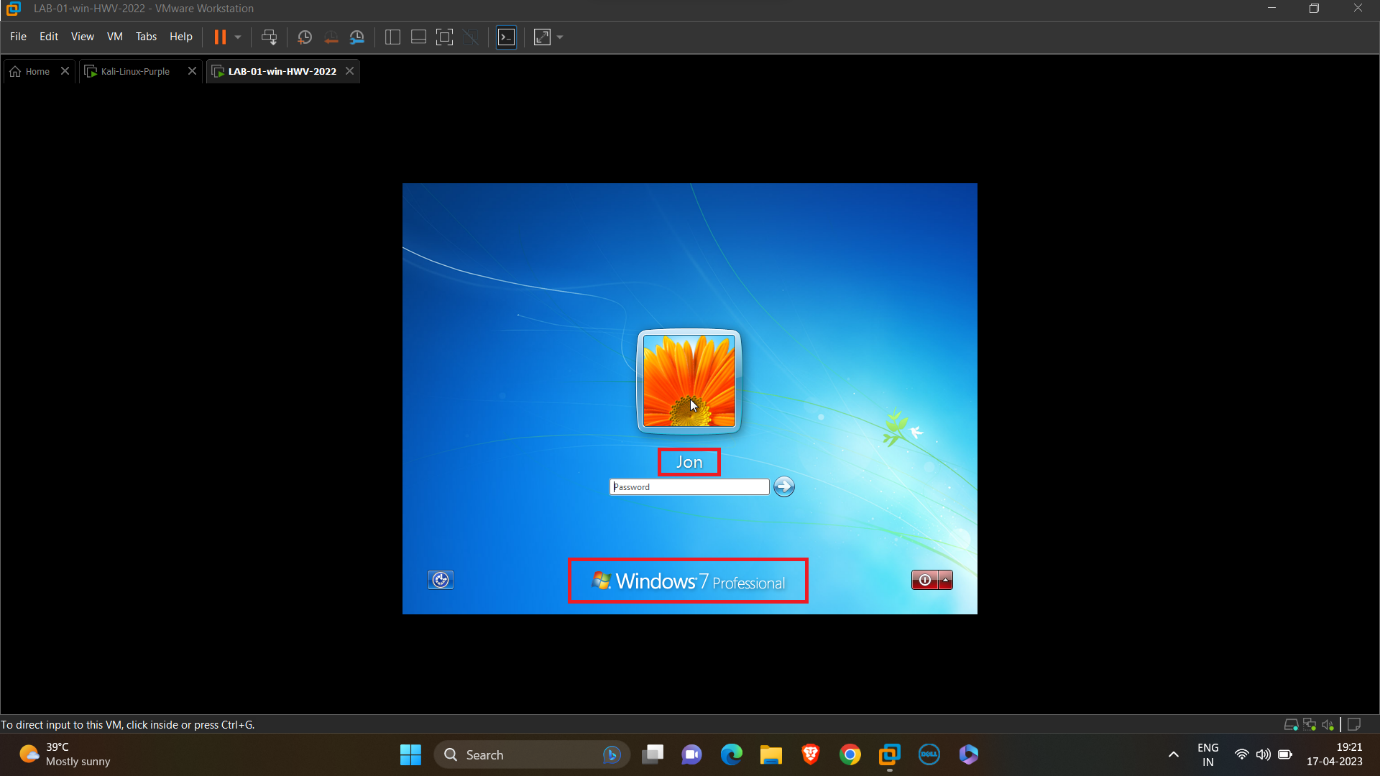


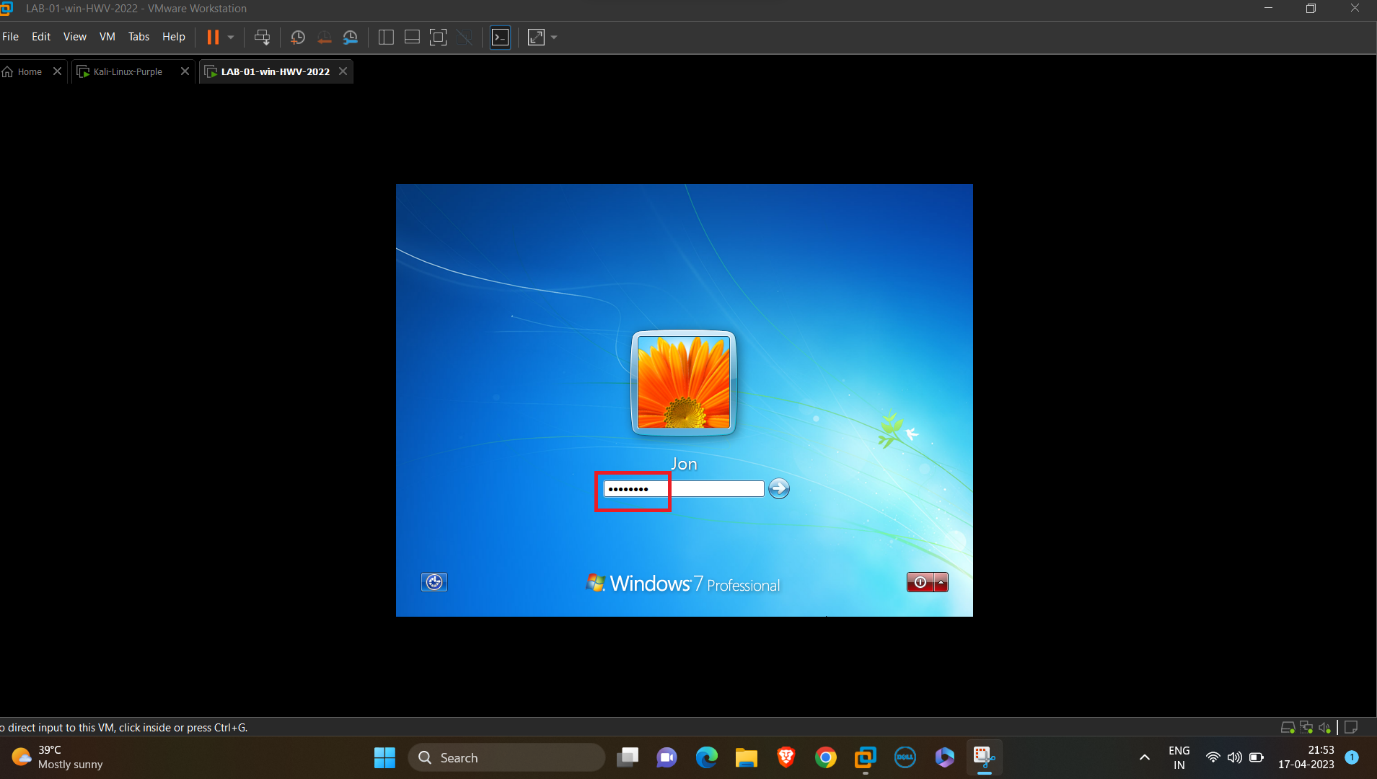
We have successfully cracked the Original Password with the help of John the Ripper.

USERNAME: JON

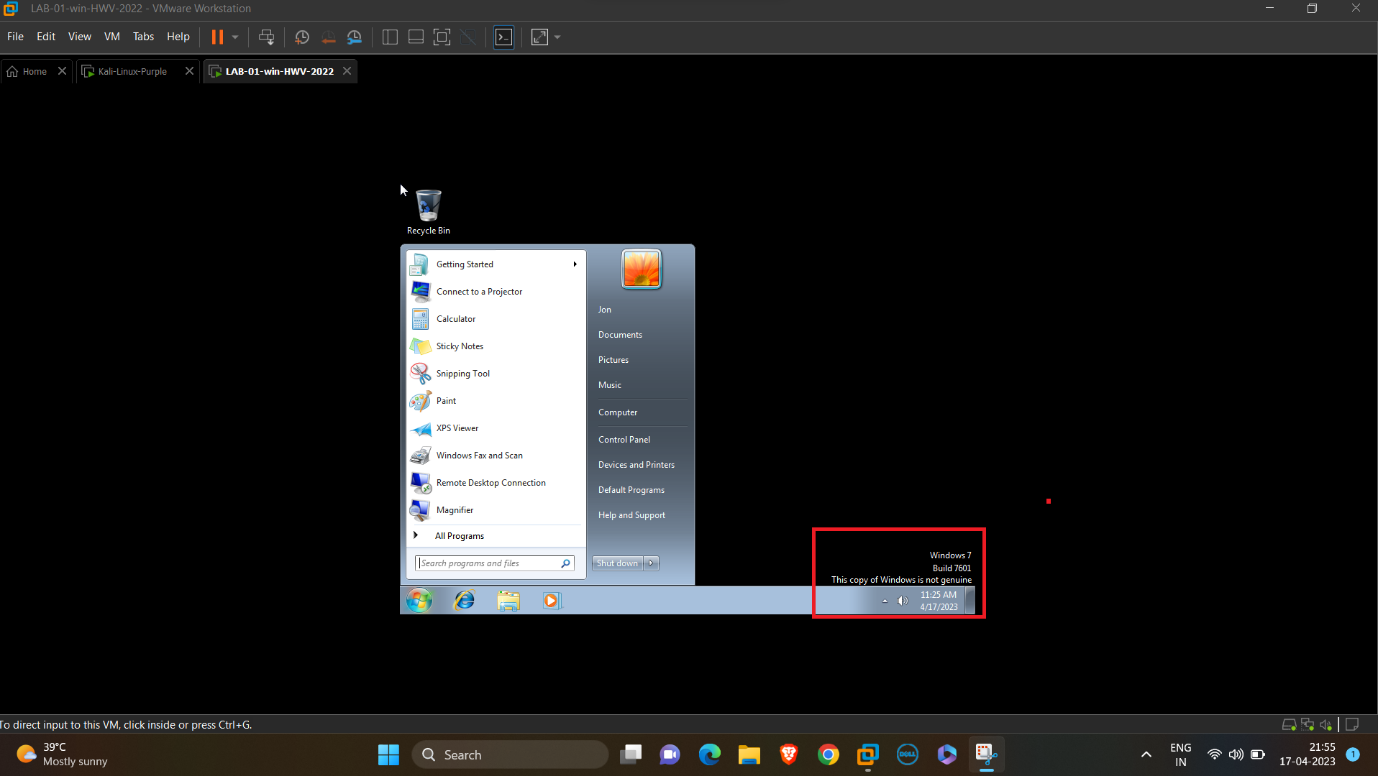
PASSWORD: alqfna22

**Log-in into the Windows 7 Machine:**





**Successfully Logged-in into the Windows 7 Machine:**



Now we have successfully compromised and logged-in into the Windows 7 Machine.