

OLD DOMINION UNIVERSITY
CYSE 301 Cybersecurity Technique and Operations

Assignment 2

Madelene McFarlane

#01096496

Each student needs to login into the **CCIA virtual environment** to complete this assignment.

Task A: Sniff LAN traffic

In this task, you will be acting as an **ATTACKER** who sniffs the internal communications between peers by using either Wireshark or tshark on **Ubuntu VM**. You need to use the following VMs to complete the assignment.

I recommend you keep the Wireshark/tshark running in the background all the time.

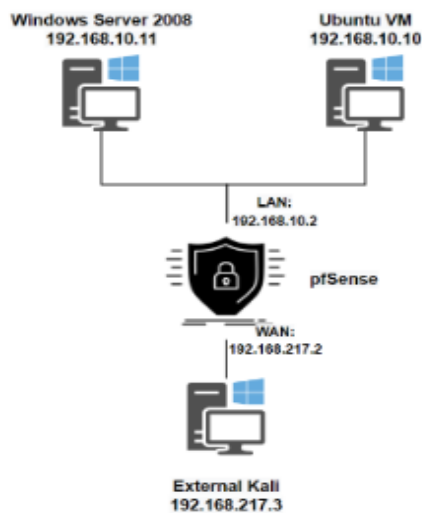


Figure 1 Required VMs for this assignment

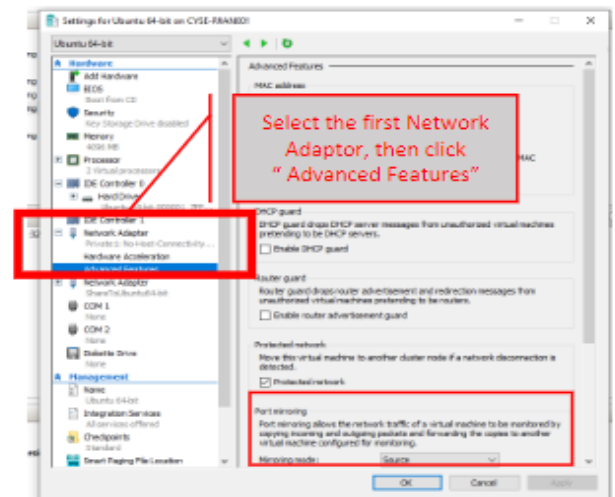


Figure 2 How to configure port mirroring in Hyper-V

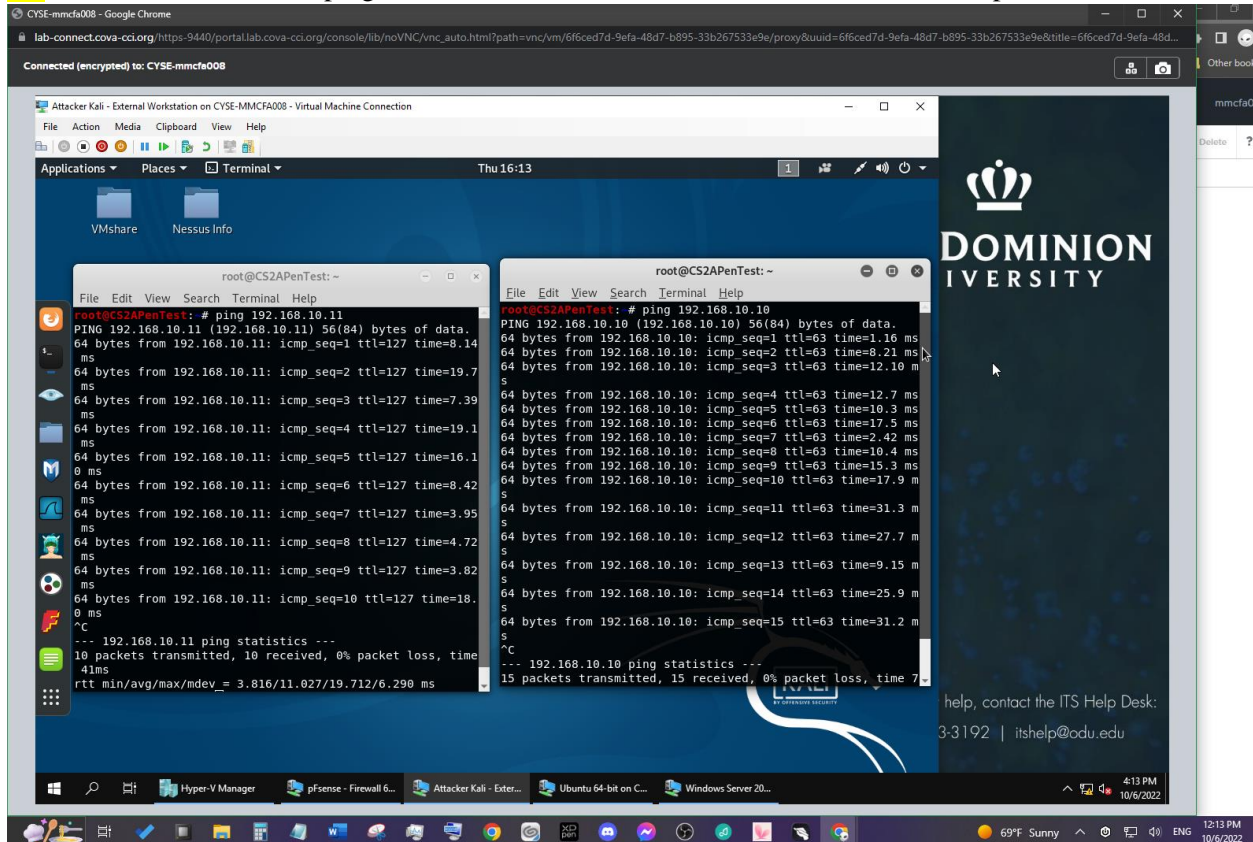
IMPORTANT! Due to the different networking configurations in Hyper-V, you need to **Enable Port Mirroring for related VMs accordingly**. This is a helpful link to follow. To be specific, you need to put the sniffer (Ubuntu VM) as the **mirroring Destination**, and the target VMs are the **mirroring Source** (Figure 2).

To be specific,

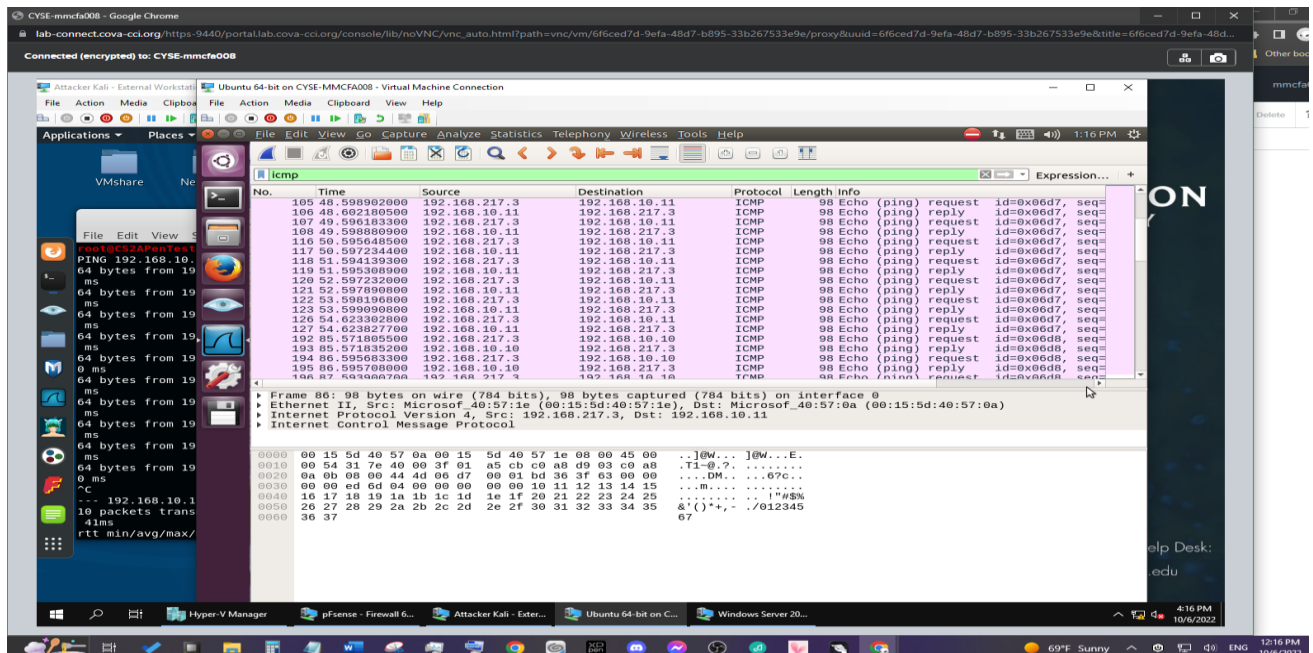
- Ubuntu VM: Set Mirroring mode to “**Destination**” in the “Port Mirroring.”
- Windows Server 2008: Set Mirroring mode to “**Source**” in the “Port Mirroring.”
- External Kali: Set Mirroring mode to “**Source**” in the “Port Mirroring.”

1. Sniff ICMP traffic (10 + 10 +20 points)

1.1. In External Kali VM, ping Windows Server 2008 and Ubuntu VM from two separate terminals.



1.2. Apply proper display or capture filter on Ubuntu VM to show all ping traffic (towards both Ubuntu and Windows Server 2008) (tip: you can filter the traffic by protocol type).



1.3. Apply proper display or capture filter on **Ubuntu VM** that **ONLY** displays **ICMP request** originated from External Kali VM and goes to Windows Server 2008 (tip: you can filter the traffic by IP address).

Connected (encrypted) to: CYSE-mmcf008

Attacker Kali - External Workstation | Ubuntu 64-bit on CYSE-MMCF008 - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Places *eth0

Filter: ip.src == 192.168.217.3 and icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|--|
| 86 | 45.579606400 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 101 | 46.581528200 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 103 | 47.585833800 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 105 | 48.598902000 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 107 | 49.596183300 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 110 | 50.595048500 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 118 | 51.594139300 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 120 | 52.597232000 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 122 | 53.598196800 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 126 | 54.623382800 | 192.168.217.3 | 192.168.10.11 | ICMP | 98 | Echo (ping) request id=0x06d7, seq=... |
| 192 | 85.571805500 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 194 | 86.595683300 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 196 | 87.593909700 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 198 | 88.598256400 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 200 | 89.606398000 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 204 | 90.605642400 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 215 | 91.608063800 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 217 | 92.618571100 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 219 | 93.626736400 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 221 | 94.629423500 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 223 | 95.636302100 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 232 | 96.637965500 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 234 | 97.626655700 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |
| 236 | 98.637333300 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0x06d8, seq=... |

Frame 86: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Microsof_40:57:1e (08:15:5d:40:57:1e), Dst: Microsof_40:57:0a (08:15:5d:40:57:0a)
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.11
Internet Control Message Protocol
Echo (ping) request id=0x06d7, seq=...

0000 00 15 5d 40 57 0a 00 15 5d 40 57 1e 08 00 45 00 ...]@W...]@W...E.
0010 00 54 31 7e 40 00 3f 01 a5 cb c9 a8 09 03 c0 a8 .T1-@.?.
0020 0a 0b 08 00 44 4d 06 d7 00 01 bd 36 f3 03 00 00DM.67c..
0030 00 00 ed 6d 04 00 00 00 00 00 10 11 12 13 14 15m.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25! "#\$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 67

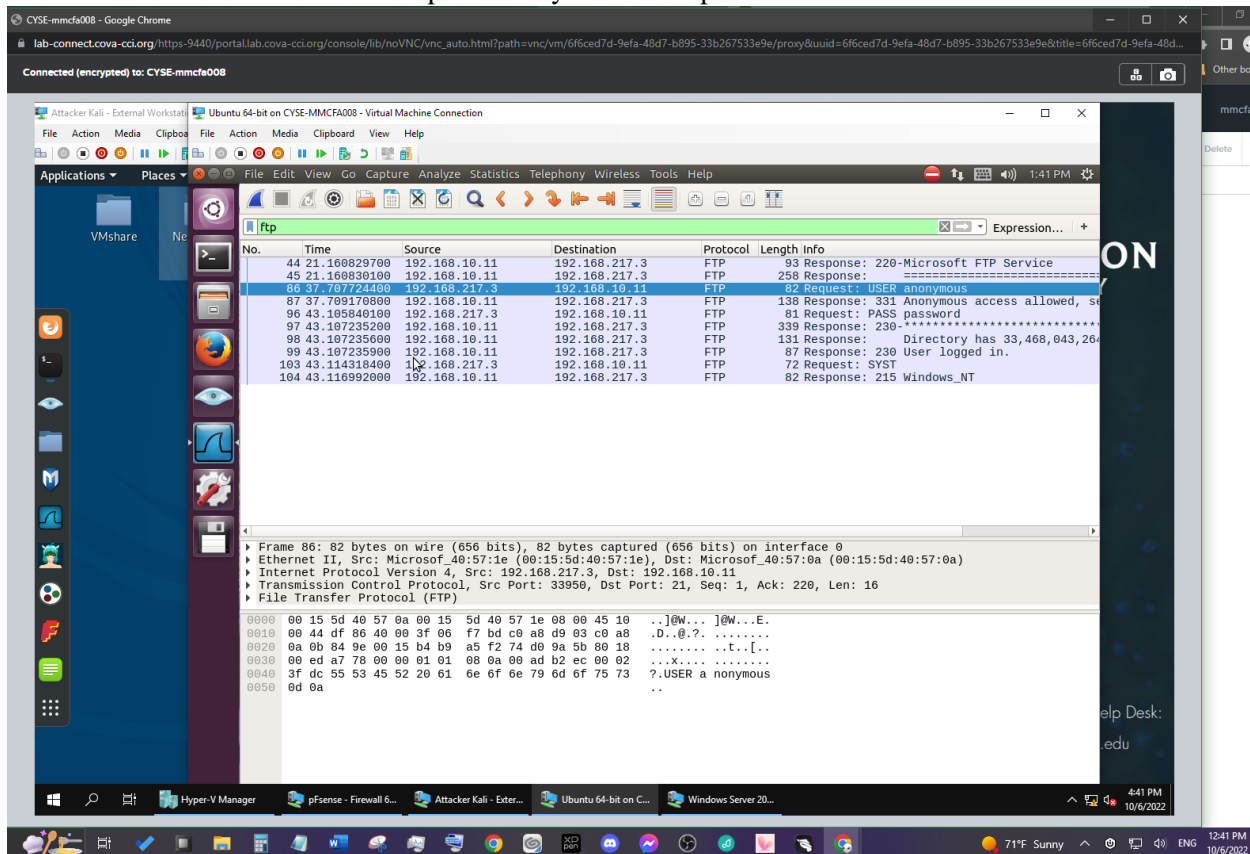
Hyper-V Manager | pfSense - Firewall 6... | Attacker Kali - Ext... | Ubuntu 64-bit on C... | Windows Server 20...

69°F Sunny | 12:23 PM 10/6/2022

2. Sniff FTP traffic (60 points)

Windows Server 2008 is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: **ftp** [*ip_addr of Windows Server 2008*]. The username for the FTP server is **anonymous**, and the password is **password**. You can follow the steps below to access the FTP server.

2.1. Unfortunately, Ubuntu VM, the attacker, is also sniffing the internal communication by using **tshark**. So, all of your communication is exposed to the attacker. Now, you need to find out the username and password entered in the External Kali in the **Wireshark** running on Ubuntu VM. You need to screenshot and explain how you find the password.



How I found the password was by filtering the protocol to ftp. Then I can see from the information that the username and password was accepted by ftp and there for exposing the username and password. If there was a lot of ftp traffic, I could filter using 'ftp contains "USER"' and 'ftp contains "PASS"' to narrow the traffic down.

2.2. After you successfully sniffed the username & password from the FTP traffic, repeat the

previous step, and use your **MIDAS ID** as the username and **UIN** as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these “secrets” from the attacker VM, which is

Ubuntu Kali.

The screenshot displays a Kali Linux virtual machine interface. The main window shows a network traffic capture on the `eth0` interface. The capture is filtered for `ftp` traffic. The table below represents the data shown in the packet list:

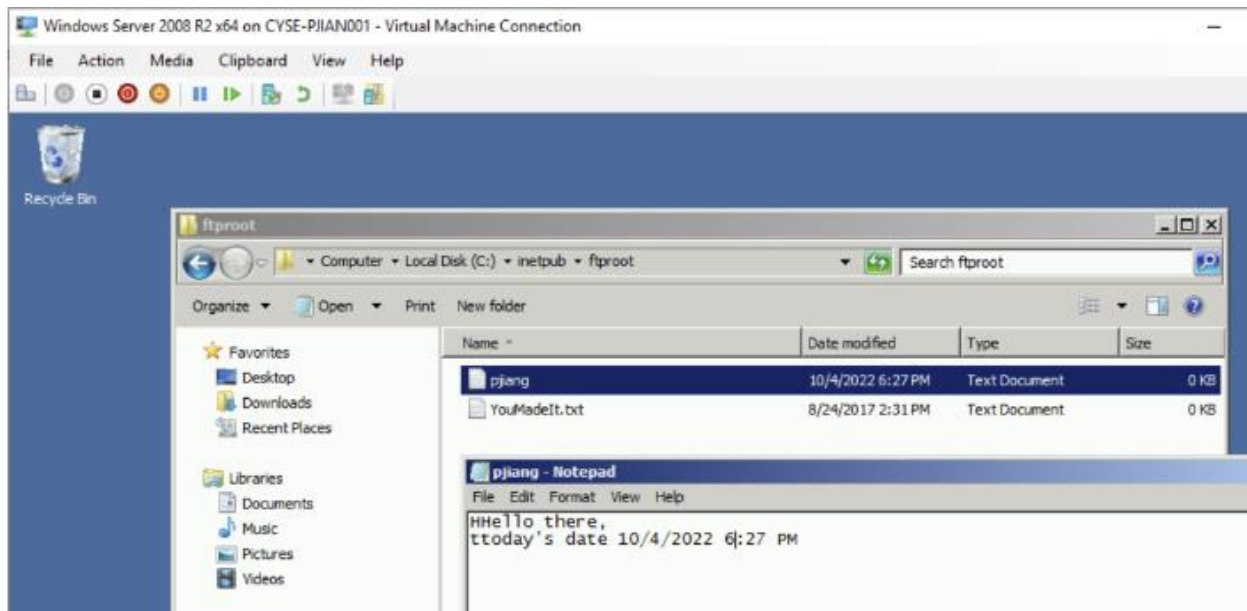
| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|---------------|---------------|----------|--------|--|
| 118 | 37.271926280 | 192.168.10.11 | 192.168.217.3 | FTP | 93 | Response: 220-Microsoft FTP Service |
| 919 | 37.271927100 | 192.168.10.11 | 192.168.217.3 | FTP | 258 | Response: ..] |
| 1179 | 48.021690300 | 192.168.217.3 | 192.168.10.11 | FTP | 81 | Request: USER mmcfa008 |
| 1180 | 48.022458700 | 192.168.10.11 | 192.168.217.3 | FTP | 103 | Response: 331 Password required for mmcfa008 |
| 1646 | 66.943210900 | 192.168.217.3 | 192.168.10.11 | FTP | 81 | Request: PASS 01096496 |
| 1647 | 66.944960500 | 192.168.10.11 | 192.168.217.3 | FTP | 91 | Response: 530 User cannot log in. |
| 1649 | 66.946793900 | 192.168.217.3 | 192.168.10.11 | FTP | 72 | Request: SYST |
| 1650 | 66.947293600 | 192.168.10.11 | 192.168.217.3 | FTP | 82 | Response: 215 Windows_NT |

The bottom pane shows the raw packet data for the selected packet (Frame 918):

```
Frame 918: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Ethernet II, Src: Microsof_40:57:0a (00:15:5d:40:57:0a), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
Internet Protocol Version 4, Src: 192.168.10.11, Dst: 192.168.217.3
Transmission Control Protocol, Src Port: 21, Dst Port: 33952, Seq: 1, Ack: 1, Len: 27
File Transfer Protocol (FTP)
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0a 08 00 45 00 ..]@W... ]@W...E.
0010 00 4f 00 9b 40 00 00 06 95 ae c9 a8 0a 0b c0 a8 .0..@.....
0020 d9 03 00 15 84 a0 47 8e 7a 41 d6 52 8f 07 80 18 ....G.ZA.R....
0030 02 02 68 7c 00 00 01 01 08 0a 00 03 c4 0b 00 bc ..h]....
0040 9c 1b 32 32 30 2d 4d 69 63 72 6f 73 6f 66 74 20 ..220-Mi crossoft
0050 46 54 50 20 53 65 72 76 69 63 65 0d 0a FTP Serv ice..
```


Task B – Extra credit: Steal files with Wireshark (15 points)

Log in to Windows Server 2008 VM, and create a file in “C:/inetpub/ftproot/” named “YOUR_MIDAS.txt”. Put the current timestamp and your name in the file.



Once you have the file ready in Windows Server 2008, switch back to **External Kali**. Get the file you just created with FTP protocol remotely. Below is an example.

```
Directory has 33,464,455,168 bytes of disk space available.
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
drwxrwxrwx  1 owner    group          0 Oct  4 18:27 upload
-rwxrwxrwx  1 owner    group          46 Oct  4 18:31 pjiang.txt
-rwxrwxrwx  1 owner    group          0 Aug 24 2017 YouMadeIt.txt.txt
226-Directory has 33,464,455,168 bytes of disk space available.
226 Transfer complete.
ftp> get pjiang.txt
local: pjiang.txt remote: pjiang.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
46 bytes received in 0.01 secs (7.9018 kB/s)
ftp>
```

As an attacker, you need to complete the following tasks in Ubuntu VM to steal the file just transferred :

1. Apply a proper display filter to display the **FTP-DATA** packets between External Kali and Windows Server 2008.

2. Follow the tcp steam of the **FTP-DATA** packet and view the content of the file just transferred.
3. Export (Save) the transferred file as a text file in Ubuntu VM and view the content. Below is an example.

