CYSE 301: Cybersecurity Technique and Operations

Assignment 1: Traffic Tracing and Sniffing

Ian Waweru

01151080

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

Students use tshark will receive extra points.

Task B: Sniff LAN traffic

In this task, you will be acting as an **ATTACKER** who sniffs the regular communications between peers (External Attacker Kali and Ubuntu) by using either Wireshark or tshark on **Internal Attacker Kali VM**.

I would recommend you keeping the Wireshark/tshark running on Internal Kali all the time.

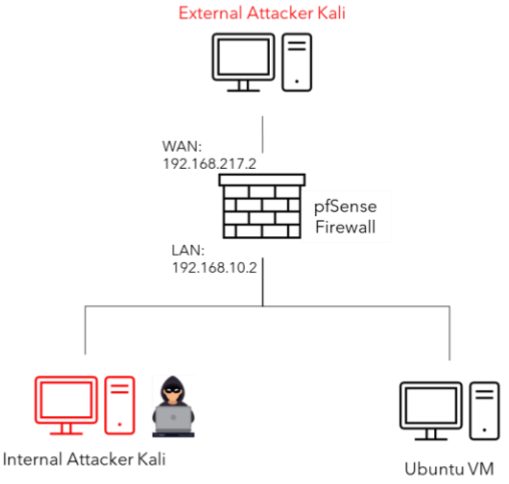
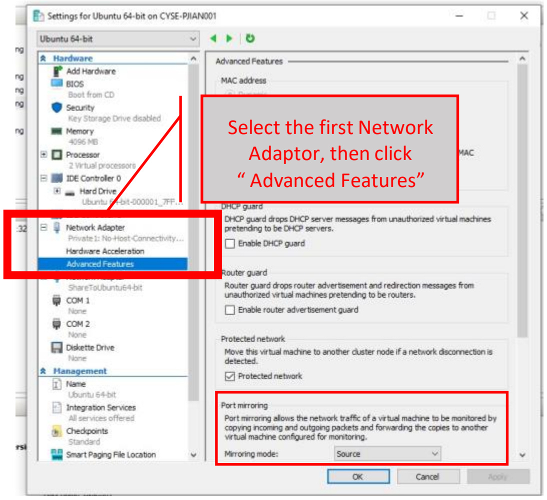


Figure 1 Required VMs for this assignment



Select the first Network Adaptor, then click " Advanced Features"

Advanced Features

MAC address

DHCP guard

DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.

☐ Enable DHCP guard

Router guard

Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.

☐ Enable router advertisement guard

Protected network

Move this virtual machine to another cluster node if a network disconnection is detected.

☑ Protected network

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode: Source

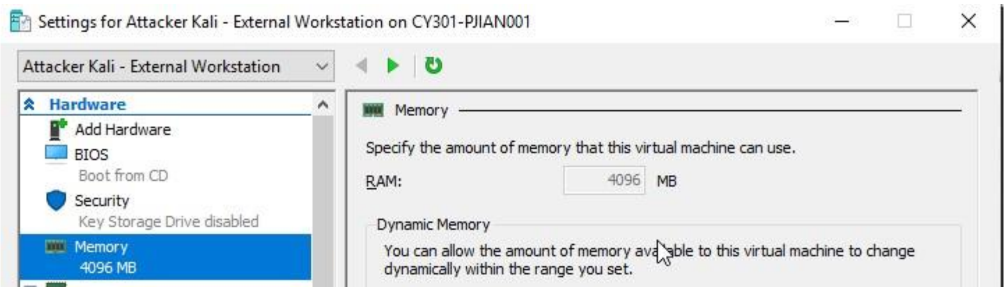
Figure 2 How to configure port mirroring in Hyper-V

IMPORTANT NOTES!

* Because the current Hyper-V setting does not "broadcast" the communication between hosts in the same network, we need to enable port mirroring to allow Internal Kali to "see" other's communication. To be specific, you need to put the sniffer (Internal Kali) as the ***mirroring Destination,*** and the target VMs are ***mirroring Source*** (Figure 2). Since each VM has two network adapters, one for regular connection and the other is sharing with the CCIA server. We need to configure port mirroring on the **first** adapter. To be specific,

- Internal Kali: Set Miorroing mode to "***Destination***" in the "Port Mirroiring"
- Ubuntu Kali: Set Miorroing mode to "***Source***" in the "Port Mirroiring"
- External Kali: Set Miorroing mode to "***Source***" in the "Port Mirroiring"

** Since each Windows 10 Host Machine has 20G memory. We need to adjust the assigned Memory for Internal Kali and External Kali from **8192** to **4096** MB to support 4 VM running simultaneously.


Settings for Attacker Kali - External Workstation on CY301-PJIAN001
Attacker Kali - External Workstation
Hardware
Add Hardware
BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
4096 MB

Memory

Specify the amount of memory that this virtual machine can use.

RAM: 4096 MB

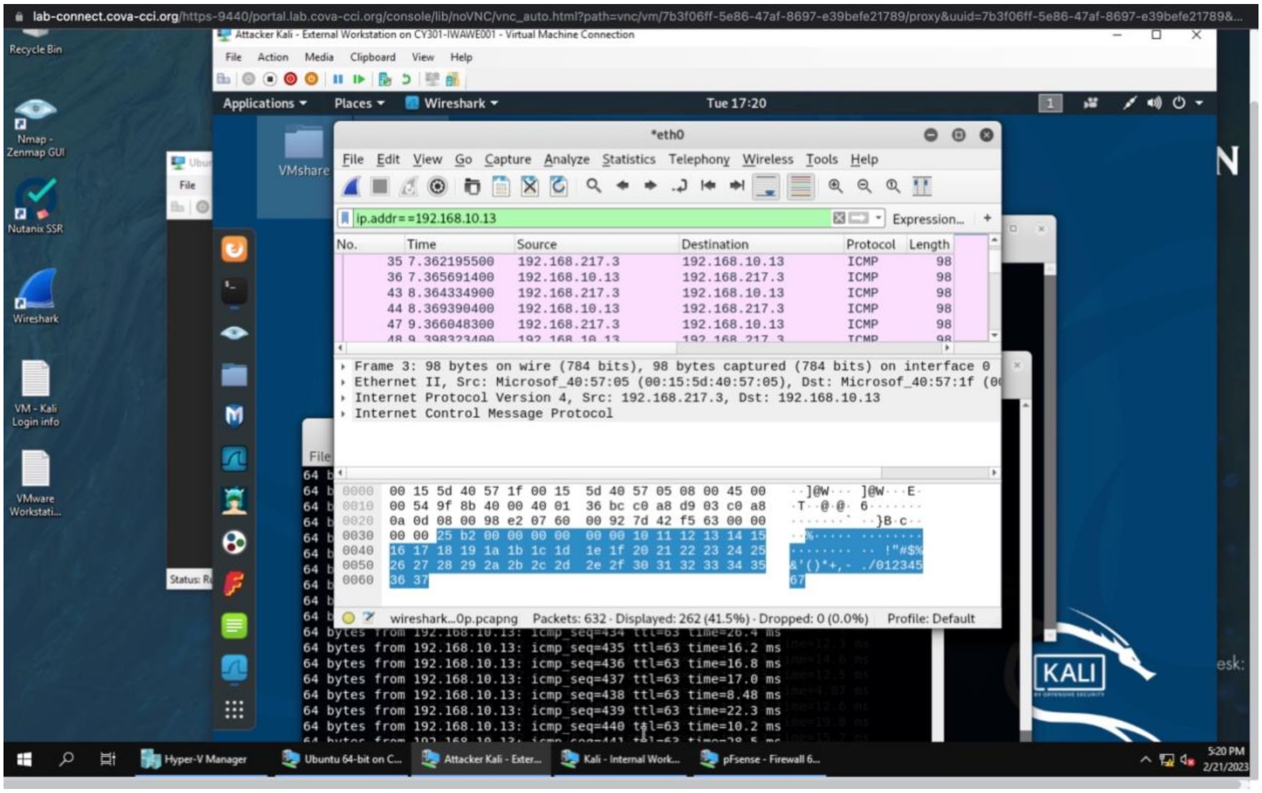
Dynamic Memory

You can allow the amount of memory available to this virtual machine to change dynamically within the range you set.

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

Open two terminals on External Kali VM. Use one ping Ubuntu VM, and use the other ping Internal Kali.

a. Apply proper display or capture filter on **Internal Kali VM** to show active ICMP traffic.



lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC/vnc_auto.html?path=vnc/vm/7b3f06ff-5e86-47af-8697-e39befe21789/proxy&uuid=7b3f06ff-5e86-47af-8697-e39befe21789&...
Attacker Kali - External Workstation on CY301-IWAWE001 - Virtual Machine Connection
Applications
Places
Wireshark
Tue 17:20
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Hyper-V Manager
Ubuntu 64-bit on C...
Attacker Kali - Exter...
Kali - Internal Work...
pFsense - Firewall 6...
5:20 PM
2/21/2023

ip.addr==192.168.10.13

```
No.       Time          Source          Destination     Protocol  Length
       35 7.362195500   192.168.217.3   192.168.10.13   ICMP          98
       36 7.365691400   192.168.10.13   192.168.217.3   ICMP          98
       43 8.364334900   192.168.217.3   192.168.10.13   ICMP          98
       44 8.369390400   192.168.10.13   192.168.217.3   ICMP          98
       47 9.366048300   192.168.217.3   192.168.10.13   ICMP          98
```

```
▸ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:05 (00:15:5d:40:57:05), Dst: Microsof_40:57:1f (00
▸ Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.13
▸ Internet Control Message Protocol
```

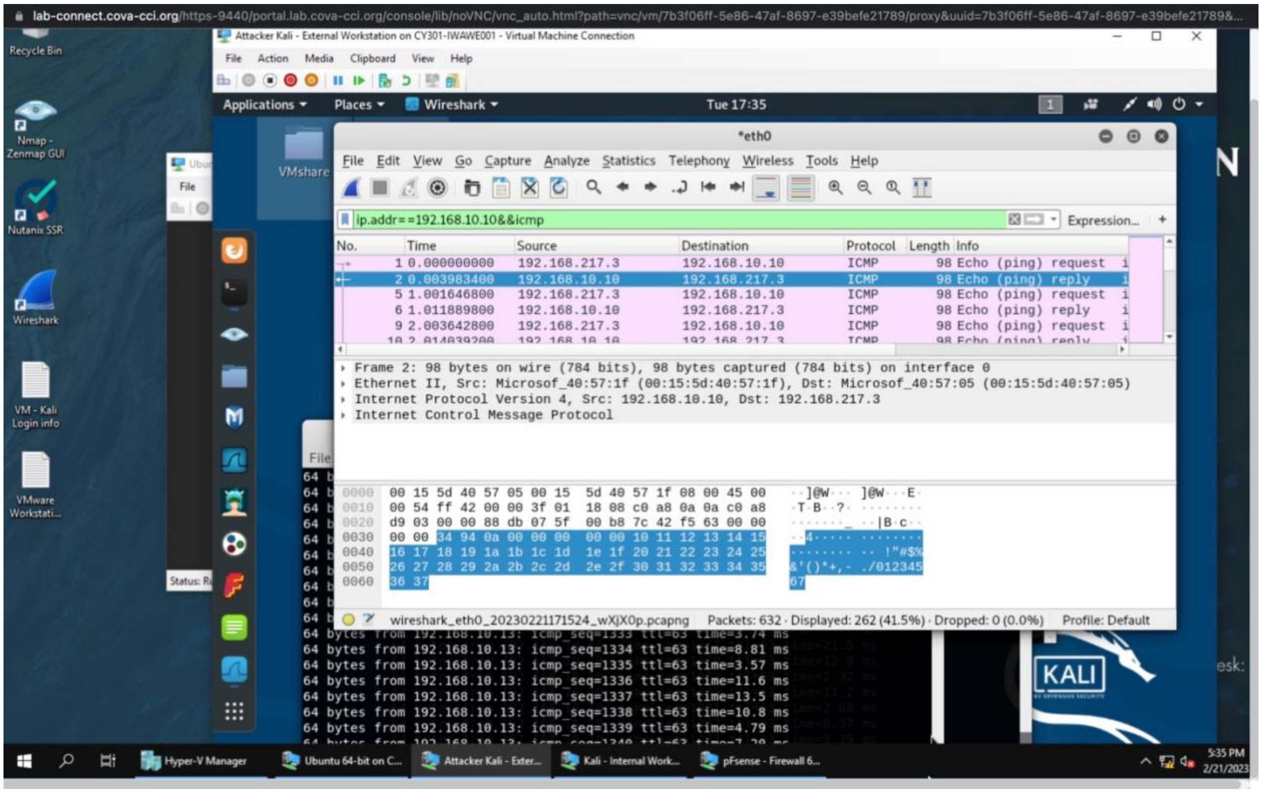
```
0000  00 15 5d 40 57 1f 00 15  5d 40 57 05 08 00 45 00   ··]@W···]@W···E·
0010  00 54 9f 8b 40 00 40 01  36 bc c0 a8 d9 03 c0 a8   ·T··@·@·6·······
0020  0a 0d 08 00 98 e2 07 60  00 92 7d 42 f5 63 00 00   ·······`··}B·c··
0030  00 00 25 b2 00 00 00 00  00 00 10 11 12 13 14 15   ··%·············
0040  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
```

wireshark...0p.pcapng   Packets: 632 · Displayed: 262 (41.5%) · Dropped: 0 (0.0%)   Profile: Default

```
64 bytes from 192.168.10.13: icmp_seq=435 ttl=63 time=16.2 ms
64 bytes from 192.168.10.13: icmp_seq=436 ttl=63 time=16.8 ms
64 bytes from 192.168.10.13: icmp_seq=437 ttl=63 time=17.0 ms
64 bytes from 192.168.10.13: icmp_seq=438 ttl=63 time=8.48 ms
64 bytes from 192.168.10.13: icmp_seq=439 ttl=63 time=22.3 ms
64 bytes from 192.168.10.13: icmp_seq=440 ttl=63 time=10.2 ms
```

I was able to locate the traffic between ubuntu and internal kali. On the display, I used ip.addr==192.168.10.13in order to locate the internal kali VM and to show the ICMP packets within that machine.

b. Apply proper display or capture filter on **Internal Kali VM** that ONLY displays **ICMP request** originated from External Kali VM and goes to Ubuntu 64-bit VM.



lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC/vnc_auto.html?path=vnc/vm/7b3f06ff-5e86-47af-8697-e39befe21789/proxy&uuid=7b3f06ff-5e86-47af-8697-e39befe21789&...
Attacker Kali - External Workstation on CY301-IWAWE001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Tue 17:35
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
VMshare
Hyper-V Manager
Ubuntu 64-bit on C...
Attacker Kali - Exter...
Kali - Internal Work...
pFsense - Firewall 6...
5:35 PM
2/21/2023

ip.addr==192.168.10.10&&icmp

```
No.   Time          Source          Destination     Protocol  Length Info
    1 0.000000000   192.168.217.3   192.168.10.10   ICMP          98 Echo (ping) request  i
    2 0.003983400   192.168.10.10   192.168.217.3   ICMP          98 Echo (ping) reply    i
    5 1.001646800   192.168.217.3   192.168.10.10   ICMP          98 Echo (ping) request  i
    6 1.011889800   192.168.10.10   192.168.217.3   ICMP          98 Echo (ping) reply    i
    9 2.003642800   192.168.217.3   192.168.10.10   ICMP          98 Echo (ping) request  i
   10 2.014039200   192.168.10.10   192.168.217.3   ICMP          98 Echo (ping) reply    i
```

```
› Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
› Ethernet II, Src: Microsof_40:57:1f (00:15:5d:40:57:1f), Dst: Microsof_40:57:05 (00:15:5d:40:57:05)
› Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
› Internet Control Message Protocol
```

```
0000  00 15 5d 40 57 05 00 15  5d 40 57 1f 08 00 45 00   ··]@W···]@W···E·
0010  00 54 ff 42 00 00 3f 01  18 08 c0 a8 0a 0a c0 a8   ·T·B··?·········
0020  d9 03 00 00 88 db 07 5f  00 b8 7c 42 f5 63 00 00   ·······_··|B·c··
0030  00 00 34 94 0a 00 00 00  00 00 10 11 12 13 14 15   ··4·············
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
```

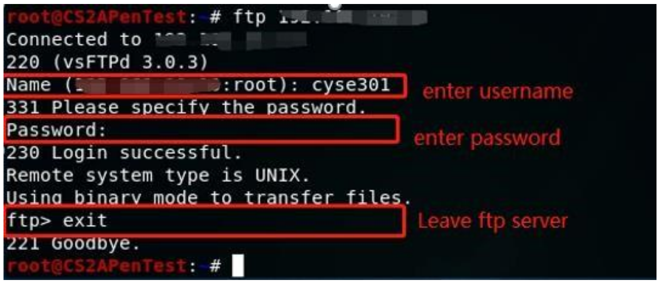
wireshark_eth0_20230221171524_wXjX0p.pcapng   Packets: 632 · Displayed: 262 (41.5%) · Dropped: 0 (0.0%)   Profile: Default

```
64 bytes from 192.168.10.13: icmp_seq=1333 ttl=63 time=3.74 ms
64 bytes from 192.168.10.13: icmp_seq=1334 ttl=63 time=8.81 ms
64 bytes from 192.168.10.13: icmp_seq=1335 ttl=63 time=3.57 ms
64 bytes from 192.168.10.13: icmp_seq=1336 ttl=63 time=11.6 ms
64 bytes from 192.168.10.13: icmp_seq=1337 ttl=63 time=13.5 ms
64 bytes from 192.168.10.13: icmp_seq=1338 ttl=63 time=10.8 ms
64 bytes from 192.168.10.13: icmp_seq=1339 ttl=63 time=4.79 ms
64 bytes from 192.168.10.13: icmp_seq=1340 ttl=63 time=7.20 ms
```

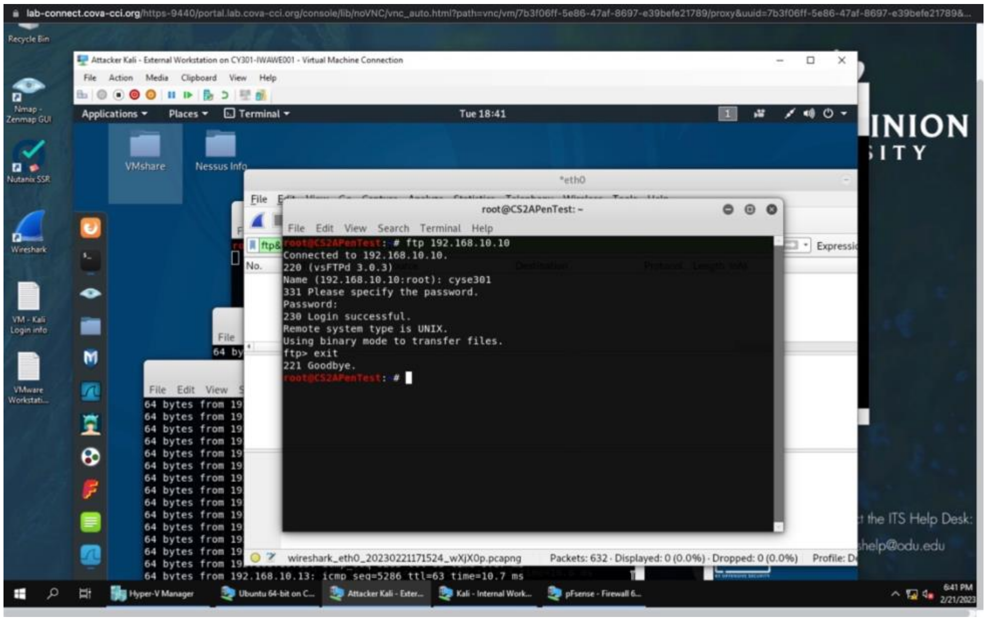
Using the formula “ip.addr==192.168.10.10&&icmp” I was able to locate ICMP requests and replies that originated from the external kali VM and go to Ubuntu 64-bit VM.

2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

a. **Ubuntu VM** 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 ubuntu VM]*. The username for the FTP server is **cyse301**, and the password is **password**. You can follow the steps below to access the FTP server.



```
root@CS2APenTest:~# ftp [redacted]
Connected to [redacted]
220 (vsFTPd 3.0.3)
Name ([redacted]:root): cyse301
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
root@CS2APenTest:~#
```

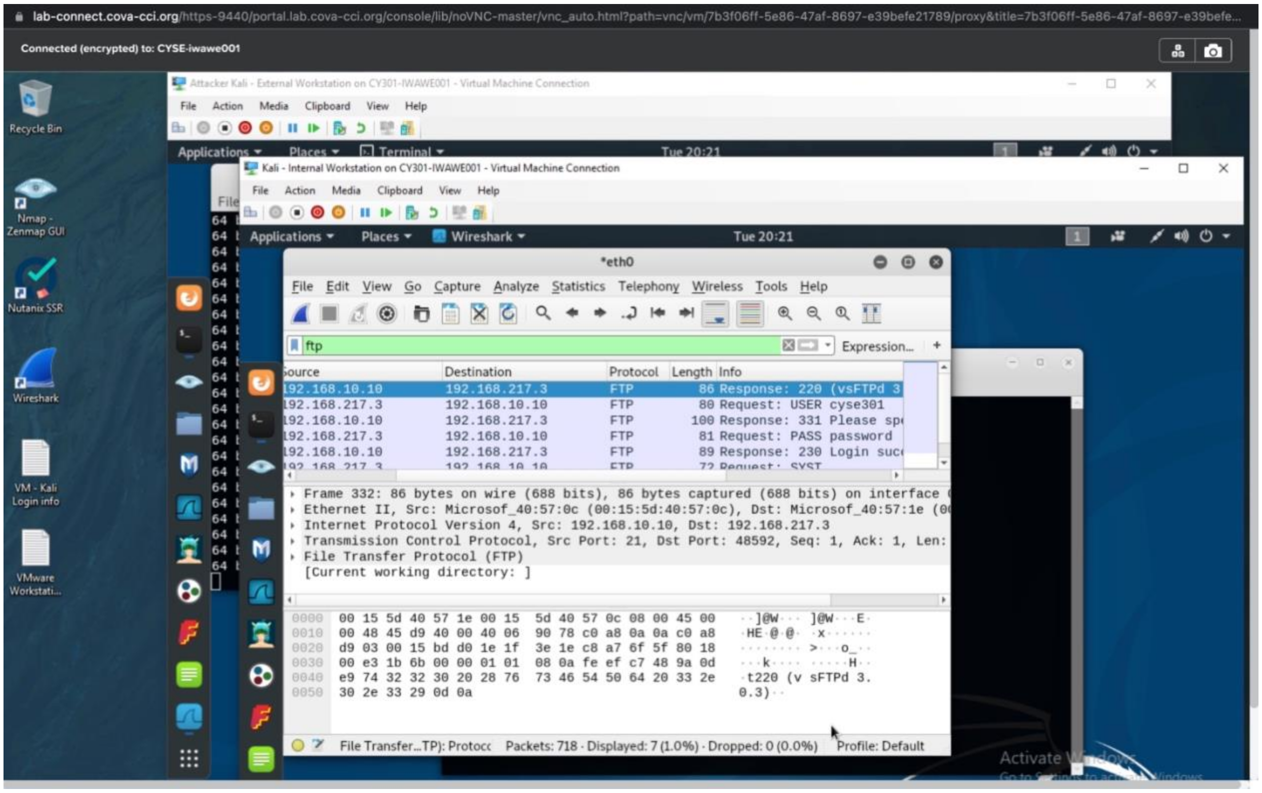


```
root@CS2APenTest:~# ftp 192.168.10.10
Connected to 192.168.10.10.
220 (vsFTPd 3.0.3)
Name (192.168.10.10:root): cyse301
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
root@CS2APenTest:~# 
```

```
64 bytes from 192.168.10.13: icmp_seq=5286 ttl=63 time=10.7 ms
```

wireshark_eth0_20230221171524_wXjX0p.pcapng Packets: 632 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%)

b. **Unfortunately**, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the **password** used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot and explain how you find the password.



```
Source          Destination     Protocol Length Info
192.168.10.10   192.168.217.3   FTP          86 Response: 220 (vsFTPd 3
192.168.217.3   192.168.10.10   FTP          80 Request: USER cyse301
192.168.10.10   192.168.217.3   FTP         100 Response: 331 Please sp
192.168.217.3   192.168.10.10   FTP          81 Request: PASS password
192.168.10.10   192.168.217.3   FTP          89 Response: 230 Login suc
192.168.217.3   192.168.10.10   FTP          72 Request: SYST
```

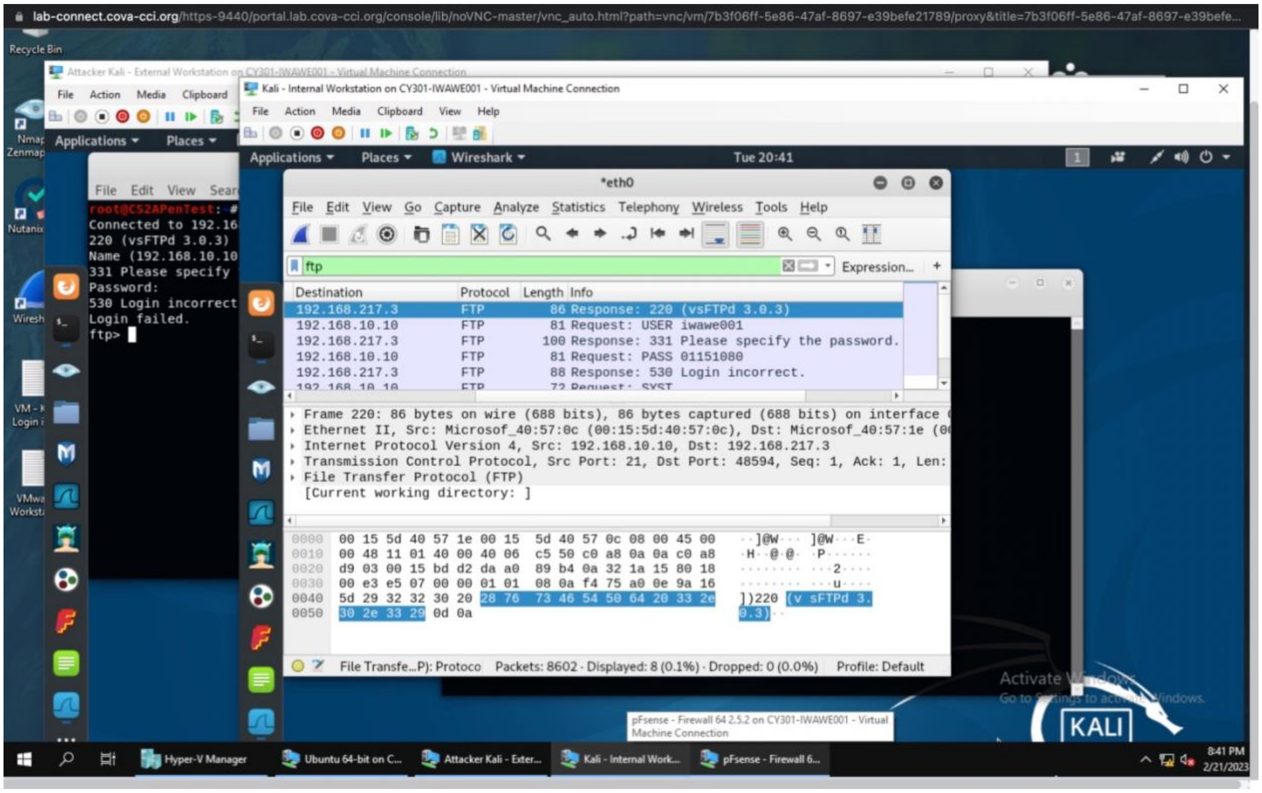
```
› Frame 332: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface
› Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (0
› Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
› Transmission Control Protocol, Src Port: 21, Dst Port: 48592, Seq: 1, Ack: 1, Len:
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 15 5d 40 57 1e 00 15  5d 40 57 0c 08 00 45 00   ··]@W···]@W···E·
0010  00 48 45 d9 40 00 40 06  90 78 c0 a8 0a 0a c0 a8   ·HE·@·@··x······
0020  d9 03 00 15 bd d0 1e 1f  3e 1e c8 a7 6f 5f 80 18   ········>···o_··
0030  00 e3 1b 6b 00 00 01 01  08 0a fe ef c7 48 9a 0d   ···k·········H··
0040  e9 74 32 32 30 20 28 76  73 46 54 50 64 20 33 2e   ·t220 (v sFTPd 3.
0050  30 2e 33 29 0d 0a                                  0.3)··
```

File Transfer…TP): Protocc Packets: 718 · Displayed: 7 (1.0%) · Dropped: 0 (0.0%) Profile: Default

I first made sure my machines were running and packets were flowing in from all three. On the External Linux, I was able to log in and then I exited it. Using the internal kali, I went on Wireshark, and I was reading the packets that were flowing in from the other machines. Using FTP, I was able to identify the username and password I used on the external kali. At first, I wasn't able to see anything when I typed in the display, but after changing my setting in the virtual machines and starting the procedure over from the beginning, I was able to get a reading on where the password and username were located.

c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), 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 **Internal Kali**.



lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC-master/vnc_auto.html?path=vnc/vm/7b3f06ff-5e86-47af-8697-e39befe21789/proxy&title=7b3f06ff-5e86-47af-8697-e39befe...
Recycle Bin
Attacker Kali - External Workstation on CY301-IWAWE001 - Virtual Machine Connection
Kali - Internal Workstation on CY301-IWAWE001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Tue 20:41
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Hyper-V Manager
Ubuntu 64-bit on C...
Attacker Kali - Exter...
Kali - Internal Work...
pFsense - Firewall 6...
pFsense - Firewall 64 2.5.2 on CY301-IWAWE001 - Virtual Machine Connection
Activate Windows
Go to Settings to activate Windows.
KALI
8:41 PM
2/21/2023

```
root@CS2APenTest:~#
Connected to 192.16
220 (vsFTPd 3.0.3)
Name (192.168.10.10
331 Please specify
Password:
530 Login incorrect
Login failed.
ftp>
```

Filter: ftp

```
Destination        Protocol  Length Info
192.168.217.3      FTP           86 Response: 220 (vsFTPd 3.0.3)
192.168.10.10      FTP           81 Request: USER iwawe001
192.168.217.3      FTP          100 Response: 331 Please specify the password.
192.168.10.10      FTP           81 Request: PASS 01151080
192.168.217.3      FTP           88 Response: 530 Login incorrect.
192.168.10.10      FTP           72 Request: SYST
```

```
▸ Frame 220: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface
▸ Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (0
▸ Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 48594, Seq: 1, Ack: 1, Len:
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 15 5d 40 57 1e 00 15  5d 40 57 0c 08 00 45 00   ··]@W···]@W···E·
0010  00 48 11 01 40 00 40 06  c5 50 c0 a8 0a 0a c0 a8   ·H··@·@··P······
0020  d9 03 00 15 bd d2 da a0  89 b4 0a 32 1a 15 80 18   ···········2····
0030  00 e3 e5 07 00 00 01 01  08 0a f4 75 a0 0e 9a 16   ···········u····
0040  5d 29 32 32 30 20 28 76  73 46 54 50 64 20 33 2e   ])220 (v sFTPd 3.
0050  30 2e 33 29 0d 0a                                  0.3)··
```

File Transfe...P): Protoco   Packets: 8602 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%)   Profile: Default

After repeating the same set as number two I was able to locate my MIDAS ID as the username and my UIN as the password.