OLD DOMINION UNIVERSITY

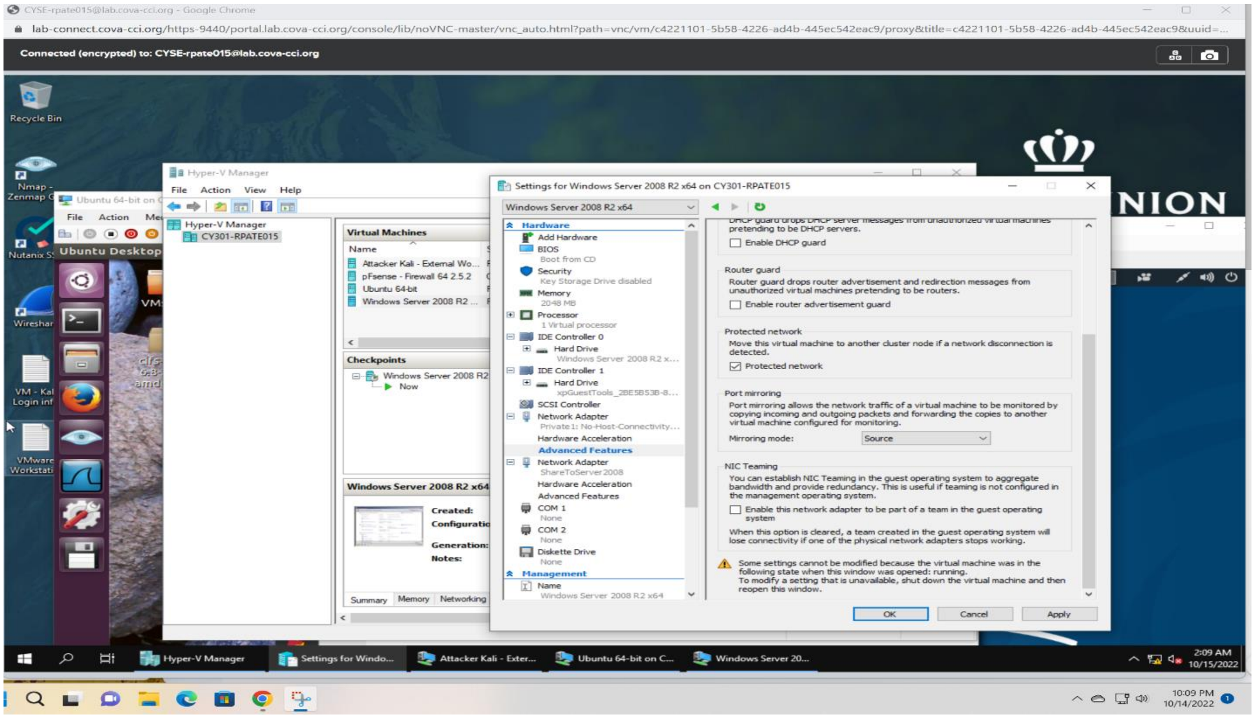
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Analysis

Rahil Patel

01208235

Task A: Sniff LAN traffic



Connected (encrypted) to: CYSE-rpate015@lab.cova-cci.org

Settings for Windows Server 2008 R2 x64 on CY301-RPATE015

Windows Server 2008 R2 x64

Hardware
- Add Hardware
- BIOS: Boot from CD
- Security: Key Storage Drive disabled
- Memory: 2048 MB
- Processor: 1 Virtual processor
- IDE Controller 0
  - Hard Drive: Windows Server 2008 R2 x...
- IDE Controller 1
  - Hard Drive: xpGuestTools_2BE5B53B-8...
- SCSI Controller
- Network Adapter: Private1: No-Host-Connectivity...
  - Hardware Acceleration
  - Advanced Features
- Network Adapter: ShareToServer2008
  - Hardware Acceleration
  - Advanced Features
- COM 1: None
- COM 2: None
- Diskette Drive: None

Management
- Name: Windows Server 2008 R2 x64

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

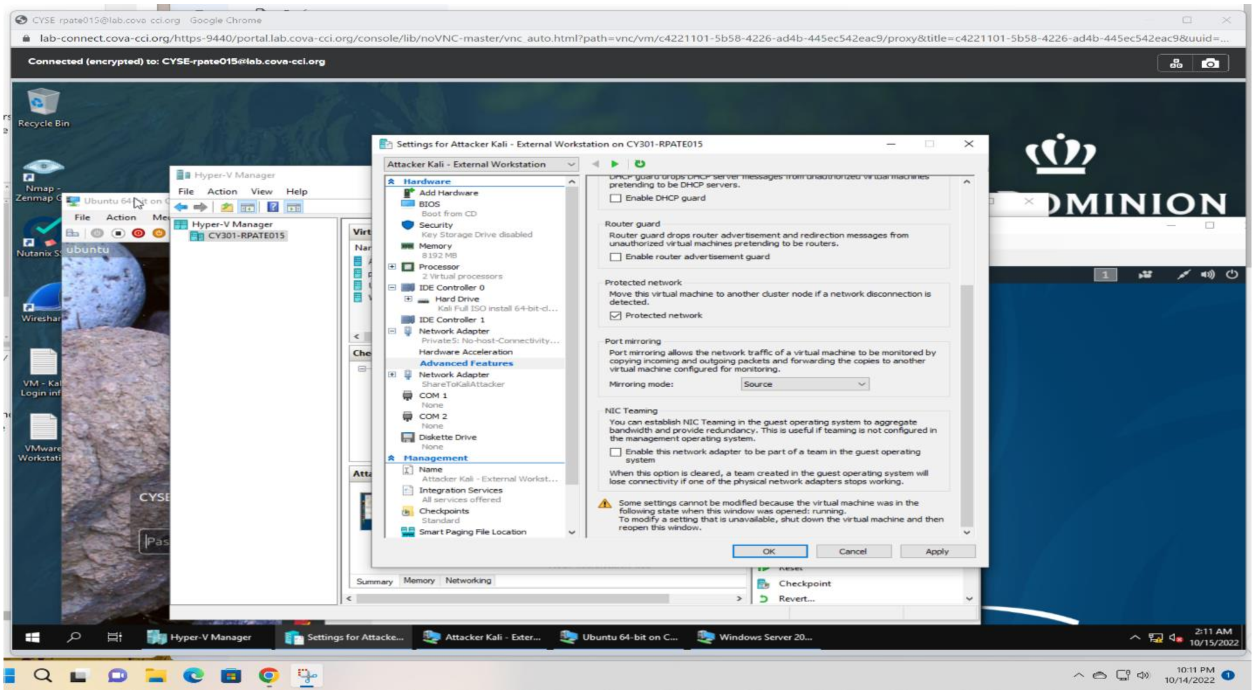
NIC Teaming

You can establish NIC Teaming in the guest operating system to aggregate bandwidth and provide redundancy. This is useful if teaming is not configured in the management operating system.

□ Enable this network adapter to be part of a team in the guest operating system

When this option is cleared, a team created in the guest operating system will lose connectivity if one of the physical network adapters stops working.

⚠ Some settings cannot be modified because the virtual machine was in the following state when this window was opened: running.
To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.



Connected (encrypted) to: CYSE-rpate015@lab.cova-cci.org

Settings for Attacker Kali - External Workstation on CY301-RPATE015

Attacker Kali - External Workstation

Hardware
- Add Hardware
- BIOS: Boot from CD
- Security: Key Storage Drive disabled
- Memory: 8192 MB
- Processor: 2 Virtual processors
- IDE Controller 0
  - Hard Drive: Kali Full ISO install 64-bit-d...
- IDE Controller 1
- Network Adapter: Private5: No-host-Connectivity...
  - Hardware Acceleration
  - Advanced Features
- Network Adapter: ShareToKaliAttacker
- COM 1: None
- COM 2: None
- Diskette Drive: None

Management
- Name: Attacker Kali - External Workst...
- Integration Services: All services offered
- Checkpoints: Standard
- Smart Paging File Location

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

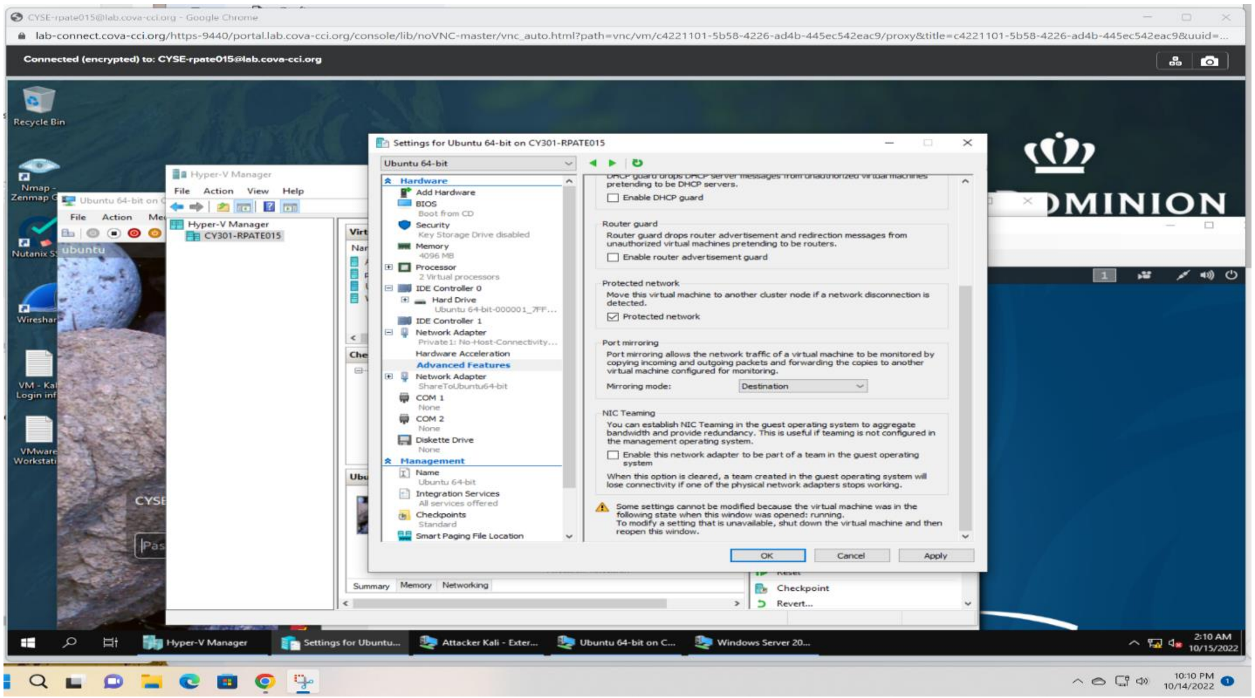
NIC Teaming

You can establish NIC Teaming in the guest operating system to aggregate bandwidth and provide redundancy. This is useful if teaming is not configured in the management operating system.

□ Enable this network adapter to be part of a team in the guest operating system

When this option is cleared, a team created in the guest operating system will lose connectivity if one of the physical network adapters stops working.

⚠ Some settings cannot be modified because the virtual machine was in the following state when this window was opened: running.
To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.



Settings for Ubuntu 64-bit on CY301-RPATE015

Ubuntu 64-bit

Hardware
- Add Hardware
- BIOS: Boot from CD
- Security: Key Storage Drive disabled
- Memory: 4096 MB
- Processor: 2 Virtual processors
- IDE Controller 0
  - Hard Drive: Ubuntu 64-bit-000001_7FF...
- IDE Controller 1
- Network Adapter: Private1: No-Host-Connectivity...
  - Hardware Acceleration
  - Advanced Features
- Network Adapter: ShareToUbuntu64-bit
- COM 1: None
- COM 2: None
- Diskette Drive: None

Management
- Name: Ubuntu 64-bit
- Integration Services: All services offered
- Checkpoints: Standard
- Smart Paging File Location

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: Destination

NIC Teaming

You can establish NIC Teaming in the guest operating system to aggregate bandwidth and provide redundancy. This is useful if teaming is not configured in the management operating system.

□ Enable this network adapter to be part of a team in the guest operating system

When this option is cleared, a team created in the guest operating system will lose connectivity if one of the physical network adapters stops working.

⚠ Some settings cannot be modified because the virtual machine was in the following state when this window was opened: running.
To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.

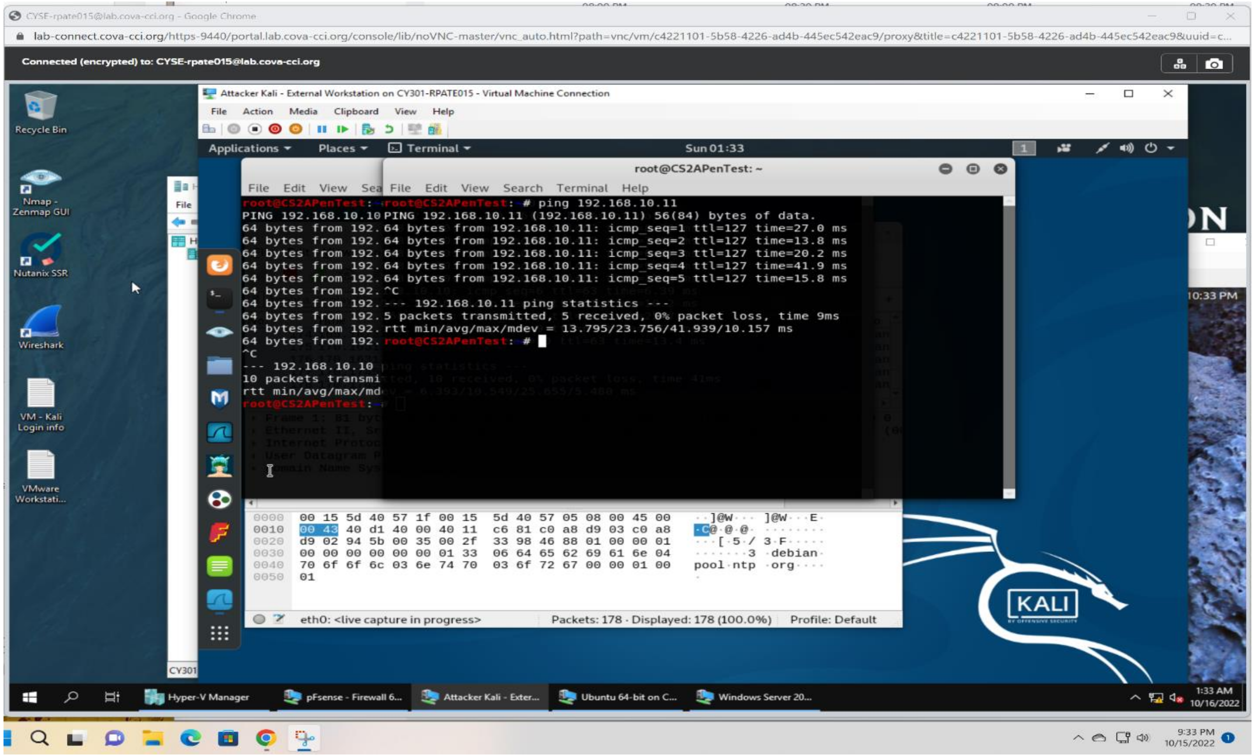
OK Cancel Apply

Description:

In this step, I have performed the mirroring actions that can sniff the local area network traffic. This activity was to sniff the traffic between two peers silently.

Sniff ICMP traffic (10 + 10 +20 points)

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



Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection

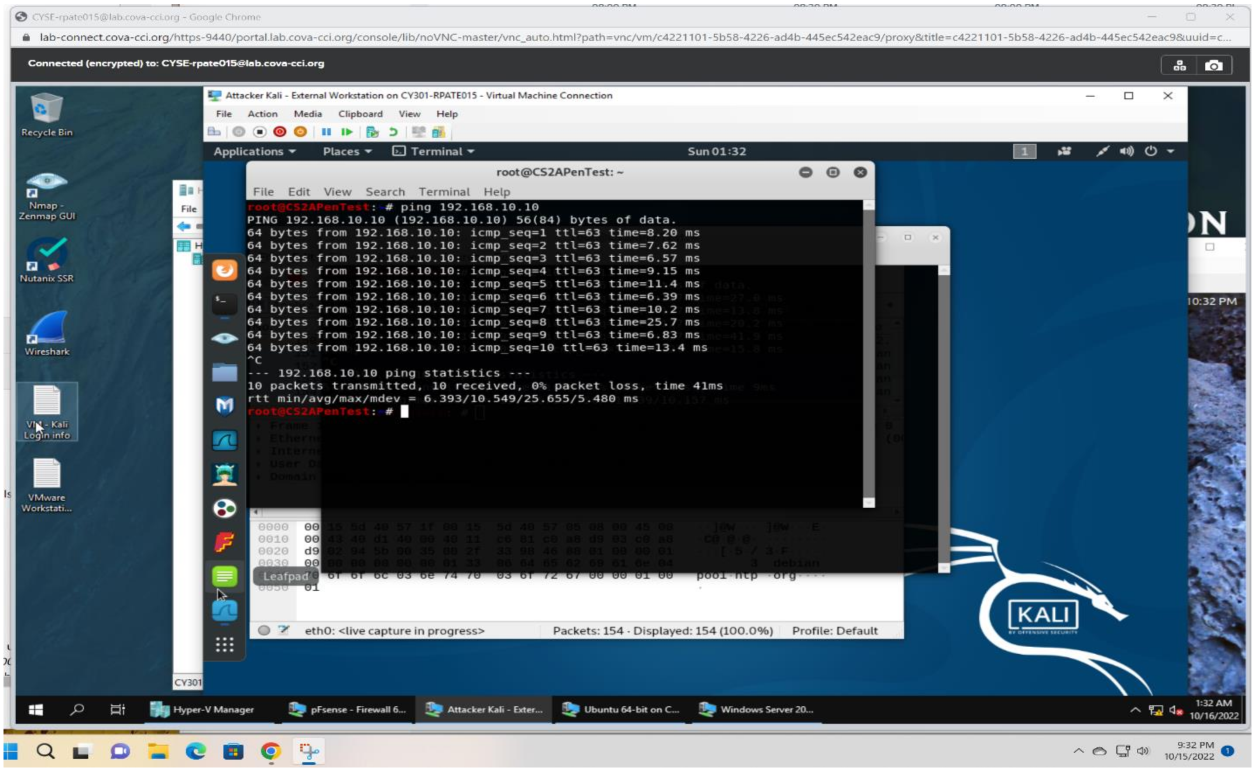
```
root@CS2APenTest: ~root@CS2APenTest:~# ping 192.168.10.11
PING 192.168.10.10PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
64 bytes from 192.64 bytes from 192.168.10.11: icmp_seq=1 ttl=127 time=27.0 ms
64 bytes from 192.64 bytes from 192.168.10.11: icmp_seq=2 ttl=127 time=13.8 ms
64 bytes from 192.64 bytes from 192.168.10.11: icmp_seq=3 ttl=127 time=20.2 ms
64 bytes from 192.64 bytes from 192.168.10.11: icmp_seq=4 ttl=127 time=41.9 ms
64 bytes from 192.64 bytes from 192.168.10.11: icmp_seq=5 ttl=127 time=15.8 ms
64 bytes from 192.^C
64 bytes from 192.--- 192.168.10.11 ping statistics ---
64 bytes from 192.5 packets transmitted, 5 received, 0% packet loss, time 9ms
64 bytes from 192.rtt min/avg/max/mdev = 13.795/23.756/41.939/10.157 ms
64 bytes from 192.root@CS2APenTest:~# 
^C
--- 192.168.10.10
10 packets transmi
rtt min/avg/max/md
root@CS2APenTest:~
```

```
0000  00 15 5d 40 57 1f 00 15  5d 40 57 05 08 00 45 00   ··]@W···]@W···E·
0010  00 43 40 d1 40 00 40 11  c6 81 c0 a8 d9 03 c0 a8   ·C@·@·@·········
0020  d9 02 94 5b 00 35 00 2f  33 98 46 88 01 00 00 01   ···[·5·/3·F·····
0030  00 00 00 00 00 00 01 33  06 64 65 62 69 61 6e 04   ·······3·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 01 00   pool·ntp·org····
0050  01                                                 ·
```

eth0: <live capture in progress>

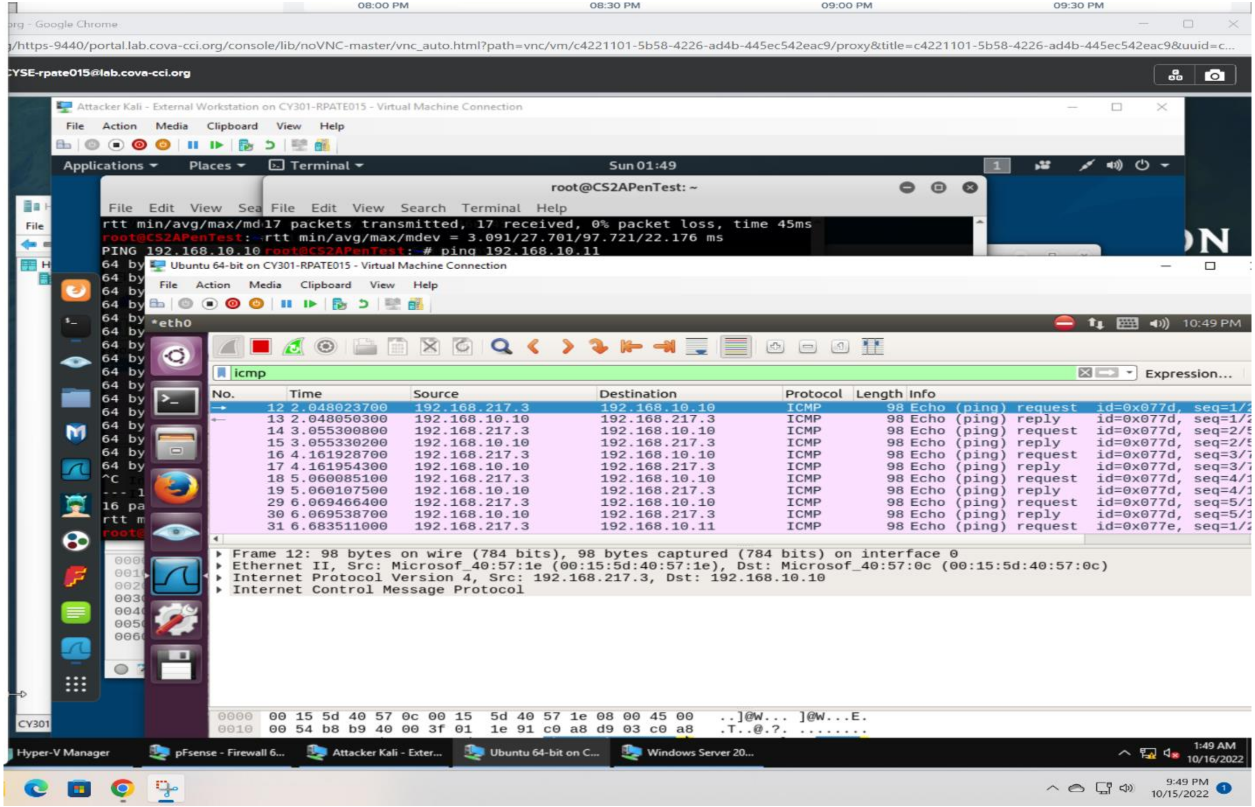
Packets: 178 · Displayed: 178 (100.0%)

Profile: Default


CYSE-rpate015@lab.cova-cci.org - Google Chrome
lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC-master/vnc_auto.html?path=vnc/vm/c4221101-5b58-4226-ad4b-445ec542eac9/proxy&title=c4221101-5b58-4226-ad4b-445ec542eac9&uuid=c...
Connected (encrypted) to: CYSE-rpate015@lab.cova-cci.org
Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 01:32
root@CS2APenTest: ~
File Edit View Search Terminal Help
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Leafpad
eth0: <live capture in progress>
Packets: 154 · Displayed: 154 (100.0%)
Profile: Default
KALI
Hyper-V Manager
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on C...
Windows Server 20...
1:32 AM
10/16/2022
9:32 PM
10/15/2022

```
root@CS2APenTest:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
64 bytes from 192.168.10.10: icmp_seq=1 ttl=63 time=8.20 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=7.62 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=6.57 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=9.15 ms
64 bytes from 192.168.10.10: icmp_seq=5 ttl=63 time=11.4 ms
64 bytes from 192.168.10.10: icmp_seq=6 ttl=63 time=6.39 ms
64 bytes from 192.168.10.10: icmp_seq=7 ttl=63 time=10.2 ms
64 bytes from 192.168.10.10: icmp_seq=8 ttl=63 time=25.7 ms
64 bytes from 192.168.10.10: icmp_seq=9 ttl=63 time=6.83 ms
64 bytes from 192.168.10.10: icmp_seq=10 ttl=63 time=13.4 ms
^C
--- 192.168.10.10 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 41ms
rtt min/avg/max/mdev = 6.393/10.549/25.655/5.480 ms
root@CS2APenTest:~# 
```

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).


08:00 PM
08:30 PM
09:00 PM
09:30 PM
Google Chrome
/https-9440/portal.lab.cova-cci.org/console/lib/noVNC-master/vnc_auto.html?path=vnc/vm/c4221101-5b58-4226-ad4b-445ec542eac9/proxy&title=c4221101-5b58-4226-ad4b-445ec542eac9&uuid=c...
CYSE-rpate015@lab.cova-cci.org
Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 01:49
root@CS2APenTest: ~
File Edit View Search Terminal Help
Ubuntu 64-bit on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
*eth0
10:49 PM
Expression...
Hyper-V Manager
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on C...
Windows Server 20...
1:49 AM
10/16/2022
9:49 PM
10/15/2022

```
rtt min/avg/max/md17 packets transmitted, 17 received, 0% packet loss, time 45ms
root@CS2APenTest:~rtt min/avg/max/mdev = 3.091/27.701/97.721/22.176 ms
PING 192.168.10.10 root@CS2APenTest:~# ping 192.168.10.11
```

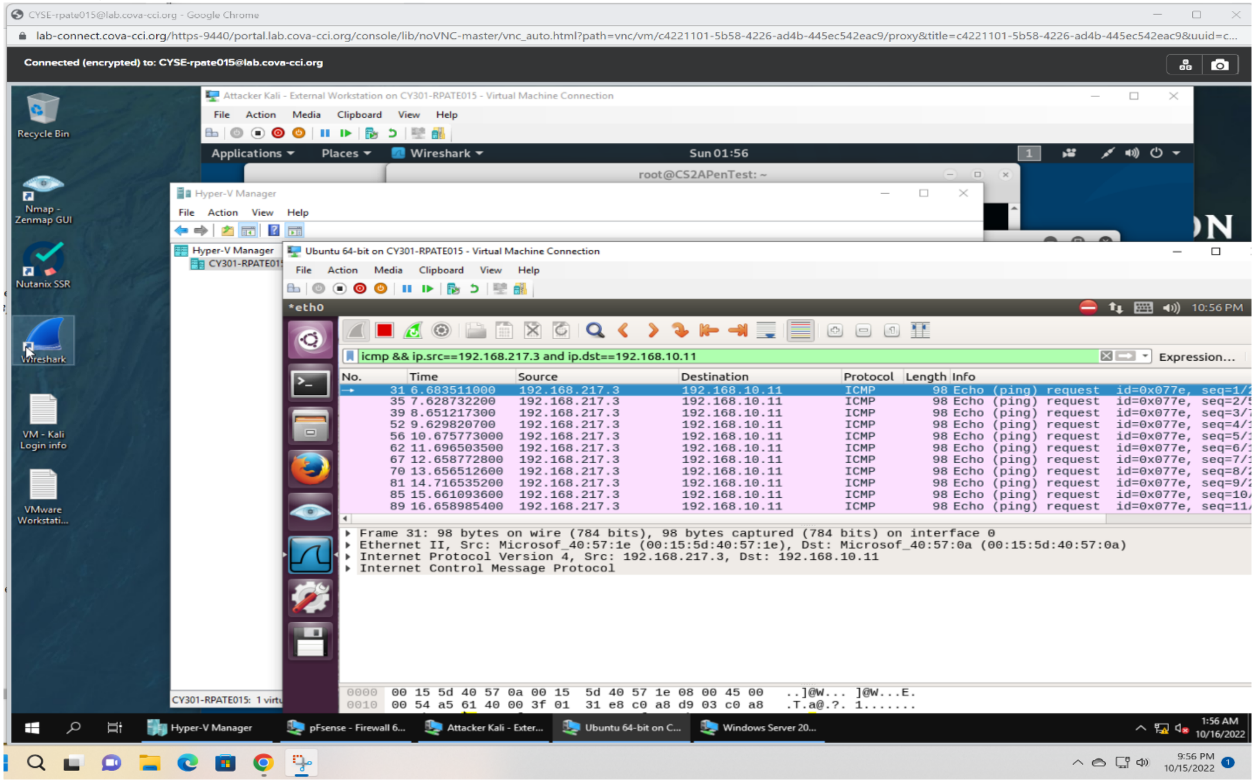
icmp

```
No.   Time          Source           Destination      Protocol Length Info
   12 2.048023700   192.168.217.3    192.168.10.10    ICMP       98 Echo (ping) request  id=0x077d, seq=1/2
   13 2.048050300   192.168.10.10    192.168.217.3    ICMP       98 Echo (ping) reply    id=0x077d, seq=1/2
   14 3.055300800   192.168.217.3    192.168.10.10    ICMP       98 Echo (ping) request  id=0x077d, seq=2/5
   15 3.055330200   192.168.10.10    192.168.217.3    ICMP       98 Echo (ping) reply    id=0x077d, seq=2/5
   16 4.161928700   192.168.217.3    192.168.10.10    ICMP       98 Echo (ping) request  id=0x077d, seq=3/7
   17 4.161954300   192.168.10.10    192.168.217.3    ICMP       98 Echo (ping) reply    id=0x077d, seq=3/7
   18 5.060085100   192.168.217.3    192.168.10.10    ICMP       98 Echo (ping) request  id=0x077d, seq=4/1
   19 5.060107500   192.168.10.10    192.168.217.3    ICMP       98 Echo (ping) reply    id=0x077d, seq=4/1
   29 6.069466400   192.168.217.3    192.168.10.10    ICMP       98 Echo (ping) request  id=0x077d, seq=5/1
   30 6.069538700   192.168.10.10    192.168.217.3    ICMP       98 Echo (ping) reply    id=0x077d, seq=5/1
   31 6.683511000   192.168.217.3    192.168.10.11    ICMP       98 Echo (ping) request  id=0x077e, seq=1/2
```

```
▸ Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:1e (00:15:5d:40:57:1e), Dst: Microsof_40:57:0c (00:15:5d:40:57:0c)
▸ Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.10
▸ Internet Control Message Protocol
```

```
0000  00 15 5d 40 57 0c 00 15  5d 40 57 1e 08 00 45 00   ..]@W... ]@W...E.
0010  00 54 b8 b9 40 00 3f 01  1e 91 c0 a8 d9 03 c0 a8   .T..@.?. ........
```

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).

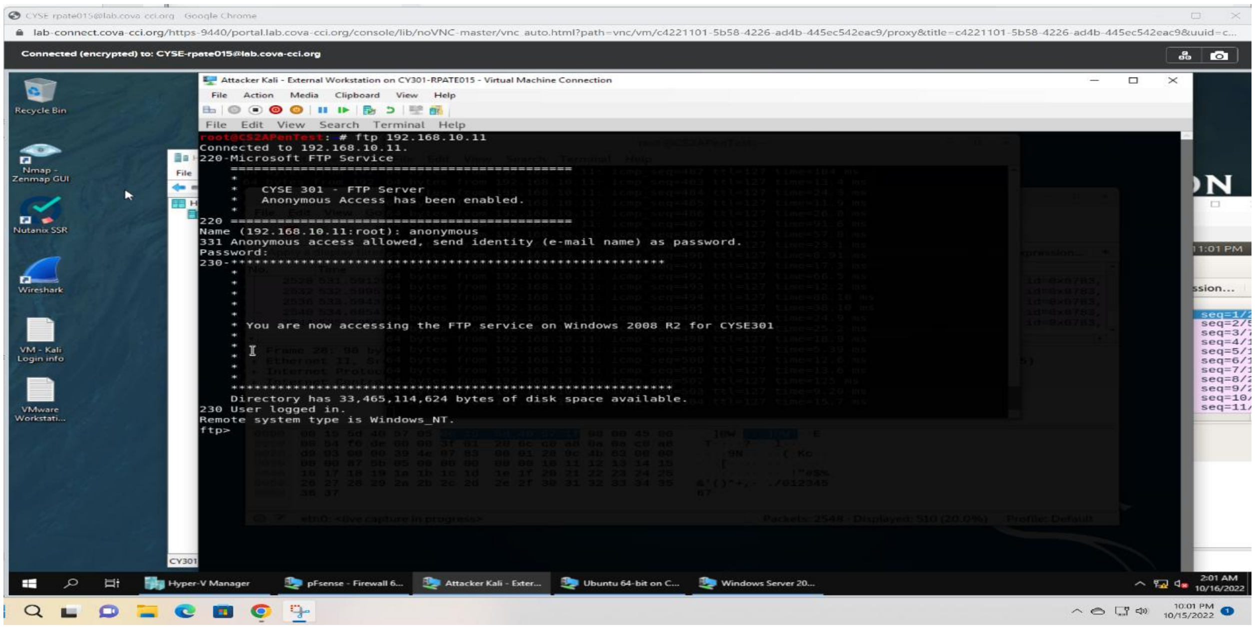

CYSE-rpate015@lab.cova-cci.org - Google Chrome
lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC-master/vnc_auto.html?path=vnc/vm/c4221101-5b58-4226-ad4b-445ec542eac9/proxy&title=c4221101-5b58-4226-ad4b-445ec542eac9&uuid=c...
Connected (encrypted) to: CYSE-rpate015@lab.cova-cci.org
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Sun 01:56
root@CS2APenTest: ~
Hyper-V Manager
File Action View Help
Hyper-V Manager
CY301-RPATE015
Ubuntu 64-bit on CY301-RPATE015 - Virtual Machine Connection
File Action Media Clipboard View Help
*eth0
10:56 PM
Expression...
CY301-RPATE015: 1 virtu
Hyper-V Manager
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on C...
Windows Server 20...
1:56 AM
10/16/2022
9:56 PM
10/15/2022

```
icmp && ip.src==192.168.217.3 and ip.dst==192.168.10.11
```

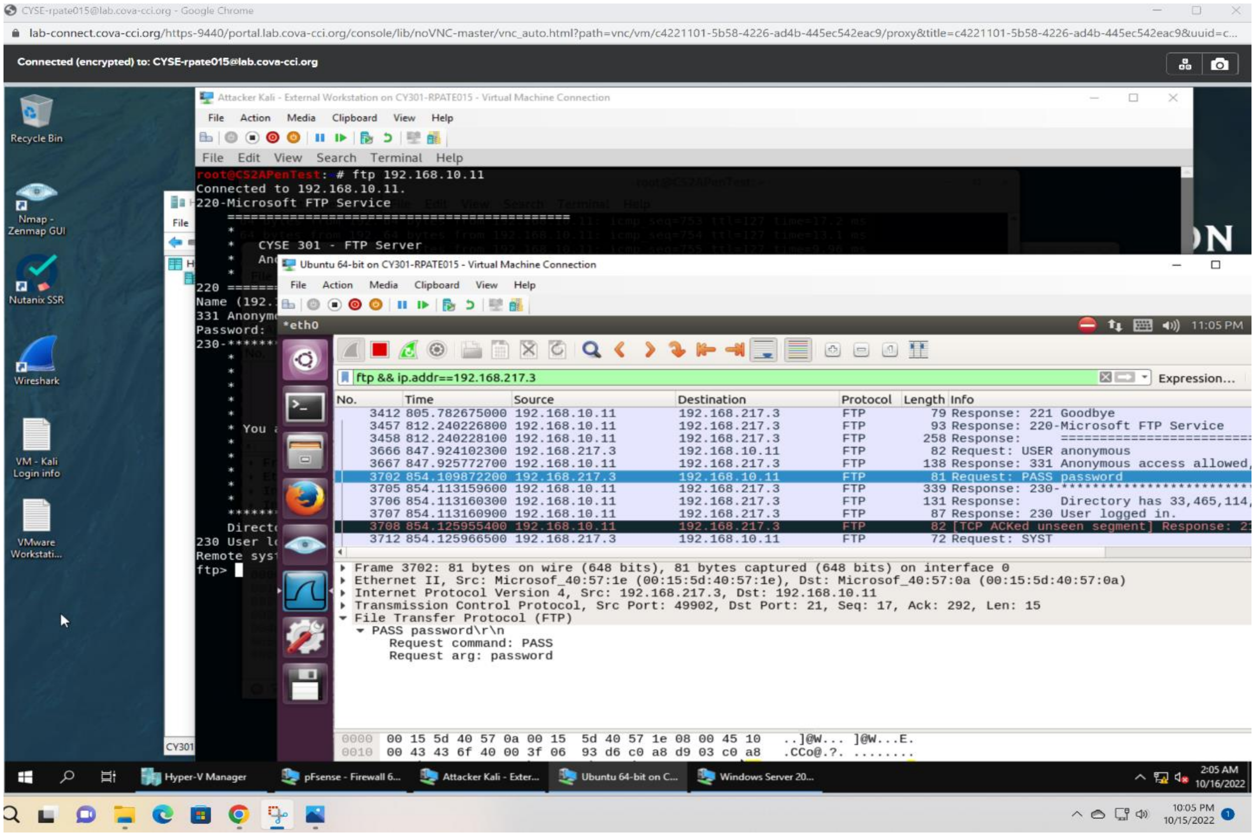
```
No.   Time          Source          Destination     Protocol Length Info
   31 6.683511000   192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=1/
   35 7.628732200   192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=2/
   39 8.651217300   192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=3/
   52 9.629820700   192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=4/
   56 10.675773000  192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=5/
   62 11.696503500  192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=6/
   67 12.658772800  192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=7/
   70 13.656512600  192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=8/
   81 14.716535200  192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=9/
   85 15.661093600  192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=10/
   89 16.658985400  192.168.217.3   192.168.10.11   ICMP       98 Echo (ping) request  id=0x077e, seq=11/

▸ Frame 31: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:1e (00:15:5d:40:57:1e), Dst: Microsof_40:57:0a (00:15:5d:40:57:0a)
▸ Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.11
▸ Internet Control Message Protocol

0000  00 15 5d 40 57 0a 00 15  5d 40 57 1e 08 00 45 00   ..]@W... ]@W...E.
0010  00 54 a5 61 40 00 3f 01  31 e8 c0 a8 d9 03 c0 a8   .T.a@.?. 1.......
```

Description:
In this step, the initial process was to generate the ICMP traffic by using the external kali. The traffic examined in the Wireshark for Ubuntu and Server 2008 with ICMP filtration. Now, the limited filter applied to keep the traffic from Kali Linux to Server 2008.

Sniff FTP traffic (60 points)

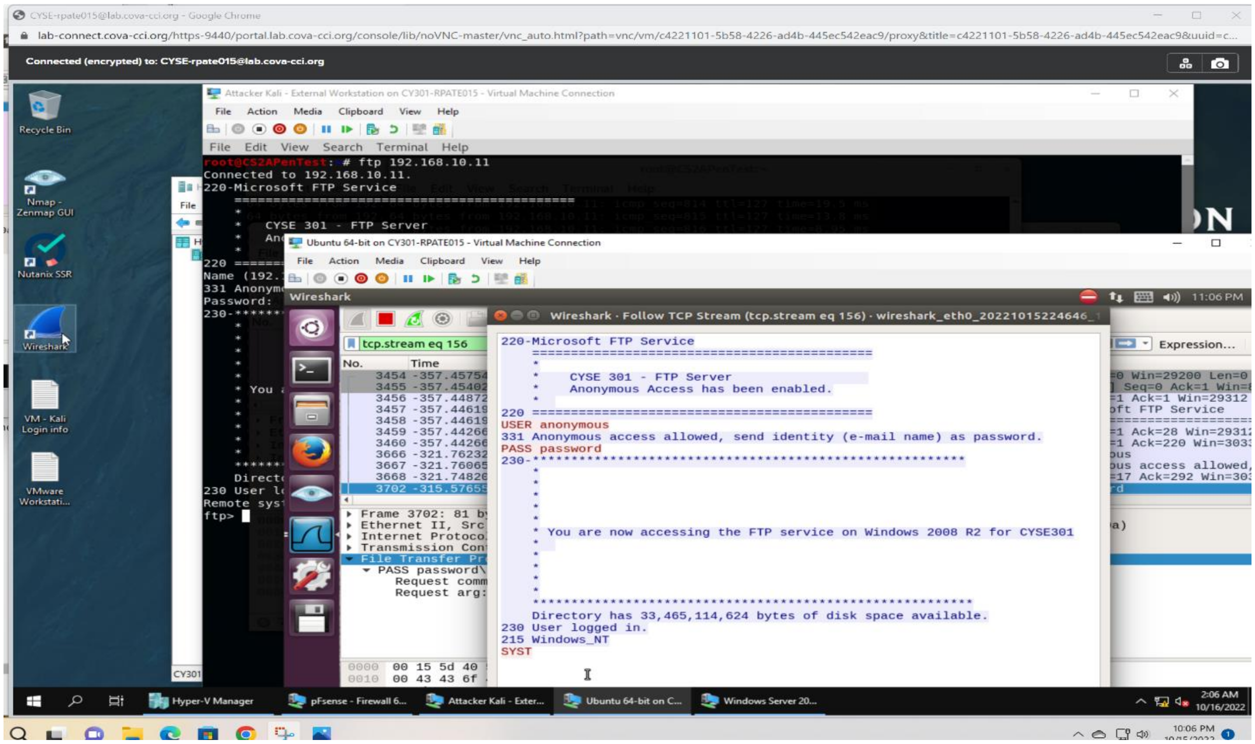


```
root@CS2APenTest: # ftp 192.168.10.11
Connected to 192.168.10.11.
220-Microsoft FTP Service
    ============================================
    *
    *   CYSE 301 - FTP Server
    *   Anonymous Access has been enabled.
    *
220 ============================================
Name (192.168.10.11:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-*********************************************************
    *
    *
    *
    *
    *
    * You are now accessing the FTP service on Windows 2008 R2 for CYSE301
    *
    *
    *
    *
    *
    *********************************************************
    Directory has 33,465,114,624 bytes of disk space available.
230 User logged in.
Remote system type is Windows_NT.
ftp>
```



```
root@CS2APenTest: # ftp 192.168.10.11
Connected to 192.168.10.11.
220-Microsoft FTP Service
    ============================================
    *
    *   CYSE 301 - FTP Server
    *   An
220 ======
Name (192.
331 Anonym
Password:
230-******
    * You a
    Direct
230 User l
Remote sys
ftp>
```

```
ftp && ip.addr==192.168.217.3

No.  Time          Source          Destination     Protocol Length Info
3412 805.782675000 192.168.10.11   192.168.217.3   FTP       79 Response: 221 Goodbye
3457 812.240226800 192.168.10.11   192.168.217.3   FTP       93 Response: 220-Microsoft FTP Service
3458 812.240228100 192.168.10.11   192.168.217.3   FTP      258 Response:     ========================
3666 847.924102300 192.168.217.3   192.168.10.11   FTP       82 Request: USER anonymous
3667 847.925772700 192.168.10.11   192.168.217.3   FTP      138 Response: 331 Anonymous access allowed,
3702 854.109872200 192.168.217.3   192.168.10.11   FTP       81 Request: PASS password
3705 854.113159600 192.168.10.11   192.168.217.3   FTP      339 Response: 230-***********************
3706 854.113160300 192.168.10.11   192.168.217.3   FTP      131 Response:     Directory has 33,465,114,
3707 854.113160900 192.168.10.11   192.168.217.3   FTP       87 Response: 230 User logged in.
3708 854.125955400 192.168.10.11   192.168.217.3   FTP       82 [TCP ACKed unseen segment] Response: 2
3712 854.125966500 192.168.217.3   192.168.10.11   FTP       72 Request: SYST

▸ Frame 3702: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:1e (00:15:5d:40:57:1e), Dst: Microsof_40:57:0a (00:15:5d:40:57:0a)
▸ Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.11
▸ Transmission Control Protocol, Src Port: 49902, Dst Port: 21, Seq: 17, Ack: 292, Len: 15
▾ File Transfer Protocol (FTP)
  ▾ PASS password\r\n
      Request command: PASS
      Request arg: password

0000  00 15 5d 40 57 0a 00 15  5d 40 57 1e 08 00 45 10   ..]@W... ]@W...E.
0010  00 43 43 6f 40 00 3f 06  93 d6 c0 a8 d9 03 c0 a8   .CCo@.?. ........
```

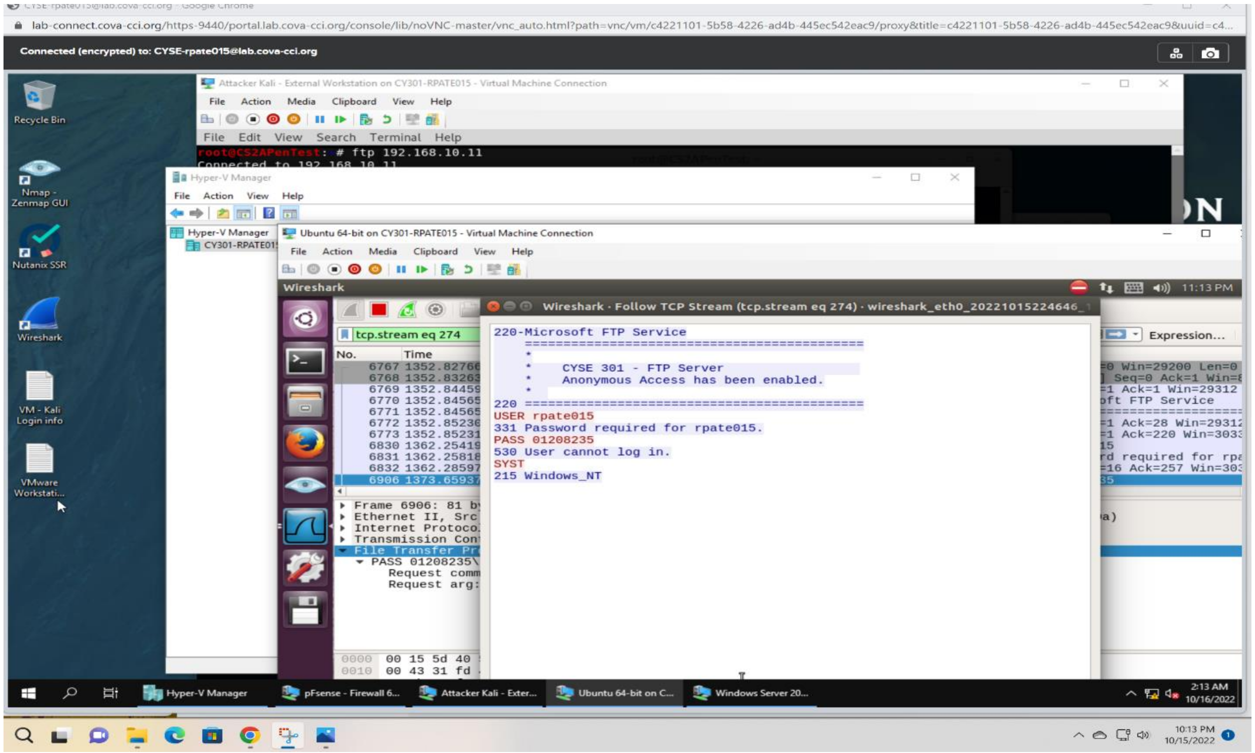


```
root@CS2APenTest:~# ftp 192.168.10.11
Connected to 192.168.10.11.
220-Microsoft FTP Service
```

Wireshark · Follow TCP Stream (tcp.stream eq 156) · wireshark_eth0_20221015224646_

```
220-Microsoft FTP Service
    ==========================================
    *
    *     CYSE 301 - FTP Server
    *     Anonymous Access has been enabled.
    *
220 ==========================================
USER anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
PASS password
230-*************************************************************
    *
    *
    *
    *
    *
    * You are now accessing the FTP service on Windows 2008 R2 for CYSE301
    *
    *
    *
    *
    *
    *************************************************************
    Directory has 33,465,114,624 bytes of disk space available.
230 User logged in.
215 Windows_NT
SYST
```

MIDAS login



Wireshark · Follow TCP Stream (tcp.stream eq 274) · wireshark_eth0_20221015224646_

```
220-Microsoft FTP Service
    ==========================================
    *
    *     CYSE 301 - FTP Server
    *     Anonymous Access has been enabled.
    *
220 ==========================================
USER rpate015
331 Password required for rpate015.
PASS 01208235
530 User cannot log in.
SYST
215 Windows_NT
```

Description:

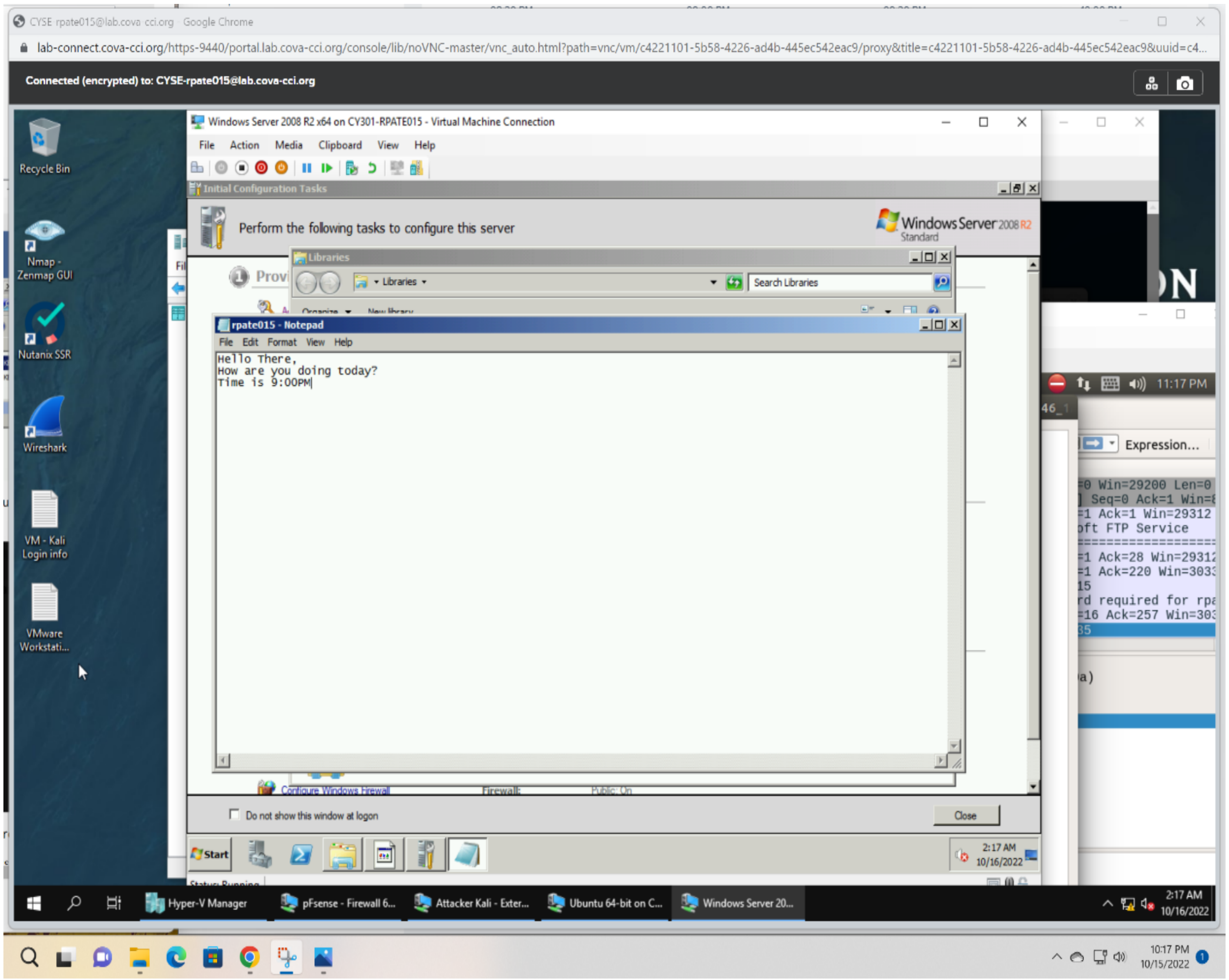
In this step, I have logged into the windows server 2008 from kali linux remotely.

The login credentials are sniffed from Wireshark in ubuntu VM. The traffic is in the plaintext method, so the details are available.

I have tried to login to the FTP server by using the MIDAS credentials, but they are not valid.

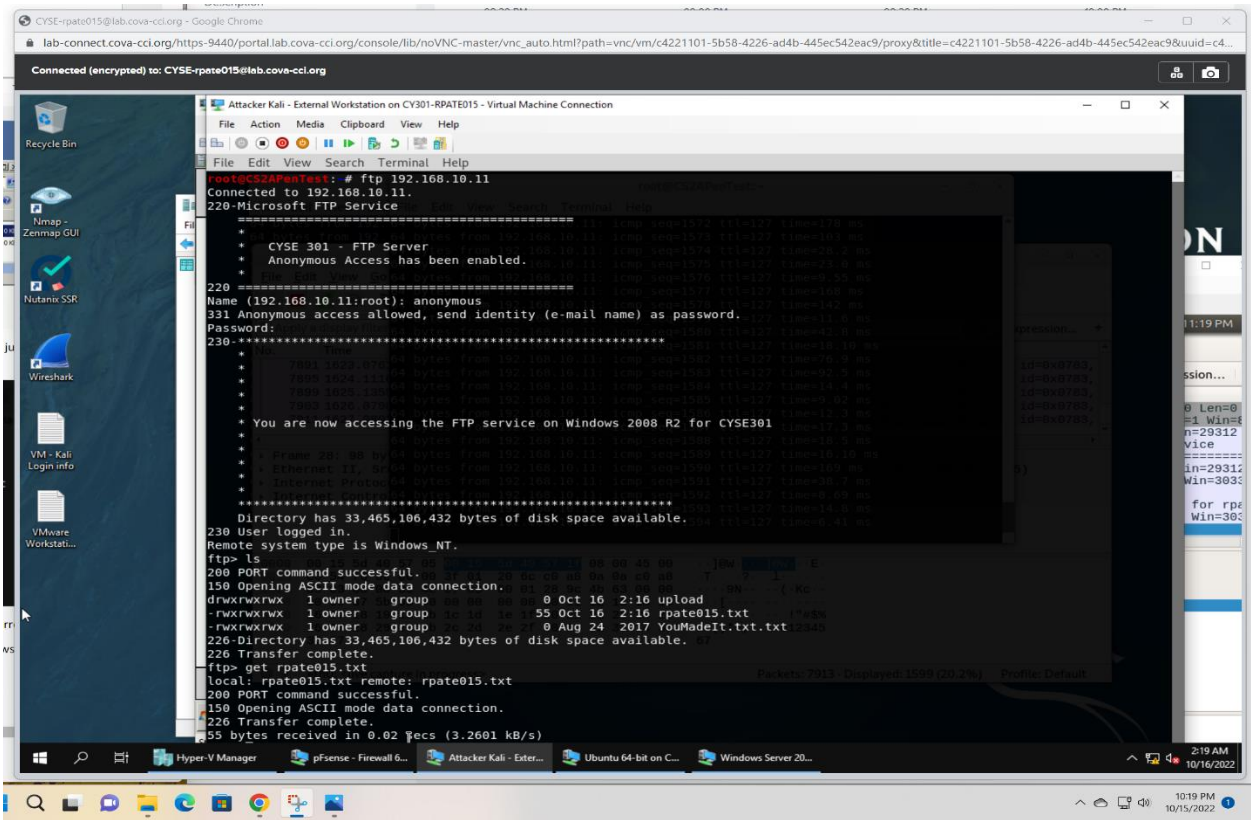
The wrong credentials detail is available in the Ubuntu through the Wireshark.

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


CYSE rpate015@lab.cova-cci.org - Google Chrome
lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC-master/vnc_auto.html?path=vnc/vm/c4221101-5b58-4226-ad4b-445ec542eac9/proxy&title=c4221101-5b58-4226-ad4b-445ec542eac9&uuid=c4...
Connected (encrypted) to: CYSE-rpate015@lab.cova-cci.org
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Windows Server 2008 R2 x64 on CY301-RPATE015 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Initial Configuration Tasks
Perform the following tasks to configure this server
Windows Server 2008 R2 Standard
Libraries
Search Libraries
rpate015 - Notepad
File
Edit
Format
View
Help
Configure Windows Firewall
Firewall:
Public: On
Do not show this window at logon
Close
Start
2:17 AM
10/16/2022
11:17 PM
Expression...
Hyper-V Manager
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on C...
Windows Server 20...
2:17 AM
10/16/2022
10:17 PM
10/15/2022

```
Hello There,
How are you doing today?
Time is 9:00PM
```

```
=0 Win=29200 Len=0
] Seq=0 Ack=1 Win=
=1 Ack=1 Win=29312
oft FTP Service
====================
=1 Ack=28 Win=2931
=1 Ack=220 Win=303
15
rd required for rp
=16 Ack=257 Win=303
35
a)
```



CYSE-rpate015@lab.cova-cci.org - Google Chrome
lab-connect.cova-cci.org/https-9440/portal.lab.cova-cci.org/console/lib/noVNC-master/vnc_auto.html?path=vnc/vm/c4221101-5b58-4226-ad4b-445ec542eac9/proxy&title=c4221101-5b58-4226-ad4b-445ec542eac9&uuid=c4...
Connected (encrypted) to: CYSE-rpate015@lab.cova-cci.org
Attacker Kali - External Workstation on CY301-RPATE015 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
File
Edit
View
Search
Terminal
Help
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Hyper-V Manager
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on C...
Windows Server 20...
2:19 AM
10/16/2022
10:19 PM
10/15/2022

```
root@CS2APenTest:~# ftp 192.168.10.11
Connected to 192.168.10.11.
220-Microsoft FTP Service
    ============================================
    *
    *   CYSE 301 - FTP Server
    *   Anonymous Access has been enabled.
    *
220 ============================================
Name (192.168.10.11:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-**********************************************************
    *
    *
    *
    *
    *
    * You are now accessing the FTP service on Windows 2008 R2 for CYSE301
    *
    *
    *
    *
    *
    **********************************************************
    Directory has 33,465,106,432 bytes of disk space available.
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
drwxrwxrwx   1 owner    group               0 Oct 16  2:16 upload
-rwxrwxrwx   1 owner    group              55 Oct 16  2:16 rpate015.txt
-rwxrwxrwx   1 owner    group               0 Aug 24  2017 YouMadeIt.txt.txt
226-Directory has 33,465,106,432 bytes of disk space available.
226 Transfer complete.
ftp> get rpate015.txt
local: rpate015.txt remote: rpate015.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
55 bytes received in 0.02 secs (3.2601 kB/s)
```

Description:

In this step, I have created a file in the windows server 2008, and that file trying to steal from the Wireshark in Ubuntu when it is requested from Kali linux.

I saw the file, but could not open the content and export it from Wireshark to the Ubuntu.