Assignment 2.1 Traffic Tracing and Sniffing

Task A: Get started with Wireshark (5 point each x 6 questions = 30 points)

In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and Ubuntu VM are talking to each other.

Tip: Please power on the pfsense VM and DO NOT revert to a previous checkpoint.

You should keep Wireshark running in the background while performing the following tasks.

1. Open Wireshark on External Kali and listen on interface “eth0”.
2. Open a new terminal then ping Ubuntu VM for 5 – 10 seocnds.
3. Stop capturing (the red button on the tool bar).

Now, answer the following questions. You need to provide a screenshot that contains the answers to each question

1. How many packets are captured in total? How many packets are displayed?

   There are a total of 120 captures, and 120 are displayed.

2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question.

   There are 56 ICMP captures.

3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

   Source ip: 192.168.10.10 Destination ip: 192.168.217.3
   Sequence number: 8
   Size: 48 Bytes
   Response time: 170.730 ms

4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?

   There are 52 DNS captures. The query selected is trying to resolve wpad.mshome.net.

5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number?

   Source ip: 192.168.217.3:50426 Destination: 192.168.217.2:53

6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

   Source ip: 192.168.217.2:53 Destination: 192.168.217.3:50426. The message from the server says refused.

Assignment 2.2

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.

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 Mirroring mode to “Destination” in the “Port Mirroring”

• Ubuntu Kali: Set Mirroring mode to “Source” in the “Port Mirroring”

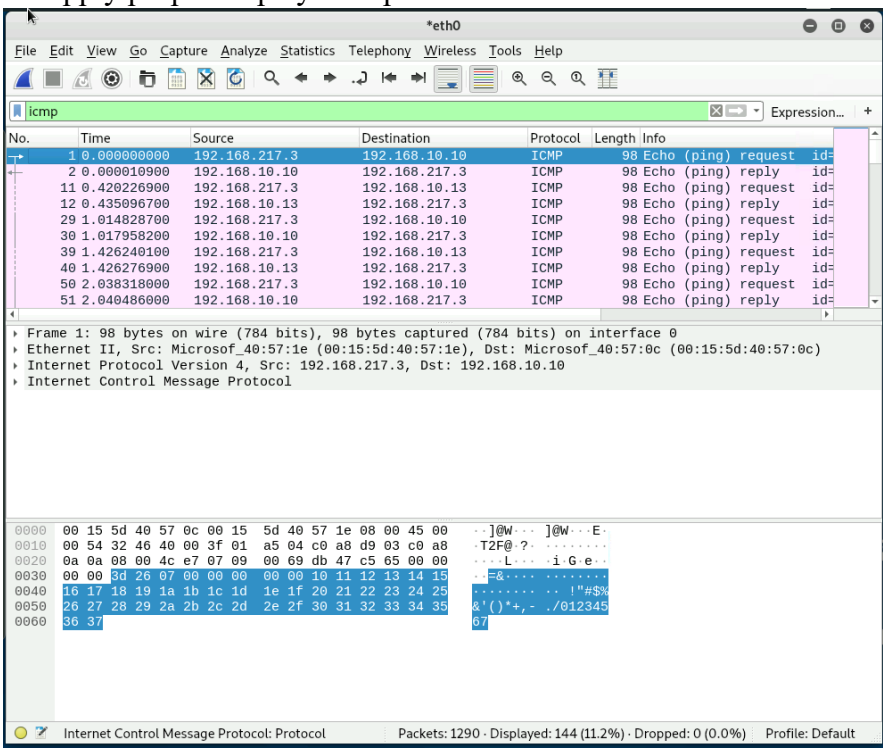
• External Kali: Set Mirroring mode to “Source” in the “Port Mirroring”

** 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. Figure 1 Required VMs for this assignment Figure 2 How to configure port mirroring in Hyper-V Select the first Network Adaptor, then click “ Advanced Features”

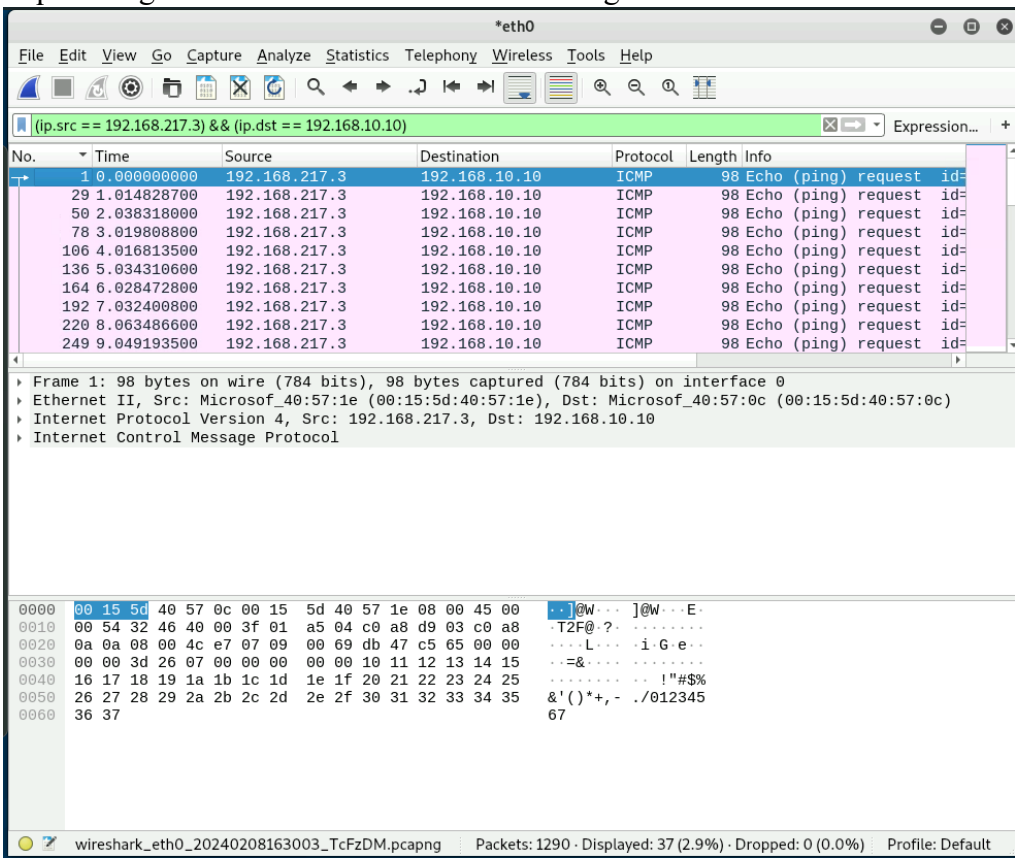
1. Sniff ICMP traffic (10 + 10 = 20 points)

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.

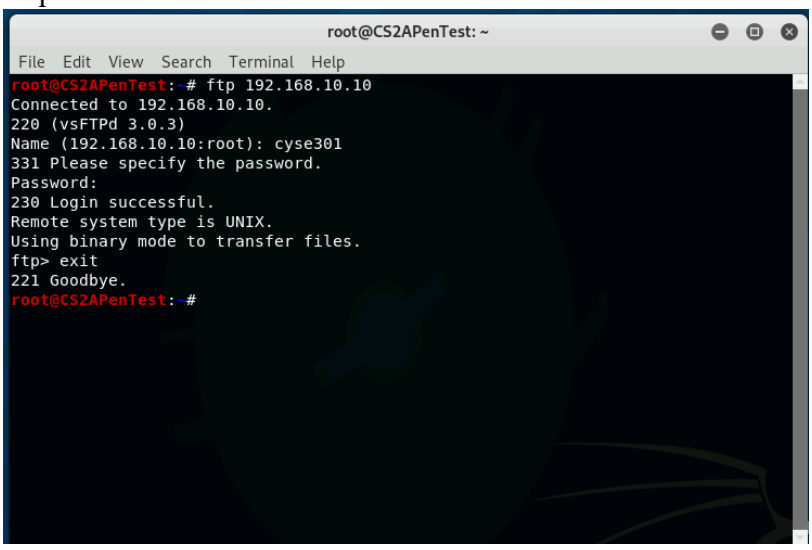


B. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM



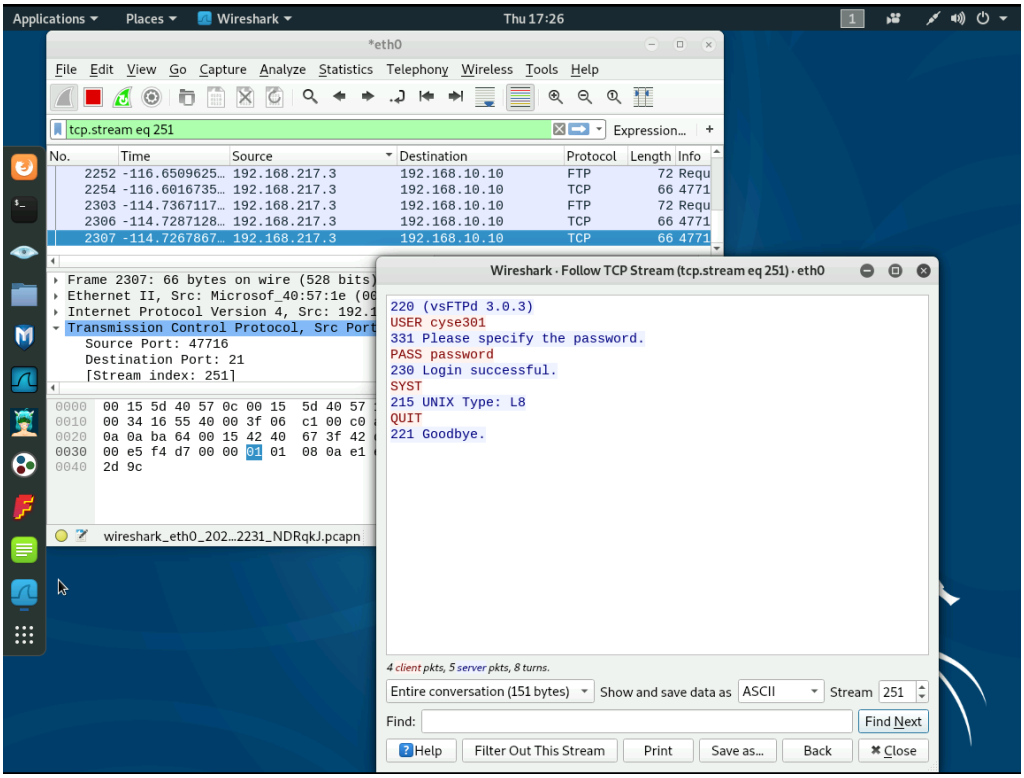
2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

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.A.

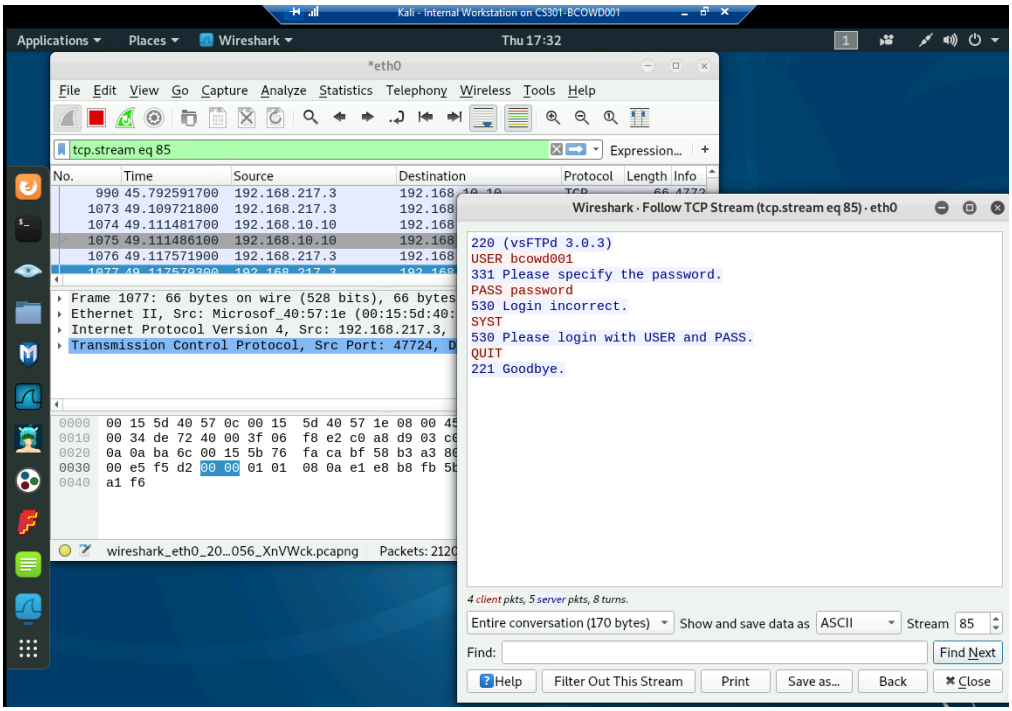


B. Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot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

I used wireshark on the internal kali which recorded the ftp connection from the exteranl kali workstation to capture the tcp connection that took place. I used the filter ip.src==192.168.217.3 in order to show traffic from that source ip and then selected the tcp that went to the 192.168.10.10 and selected follow tcp stream in order to show usernam and password that was used for connection.

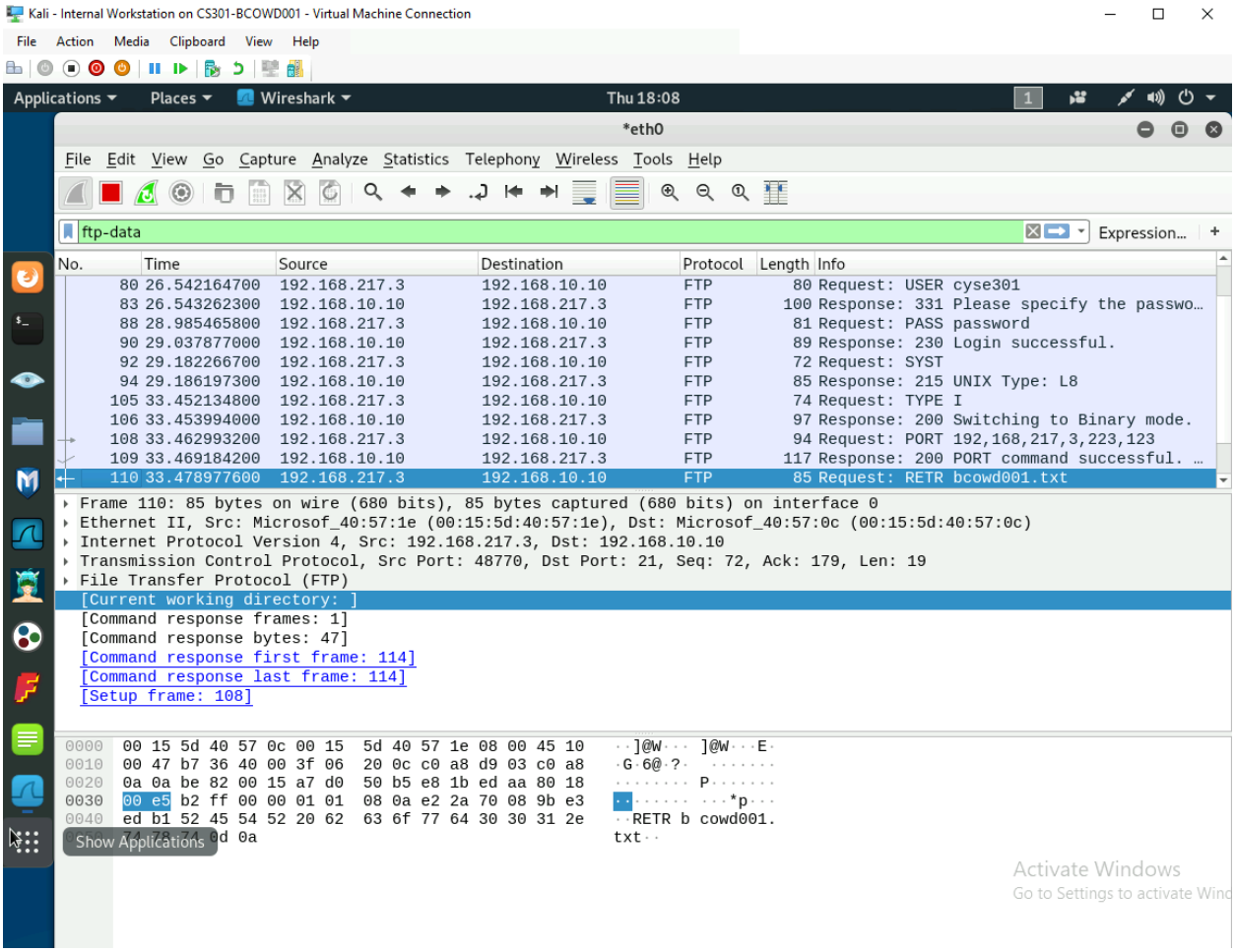


C. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these “secrets” from the attacker VM, which is Internal Kali.

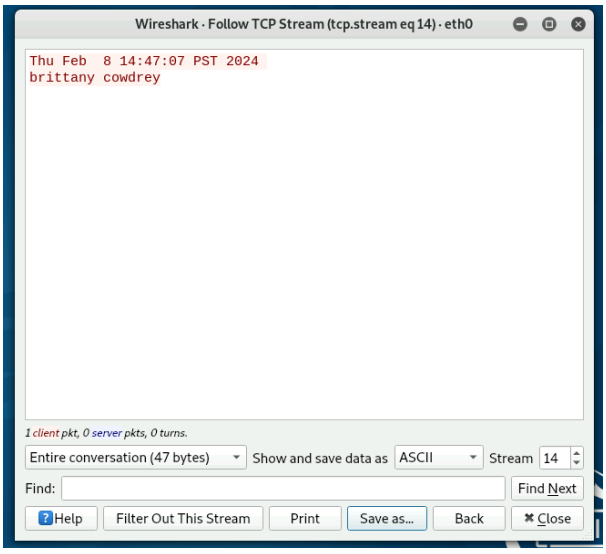

Kali - Internal Workstation on CS301-BCOWD001
Applications
Places
Wireshark
Thu 17:32
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 85
Expression...
No. Time Source Destination Protocol Length Info
990 45.792591700 192.168.217.3
1073 49.109721800 192.168.217.3
1074 49.111481700 192.168.10.10
1075 49.111486100 192.168.10.10
1076 49.117571900 192.168.217.3
Frame 1077: 66 bytes on wire (528 bits), 66 bytes
Ethernet II, Src: Microsof_40:57:1e (00:15:5d:40:
Internet Protocol Version 4, Src: 192.168.217.3,
Transmission Control Protocol, Src Port: 47724, D
0000 00 15 5d 40 57 0c 00 15 5d 40 57 1e 08 00
0010 00 34 de 72 40 00 3f 06 f8 e2 c0 a8 d9 03
0020 0a 0a ba 6c 00 15 5b 76 fa ca bf 58 b3 a3
0030 00 e5 f5 d2 00 00 01 01 08 0a e1 e8 b8 fb
0040 a1 f6
wireshark_eth0_20...056_XnVWck.pcapng
Wireshark · Follow TCP Stream (tcp.stream eq 85) · eth0
220 (vsFTPd 3.0.3)
USER bcowd001
331 Please specify the password.
PASS password
530 Login incorrect.
SYST
530 Please login with USER and PASS.
QUIT
221 Goodbye.
4 client pkts, 5 server pkts, 8 turns.
Entire conversation (170 bytes)
Show and save data as ASCII
Stream 85
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

Extra Credit: Steal files with Wireshark (15 points)

1. Apply a proper display filter to display the FTP-DATA packets between External Kali and Ubuntu VM



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 Internal Kali, and view the content.