Lab 9: OT/SCADA Penetration Testing

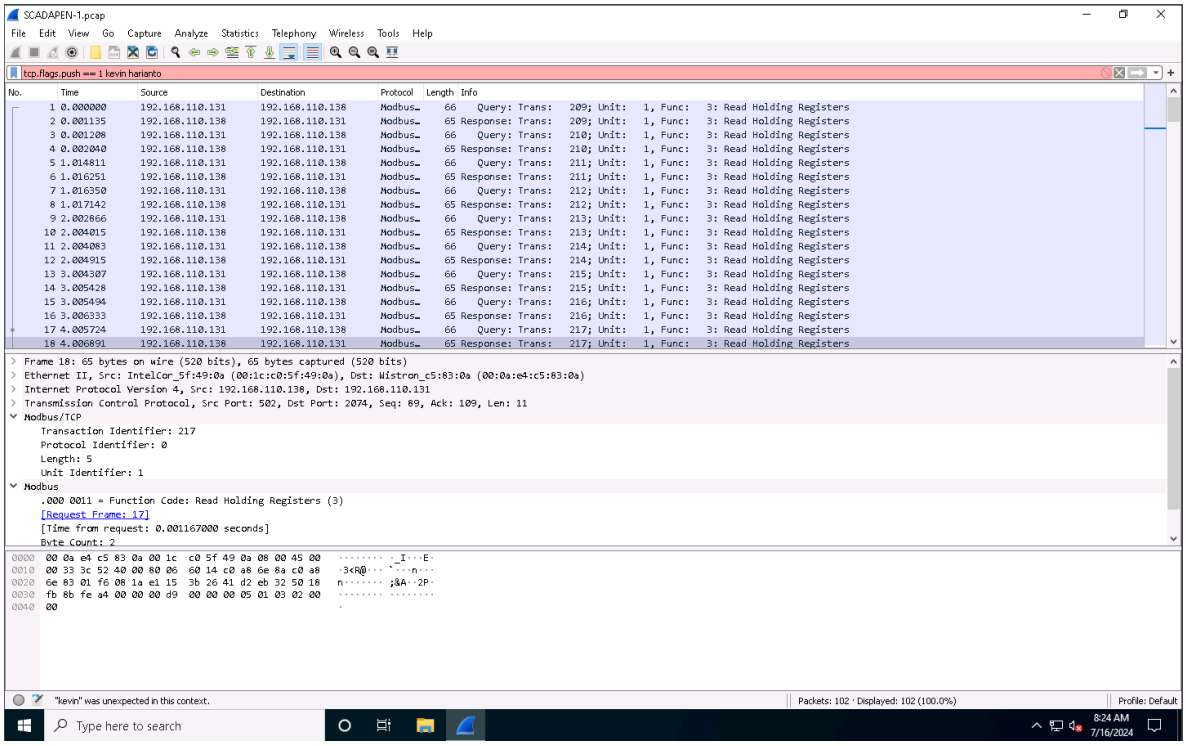
INFO40587: ETHICAL HACKING

Kevin Harianto| 991602128| July 16, 2024

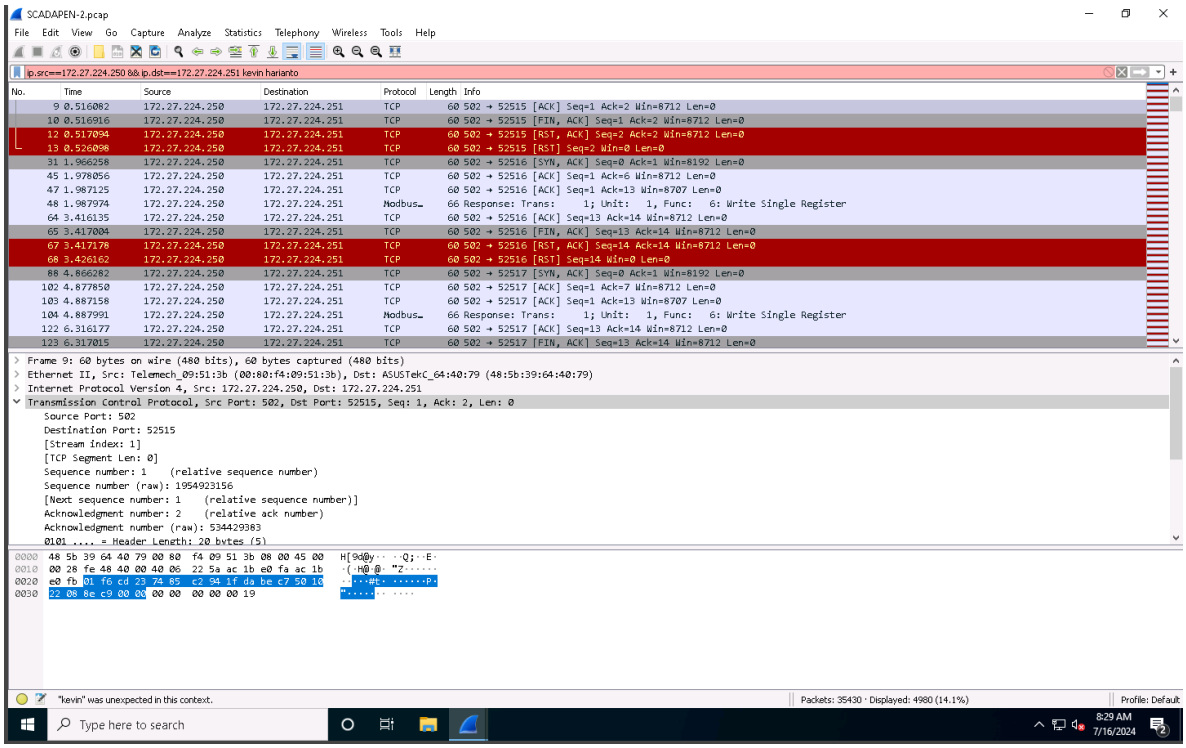
Exercise 1: ModBus Protocol Analysis - I

1.1 OUTPUT SCREENSHOTS

Exercise 1, Step 18: Now, select packet number **10** and observe the **Modbus** node in the middle section. Since the image is a response, the data include the information in the register. There are two types of places where information can be stored: coils and registers. Each of these datastore types has two different types of registers: a read/write and a read only. Each of these datastore types, in turn, is a reference to a memory address.

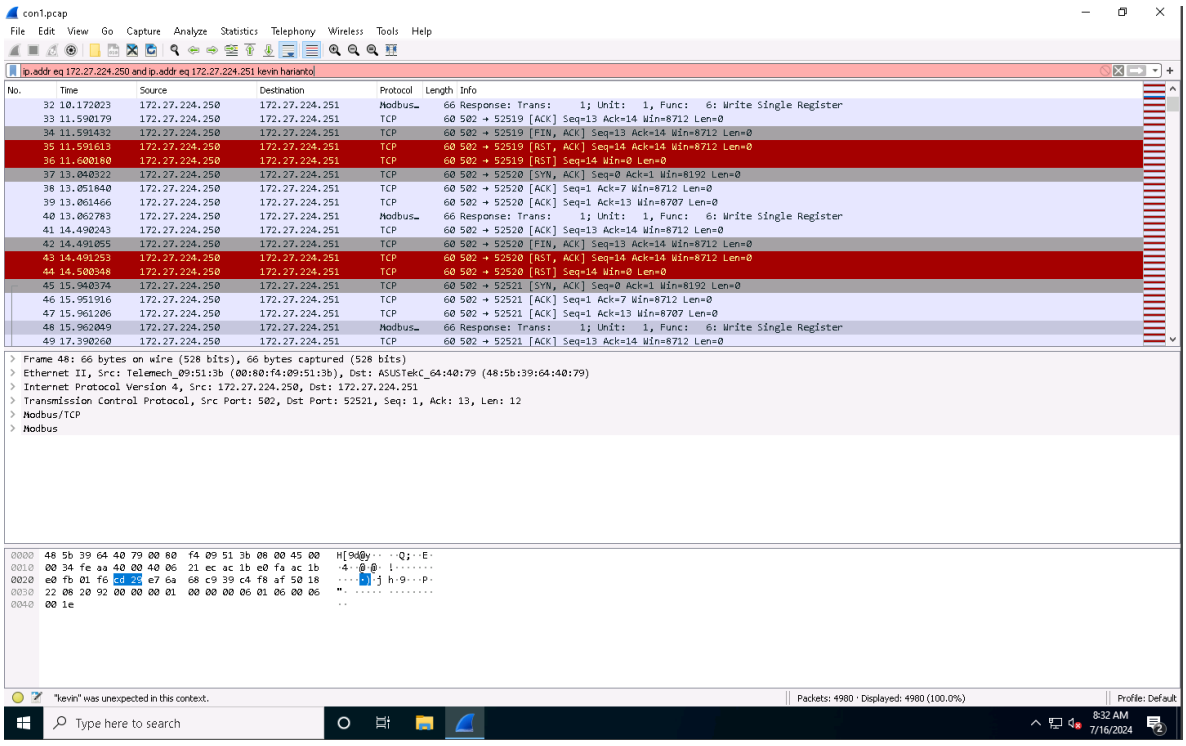


Exercise 1, Step 32: The process of applying this filter reduces the amount of packets to perform the process against. Observe at **lower right corner** of the window. The packets have been reduced from 35,430 to 11,490, which is an improvement. This way, you can make these conversations more digestible for analysis.

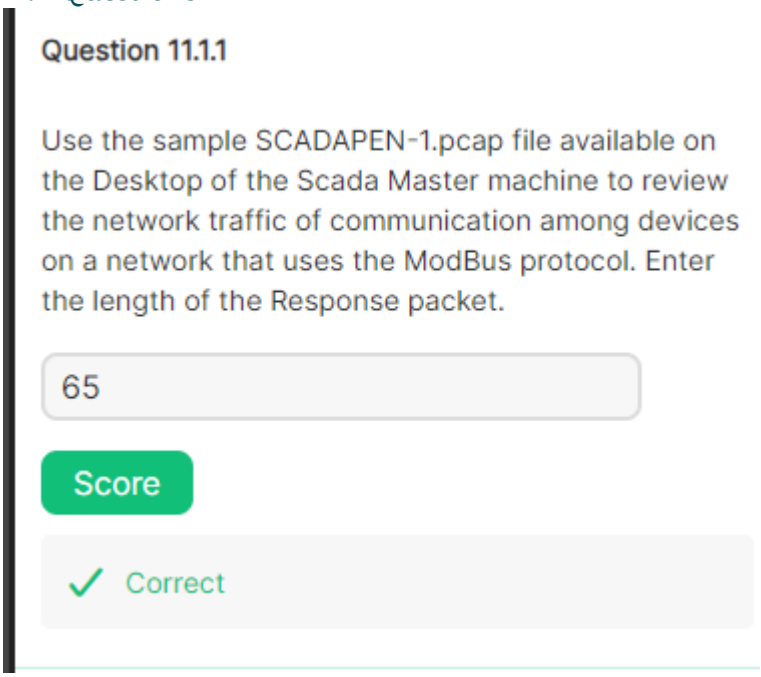


Exercise 1, Step 36:

You have a request that is writing data **001e** to the register. You will not see the response, because, when you captured the specific packets, you only explored one direction. You can either show this by naming the file or capturing both sides of the conversation. When you return to the original file, you can review the conversation again. This time, select the filter for both directions and review the "**write**" statement to check if it was successful.



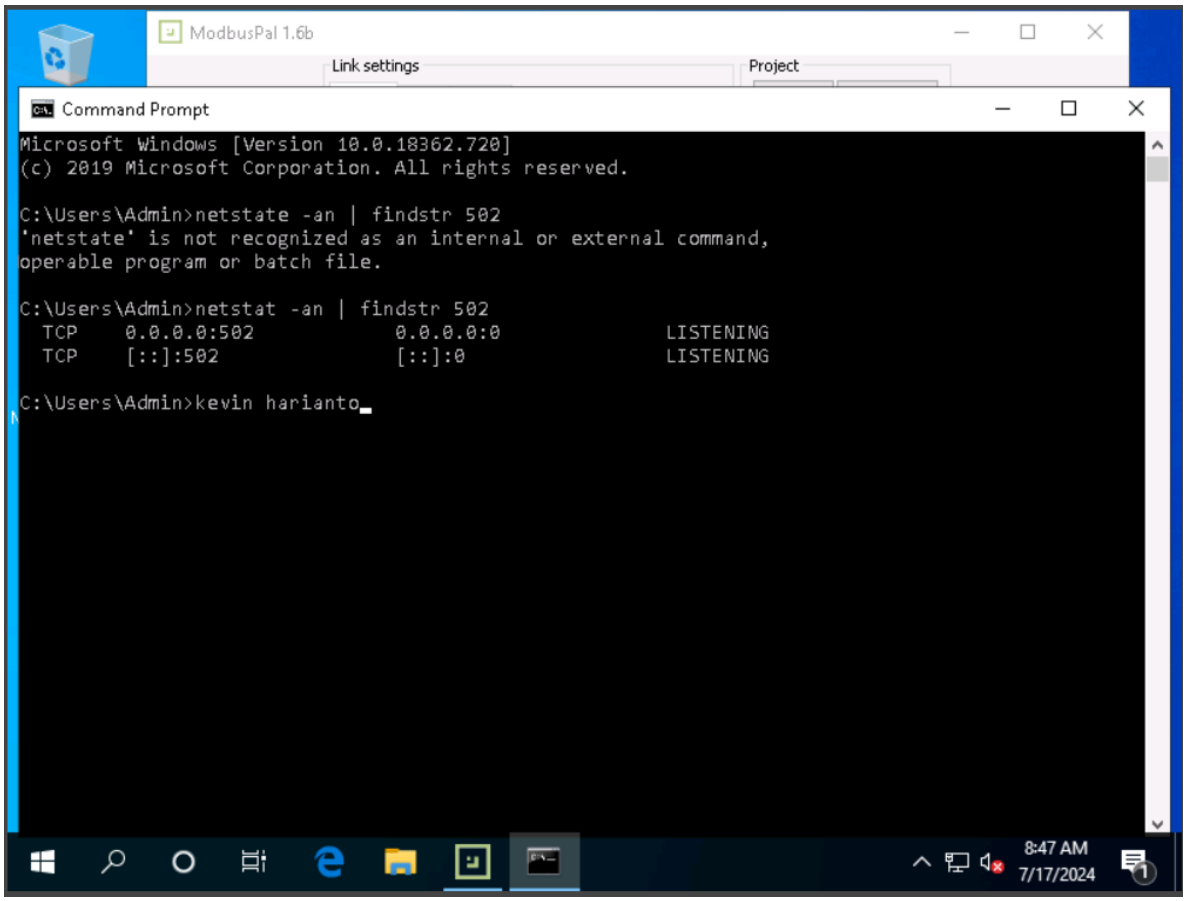
1.2 Questions



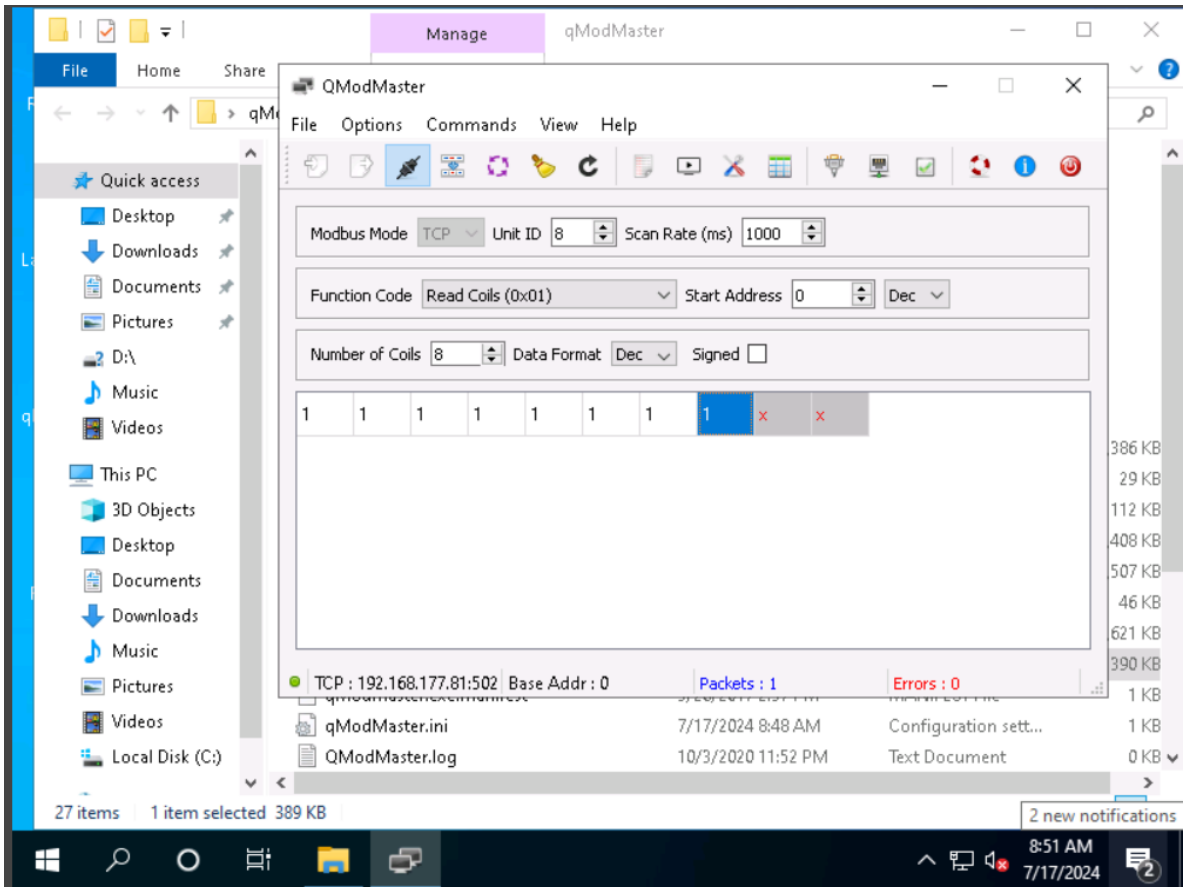
Exercise 2: ModBus Protocol Analysis - II

2.1 OUTPUT SCREENSHOTS

Exercise 2, Step 37: To verify the slave has started, open Command prompt and type **netstat -an | findstr 502** and **Enter**; the port should be listening, as shown in the screenshot. **Close** the Command Prompt window.



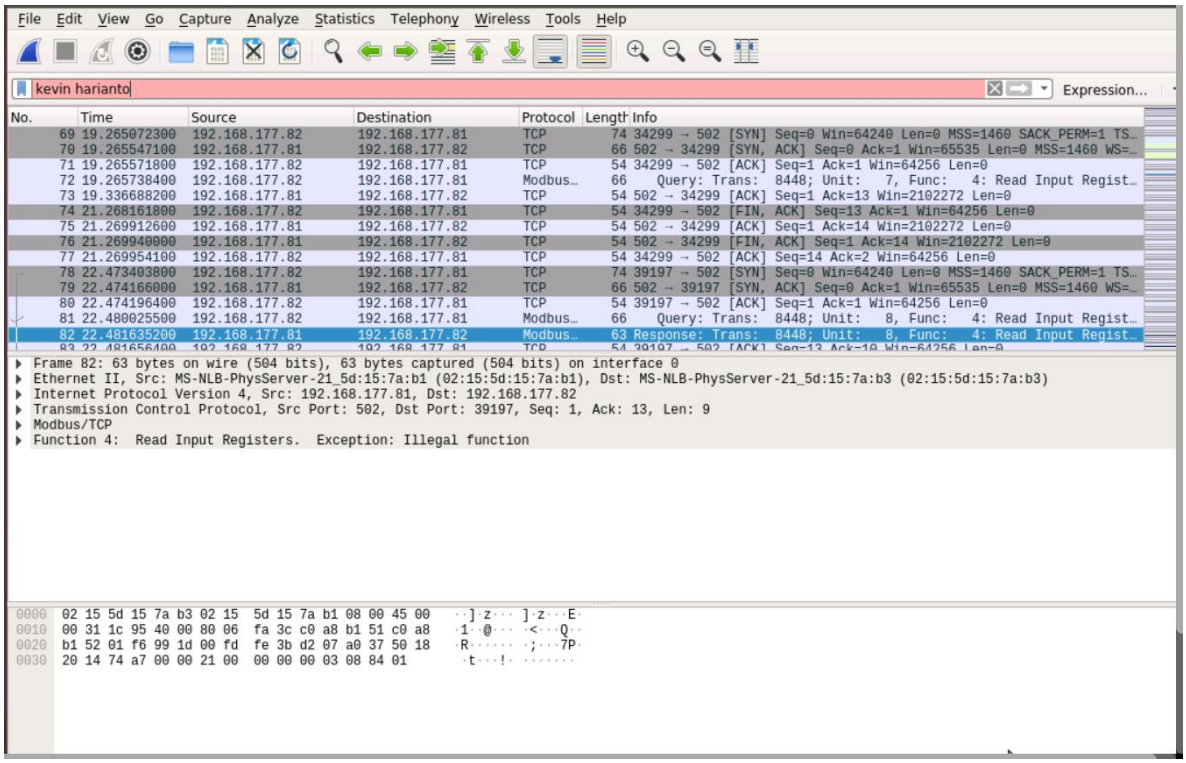
Exercise 2, Step 44:
Switch to SCADA Master. Click **Connect** icon to **Disconnect** the connection and then click **Connect** icon to **reconnect**. Click **Read / Write** icon next to the **Connect** icon. The master should be updated with the new values, as shown in the screenshot.



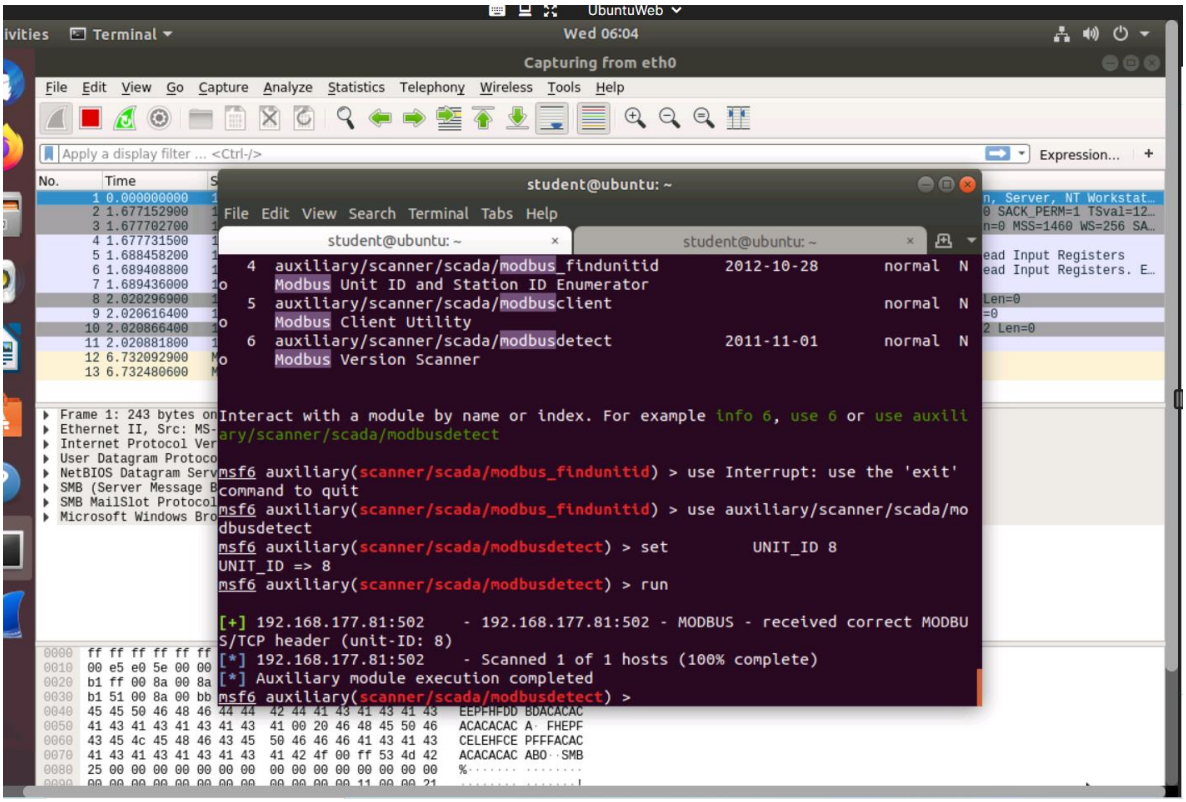
Exercise 2, Step 47: Once you have verified the machine, use the Nmap scripting engine script against it. Type **sudo nmap --script modbus-discover.nse 192.168.177.81 -p 502 -Pn**

```
student@ubuntu:~$ echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T
"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
student@ubuntu:~$
```

Exercise 2, Step 59: With the **UNIT-ID** identified, return to **Wireshark**; capture and review the data at the packet level. Look for when the ID is **correctly discovered**. **Stop** the capture to review.



Exercise 2, Step 60: **Restart** your capture in Wireshark.
In **msfconsole** press **Ctrl+C** to stop, and then return to the **modbusdetect** module by typing **use auxiliary/scanner/scada/modbusdetect** and press **Enter**, and type **set UNIT_ID 8** and press **Enter**. Type **run** and press **Enter** to perform the exploit.



2.2 QUESTIONS

Question 11.2.1

Use the Internet resources https://whois.com, https://www.exploit-db.com, and https://archive.org to extract information about SCADA networks. Flag submission is not required for this task; enter "No flag" as the answer.

No flag

Score

✓ Correct

Congratulations, you passed!

Your score: 2 / 2

Close Window