OT/SCADA Penetration Testing Methodology

54 Minutes Remaining

Instructions Resources Help  100%

Exercise 2: ModBus Protocol Analysis - II

Objective

* In this lab, you will explore Internet resources to extract information about SCADA networks
* Create a simulation of ModBus master-to-slave communication and explore it at the packet level

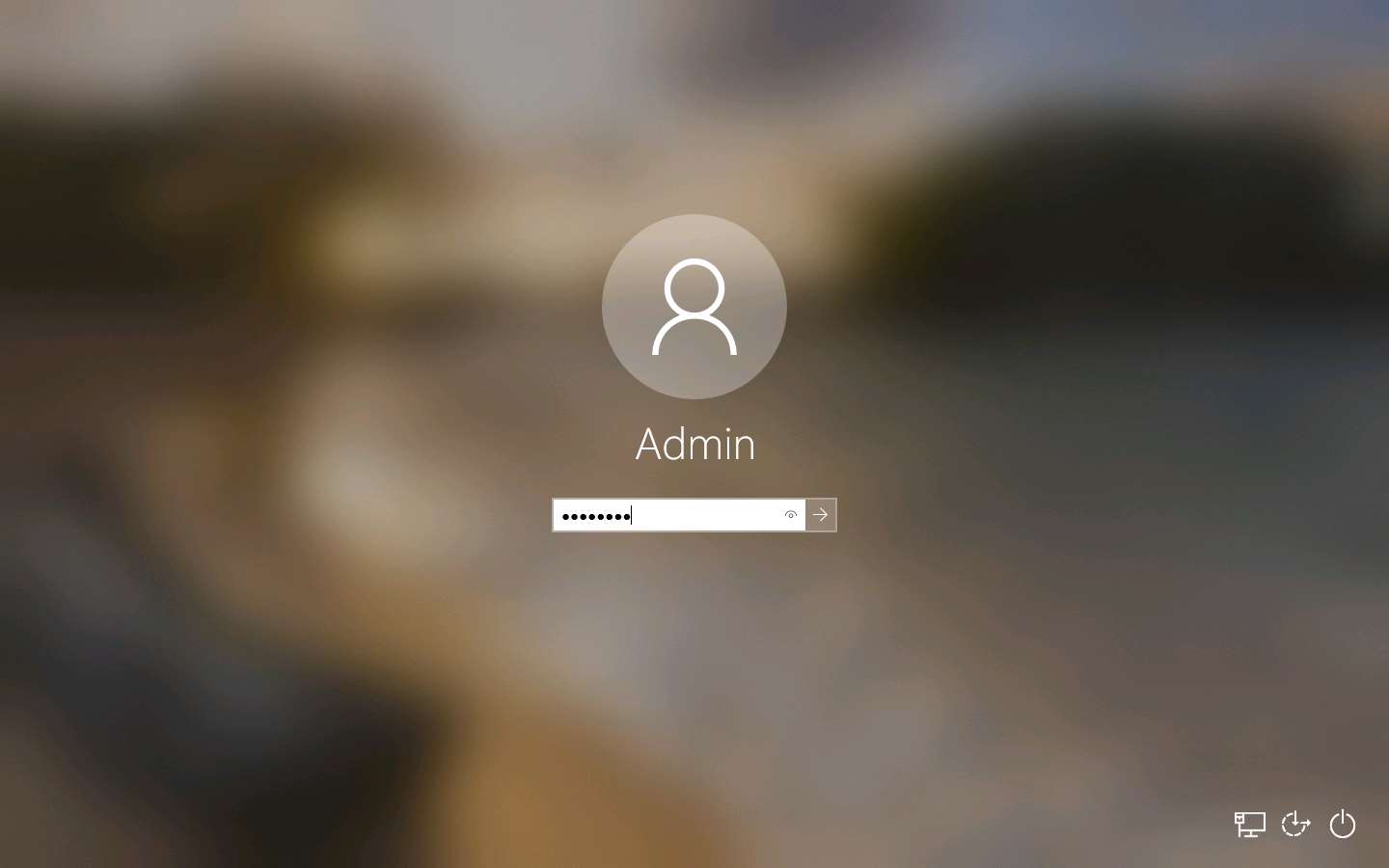
**Lab Duration**: **30** Minutes

1. Click [SCADA Master](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10) and click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10).

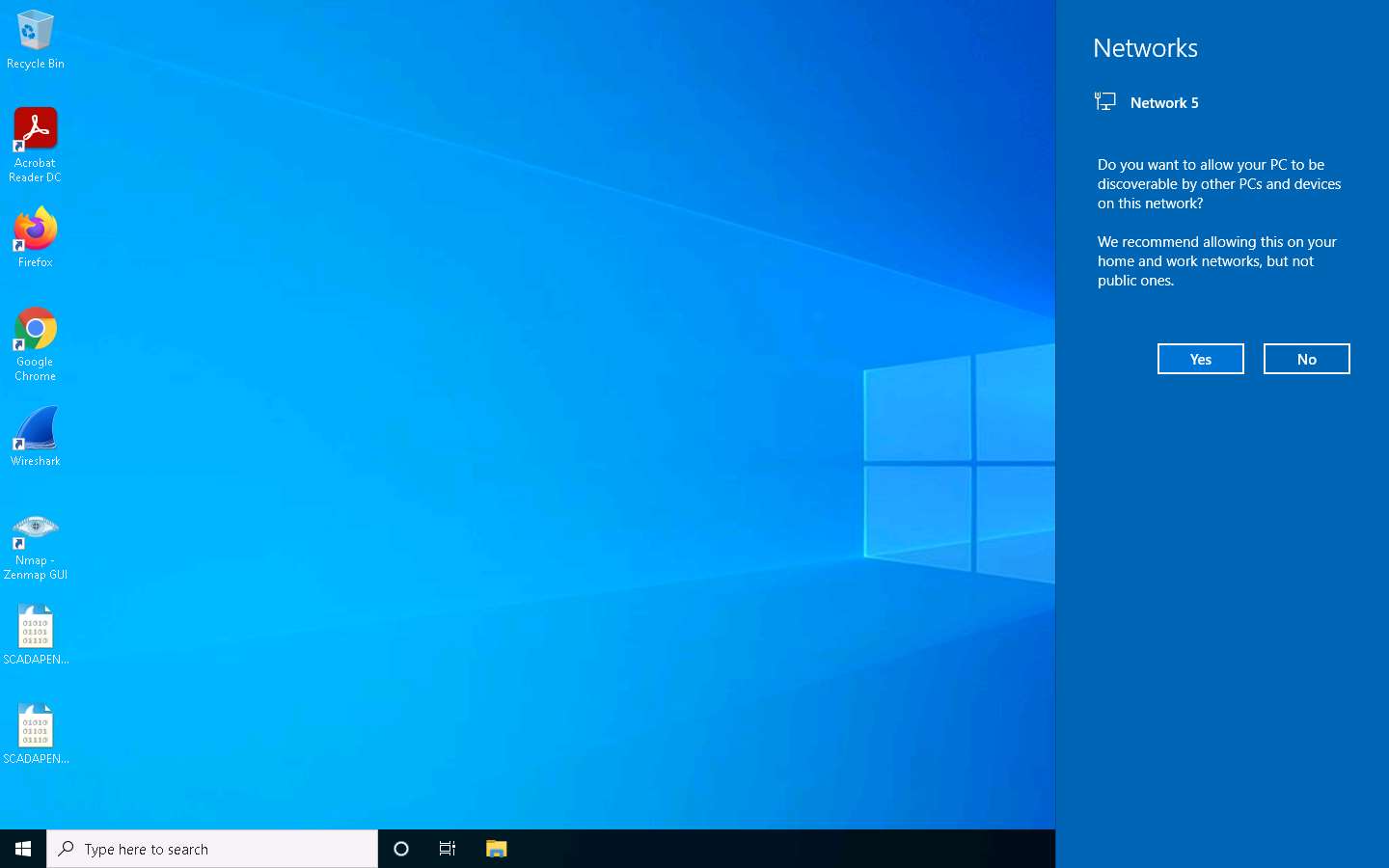
If you are already logged in, skip to step **4**.



1. Click Pa$$w0rd or type **Pa$$w0rd** and press **Enter**.

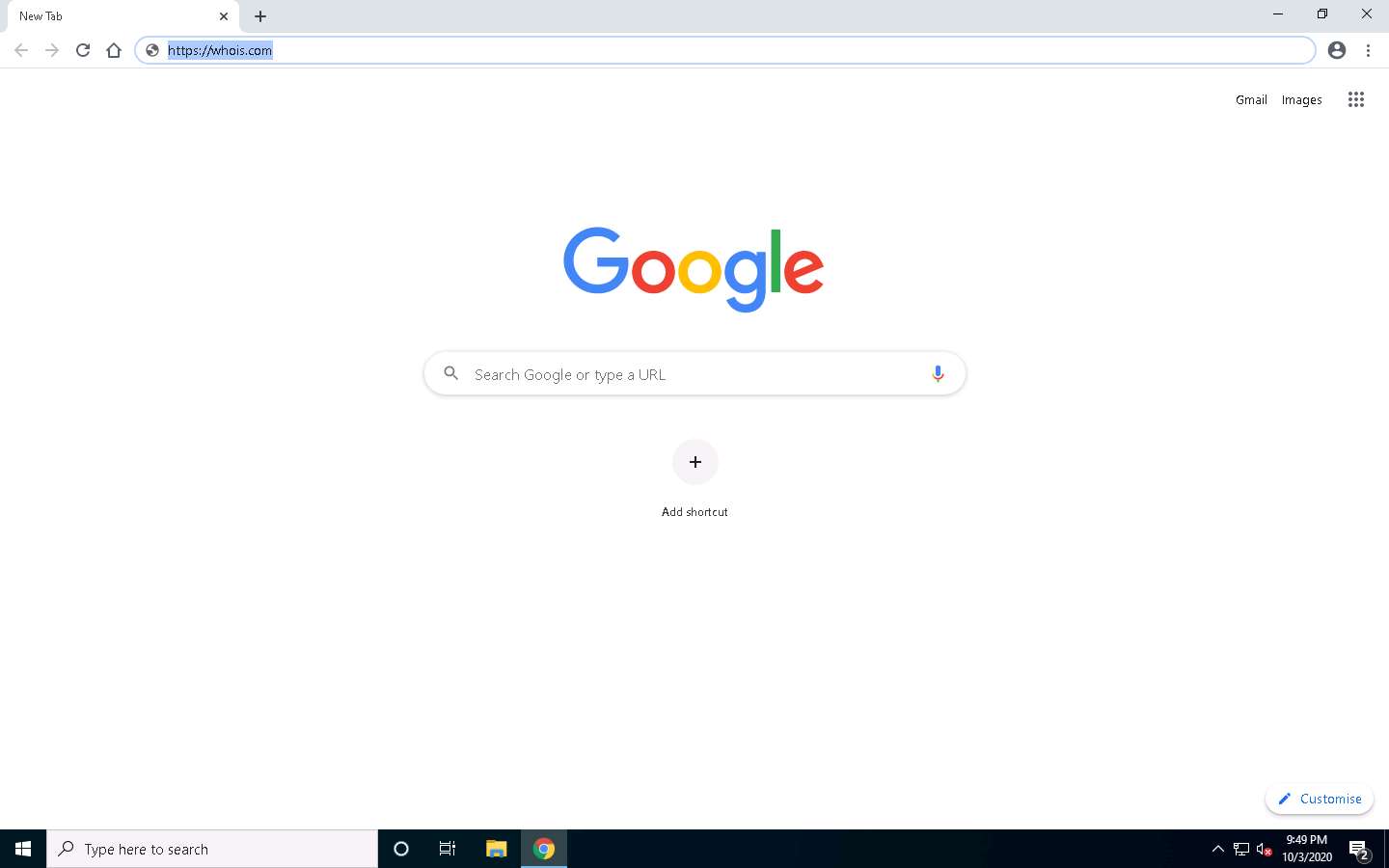


1. Networks screen appears, click **Yes**.



1. Launch a browser, in this Exercise we are using **Google Chrome** browser. Place your mouse cursor in the address bar and click https://whois.com link and press **Enter** to browse the page.

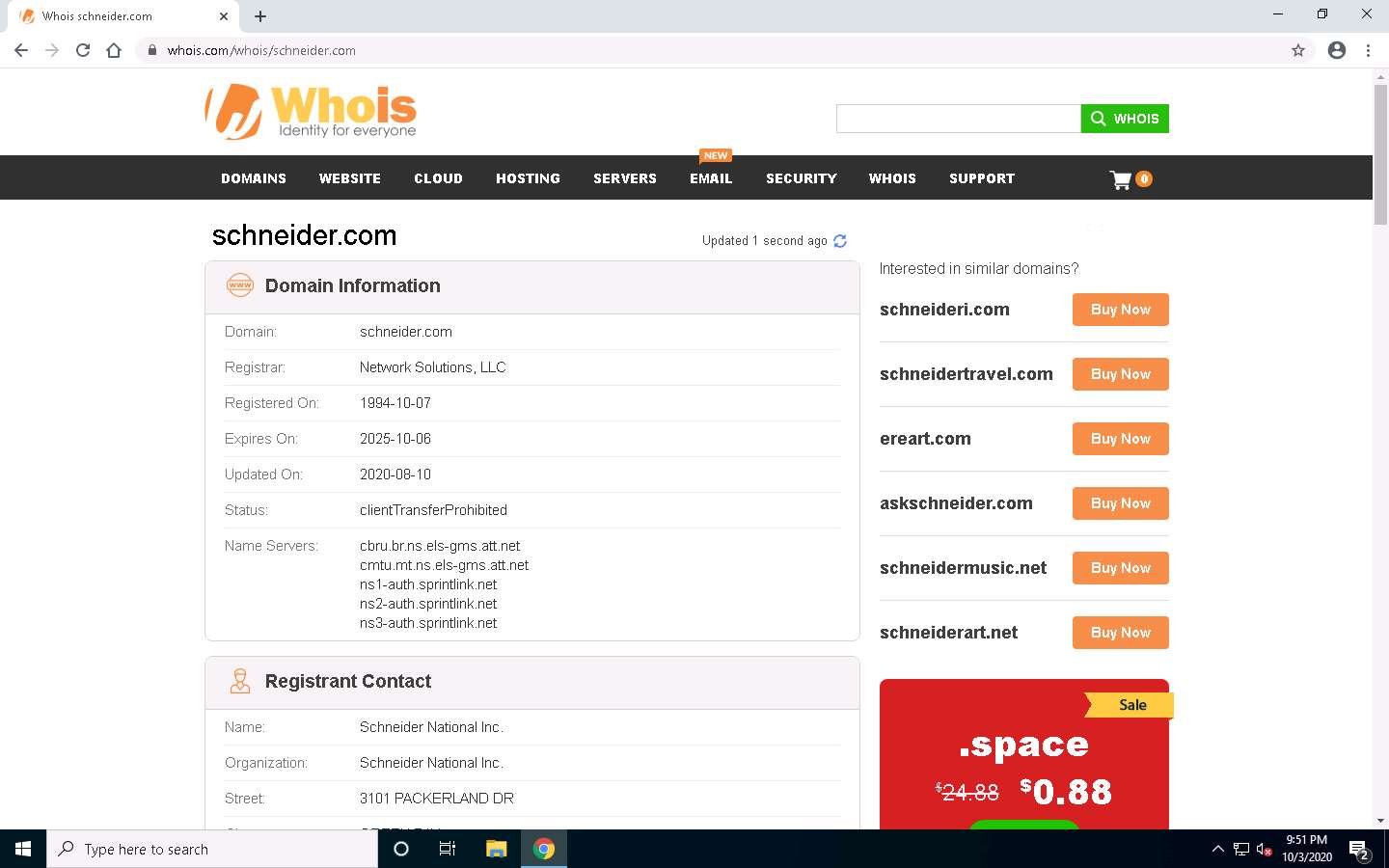
If you use a different browser then screenshots will differ.



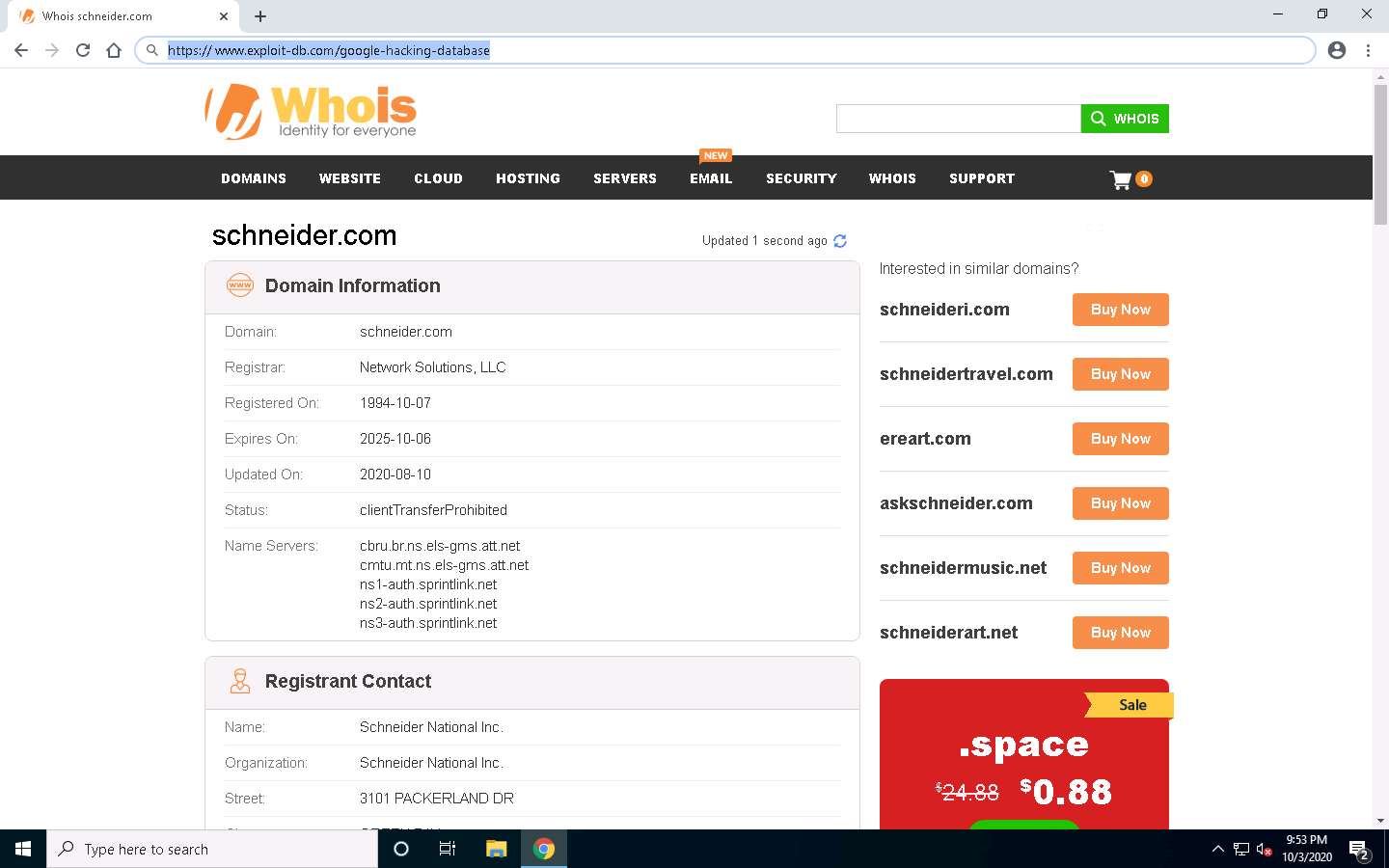
1. The main page of Whois.com appears, in the search field type **Schneider.com** and press **Enter**.



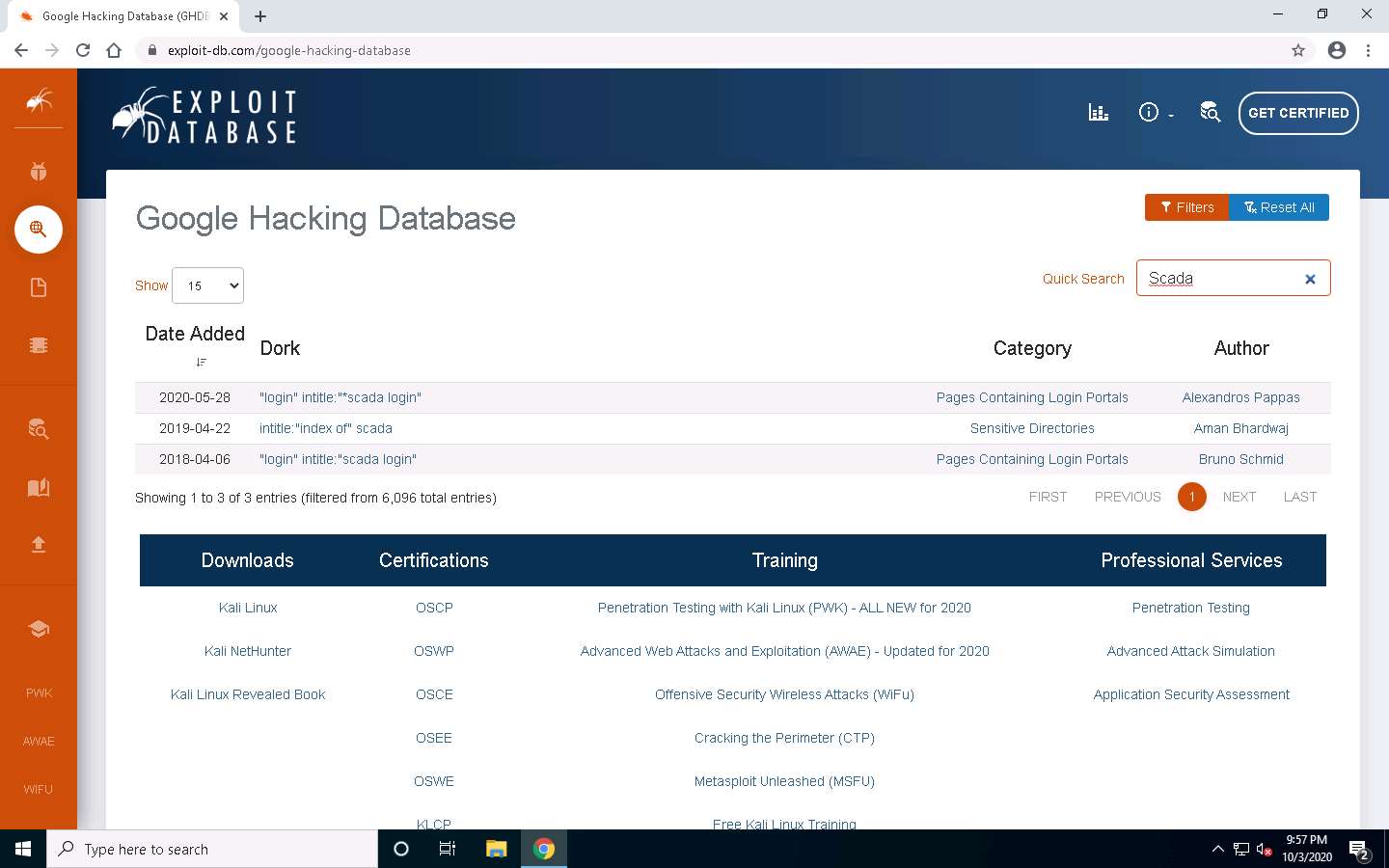
1. The screenshot shows the **name servers**, which will help you start building the footprint for the either attack or defense.



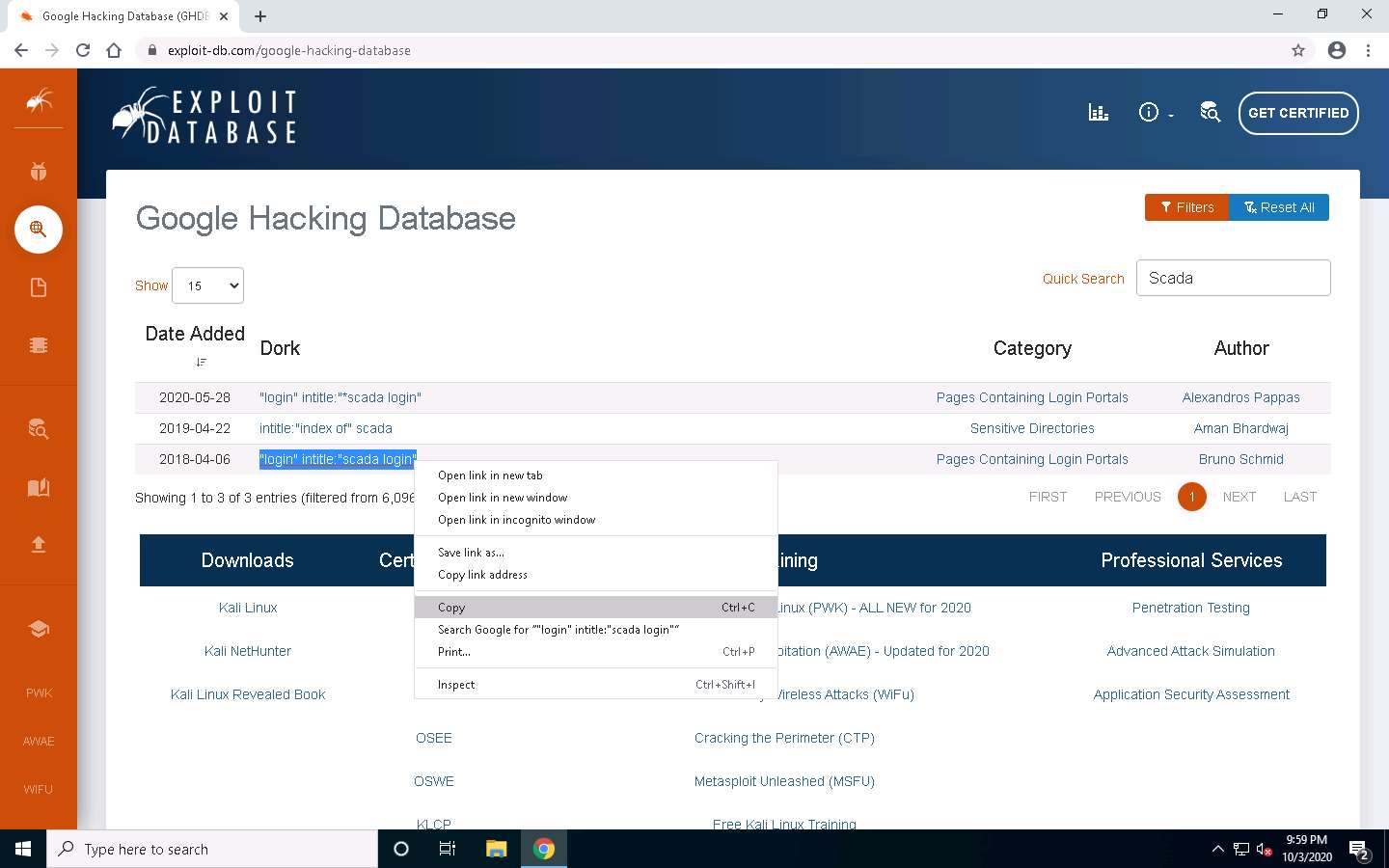
1. This company was formerly **Modicon** that invented the **ModBus** protocol. It is important to be familiar with it as well as track announcements. Next, review the site that contains the **Google Hacking Data Base**. In the address bar of the browser, place mouse cursor and click https://www.exploit-db.com/google-hacking-database and press **Enter**.



1. The Exploit-DBs Google Hacking Database page appears, as shown in the screenshot. Carefully read the different queries, as you may find a dork related to Industrial Control Systems. You can also do a search for a dork as well. Enter **SCADA** in the search field to check if the query returns any results.

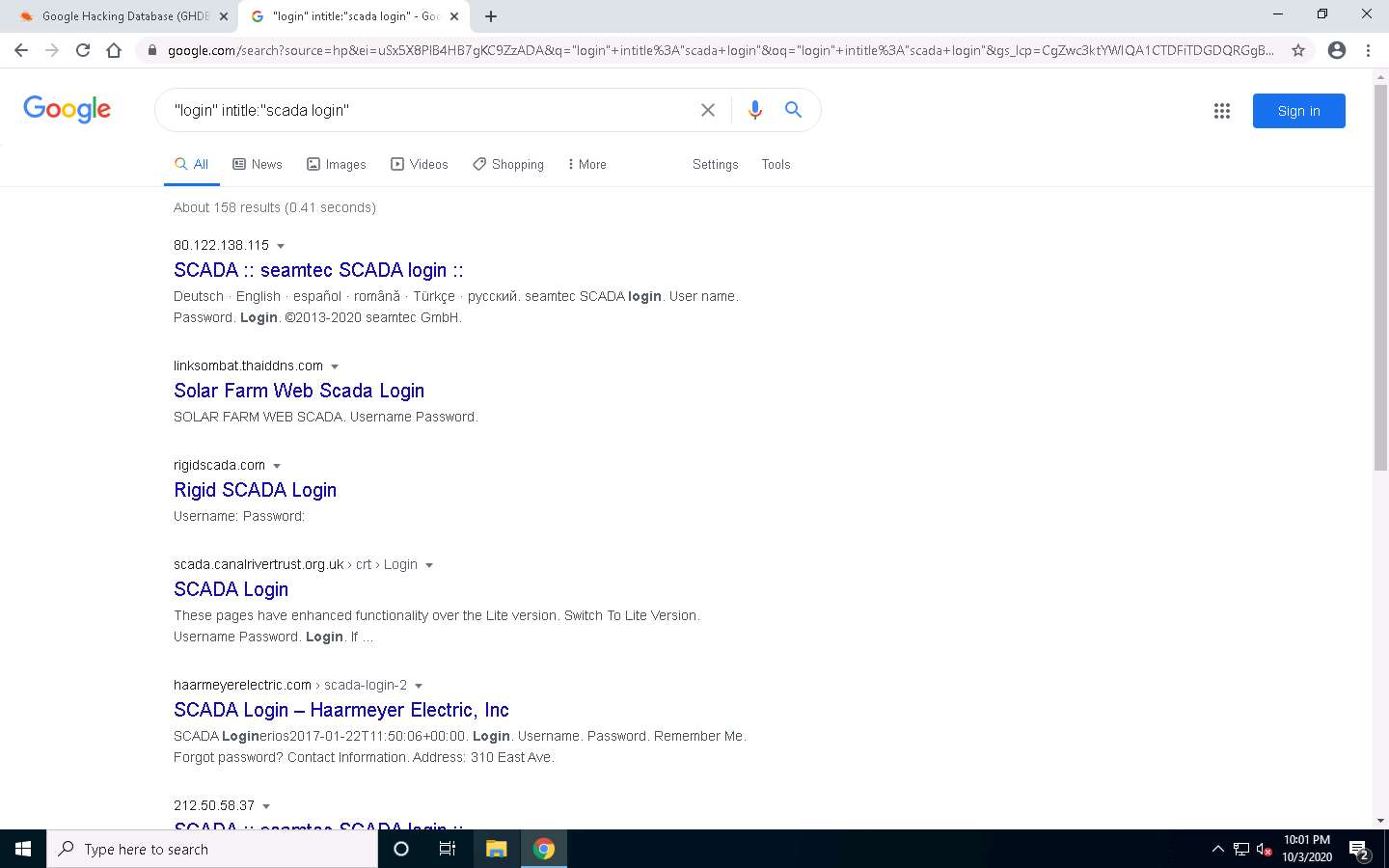


1. In the search results right-click on the **"login" intitle:"scada login"** and click **Copy** as shown in the screenshot.

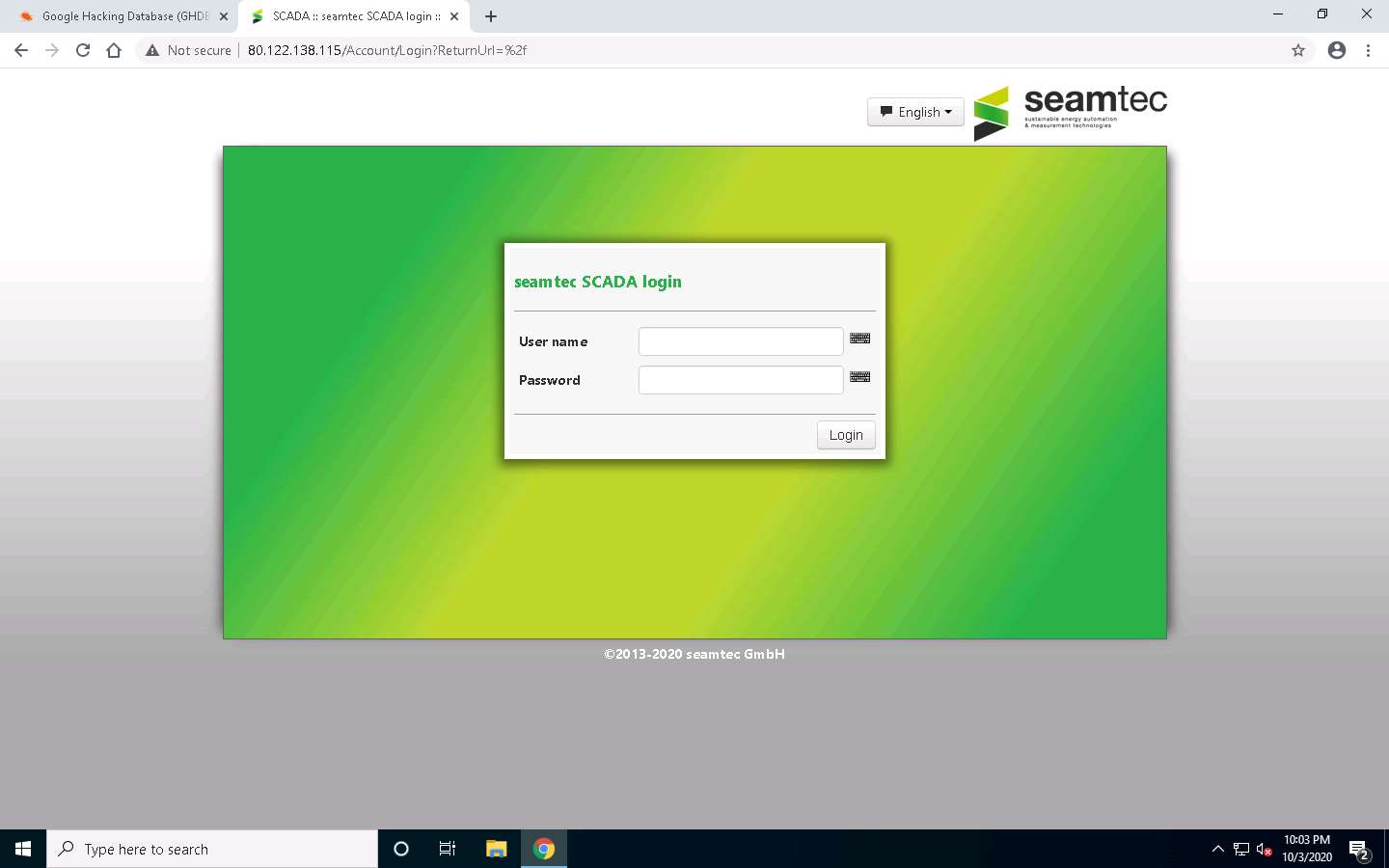


1. Next, explore the query results in Google Search. Open a new tab and browse google.com. In the Google search paste the copied content and search for the results, as shown in the screenshot.

If Google Before you continue pop-up appears, click **I agree**.



1. As with any query results, some information will not be of interest. You must accept and pull the relevant data out. Note that the last entry in the image has a login field. Click on it to see the result.
2. This is a great find, if this were a site you were penetration testing because it uses the **HTTP** protocol. You could potentially **brute-force** attack it or opt for the **MITM** to obtain the credential information. In testing, it is important to discover these elements.

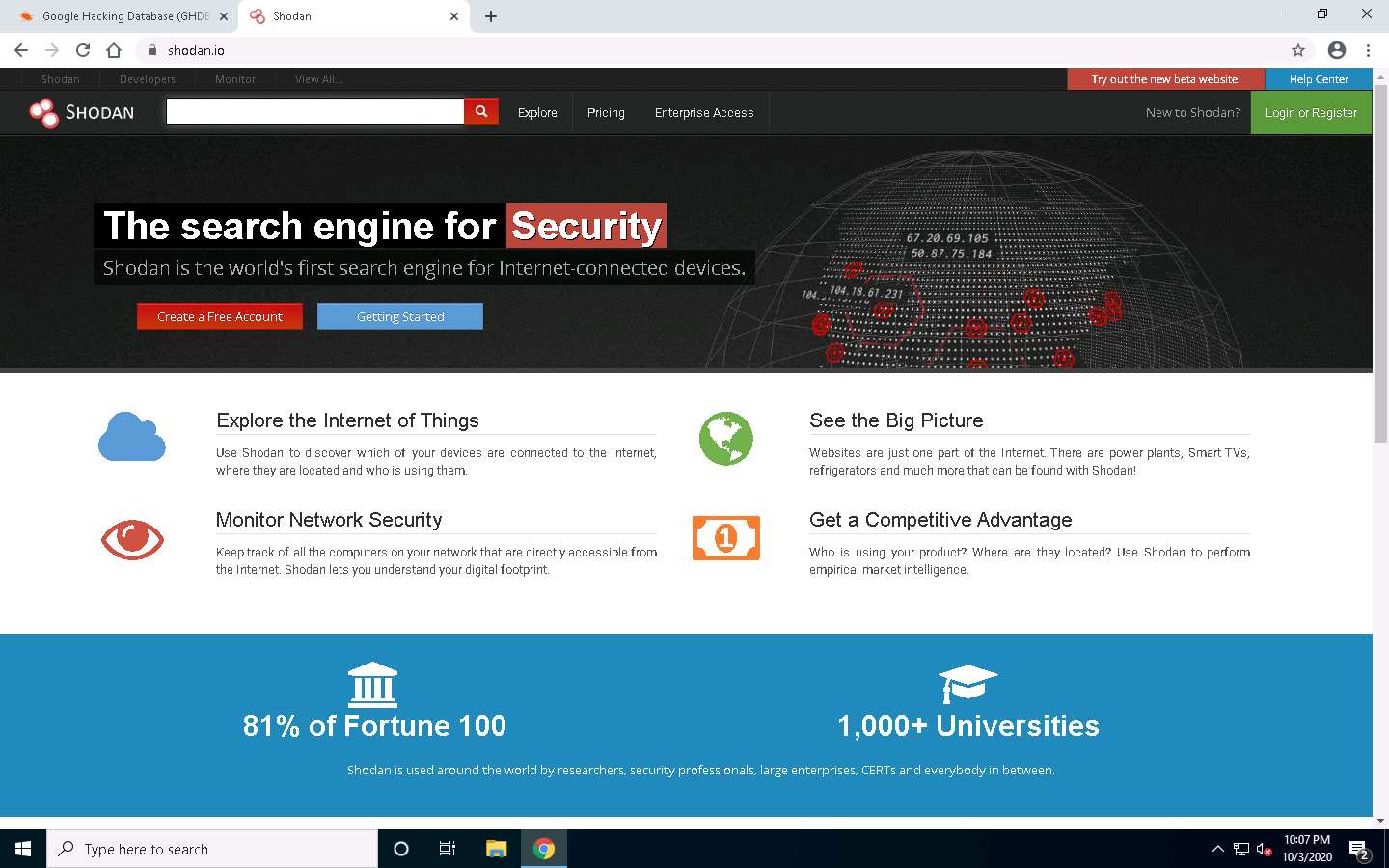


1. Next, review the **WayBack** Machine. In the browser, enter https://archive.org. In the WayBack Machine form, enter **Schneider.com**. Review the company site and see how far you can go back to extract information. An example of the number of times the page has been stored is shown in the screenshot. There are many times that the site has been archived. Review the different sites and check what information you can extract.

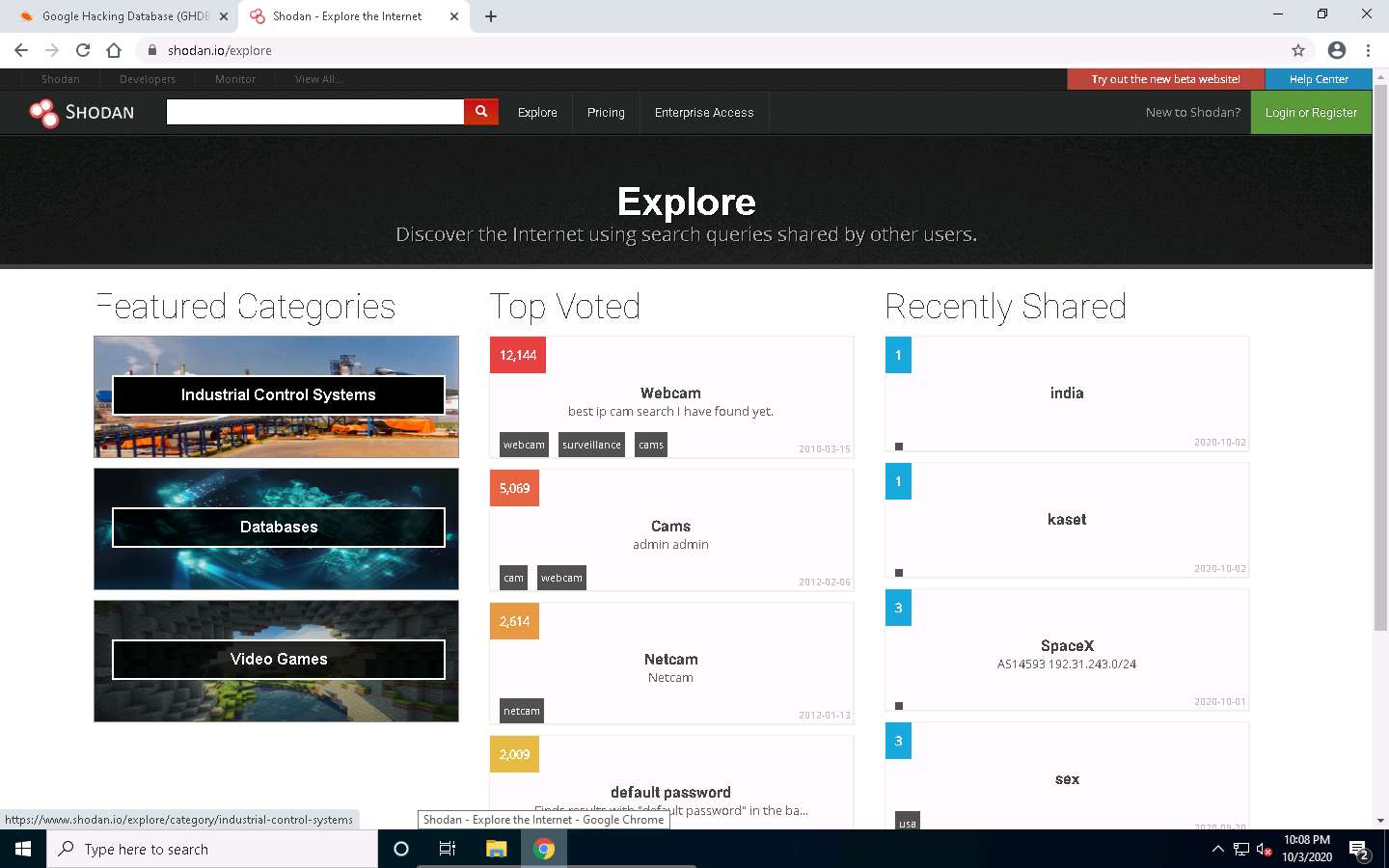
If Can You Chip In? option appears, click **X** (close) icon.



1. Next, review **Shodan**, a powerful search engine. In the browser, enter https://shodan.io.

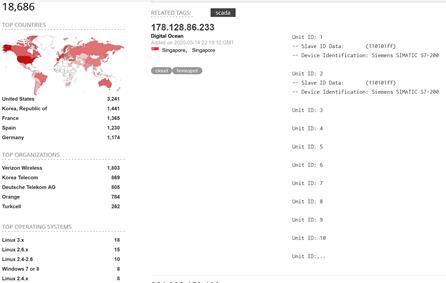


1. You will obtain the best results if you create an account, although you can still extract some data. Next to the search window, click **Explore**. In the menu, click **Industrial Control Systems**.

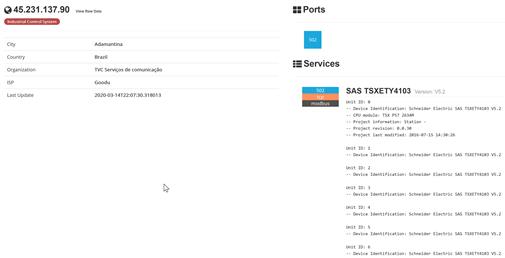


1. Scroll down and click **Explore Modbus**. This will result in an error, since you are not logged in. You may create an account or refer to the following screenshot that shows the results if you were logged in.

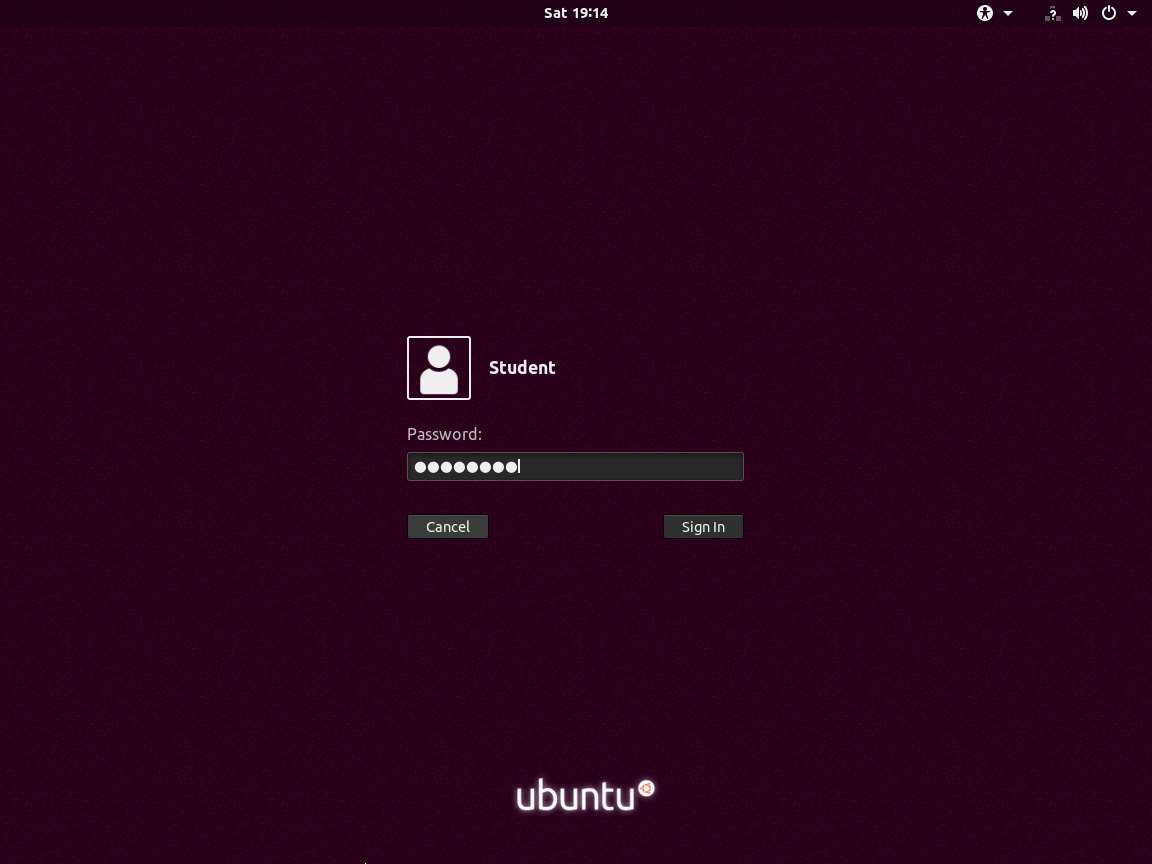




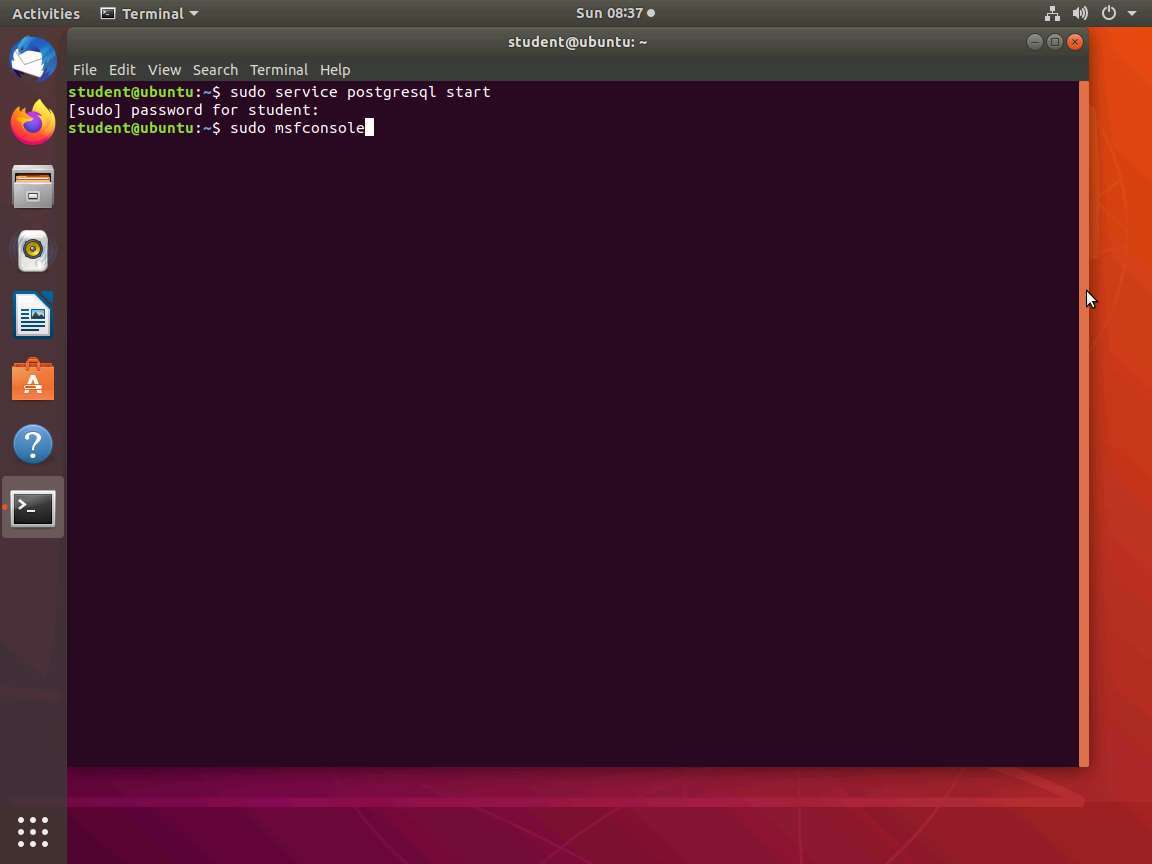
1. As shown, this is a suspected honeypot. However, you will have to explore it further to ascertain the suspicion. This requires written authorization, or you may be identified as a malicious hacker. An example from one of the sites from the search results is shown in the screenshot.



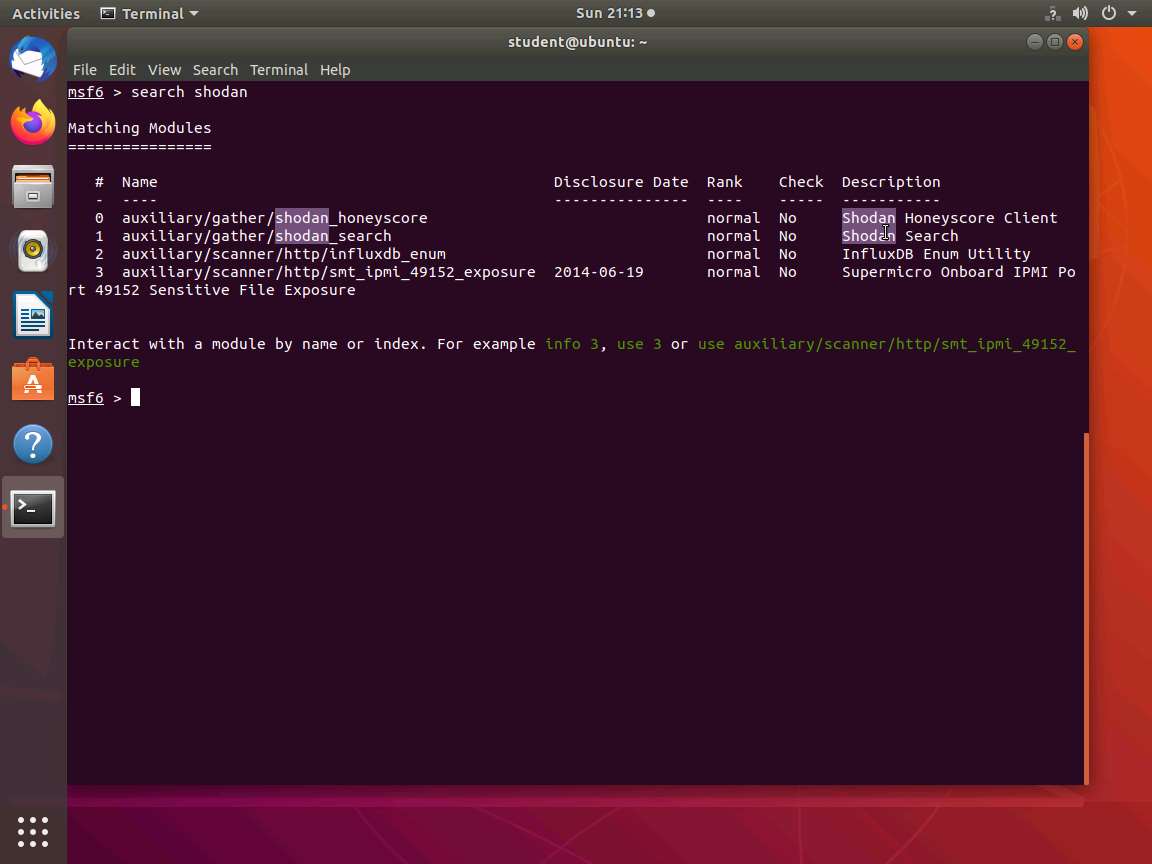
1. Extraction of the **Unit ID** here is a leakage that is invaluable to testers. There is only the one port that is open, port **502**, which is the port for the **ModBus** protocol. Additionally, when you review the data, this is the information from the registers and the device ID information.
2. Switch to [UbuntuWeb](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10) machine, click **Student** profile and type the **password** in Password field and press **Enter**.

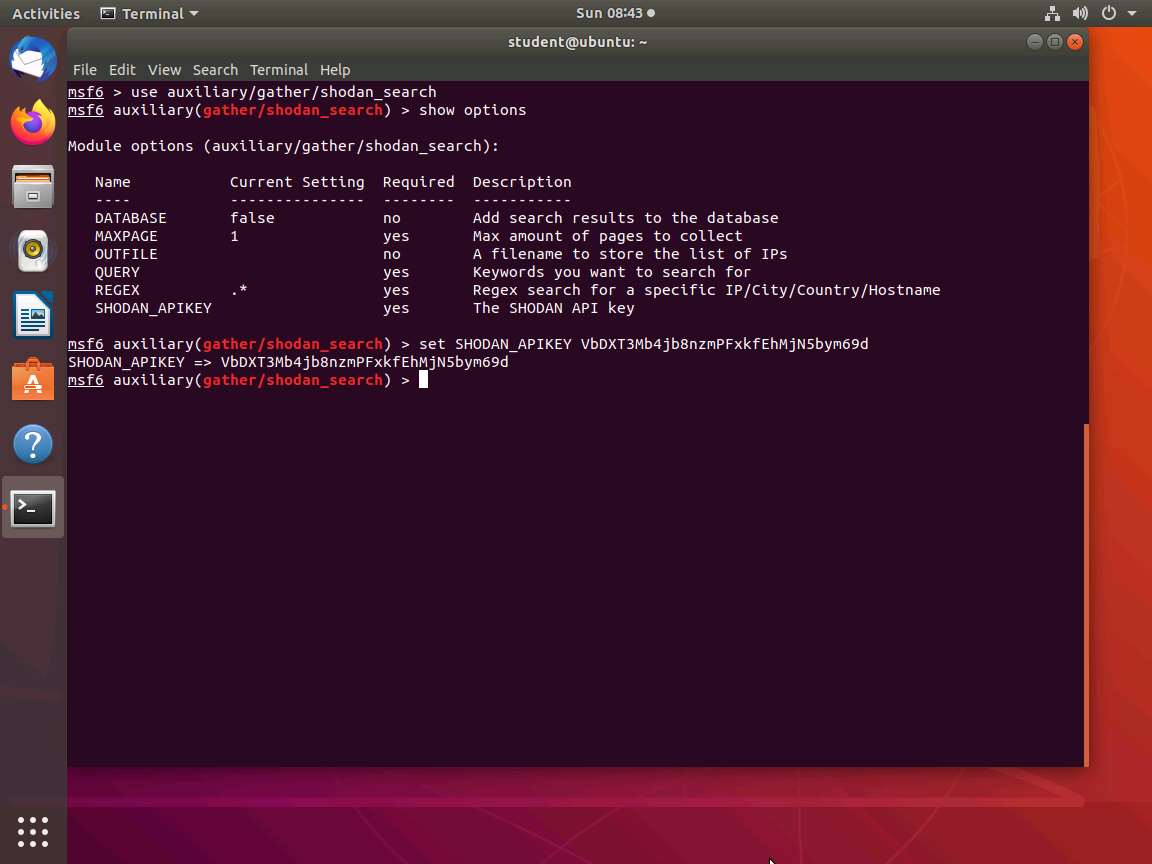


1. Within the **Metasploit** framework, there is a module for **Shodan**. Once you are logged in, open a **terminal** window and type **sudo service postgresql start** and press **Enter**, type **password** and press **Enter** to attain root privileges. Then, type **sudo msfconsole** and press **Enter** to start the Metasploit framework.

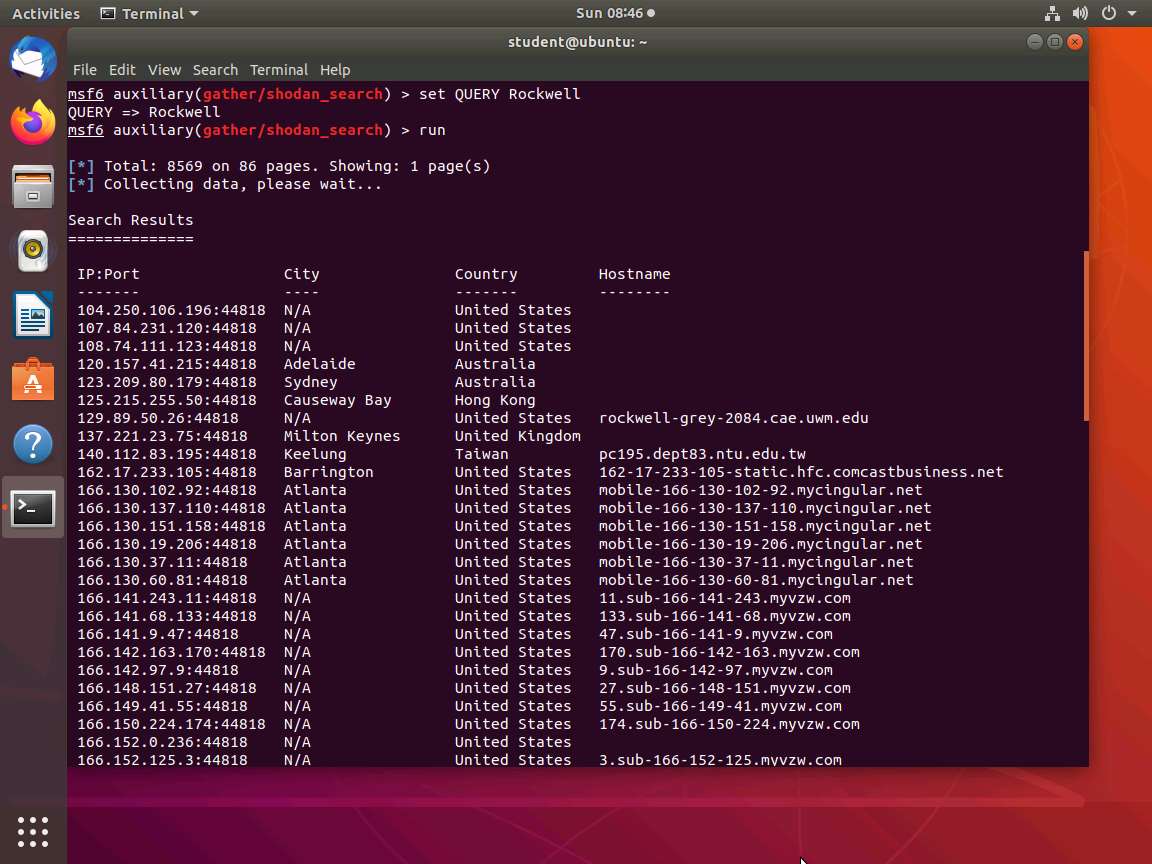


1. The module can be found by entering a search for **Shodan**. The results of the search will show an **auxiliary scanning module** for the tool, but you will need to load an application programming interface (API). An example of the query you can construct once you have an API key is shown in the screenshot.





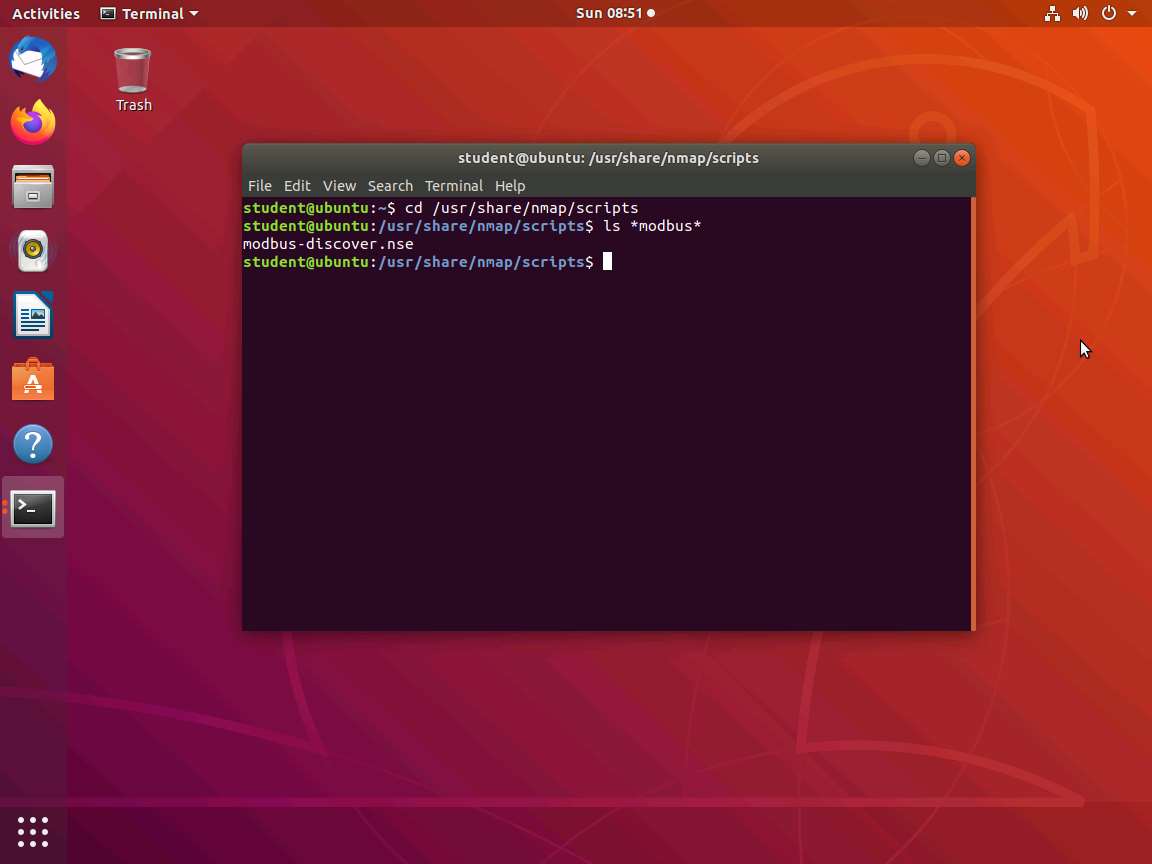
1. Next, set the **QUERY** option. For the example here, use the query for **Rockwell** systems, and then type **run** and press **Enter** as shown in the screenshot. To use the module, register for an API with Shodan, although you may want to consider this for your testing engagements. **Close** the **msfconsole**.



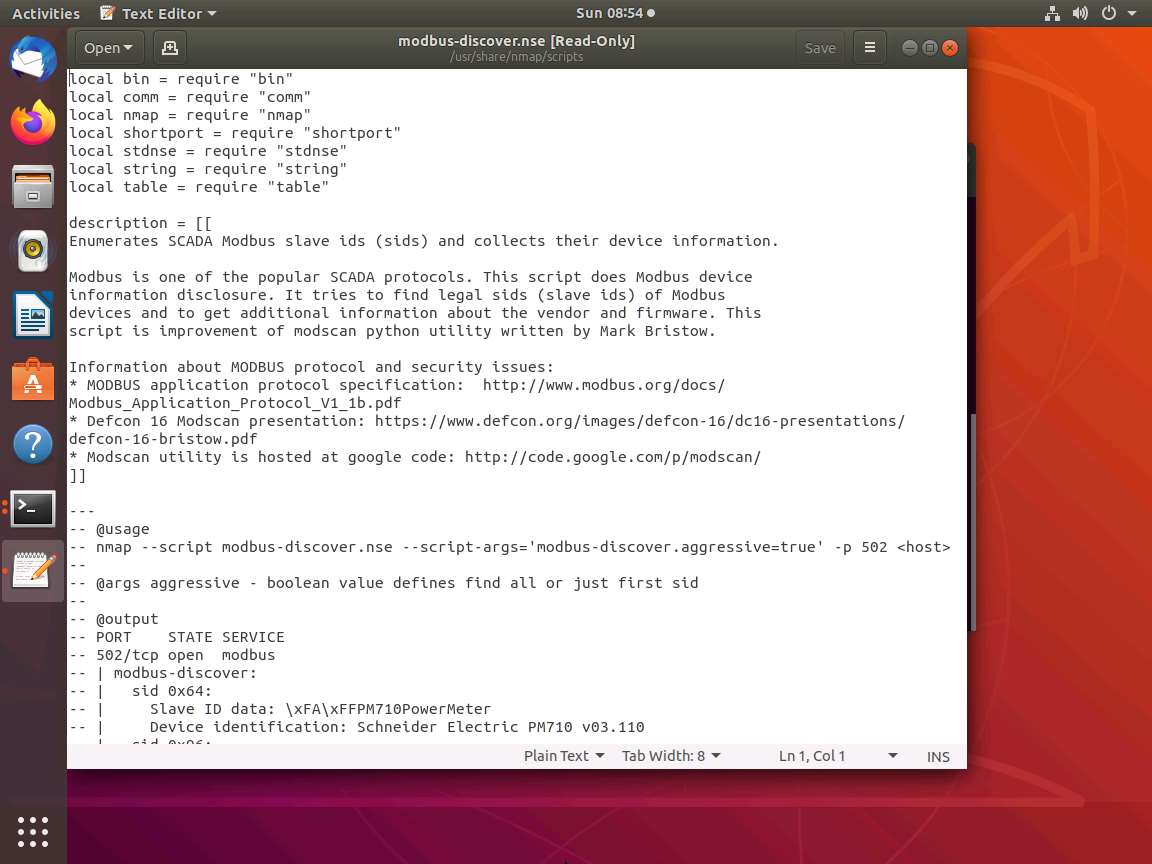
1. Now, right-click on **Terminal** icon from the **Favorites** bar and click **New Terminal**.



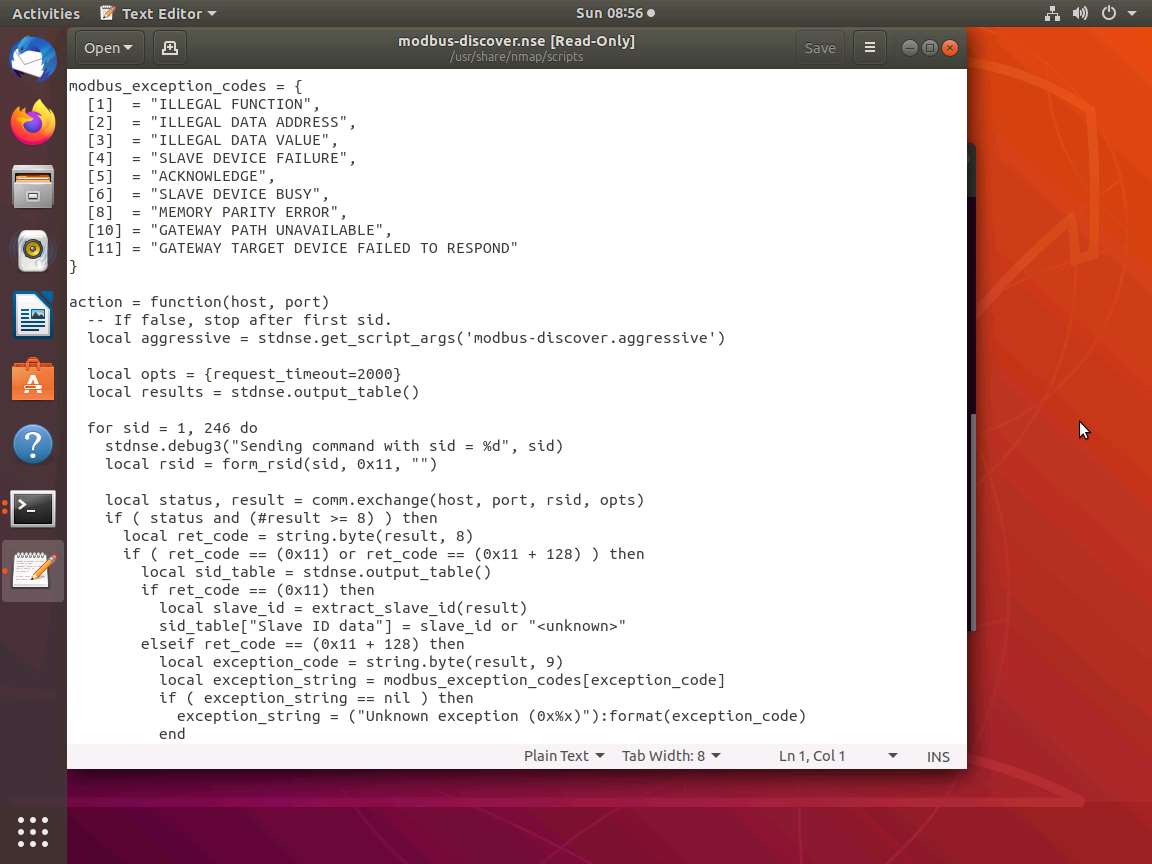
1. The Nmap also has engine scripts for **SCADA**. type **cd /usr/share/nmap/scripts** and press **Enter**. Once you are in the folder, type the command as shown in the screenshot and press **Enter**.



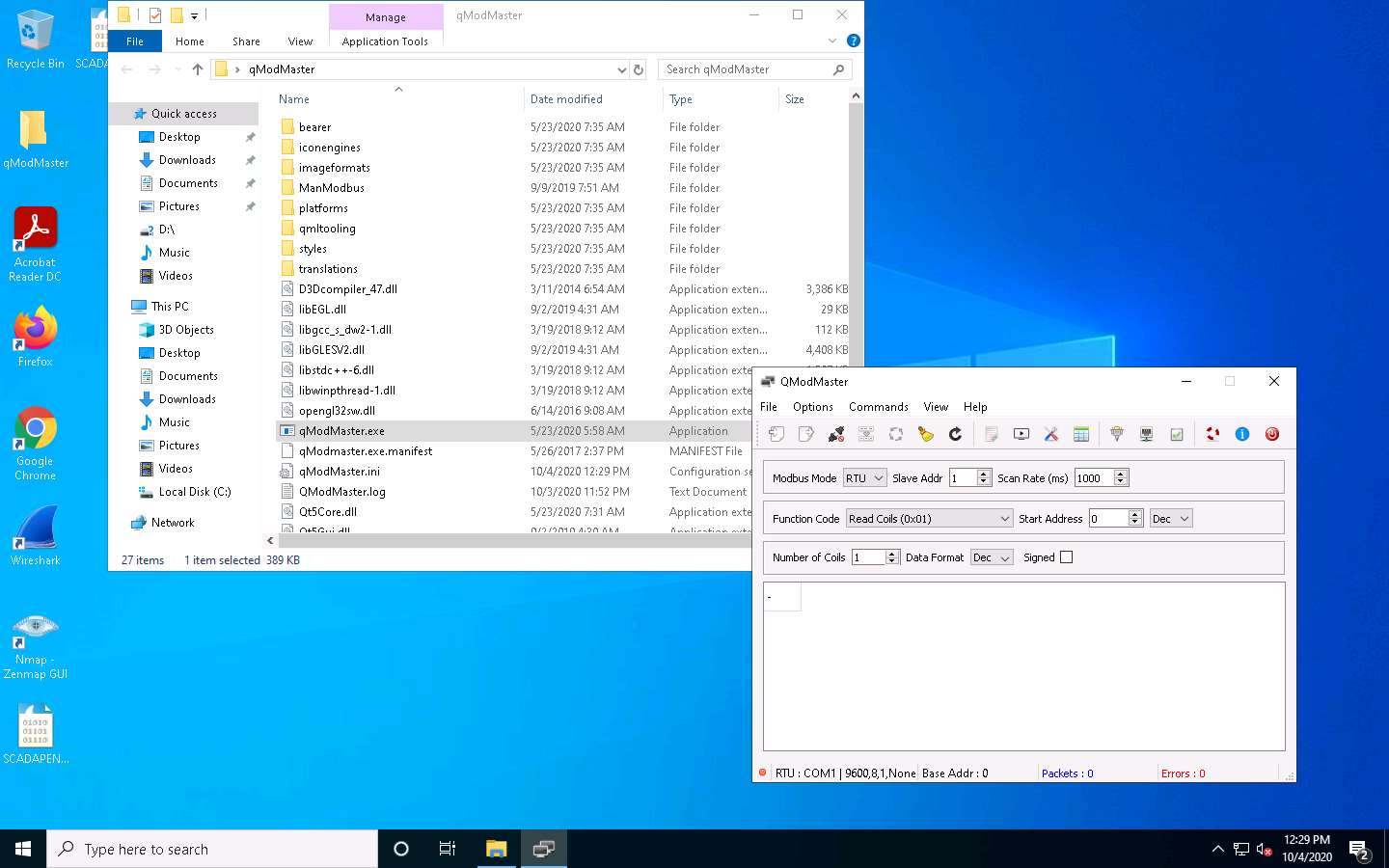
1. Open the **modbus script** in the editor of your choice and review it. An example of the contents of the script is shown in the screenshot.



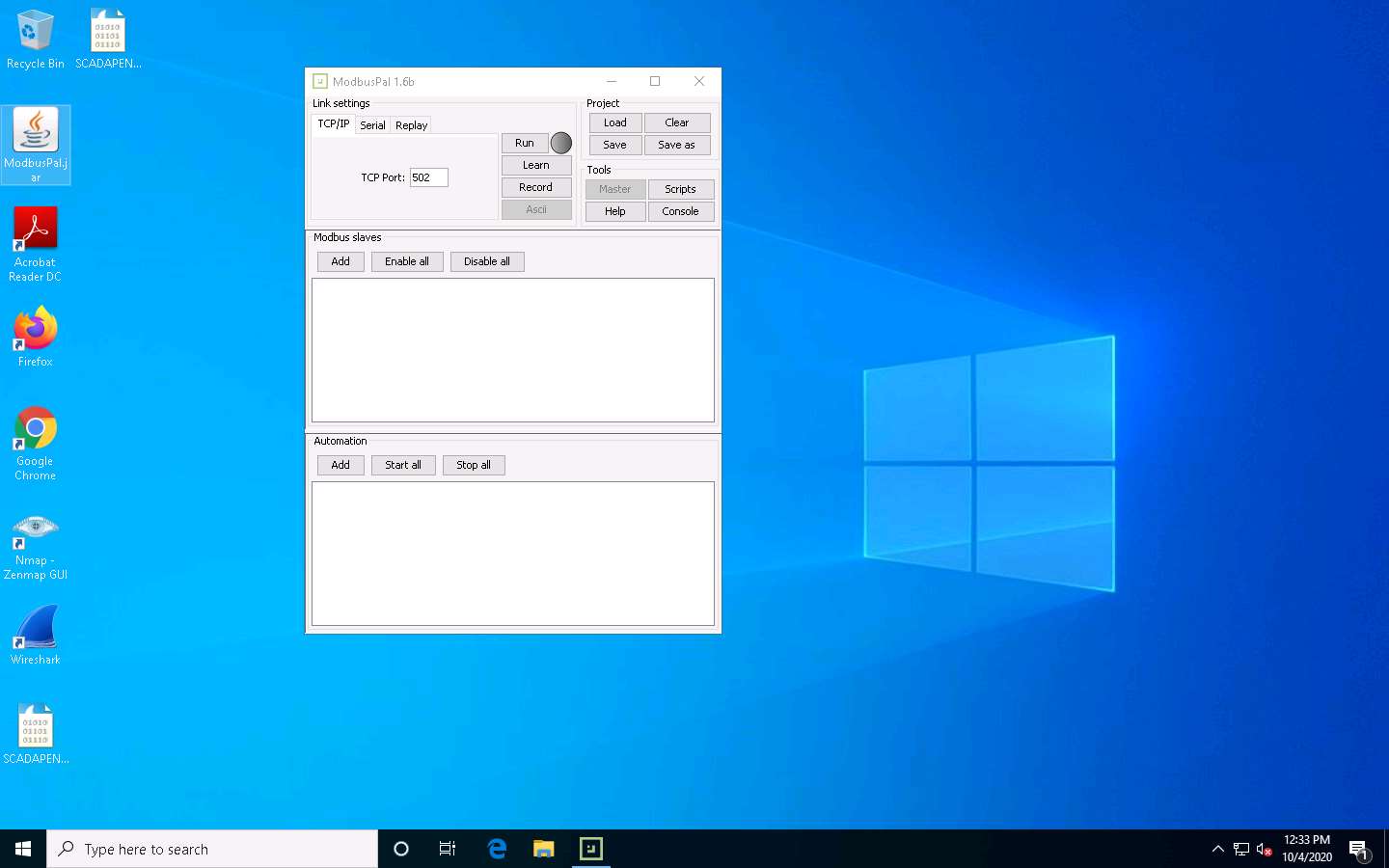
1. Carefully review the working of the scripts; you may create this for your own testing script as well. These scripts are usually well documented, so you can review and understand them without too many problems. Located at the bottom of the script, you will see the function codes that we have shown earlier. **Close** the text editor window once you reviewed the file.



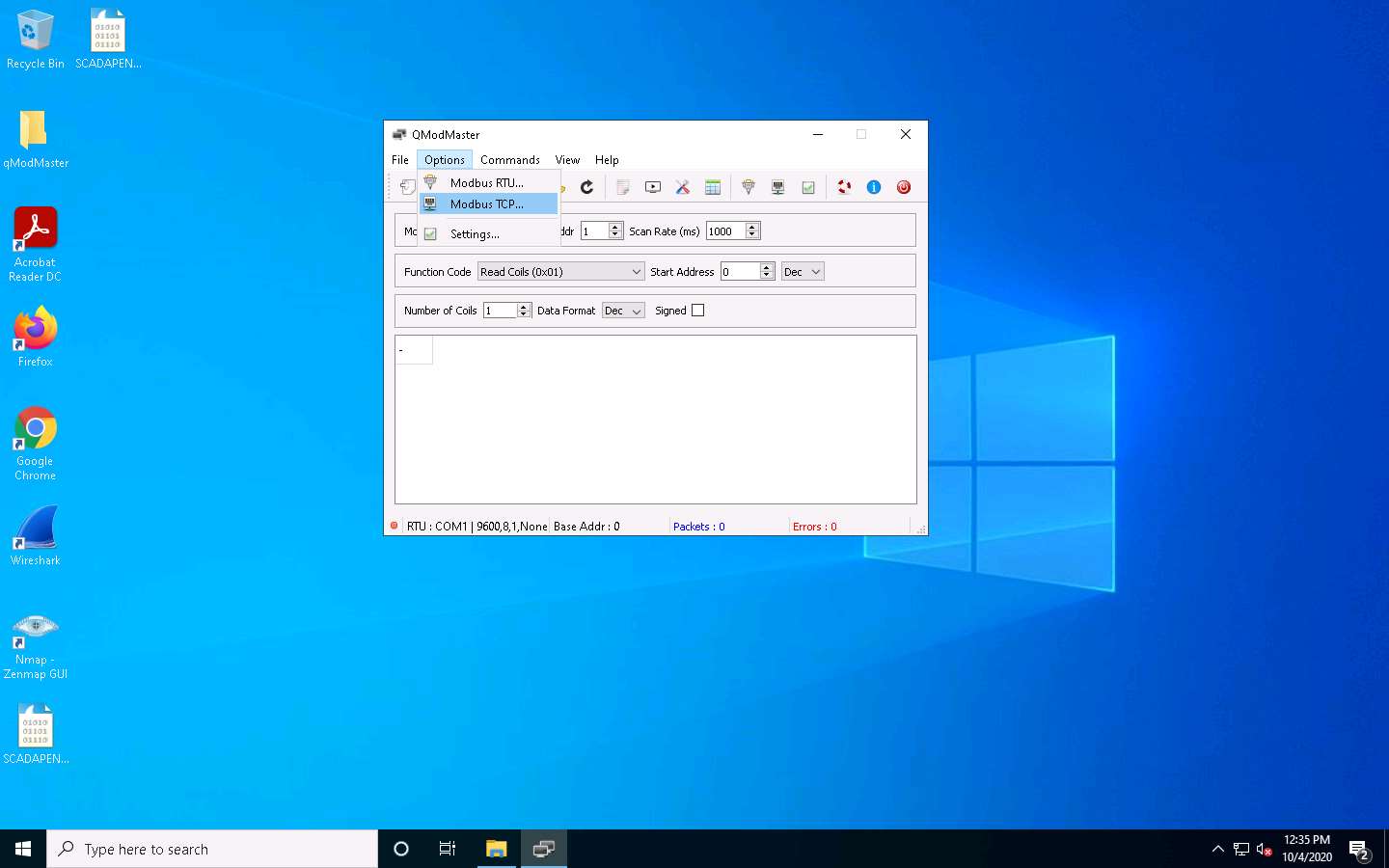
1. Since you have a script, begin testing it. This requires communication with the **Modbus** protocol, the two **SCADA Master** and **SCADA Slave**.
2. Switch to [SCADA Master](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10), and login to the machine with the Password as **Pa$$w0rd**. Double-click **qModMaster** folder on the **Desktop**. In the qModMaster folder, double-click **qModMaster.exe** to launch the application. **QModMaster** main window appears as shown in the screenshot.



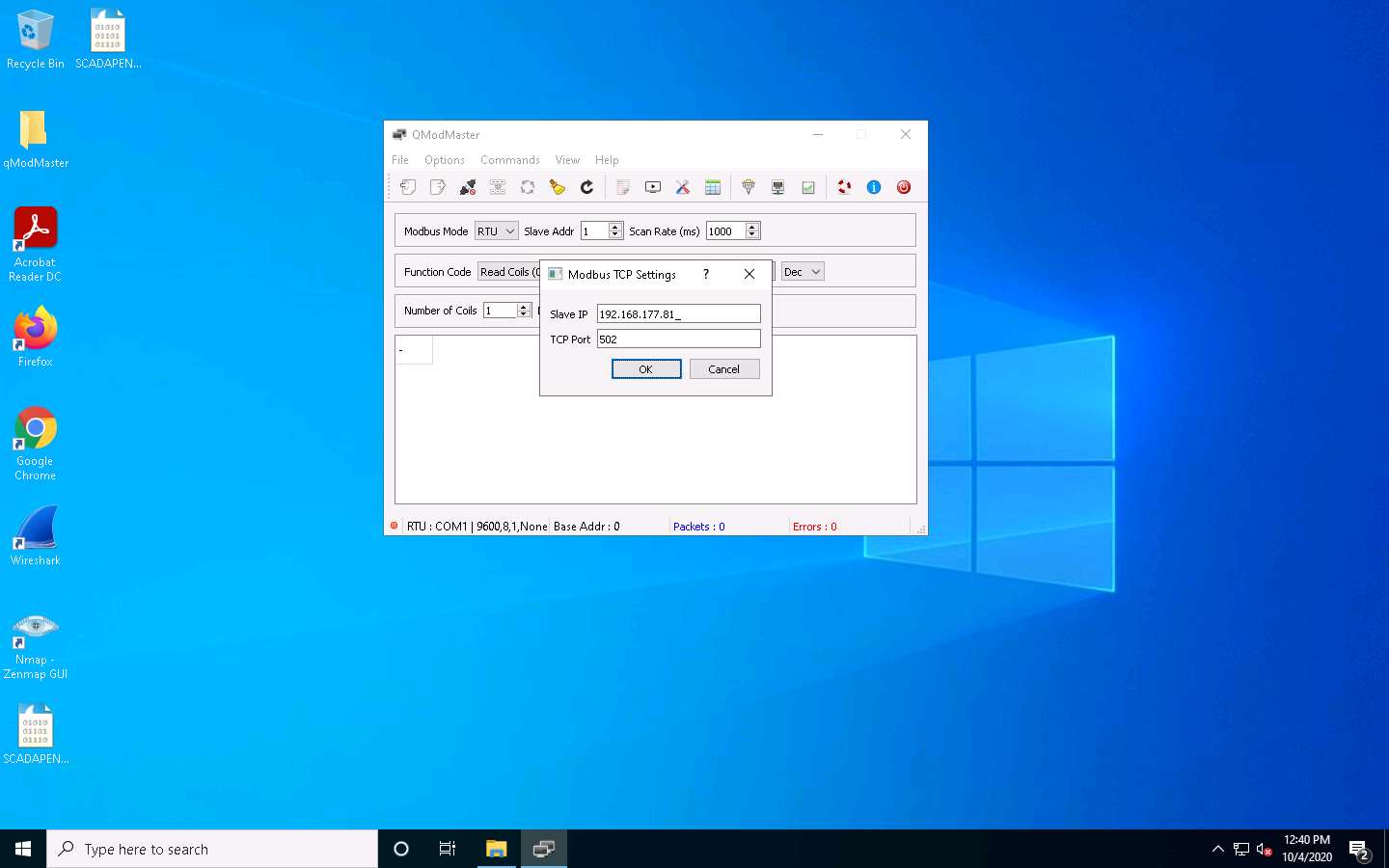
1. Switch to [SCADA Slave](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10), and login to the machine with the Password as **Pa$$w0rd**. Double-click **ModBus-Pal.jar** file on the desktop. **Modbus-Pal** main window appears as shown in the screenshot.



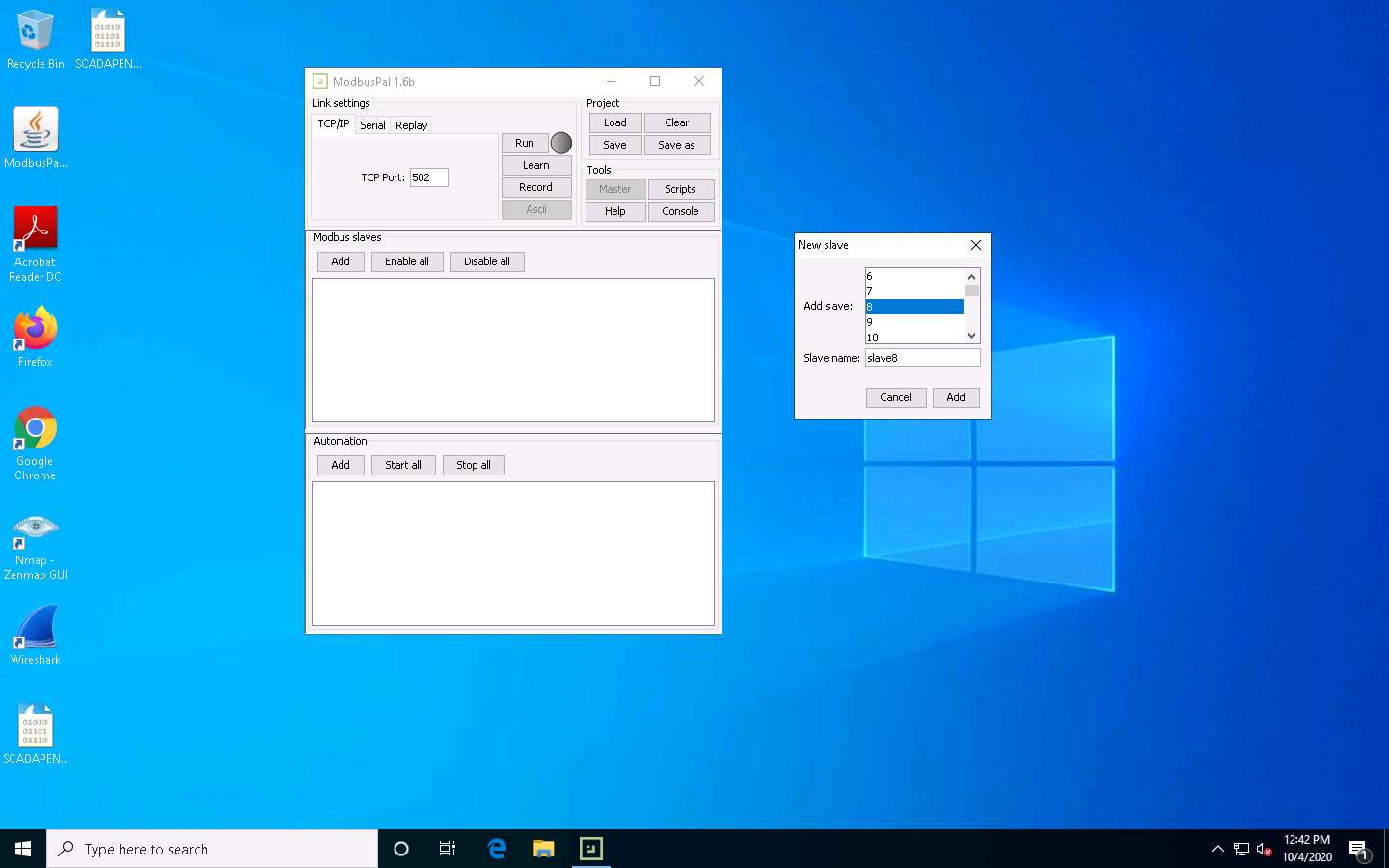
1. Next, populate the simulator with data values. To begin, configure these simulators to run in **TCP** mode. **Modbus** was originally designed to run over a **serial connection** and this simulator is capable of using the **TCP** or serial. Ensure that both are operating on port **502**. Switch to [SCADA Master](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10). In **QModMaster** window click **Options** tab. In the drop-down menu, select **Modbus TCP…**.



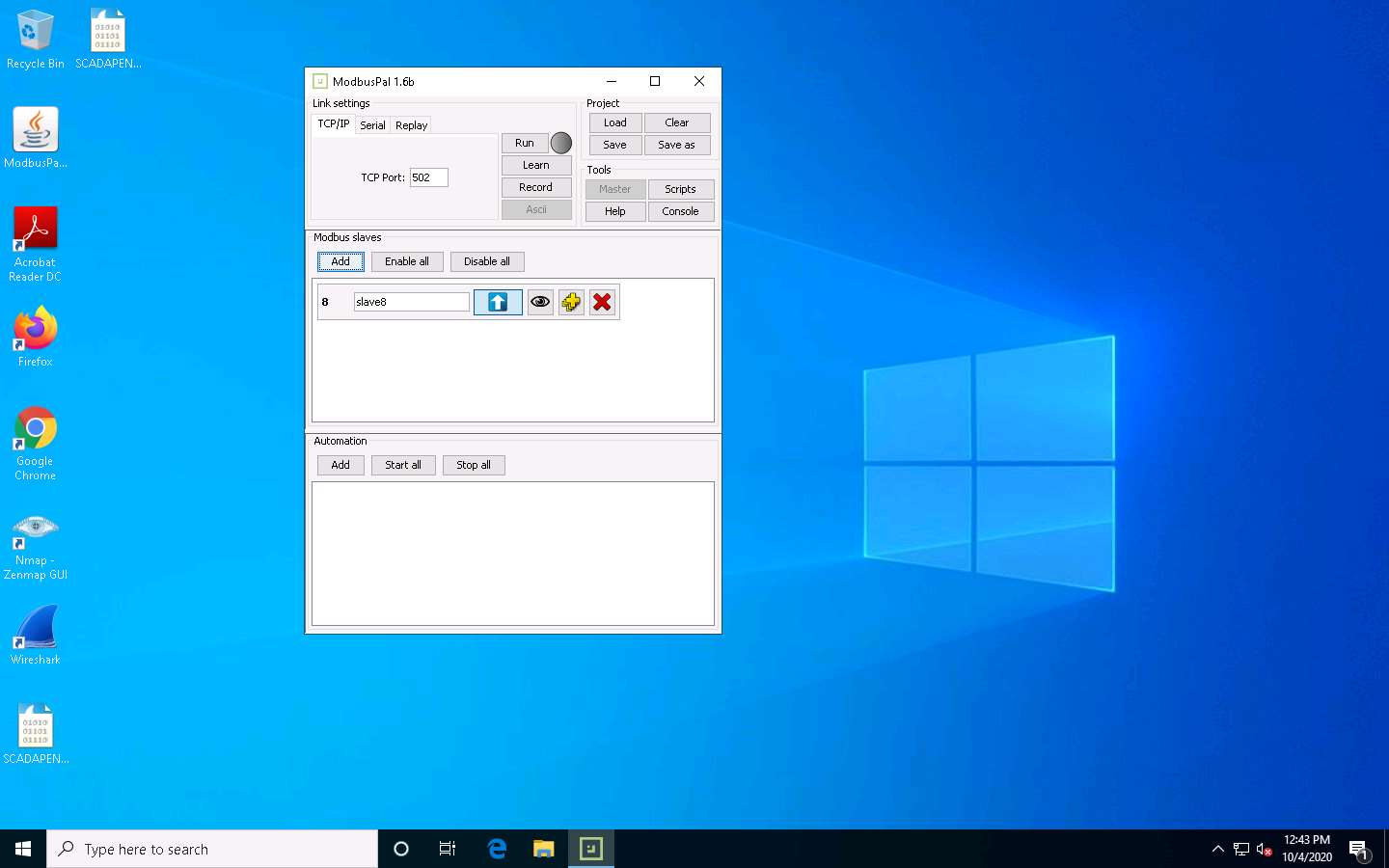
1. A pop-up window appears, which will help you configure the **Slave IP** and **TCP Port**. Change the IP address to the address of the **SCADA Slave** machine. The IP address of the SCADA Slave machine is **192.168.177.81**. Leave the **TCP Port** to default i.e., **502**, and click **OK**.



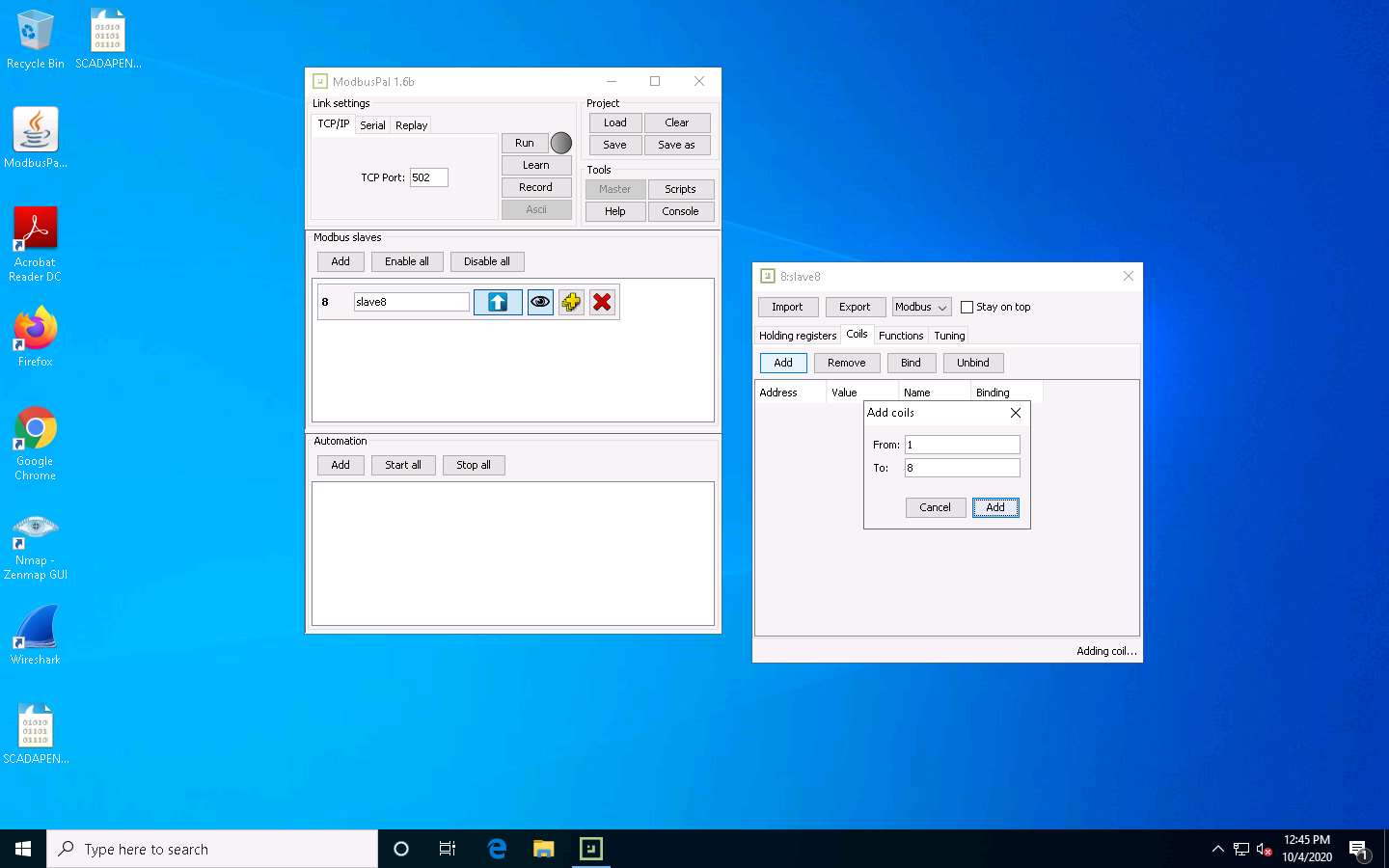
1. Switch to [SCADA Slave](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10) machine. Then, add the **slaves** under **Modbus slaves** section. For this demonstration, add **8** slaves. Click **Add** button and scroll down; select the number **8** and enter the name **slave8**, and then click **Add**.



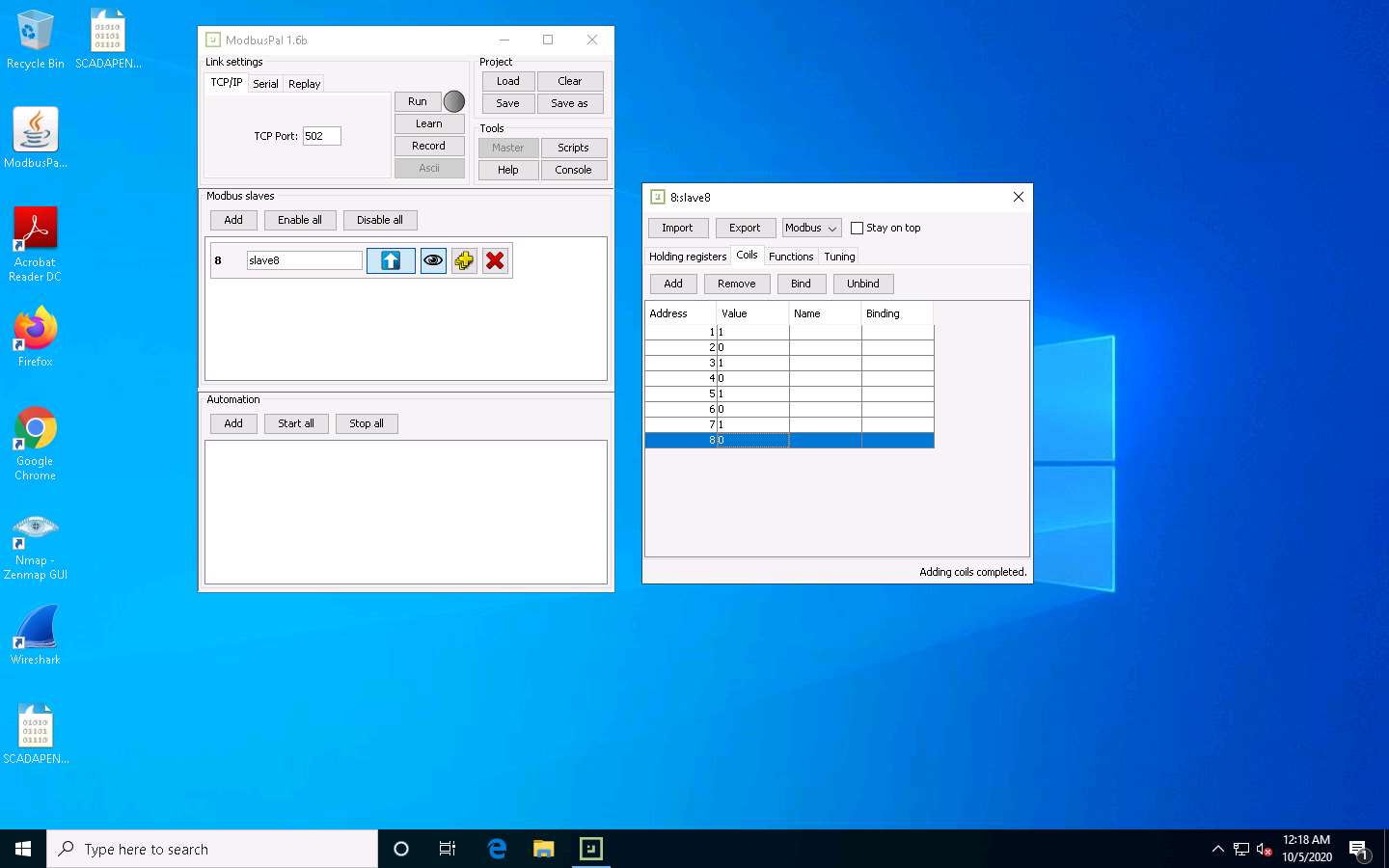
1. Next, click on the **eye** icon.



1. This will bring up the menu for setting the **coils** and adding the values to the **registers**. Click on the **Coils** tab, and then on **Add**. Enter From **1** to: and enter **8** coils, as shown in the screenshot.



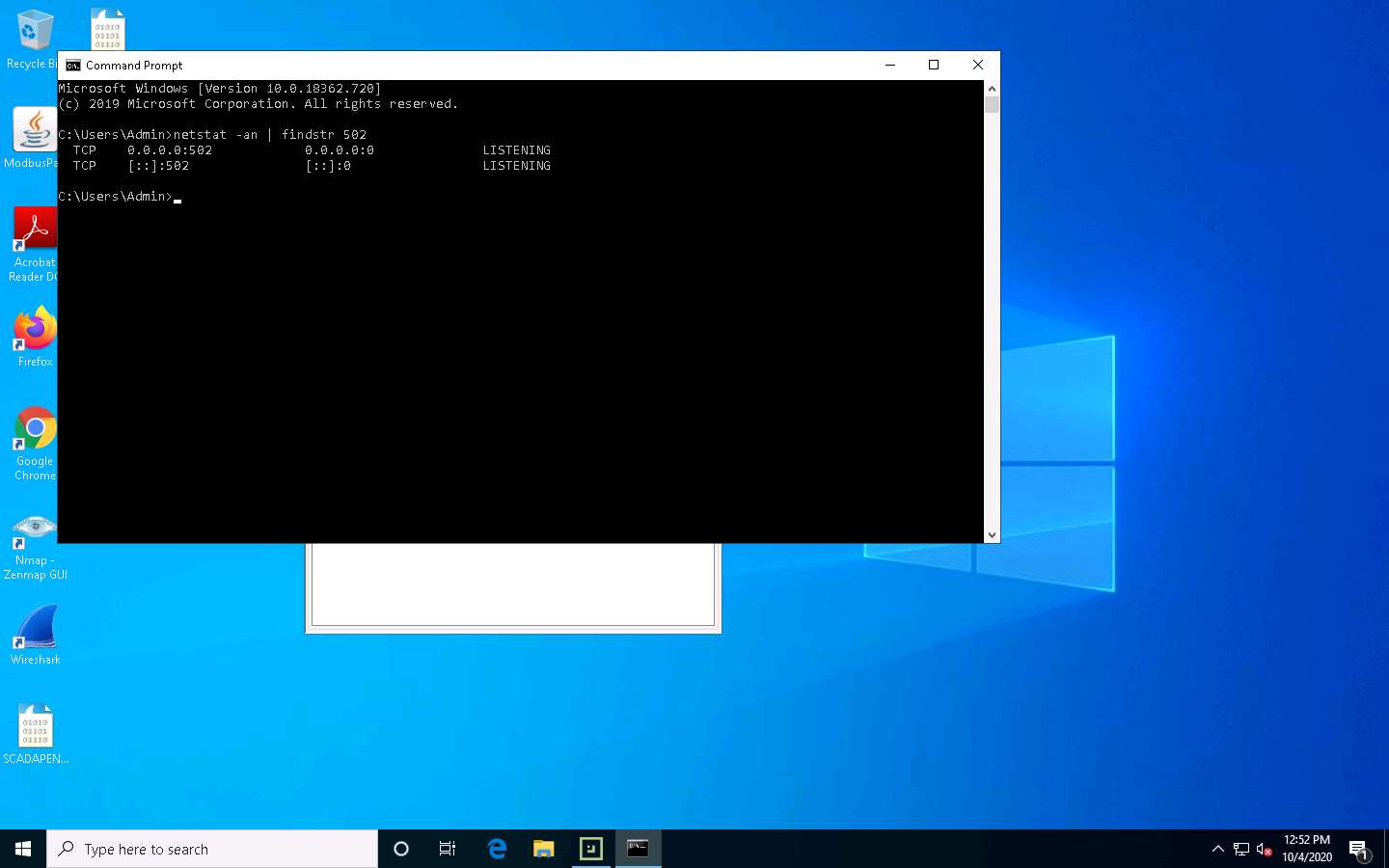
1. Once the **Coils** are added, **change the values** as shown in the screenshot. Once you have entered the values, close the window.



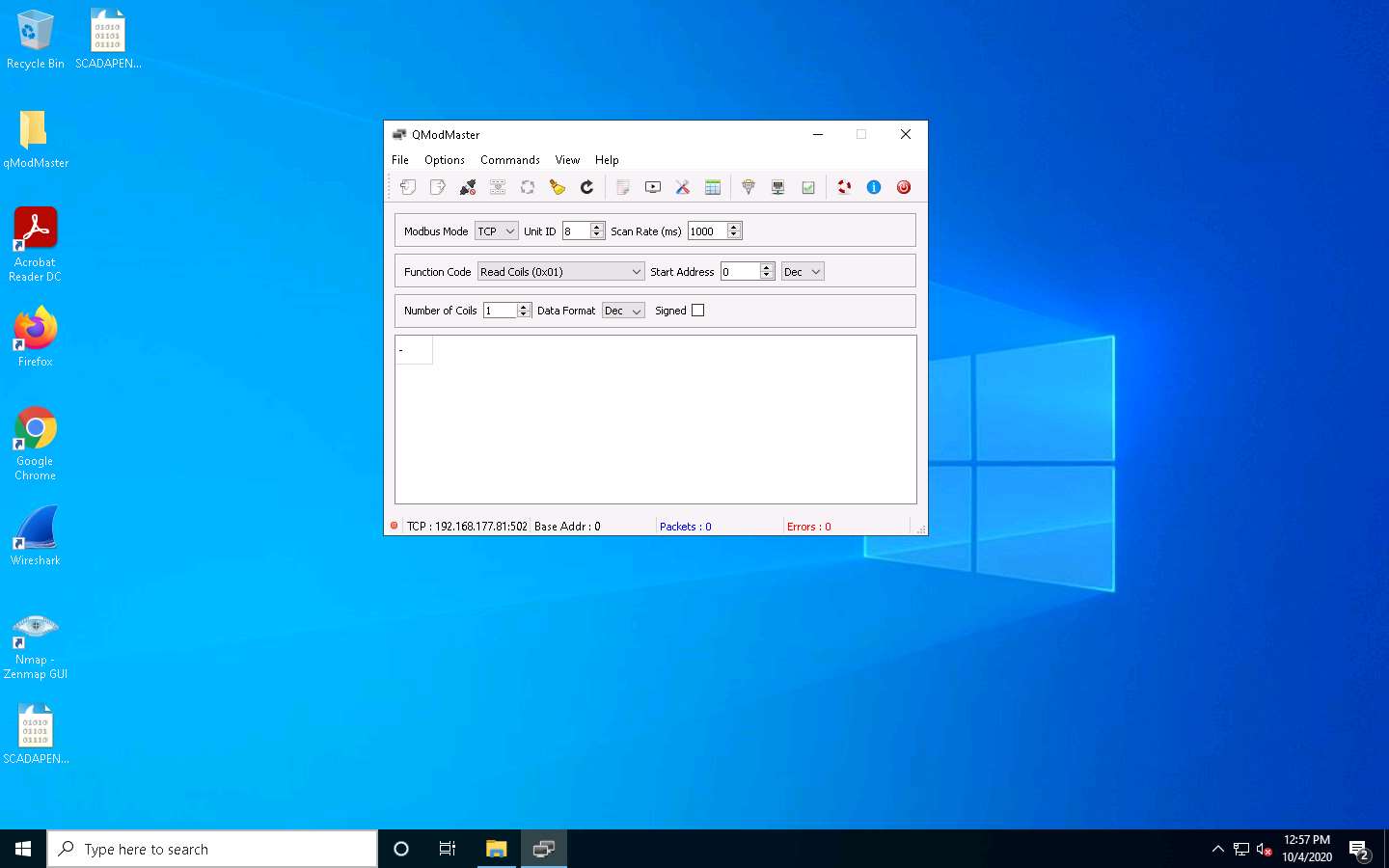
1. Click **Run** on the ModbusPal window. If you receive a firewall prompt, **allow access**. Consider disabling the firewall if you have any problems with the lab.



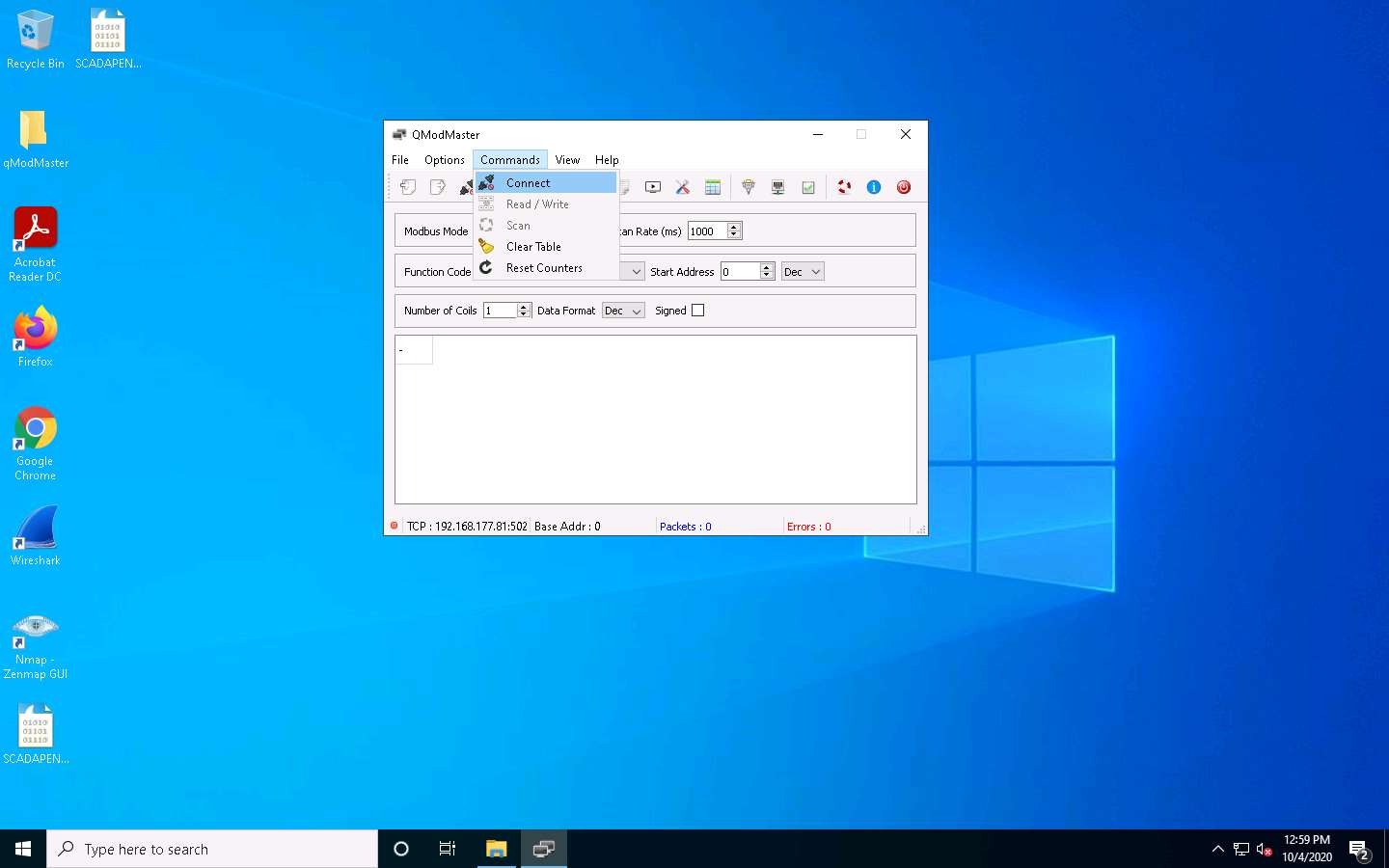
1. To verify the slave has started, open Command prompt and type **netstat -an | findstr 502** and **Enter**; the port should be listening, as shown in the screenshot. **Close** the Command Prompt window.



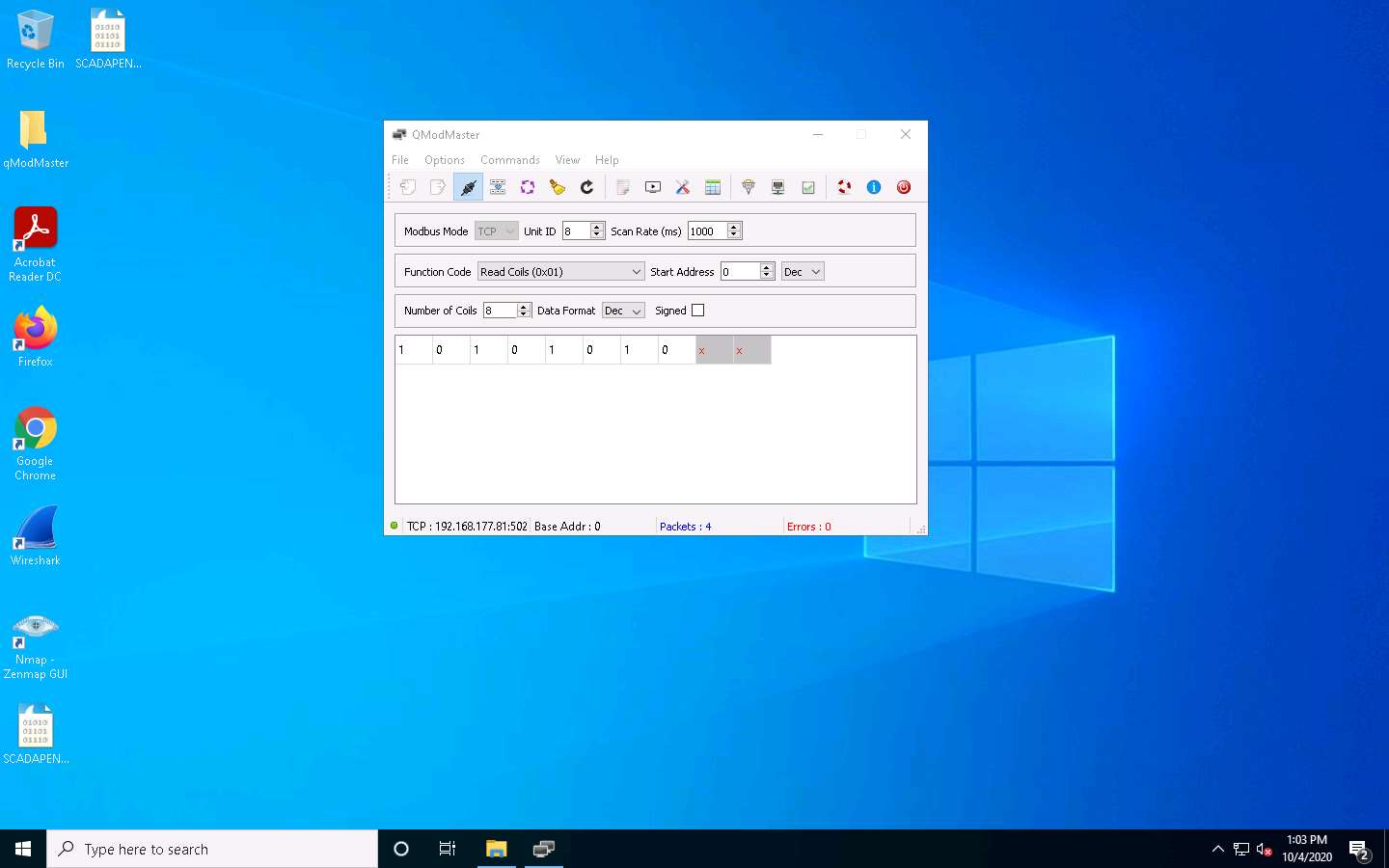
1. Switch to [SCADA Master](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10) and select **TCP** under **Modbus Mode** and set **Unit ID** to **8**. Set the **Number of Coils** to **8** as shown in the screenshot.



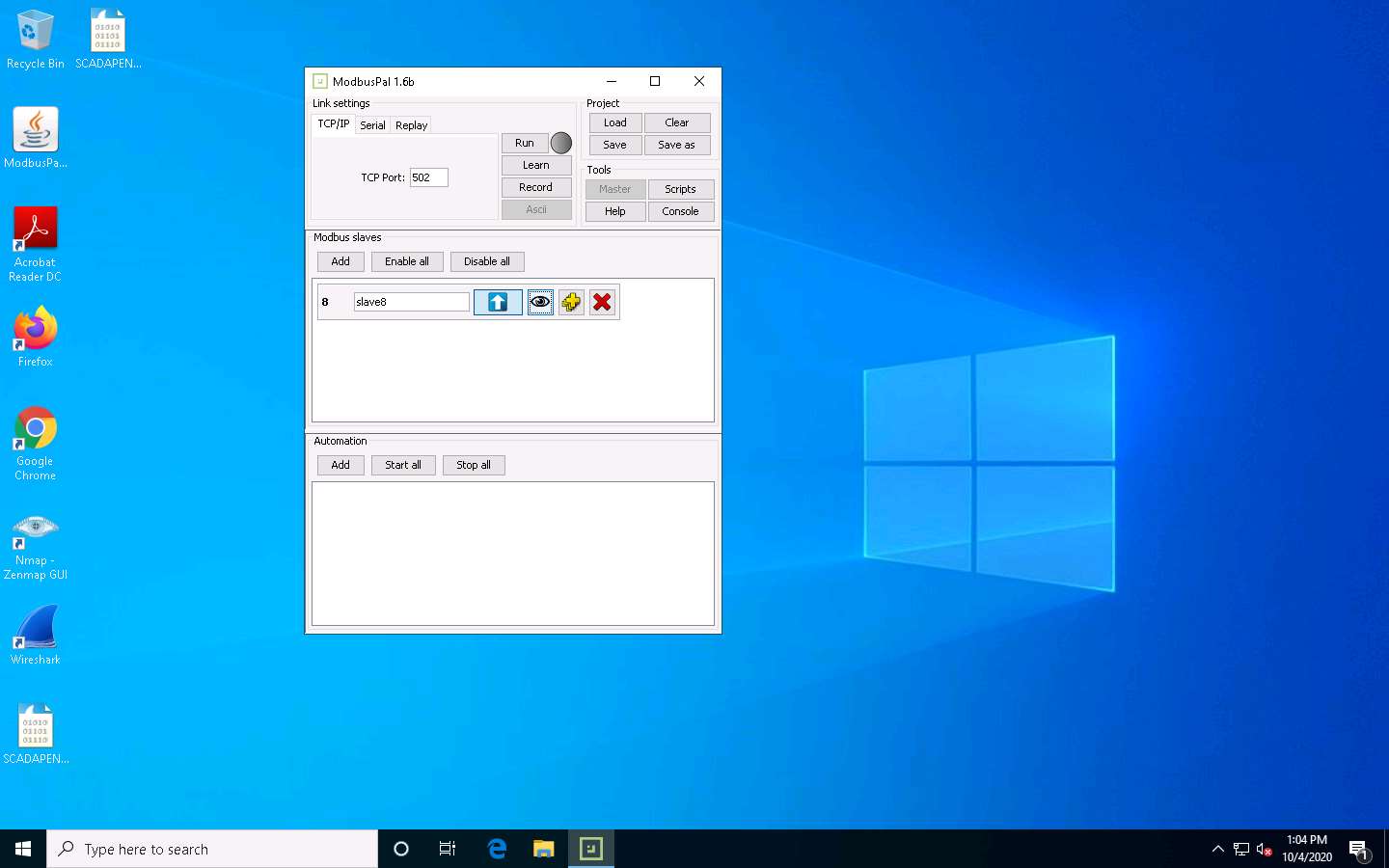
1. Finally, click **Connect** icon or choose **Connect** option from the **Commands** menu at the left of the top menu.



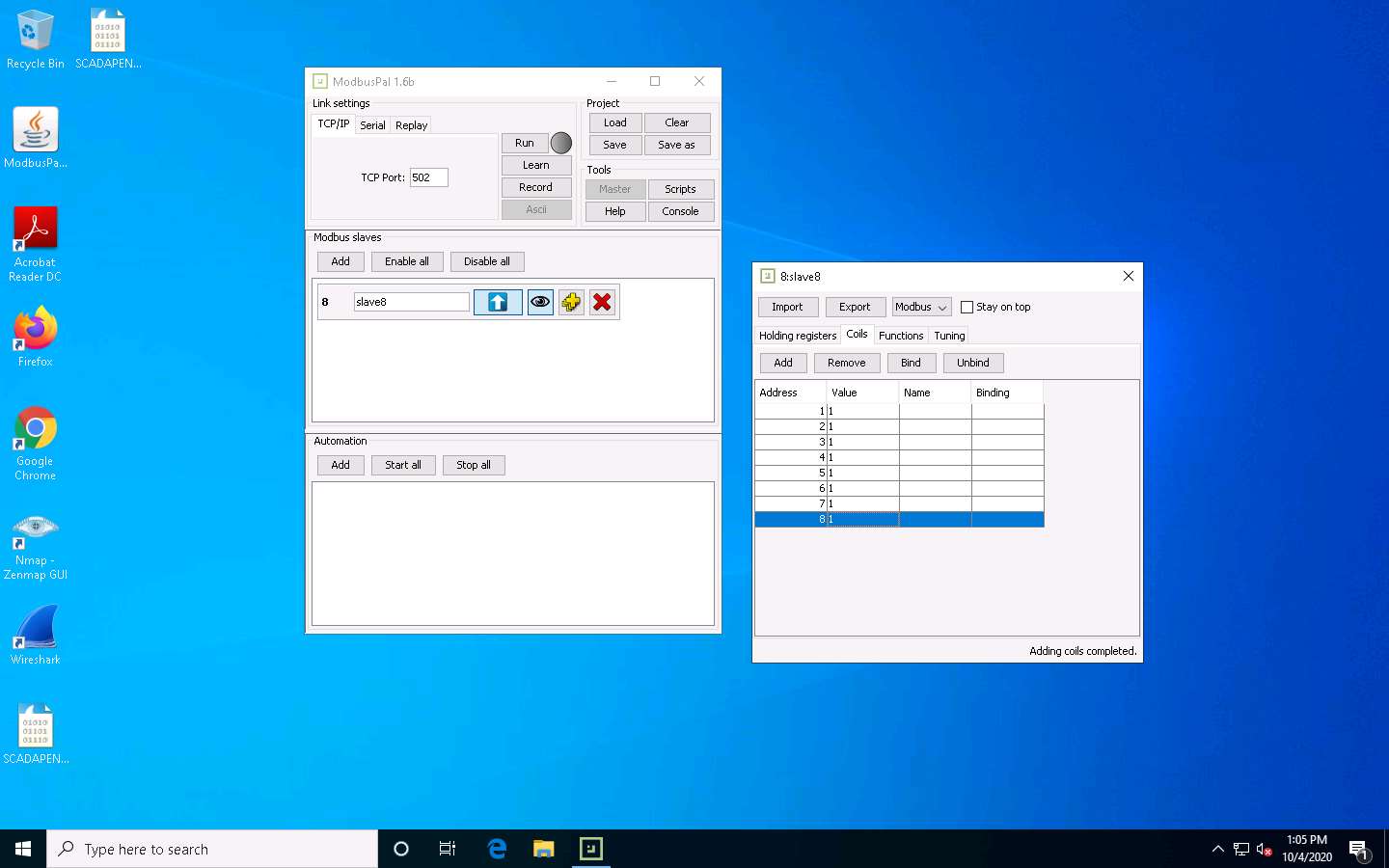
1. Next, you must read the coils. Click **Read / Write** icon next to the **Connect** icon.



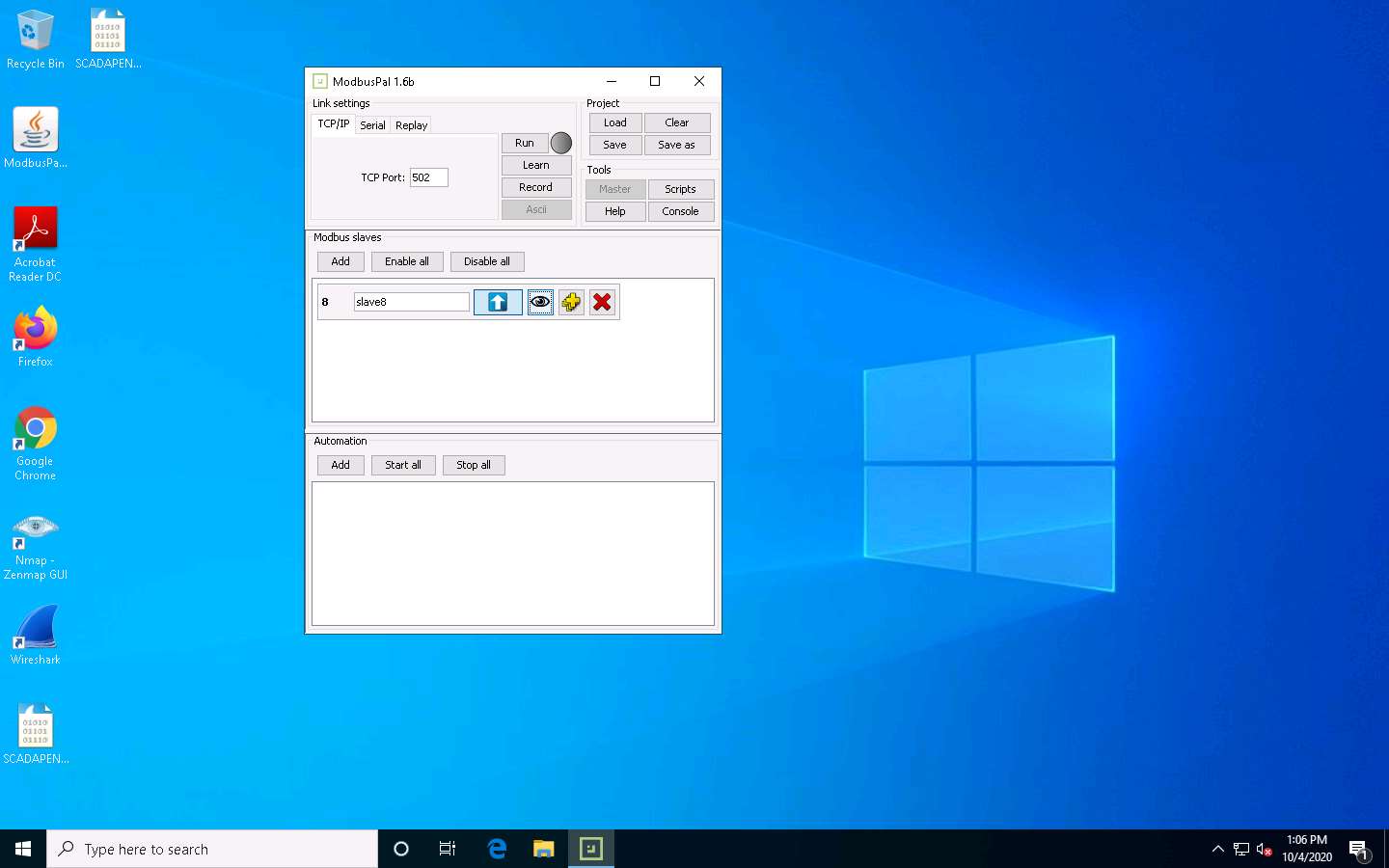
1. Switch to [SCADA Slave](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10) machine, click **Run** to stop the ModbusPal, and then click **eye** icon in the **Modbus slaves** section.



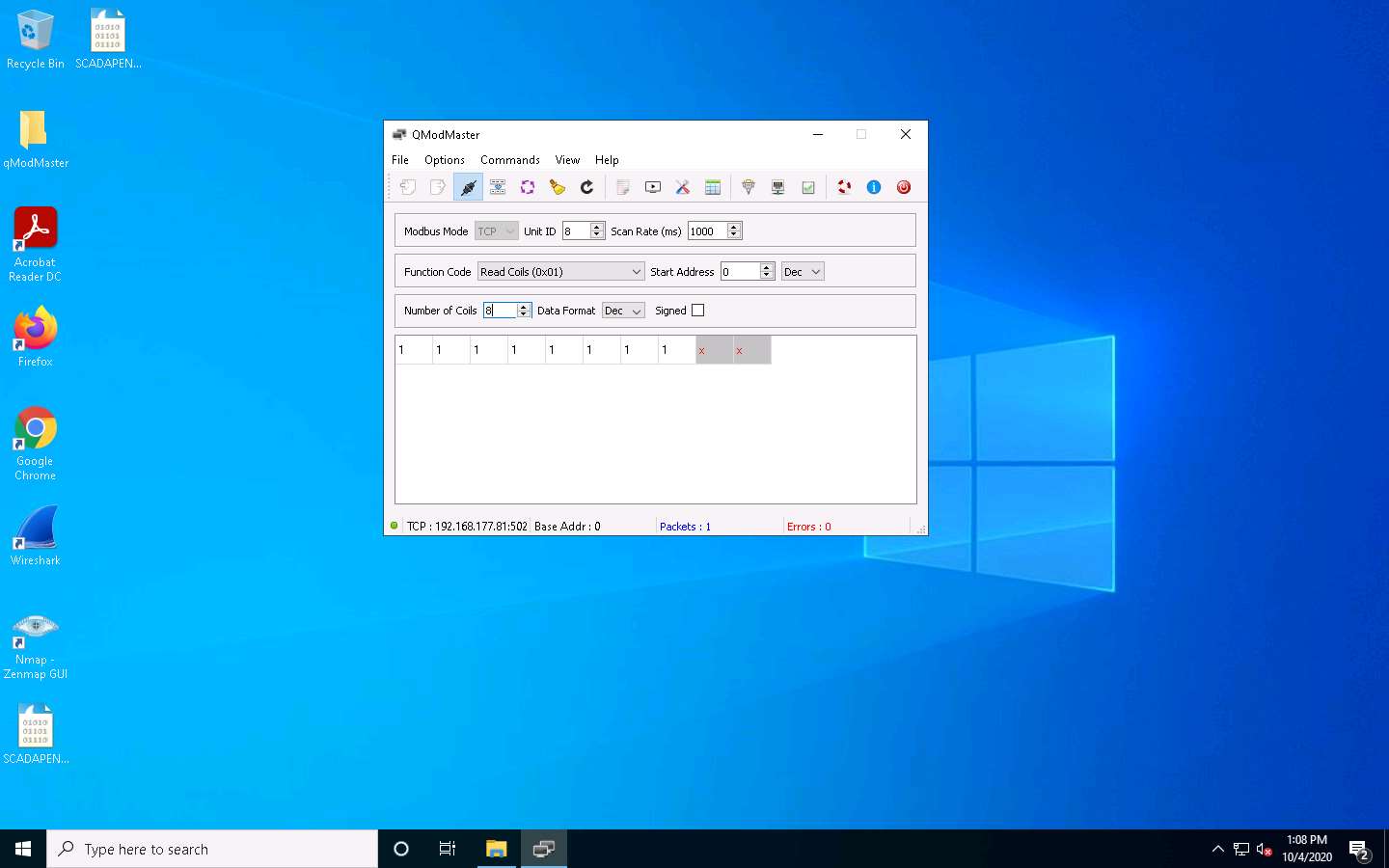
1. Edit the values of **slave8** as shown in the screenshot and then close the window.



1. Click **Run** to start the ModbusPal.

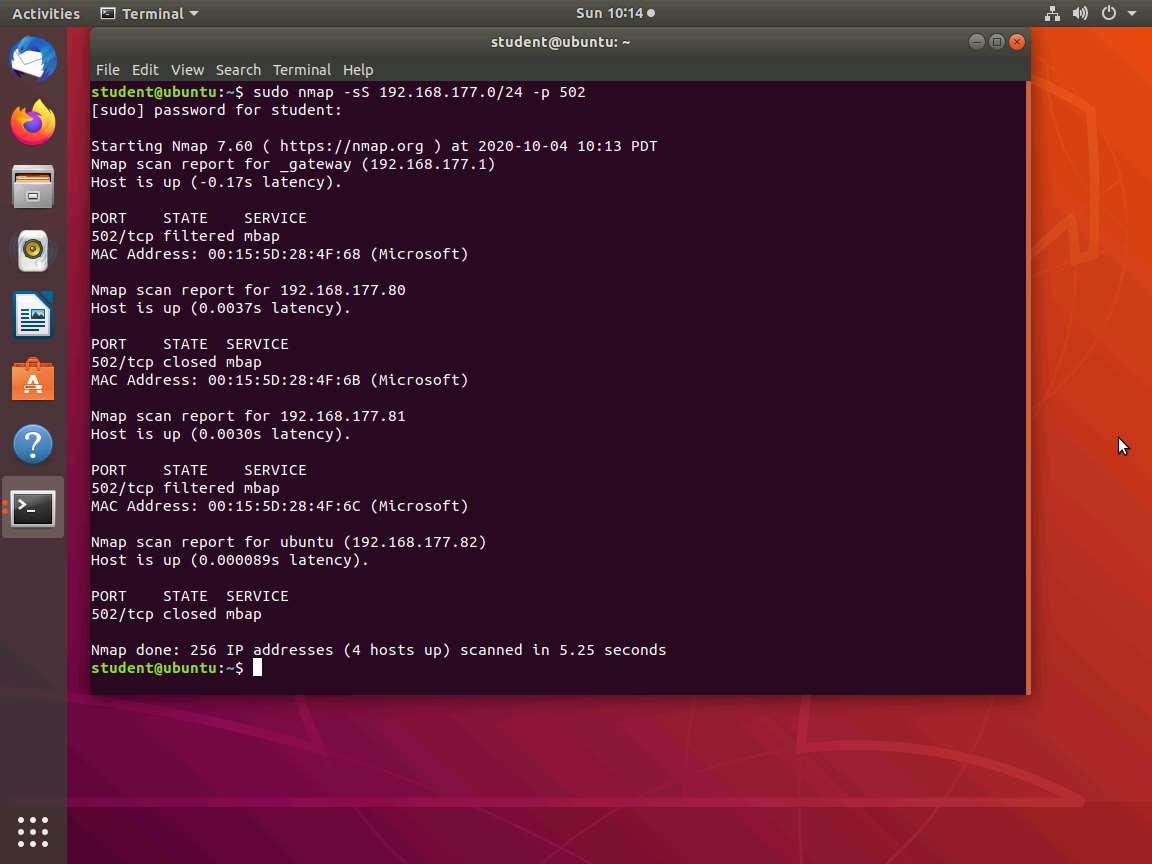


1. Switch to [SCADA Master](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10). Click **Connect** icon to **Disconnect** the connection and then click **Connect** icon to **reconnect**. Click **Read / Write** icon next to the **Connect** icon. The master should be updated with the new values, as shown in the screenshot.



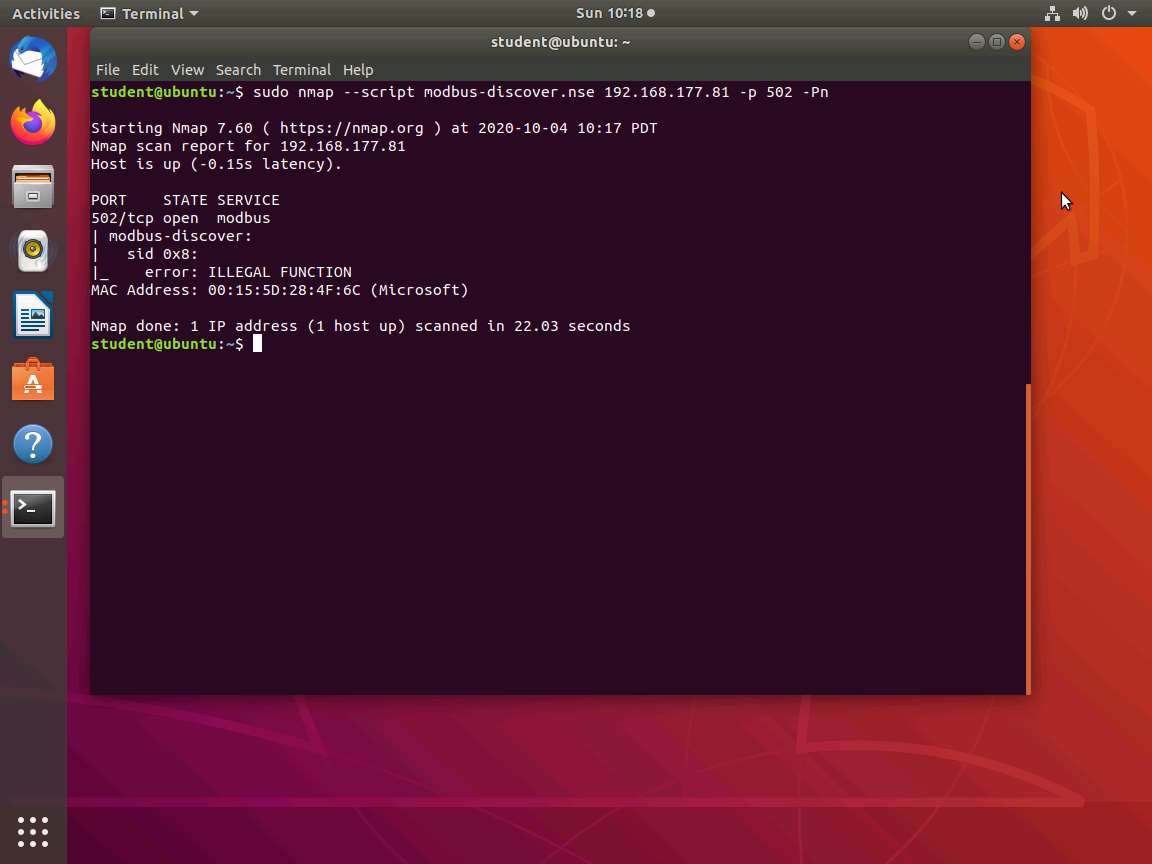
1. Note that the master reads from **0**, although the register starts at **1**. In the master, the first 0 address will not be visible. This is quite common to encounter. You now have a working **Master** and **Slave** Modbus connection. This **ModBus simulator** demonstrates the basics of the **communication between** the ModBus master and slave. Although you only used some functions, this simulator is capable of nearly all ModBus functions. Thus, you are encouraged to explore it in case you add additional steps to your penetration testing methodology.
2. Switch to [UbuntuWeb](https://labclient.labondemand.com/Instructions/f213e2c3-c5a7-47dc-a7af-efba687edcf4?rc=10) machine, launch a terminal from the **Favourites** bar, and in the terminal type **sudo nmap -sS 192.168.177.0/24 -p 502** and press **Enter**, type **password** and press **Enter** to attain the root privileges.

If the machine is locked move your mouse cursor in upward direction and then login.

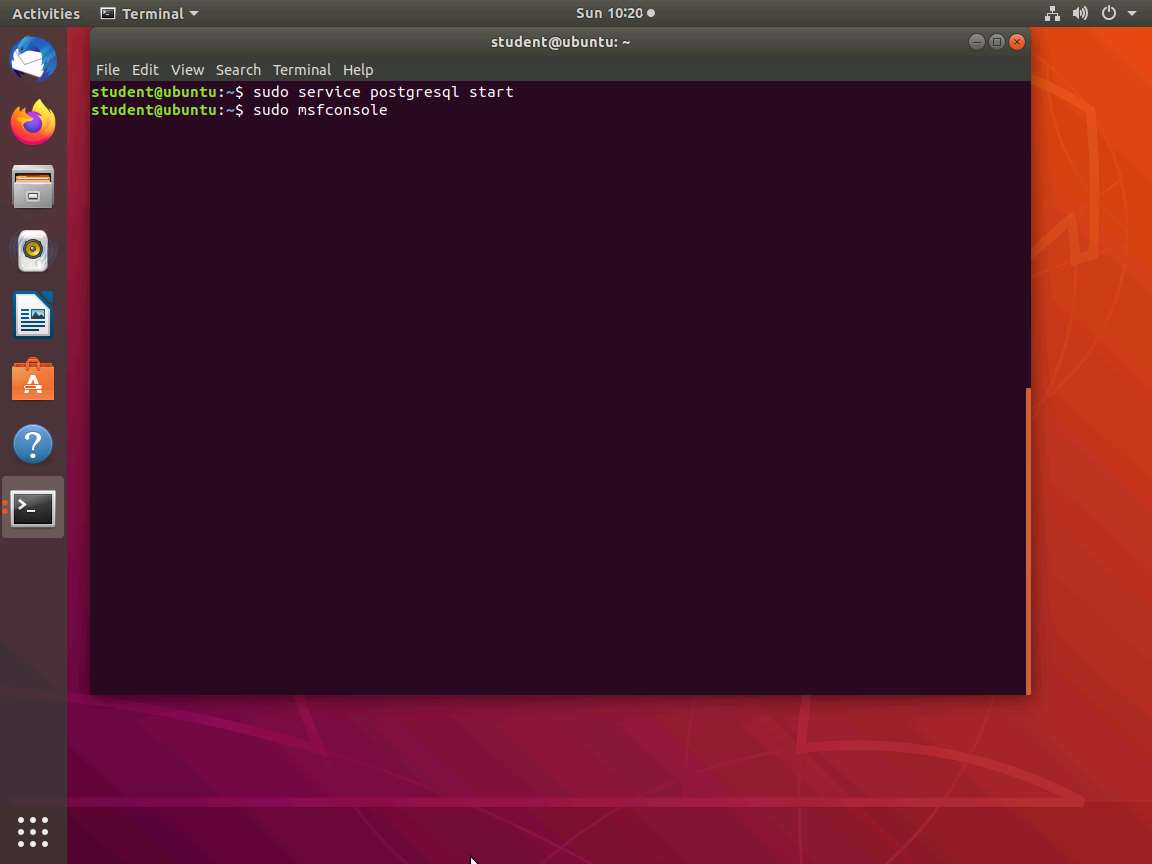


1. Once you have verified the machine, use the Nmap scripting engine script against it. Type **sudo nmap --script modbus-discover.nse 192.168.177.81 -p 502 -Pn**.

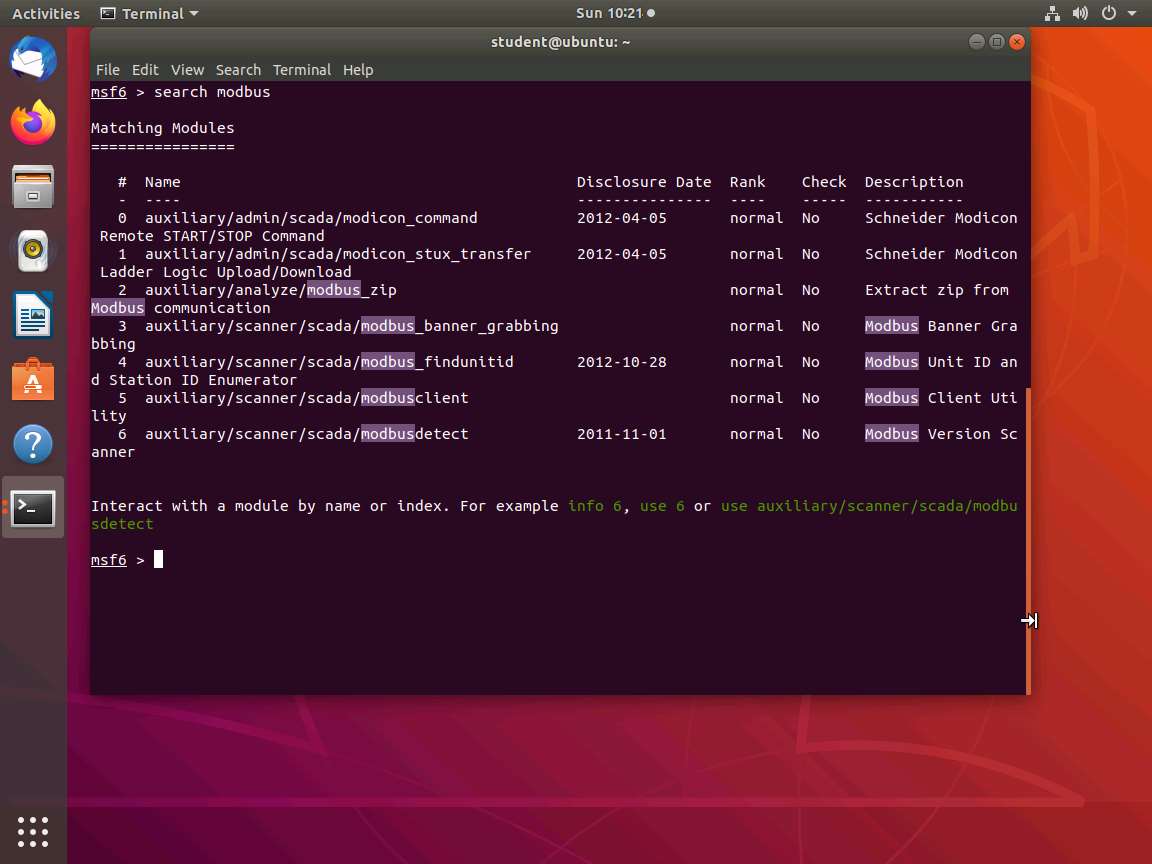
192.168.177.81 is the IP address of the **SCADA Slave** machine.



1. Explore the modules in **Metasploit** next. In the terminal, type **sudo service postgresql start** and press **Enter**, and then type **sudo msfconsole** and press **Enter**.



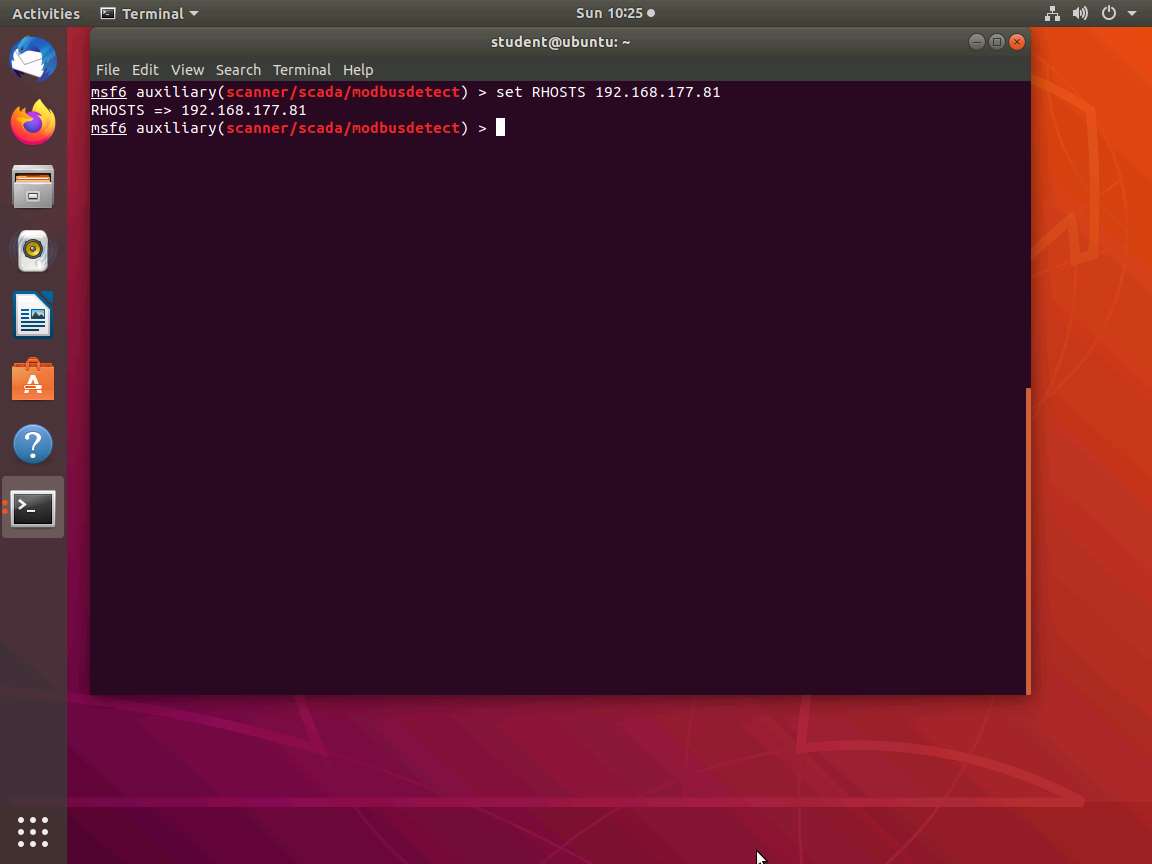
1. In the msfconsole type **search modbus** and press **Enter**.



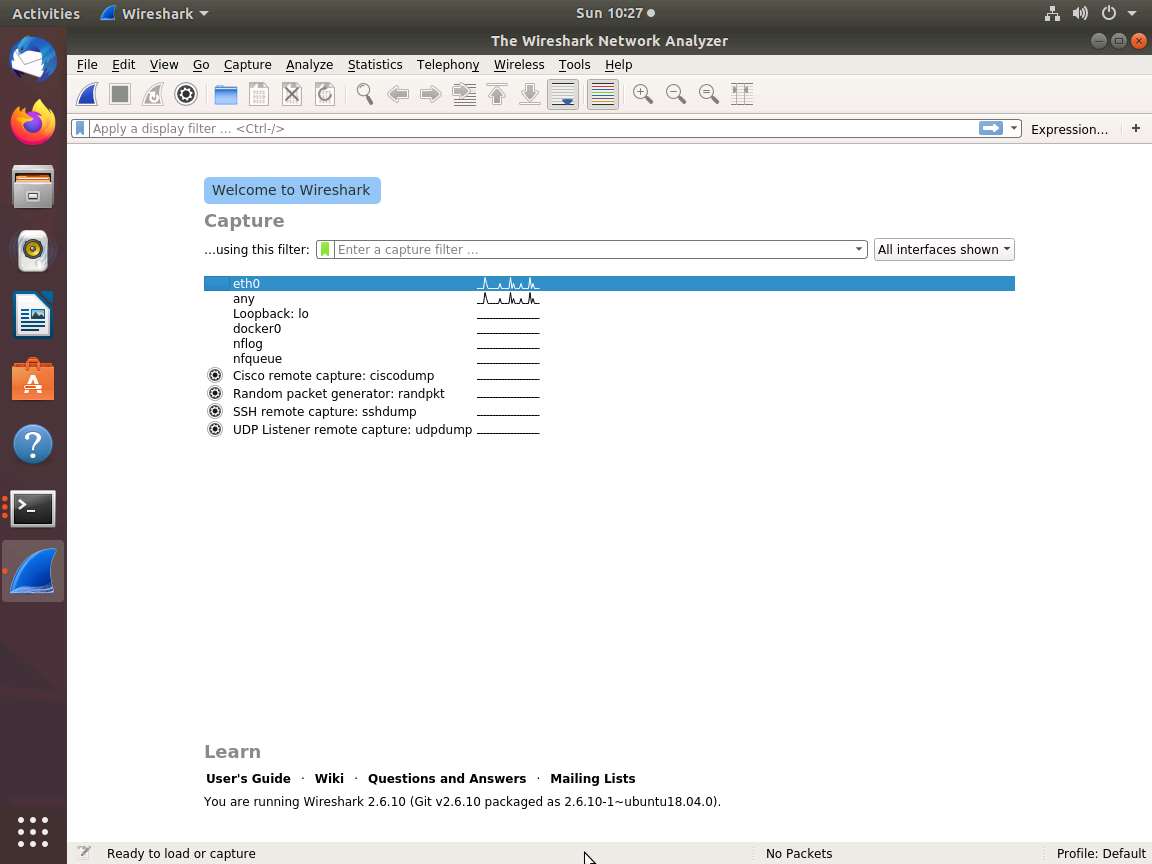
1. You have already detected the ModBus using the Nmap scripting engine. This is one of the modules that you will often use in your testing. You must use it here to compare it with Nmap.
2. Type **use auxiliary/scanner/scada/modbusdetect** and press **Enter**. Once you are in the module, type **info** and press **Enter**.



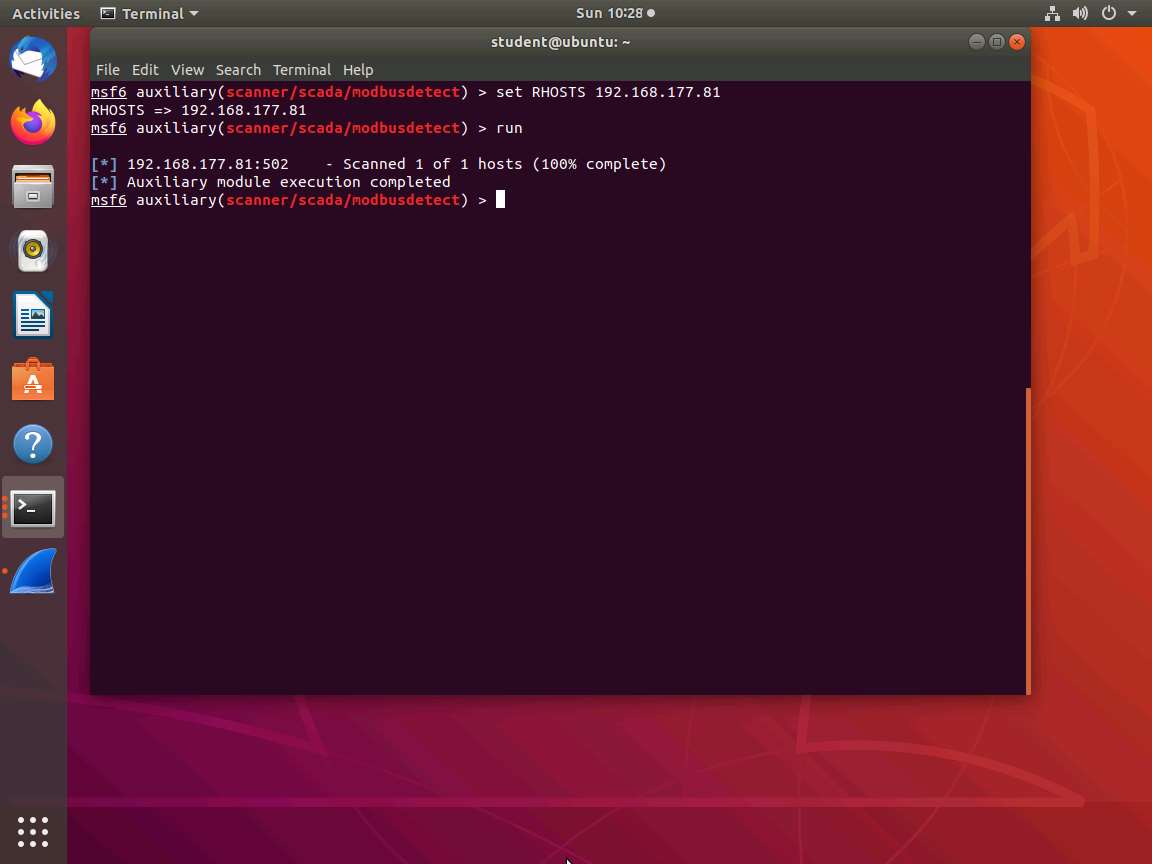
1. The output shows that the only option you need and do not have is the **RHOSTS** option. Type **set RHOSTS** **192.168.177.81** and press **Enter**.



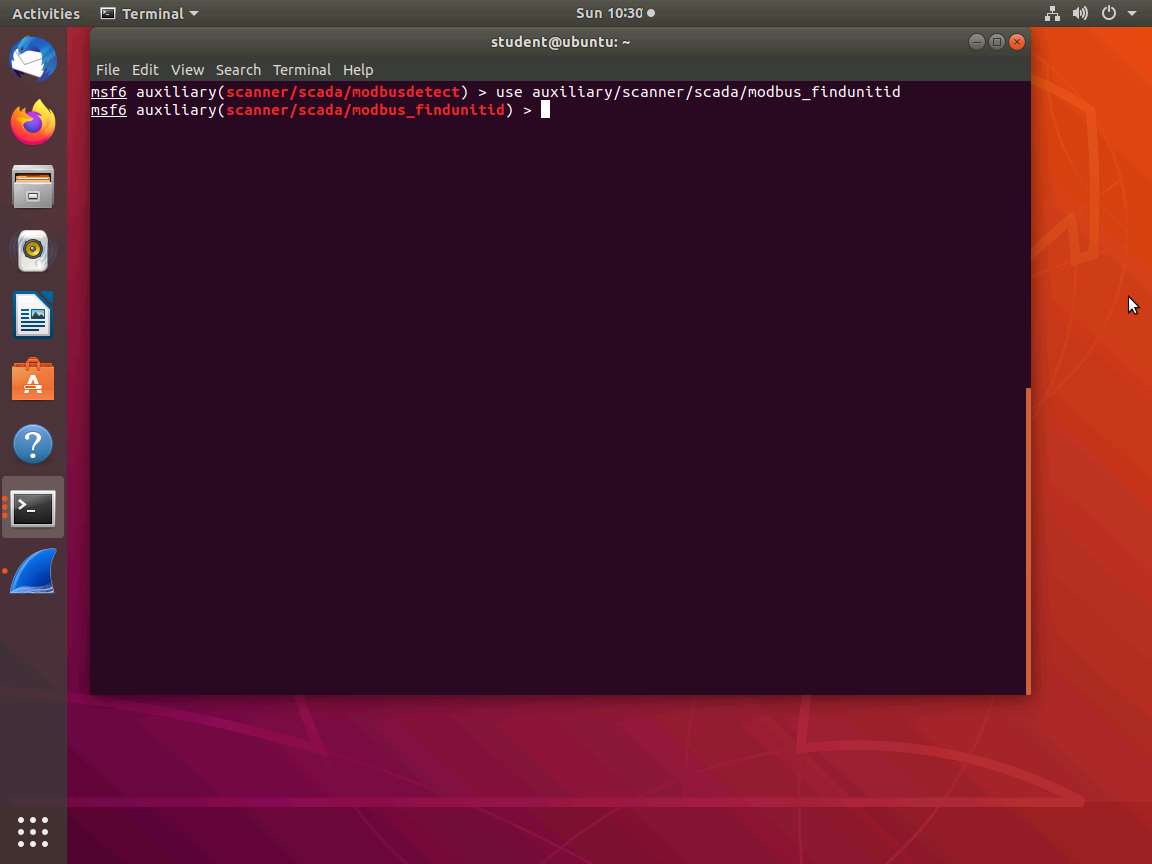
1. Open a New terminal from the Favourites bar and type sudo wireshark and press Enter, type **password** and press **Enter** to attain the root privileges. This will launch the Wireshark application. Double-click on **eth0** to start the capture, and then minimize the Wireshark window.



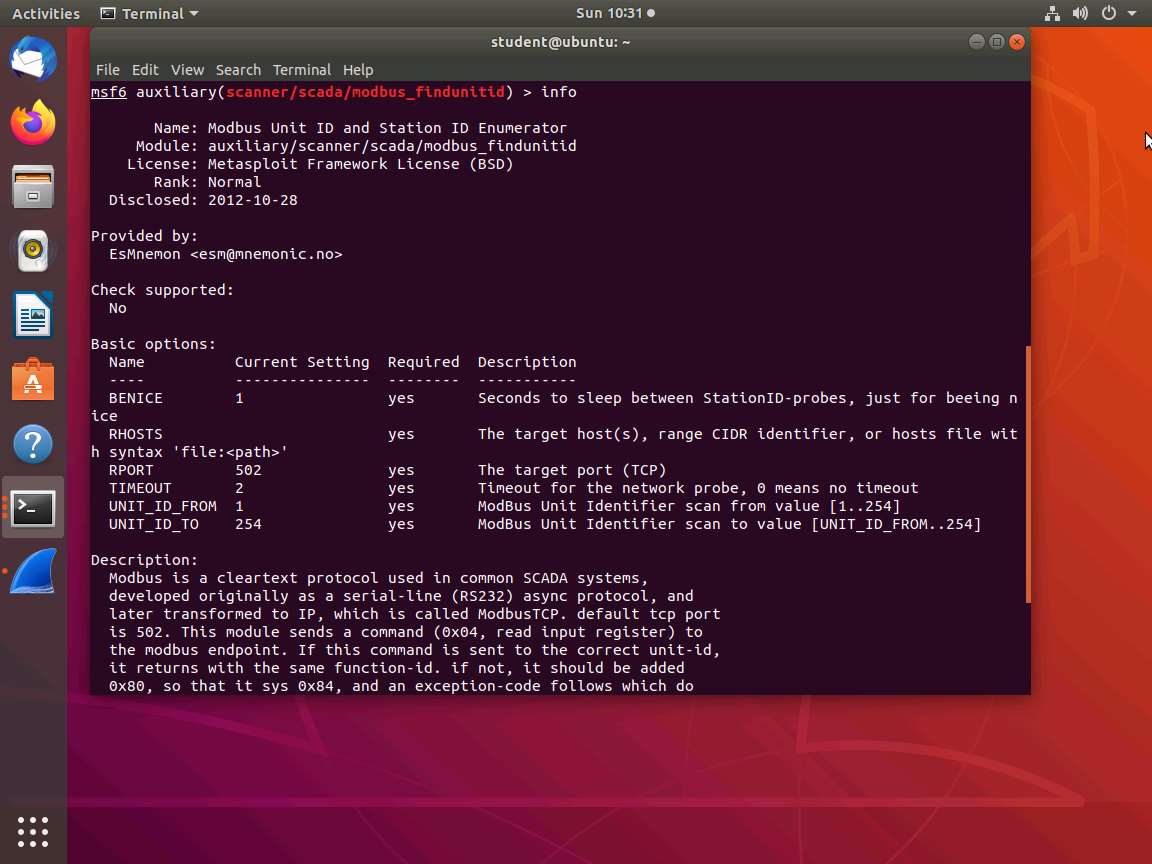
1. Switch to msfconsole and type **run** and press **Enter**.



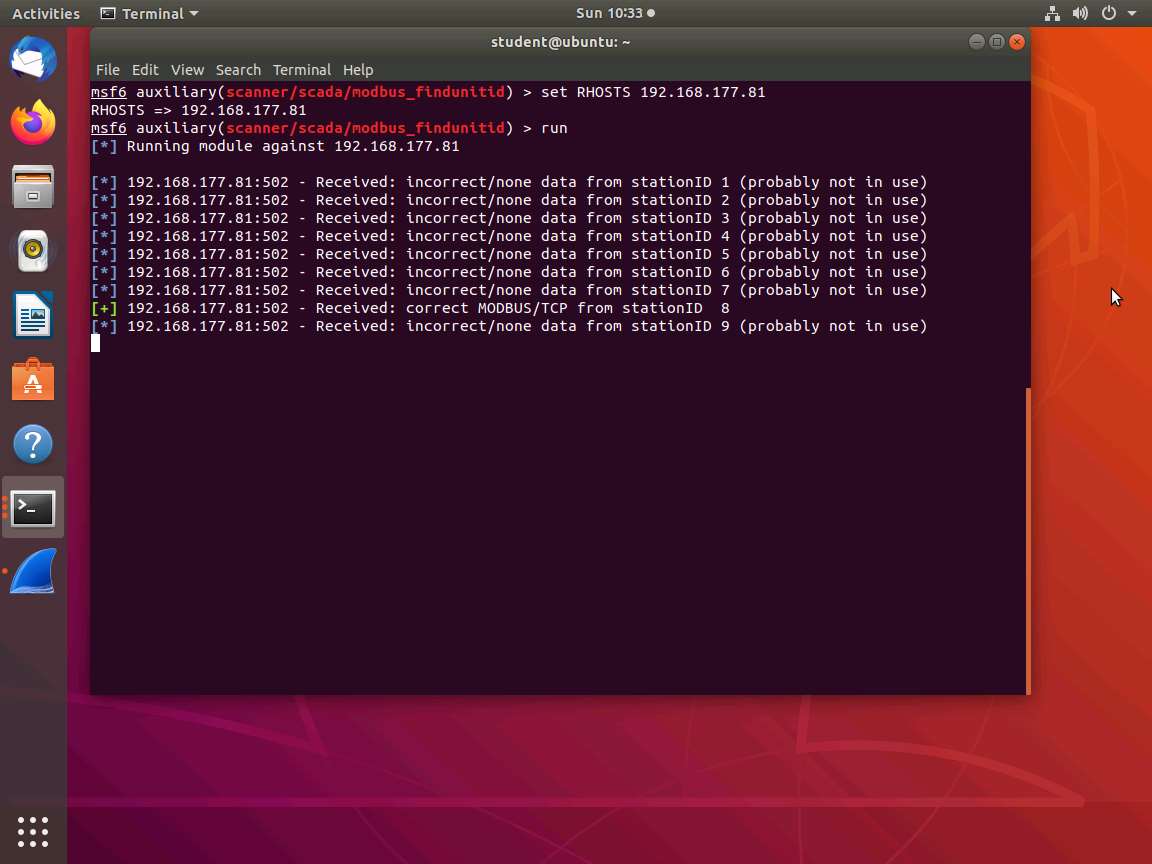
1. However, Wireshark does not reveal the reason. Determine what is occurring when you submit a query. No response indicates that you do not have the correct Unit Identifier. Since you created this, we know it is 8 (A different module will explain the solution when this information is not available).
2. Type **use auxiliary/scanner/scada/modbus\_findunitid** and press **Enter**.



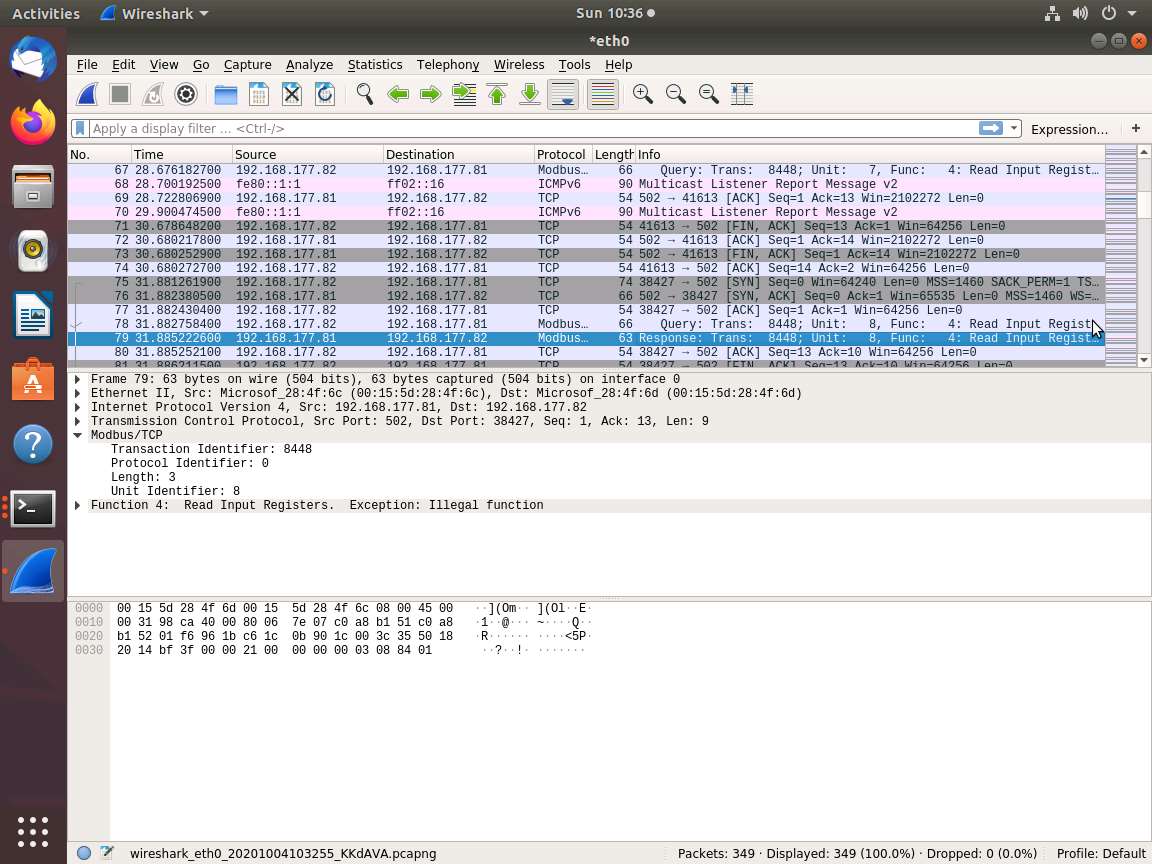
1. Type **info** and press **Enter** to view the information of the module.



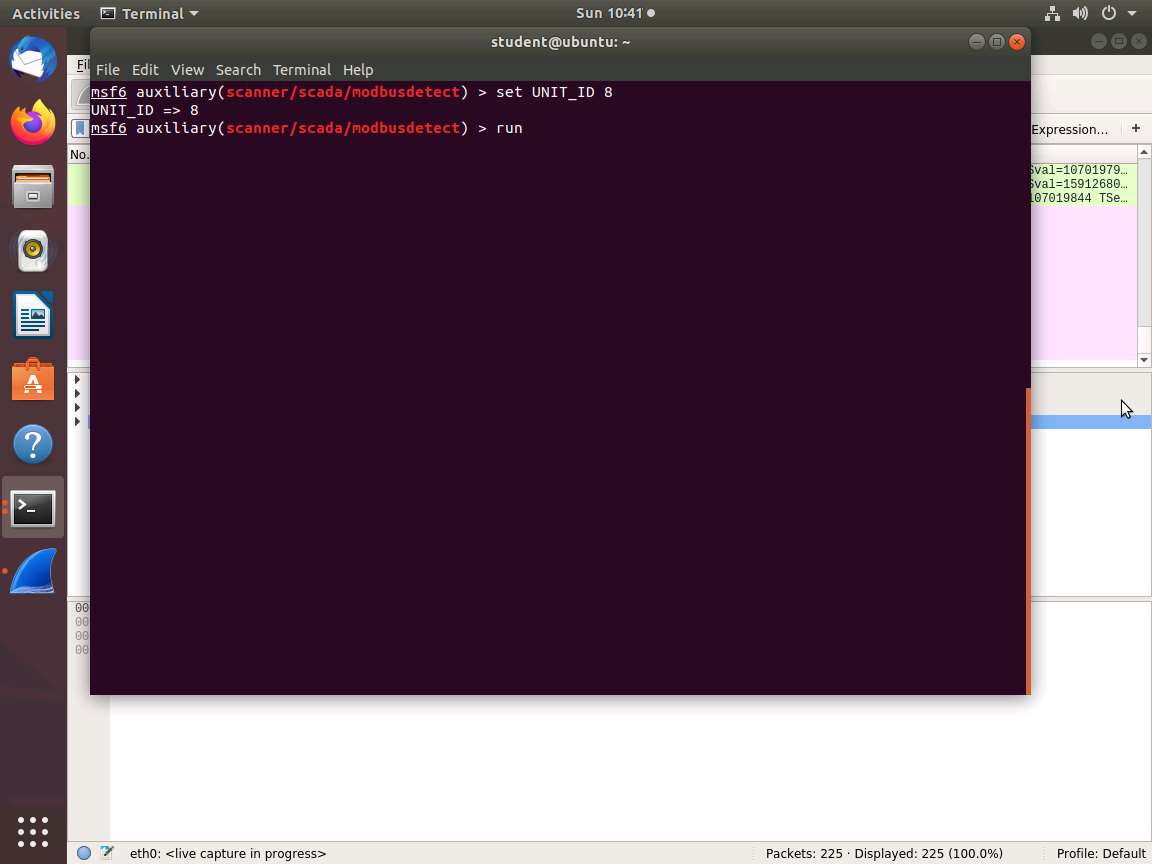
1. As noted, you will need **Unit\_ID**. Type **set RHOSTS 192.168.177.81** and press **Enter**. **Restart** the capture in **Wireshark** and then type **run** and press **Enter**.

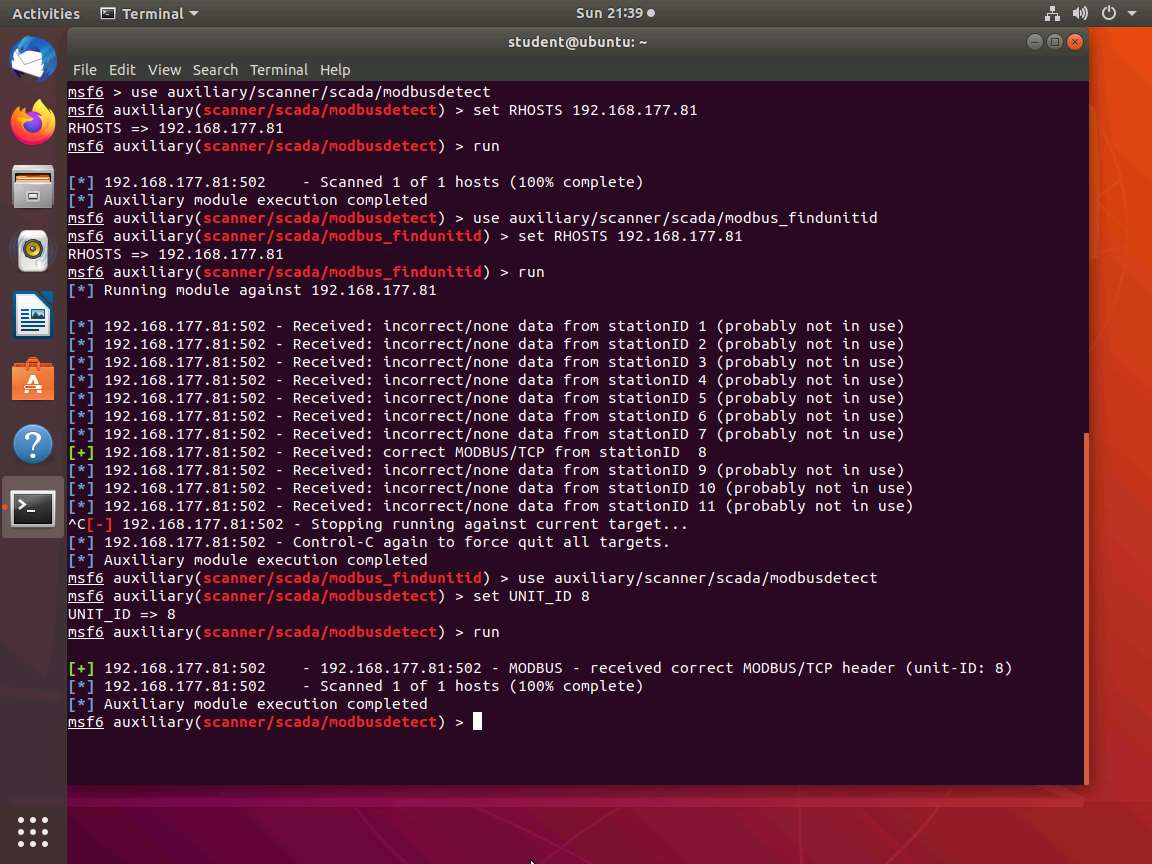


1. With the **UNIT-ID** identified, return to **Wireshark**; capture and review the data at the packet level. Look for when the ID is **correctly discovered**. **Stop** the capture to review.



1. **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.





1. You have now identified that it is the **ModBus** protocol. Switch to Wireshark and review the data. **Close** all windows as required. This concludes the lab exercise.