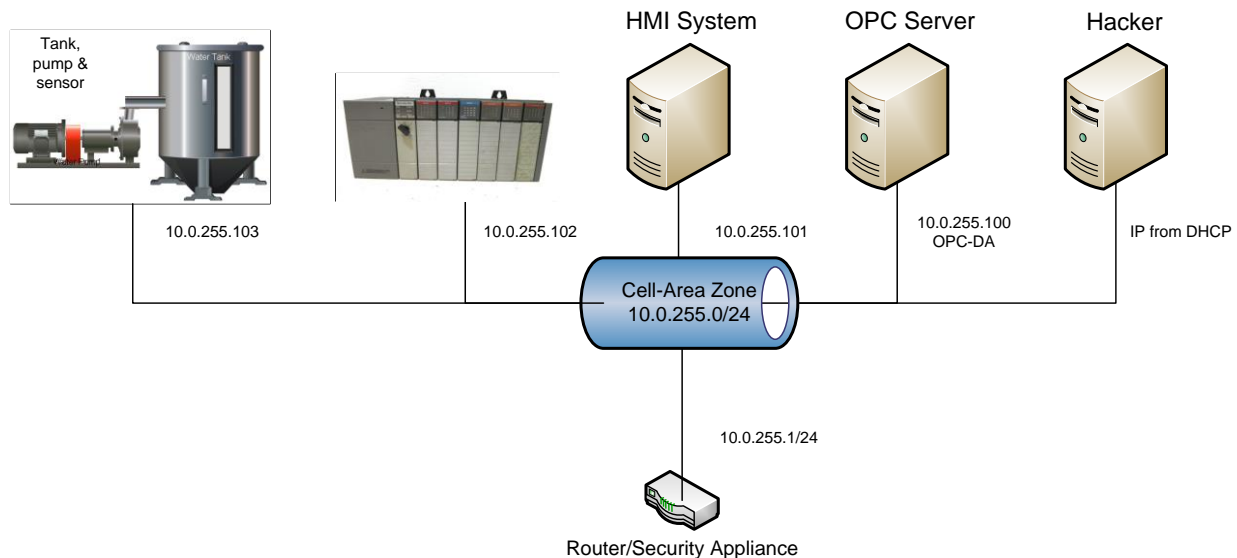


Lab 1

Scenario Overview

The industrial control system (ICS) used in this scenario simulates an environment that might be used to cool industrial equipment. The ICS is made up of five systems. The first system contains a tank, tank level sensor and a water pump. The second system is a programmable logic controller (PLC) which controls the water pump based on the level of water found in the attached tank. The third system is an Open Platform Communications (OPC) server which accesses and modifies data found on the PLC. The fourth system is running Human Machine Interface (HMI) software which communicates with the OPC server to provide a human system operator with system statistics and control. The final system in the ICS is a security appliance that provides routing and firewall services for all systems. This scenario also make use of a system running Kali Linux. In this lab the virtual network switch is configured so that the Kail system receives all data transmitted.



In this lab you are going to observe that when a hacker is connected to the same network segment as the ICS systems, they are easily able to view data being shared between all devices. After verifying this you will move the hacker system to its own network and again attempt to view data being transferred. You will discover that when a hacker is connected to a different segment then the ICS systems they are no longer able to view data transfers..

Part 1

Install Systems

In this part of the lab you are going to install and configure the systems needed to complete the lab.

1. If necessary, install the free Oracle VirtualBox Manager software on your system.

2. Download, and if necessary, extract, the lab image ICS-VirtualBox.ova found at <https://www.nl.northweststate.edu/CAMO/software/VirtualMachine/VirtualBox/>.
3. Start the Oracle VM VirtualBox program.
4. Import the ICS-VirtualBox.ova lab image.
5. After the import has completed access the Settings for the Security Appliance virtual machine and change its configuration so that it is bridged to the network device in your host computer.
6. Power on the systems in the following order:
 - Security Appliance
 - Sensor
 - PLC
 - OPC
 - HMI
 - Kali

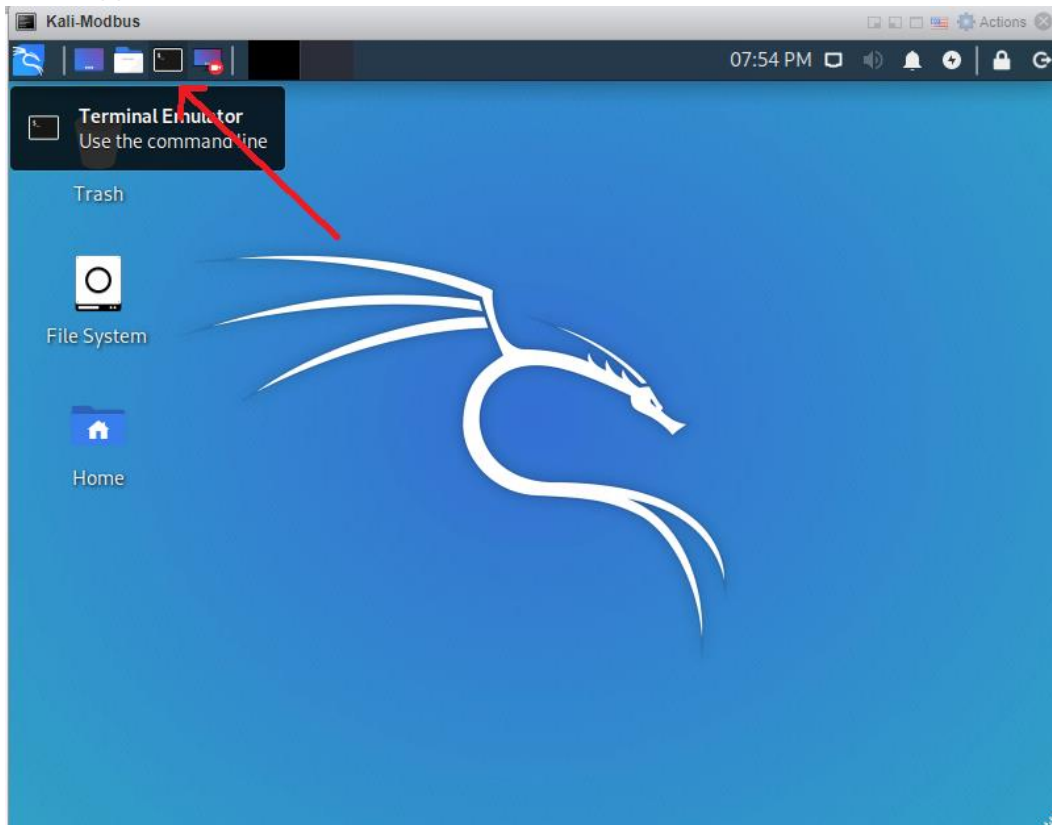
Part 2

Login and verify connectivity

In this part of the lab you are going to login to the hacker system, view the system's IP address and verify that it can connect to the PLC.

1. Access the Kali system.
2. At the login screen enter **student** into the Enter your username field and **Password01** into the Enter your password field.
3. Click the Log In button.

4. Open a terminal (command prompt) window by clicking the Terminal Emulator button found at the upper left hand corner of the window.



5. View the network address of the system by typing the command **ip address show** (NOTE: You must press the <ENTER> key after typing a command).

6. Examine the output of the command and find the IPv4 address associated with the active network card viewing the inet value associated with the network card labeled cell-area-zone.

```
student@kali:~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: cell-area-zone: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:41:0c:2c brd ff:ff:ff:ff:ff:ff
    inet 10.0.255.201/24 brd 10.0.255.255 scope global dynamic noprefixroute
        valid_lft 6321sec preferred_lft 6321sec
    inet6 fe80::a9c:458d:f1a0:34c1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: manufact-zone: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 00:0c:29:41:0c:36 brd ff:ff:ff:ff:ff:ff
student@kali:~$
```

- Notice that the system contains multiple network cards. Network card 1: labeled lo: is the loopback card which is used for internal communications and testing, network card 2: labeled cell-area-zone: is the card connected to the Cell/Area zone along with the ICS systems, network card 3: labeled manufact-zone is currently disabled (DOWN) and is connected to the Manufacturing zone network segment which is separated from the ICS systems by a router/firewall.
7. Verify that the hacker can communicate with the PLC by typing the command **ping 10.0.255.102 -c 4** and observing that 4 packets are transmitted and 4 packets are received.
 8. Verify that the PLC is running by typing the command **nc 10.0.255.102 23** and observing that the PLC is running, and that the IP address of the PLC and the address of the connecting system is shown.
 - The nc command starts the netcat program which is a useful network utility that allows a quick connection to network services. In this case netcat is connecting to the telnet service running on the PLC.
 - Note that the Kali system is on the same IP network (10.0.255.0/24) as the ICS systems (10.0.255.0/24).

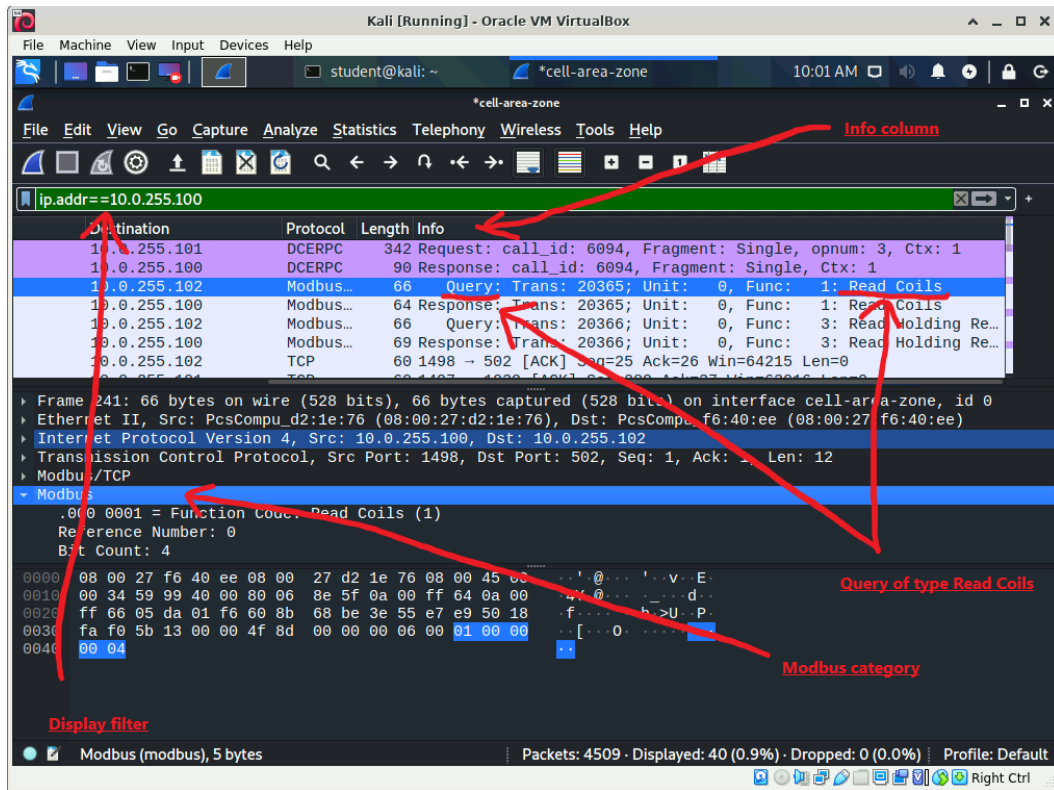
Part 3

Capture and view data transmitted in the Cell-Area zone

In this part of the lab you are going to use the Wireshark network monitoring software to capture and view data being transmitted on the Cell-Area zone.

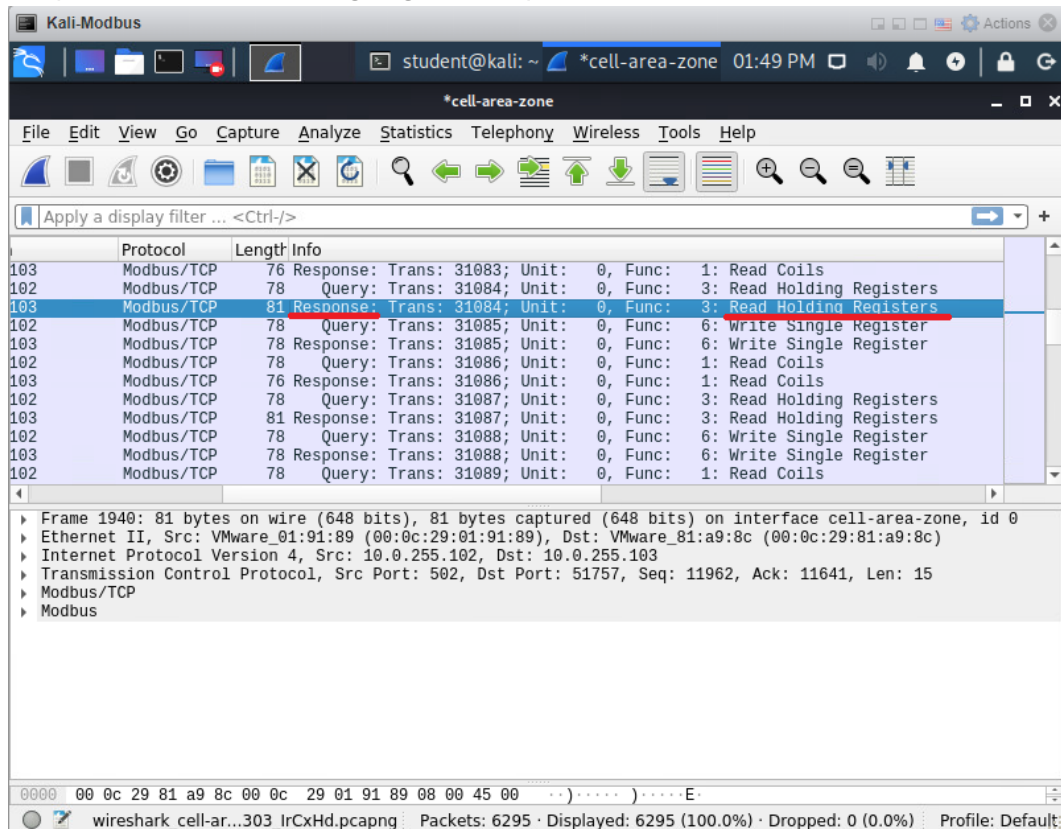
1. Start the Wireshark program by typing the command **sudo wireshark**.
 - The Wireshark program requires administrative privileges to the system, since you are currently logged in as the student user you must indicate that you wish to use administrative privileges prefixing the command to be executed with sudo.
2. Authenticate to the system by typing in the password **Password01** followed by the **<ENTER>** key.
 - To prevent people from looking over your shoulder and writing down the password it will not be displayed as you are typing.
3. After the Wireshark program starts select the cell-area-zone network device to indicate that you wish to capture data on that device.
4. Click the Capture menu then select the Start option.
5. The data you need to view will be captured very quickly so immediately return to the Capture menu and select the Stop option.

6. If necessary scroll to the right in the top, packet list panel, until you are able to view the data shown in the Info column.



- The standard Wireshark output window is divided into three panels, the top panel is named the packet list panel and contains a summary of each packet captured.
- The middle panel is named the packet details panel and shows a decoded view of the packet currently selected in the packet list panel.
- The bottom panel is named the packet bytes panel and shows the raw data contained in the packet currently selected in the packet list panel.

7. Scroll through the packets in the top packet list panel until you find a packet labeled as a Response to a Read Holding Registers request.



8. In the top packet list panel, select the packet containing Info related to a Response: associated with a Read Holding Registers request.

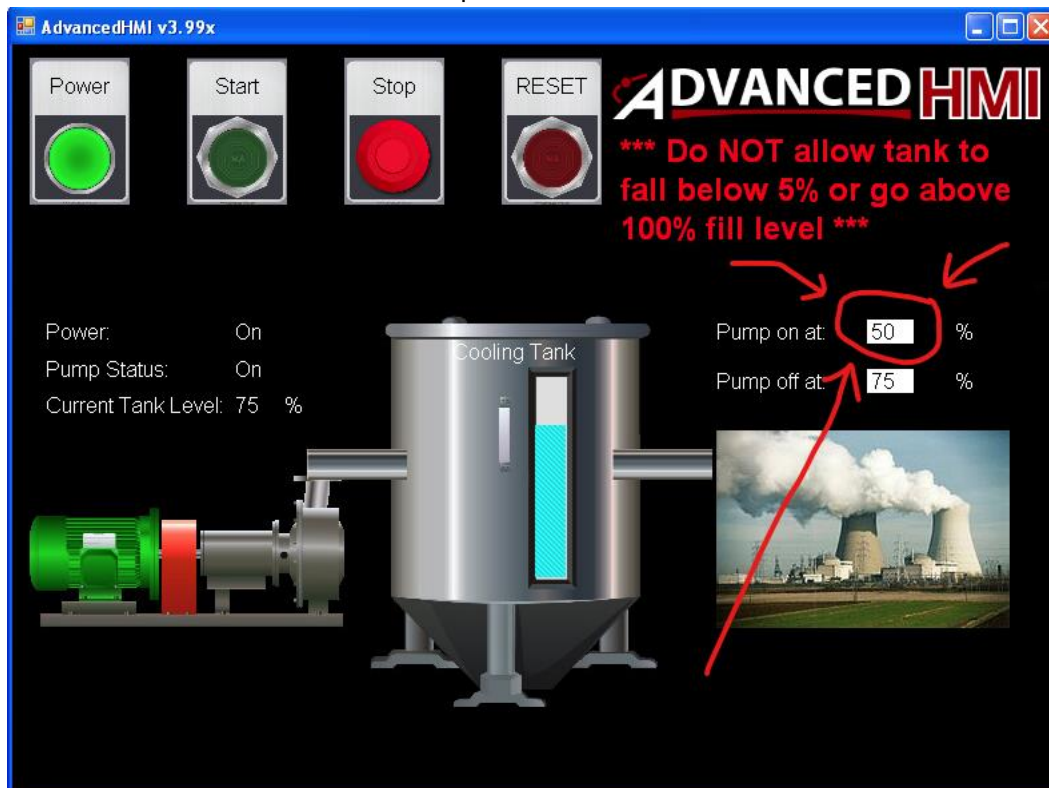
9. In the middle packet details panel expand the Modbus category of detail data (Example).

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes:

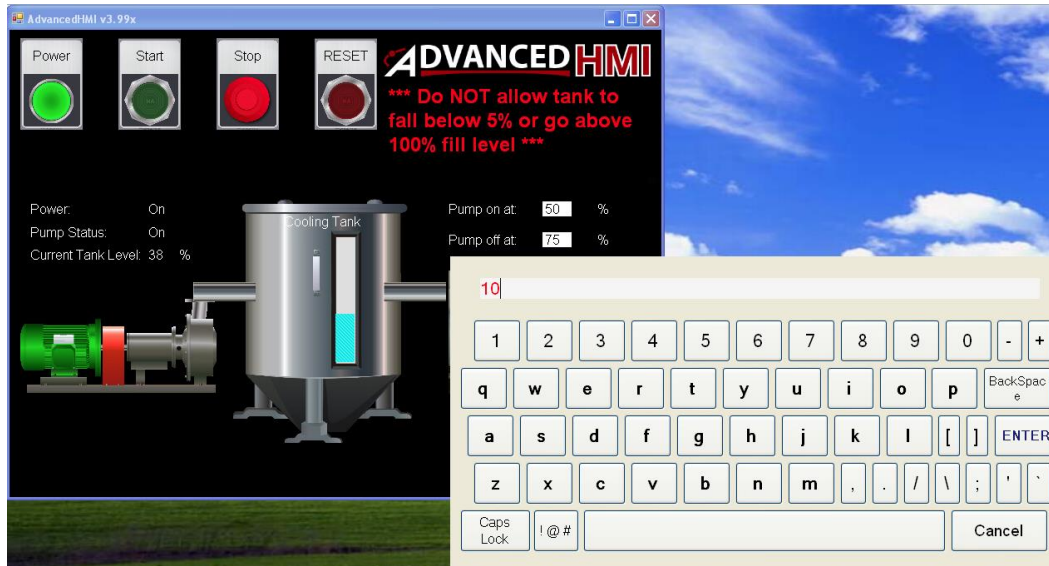
- Packet List:** Shows a list of captured packets. Packet 103 is selected, which is a Modbus/TCP response. The details pane on the right shows the structure of this packet: Trans: 31083, Unit: 0, Func: 1: Read Coils.
- Packet Details:** The selected packet (103) is expanded, showing the following details:
 - Frame 1940: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface cell-area-zone, id 0
 - Ethernet II, Src: VMware_01:91:89 (00:0c:29:01:91:89), Dst: VMware_81:a9:8c (00:0c:29:81:a9:8c)
 - Internet Protocol Version 4, Src: 10.0.255.102, Dst: 10.0.255.103
 - Transmission Control Protocol, Src Port: 502, Dst Port: 51757, Seq: 11962, Ack: 11641, Len: 15
 - Modbus/TCP
 - Request Frame: 1939
 - Time from request: 0.000434099 seconds
 - Byte Count: 6
 - Register 0 (UINT16): 67
 - Register 1 (UINT16): 75
 - Register 2 (UINT16): 50
- Packet Bytes:** The bottom pane shows the raw packet data in hexadecimal and ASCII. The first few bytes are 00 0c 29 81 a9 8c, which correspond to the Ethernet II header.

10. Make a note of the data contained in Register 0, Register 1 and Register 2.
11. Access the HMI virtual machine and take a moment to examine the data and controls available in the running AdvancedHMI program.

12. Click on the value shown in the Pump on at: field.



13. Change the pump on value to 10.



14. Take a minute to observe how this modifies the behavior of the system.

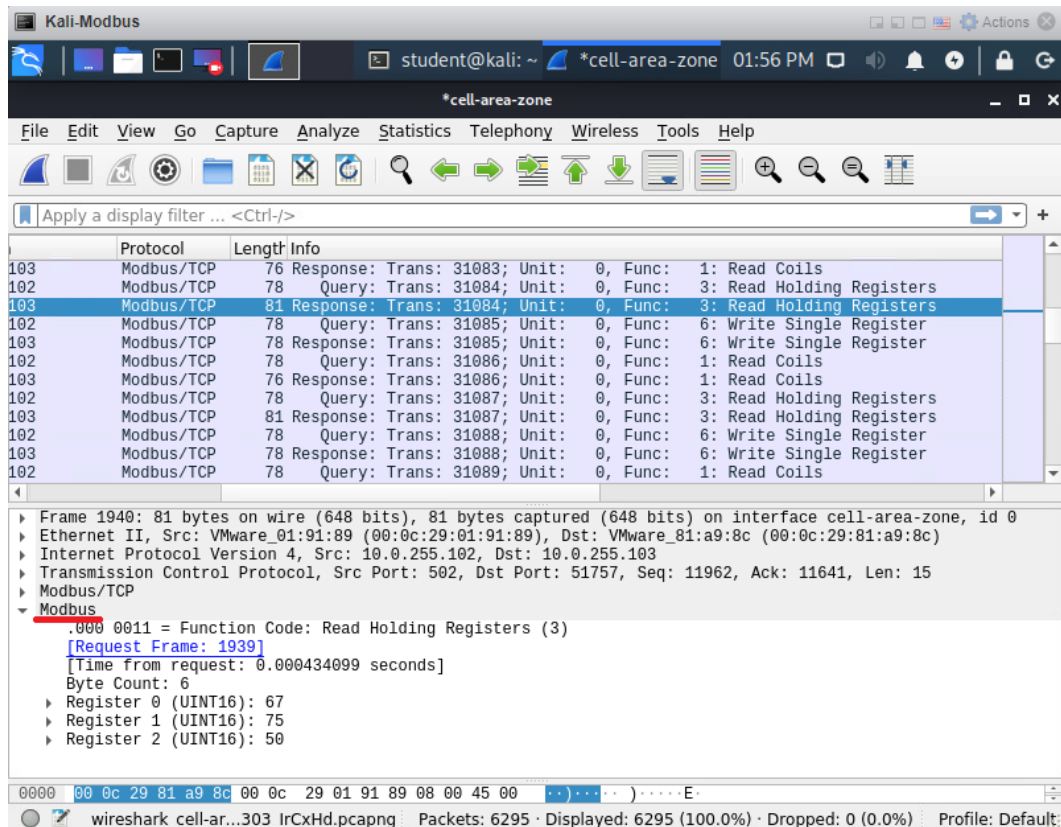
15. Access the Kali system.

16. Begin a new network data capture by accessing the Capture menu in Wireshark and choosing the Start option.

17. Click the Continue without Saving button when you are informed that there are unsaved packets in the problem

18. The data you need to view will be captured very quickly so immediately return to the Capture menu and select the Stop option.
19. Scroll through the packets in the top packet list panel until you find a packet labeled as a Response to a Read Holding Registers request.
20. In the top packet list panel, select the packet containing a Response to Read Holding Register request.
21. In the middle packet details panel expand the Modbus category of detail data.

22. Take a screen shot showing the data in Register 0, Register 1 and Register 2 and paste it into the lab form.

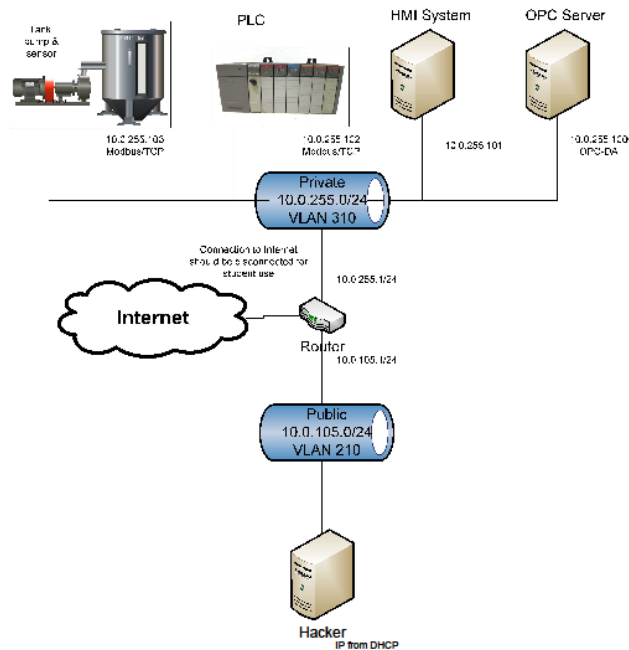


23. Based on the packets captured it appears that the value in Register 2 tells the system to turn the pump on when the level of liquid drops to 10%. What do the values stored in Registers 0 and 1 represent? Answer these questions in the lab form.

Part 4

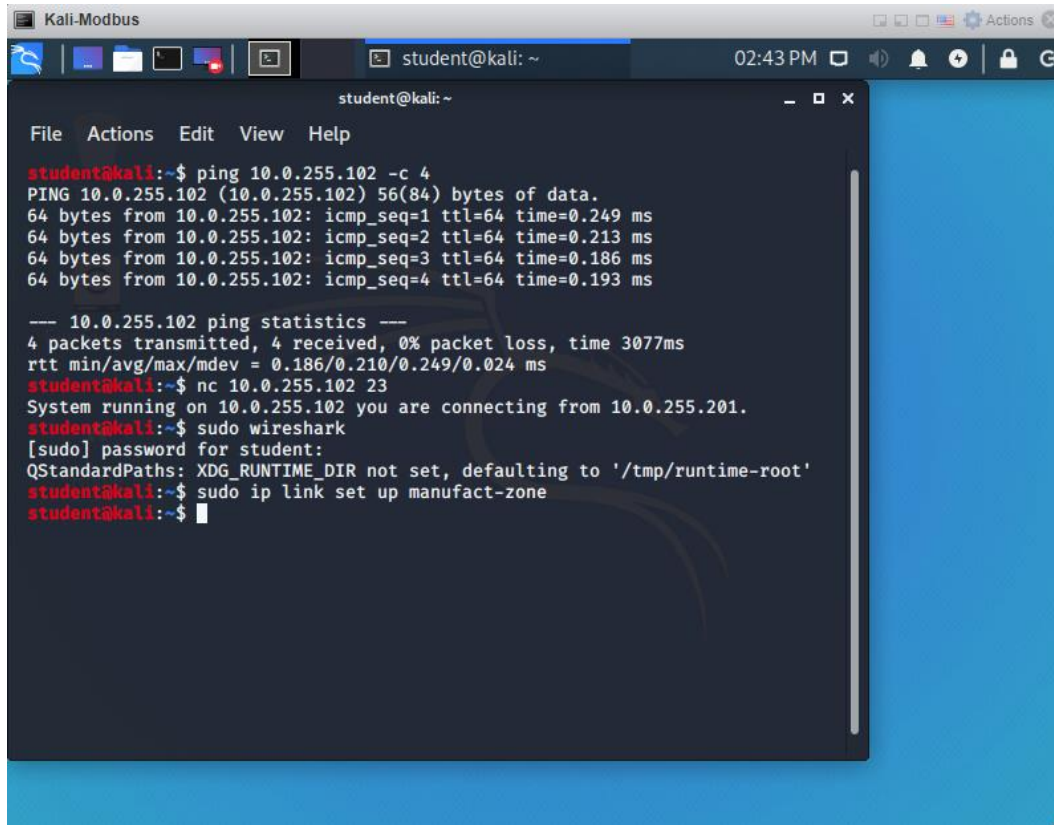
Change the hacker's network segment

In this part of the lab you are going to remove the hacker from the network containing the ICS systems. The hacker system will be moved from the Cell/Area zone to the Manufacturing zone.



1. Close the Wireshark program without saving any data.
2. Access the terminal (command prompt).

3. Bring up the network device connected to the manufacturing zone network segment using the command **sudo ip link set up manufact-zone**.

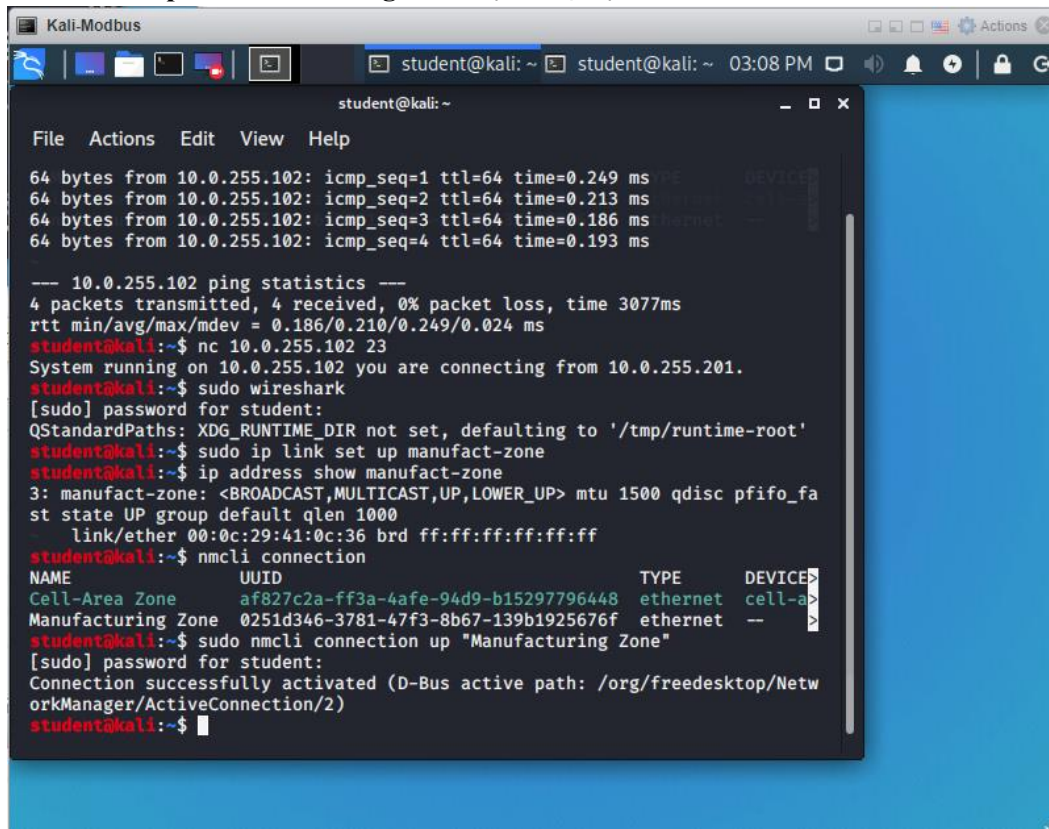


```
Kali-Modbus
student@kali: ~
02:43 PM
student@kali: ~
File Actions Edit View Help
student@kali:~$ ping 10.0.255.102 -c 4
PING 10.0.255.102 (10.0.255.102) 56(84) bytes of data:
64 bytes from 10.0.255.102: icmp_seq=1 ttl=64 time=0.249 ms
64 bytes from 10.0.255.102: icmp_seq=2 ttl=64 time=0.213 ms
64 bytes from 10.0.255.102: icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from 10.0.255.102: icmp_seq=4 ttl=64 time=0.193 ms

--- 10.0.255.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.186/0.210/0.249/0.024 ms
student@kali:~$ nc 10.0.255.102 23
System running on 10.0.255.102 you are connecting from 10.0.255.201.
student@kali:~$ sudo wireshark
[sudo] password for student:
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
student@kali:~$ sudo ip link set up manufact-zone
student@kali:~$
```

- If you are using sudo and are prompted to authenticate type in the password **Password01** followed by the **<ENTER>** key.
4. Verify that the device is connected to the network by typing the command **ip address show manufact-zone** and verifying from the output that the device's state is UP but that it has not yet been assigned an IP address.
 5. View the available network configurations by typing the command **nmcli connection**.
 6. Notice that the Cell-Area Zone configuration is associated with a device but the Manufacturing Zone configuration is not.
 7. Type the letter **q** to stop viewing the network configurations.

8. Enable the ManufacturingZone network configuration by typing the command **sudo nmcli connection up "Manufacturing Zone"** (Example).



```
Kali-Modbus
student@kali: ~ 03:08 PM
student@kali: ~
File Actions Edit View Help

64 bytes from 10.0.255.102: icmp_seq=1 ttl=64 time=0.249 ms
64 bytes from 10.0.255.102: icmp_seq=2 ttl=64 time=0.213 ms
64 bytes from 10.0.255.102: icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from 10.0.255.102: icmp_seq=4 ttl=64 time=0.193 ms

--- 10.0.255.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.186/0.210/0.249/0.024 ms
student@kali:~$ nc 10.0.255.102 23
System running on 10.0.255.102 you are connecting from 10.0.255.201.
student@kali:~$ sudo wireshark
[sudo] password for student:
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
student@kali:~$ sudo ip link set up manufact-zone
student@kali:~$ ip address show manufact-zone
3: manufact-zone: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
st state UP group default qlen 1000
    link/ether 00:0c:29:41:0c:36 brd ff:ff:ff:ff:ff:ff
student@kali:~$ nmcli connection
NAME                                UUID                                TYPE    DEVICE
Cell-Area Zone                      af827c2a-ff3a-4afe-94d9-b15297796448 ethernet cell-a
Manufacturing Zone                  0251d346-3781-47f3-8b67-139b1925676f ethernet --
student@kali:~$ sudo nmcli connection up "Manufacturing Zone"
[sudo] password for student:
Connection successfully activated (D-Bus active path: /org/freedesktop/Netw
orkManager/ActiveConnection/2)
student@kali:~$
```

9. Verify that the Manufacturing Zone configuration is now associated with a device by again typing the command **nmcli connection**.
10. Type the letter **q** to stop viewing the network configurations.
11. Verify that the manufact-zone device has been assigned an IP address by again typing the command **ip address show manufact-zone**.
12. To prevent confusion later disable the Cell-Area Zone configuration by typing the command **sudo nmcli connection down "Cell-Area Zone"**.
13. Verify that now the Manufacturing Zone configuration is associated with a device but the Cell-Area Zone configuration is not by typing the command **nmcli connection**.
14. Type the letter **q** to stop viewing the network configurations.

Part 5

Capture and view data transmitted in the Manufacturing zone

In this part of the lab you are going to use the Wireshark network monitoring software to capture and view data being transmitted on the Manufacturing zone.

1. Verify that the hacker can communicate with the PLC by typing the command **ping 10.0.255.102 -c 4** and observing that 4 packets are transmitted and 4 packets are received.

2. Verify that the PLC is running by typing the command **nc 10.0.255.102 23** and observing that the PLC is running, and that the IP address of the PLC and the address of the connecting system is shown.
 - Note that this time the Kali system is on a different IP network (10.0.105.0/24) than the ICS systems (10.0.255.0/24).
3. Start the Wireshark program by typing the command **sudo wireshark**.
4. After the Wireshark program starts select the manufact-zone network device to indicate that you wish to capture data on that device.
5. Click the Capture menu then select the Start option.
6. Wait a few moments and note that little to no network traffic is currently being captured.
7. Access the HMI virtual machine.
8. Click on the value shown in the Pump off at: field in the AdvancedHMI program running on the HMI virtual machine.
9. Change the pump off value to **60**.
10. Observe the system for a minute and verify that this change modifies the behavior of the system.
11. Return to the Kali system and note that none of the changes or activity between the ICS systems has been captured.
12. Open a new Terminal (command prompt) window by clicking the Terminal Emulator button found at the upper left hand corner of the Kali system.
13. Ping the PLC by typing the command **ping 10.0.255.102 -c 4**.
14. Return to the Wireshark screen and notice that since the Kali system was involved in the network communication the ping (ICMP) traffic was captured.
15. Stop the network traffic capture by accessing the Capture menu and selecting the Stop option.
16. Take a screen shot showing a captured ping (ICMP) request and reply and paste it into the lab form.
17. In the lab form, answer the question "Why was the network ping traffic between the Kali system and the PLC captured but the data between the PLC and other ICS systems was not?".
18. In the lab form, answer the question "If using proper zoning techniques is more secure why might companies not configure their systems using this technique?".
19. To end the lab, power off the virtual machines.