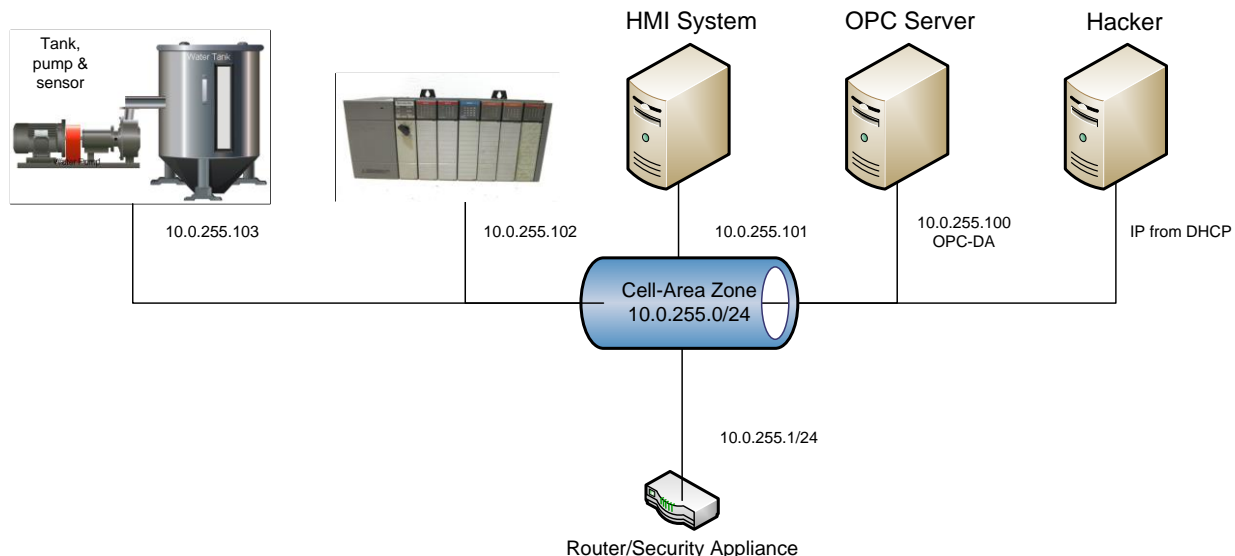


Lab 1

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 students will use nmap to perform basic and advanced network scanning. Multiple methods for accessing common built-in nmap resources will be demonstrated. Students will learn to modify nmap's behavior using switches. Students will learn to use caution when using nmap by observing how it can disrupt system functionality.

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

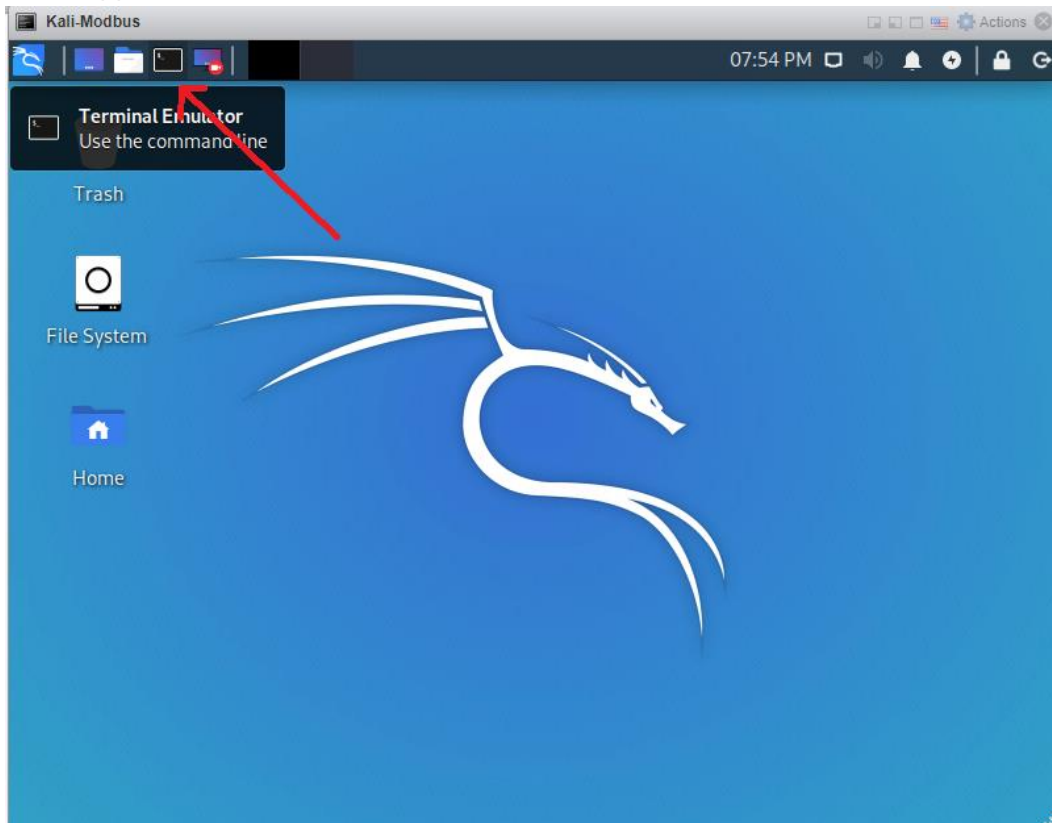
Part 2

Practice Nmap Basics

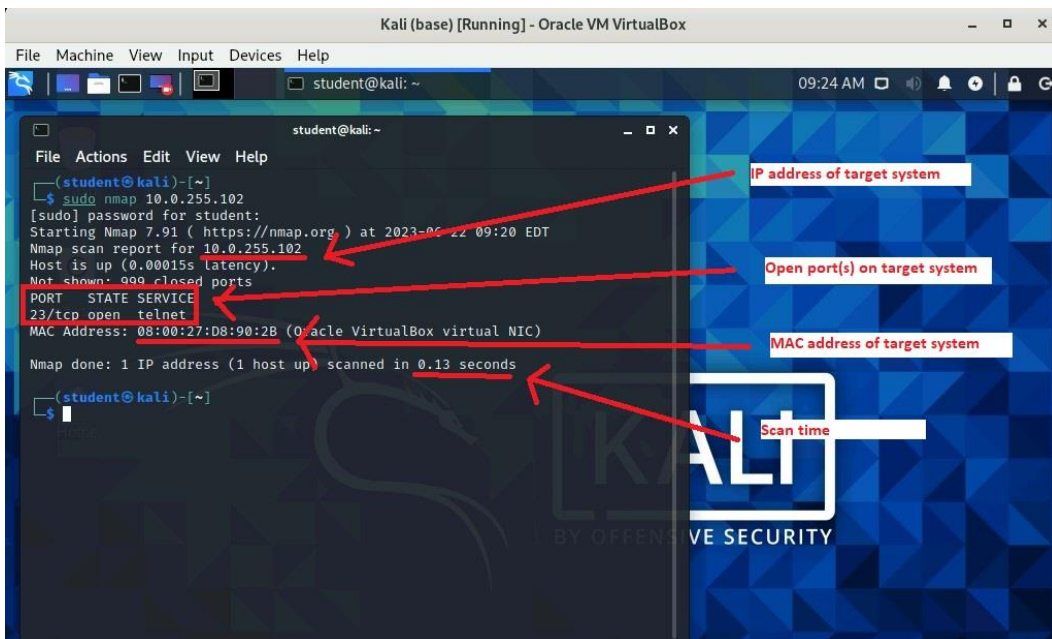
In this part of the lab you are going to practice basic nmap use.

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. Use nmap to perform a default scan of the PLC system by typing the command **sudo nmap 10.0.255.102**.



- If when using sudo, you are prompted to authenticate type in the password **Password01** followed by the **<ENTER>** key.

6. Type the command **ip address show** to view the basic network configuration of the Kali system.

```
(student@kali)-[~]
$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  ault 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_fas
  t state UP group default qlen 1000
  link/ether 08:00:27:2d:32:d4 brd ff:ff:ff:ff:ff:ff
  inet 10.0.255.100/24 brd 10.0.255.255 scope global dynamic noprefixroute
    cell-area-zone
      valid_lft 4197sec preferred_lft 4197sec
      inet6 fe80::1831:23a9:a3%:8bf3/64 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 08:00:27:78:83:d4 brd ff:ff:ff:ff:ff:ff
```

7. Type the command **sudo nmap 10.0.255.1-255** to perform a default scan of all of the systems on the same network as the Kali system.
8. Record the amount of time that the default scan took and the number of systems found in the lab form.

Part 3

Use switches with Nmap

In this part of the lab you will practice using nmap switches.

1. Type the command **nmap --help** to view the switches available to the nmap program.
2. Type the command **man nmap** to view the online manual for the nmap program.
 - Type the **q** key on the keyboard when you are finished viewing the manual.
3. Type the command **sudo nmap -sn 10.0.255.1-255** to perform a ping scan of all of the systems on the same network as the Kali system.
4. Record the amount of time that the ping scan took and the number of systems found in the lab form.
5. Type the command **sudo nmap -T5 10.0.255.1-255** to perform a fast (insanely fast) scan of all of the systems on the same network as the Kali system.
6. Record the amount of time that the fast scan took and the number of systems found in the lab form.
7. Type the command **sudo nmap -A 10.0.255.101** to scan the HMI system's operating system and service details.
8. Type the command **sudo nmap -A localhost** to scan the local (Kali) system's operating system and service details.
9. Type the command **sudo nmap 10.0.255.102** to perform a default scan of the PLC system.
 - Note that the default settings do not scan for the Modbus server/client which runs on TCP port 502.

10. Type the command **sudo nmap -p 502 10.0.255.102** to scan the Modbus port on the PLC system.
11. Type the command **sudo nmap --script banner 10.0.255.102** to execute the banner script targeting the PLC system.
12. Type the command **sudo nmap --script-help plc-caution** to display the help documentation for the plc-caution script.
13. Type the command **sudo nmap --script plc-caution 10.0.255.102** to execute the plc-caution script targeting the PLC system.
14. Access the PLC system and answer the question regarding its current functional state in the lab form.

Part 4

Challenge

In this part of the lab you will use what you have learned to answer some challenge questions.

1. Use nmap to determine the IP address of the system which has the NetBIOS computer name OPC\x00.
2. Record the answer to the question in the lab form.
3. Two systems on the same network as the Kali system are listening on the Modbus protocol port (TCP port 502), use nmap to determine what their IP addresses are.
4. Record the answer to the question in the lab form.