Getting Started in ICS/OT Cyber Security Lab Manual

Contents

Part 1: Course Introduction

Industrial Control Systems (ICS) and Operational Technology (OT) run the world around us. Power plants, offshore oil rigs, trains and other transportation systems, manufacturing plants – these are just a few examples of the critical infrastructure that society depends on. Each ICS/OT environment is unique and has specialized security requirements.

Protecting critical infrastructure becomes more important each day as the frequency of cyber attacks and the number of attackers continues to grow. Nation state adversaries are no longer the only ones targeting these specialized environments. Today's attackers include ransomware groups, hacktivists, cyber mercenaries, and more.

ICS/OT cyber security can seem complicated and even daunting at first, but it does not have to be. This course will help participants understand the fundamentals of how these environments operate and how to secure such specialized networks.

Exercise 1.1: Setting Up VMware Workstation for Personal Use

Throughout this course, many of the exercises use virtual machines. While there are several virtual machine applications available for use, VMware Workstation is my preference and is free as of early May 2024. And I'll always point students towards free resources!

NOTE: You can use other virtualization software such as Oracle VirtualBox to complete the labs in this course, but any special instructions in this lab manual are specifically for VMware Workstation.

1. First, you will need to register for a Broadcom free account if you do not already have one. You can register at https://profile.broadcom.com/web/registration.

2. Next, access the Broadcom portal download page at https://support.broadcom.com/group/ecx/productdownloads?subfamily=VMware+Workstation+Pro.

3. In the Broadcom portal, navigate to the download for the latest version of "VMware Workstation Pro for Personal Use (For Windows)."

4. Once downloaded, launch the VMware Workstation Pro installer executable.

5. On the "Welcome to the VMware Workstation Pro Setup Wizard" screen, click 'Next.'

6. On the 'End-User License Agreement" screen, review the general terms presented, check the box for "I accept the terms in the License Agreement" if you agree and click 'Next.'

7. If you receive the "Compatible Setup" message, you will typically need to install Windows Hypervisor Platform (WHP) which Windows can do for you automatically. Check the box for "Install Windows Hypervisor Platform (WHP) automatically" and click 'Next.'

8. On the "Custom Setup" screen, click "Next."

9. On the "User Experience Settings" screen, make your privacy and product selections. Afterwards, click 'Next.'

10. On the "Shortcuts" screen, click 'Next.'

11. On the "Ready to install VMware Workstation Pro" window, click 'Install.'

12. Once the installation is complete, click the "Finish" button on the "Completed the VMware Workstation Pro Setup Wizard" window.

    NOTE: You'll have the option for configuring the License later.
    Reboot your system.

13. Reboot your system.

Exercise 1.2 Installing Python on Windows

In this exercise, you will install the current version of the Python language on your Windows system. Python will be the main language used to write scripts in this course as it can run on both Windows and Linux.

1. On your main Windows host, download the current version of Python at https://www.python.org/downloads/. You should see a yellow button near the top of the page under the header "Download the latest version for Windows."

2. Once downloaded, install Python. For the purpose of this course, accept all defaults.

3. To verify that Python is installed correctly on your system, open a command prompt and type the following:

```
python --v
```

4. The screen should display output something similar to the following:

```
C:\Users\micha>python --version
Python 3.12.2
```

Exercise 1.3 Installing PIP

While PIP comes installed with Python 3.4 or higher, it is important to ensure that it is installed on your system. PIP allows additional modules of Python functionality to be added easily to the system. Many of the scripts we will be creating in this course will require such modules to be installed and PIP is the easiest way to make that happen!

1. Run the following command to see if PIP is installed:

   ```
   python -m ensurepip --default-pip
   ```

   If you receive a message that starts with “Requirement already satisfied” then you do not need to take any further action.
2. If it appears that PIP is not installed on your system, download the current version of PIP using the following link: https://bootstrap.pypa.io/pip/pip.pyz.

3. Once downloaded, launch the .pyz file which is a specially crafted ZIP file for Python. At this point, PIP should install on your system.

Part 2: ICS/OT Cyber Security Overview

In Part 2, we dive into what exactly is cyber security for ICS/OT, including: - Differences Between IT and ICS/OT - Common Ways Attackers Enter ICS/OT Networks - A Simple OT Example - Types of Industrial Control Environments - What is ICS/OT Cyber Security? - Annotated History of ICS/OT Cyber Security - Hybrid Approach to ICS/OT Cyber Security - The Sliding Scale of Cyber Security

Exercise 2.1: Top Critical Controls for ICS/OT Cyber Security

Text

Read the LinkedIn post on the top Critical Controls for ICS/OT Cyber Security. The post can be found at https://www.linkedin.com/posts/mikeholcomb_the-top-ten-icsot-cyber-security-controls-activity-7191814014316732416-HfZg.

Answer the following questions based on the post.

1. Which of the listed Critical Controls reduces the most risk?

2. Which of the listed Critical Controls reduces risk the least?

3. Which of the listed Critical Controls should be addressed first?

4. Which of the listed Critical Controls should be addressed last?

5. In which Critical Control would the business determine its overall exposure in the event of a significant incident? For example, if a company was calculating how much money they would lose per hour of downtime, this type of activity would fall under which control?

6. Which Critical Control ensures that operators can restore operations as quickly and as efficiently as possible in the event of a significant incident?

7. Which of the Critical Controls listed involves deploying an IT/OT DMZ between the IT and OT networks?

8. Which of the Critical Controls listed involves establishing an asset register and ensuring that it is populated and kept up to date over time?

9. Which of the Critical Controls listed involves deploying network traffic sensors to provide the OT security team with the ability to watch network activity for anomalies which might indicate an operational or security issue is occurring?

10. Which of the Critical Controls is often exploited when an attacker gains control over a vendor's assets from over the Internet?

11. Which of the Critical Controls should be implemented as early as possible in the design of an ICS/OT environment?

12. Which of the Critical Controls is less a technical control and more of a “people” one?

13. Which of the Critical Controls includes performing a risk assessment of a known issue in the ICS/OT network which could be exploited by an attacker?

Part 3: Main Types of Control Systems & Protocols

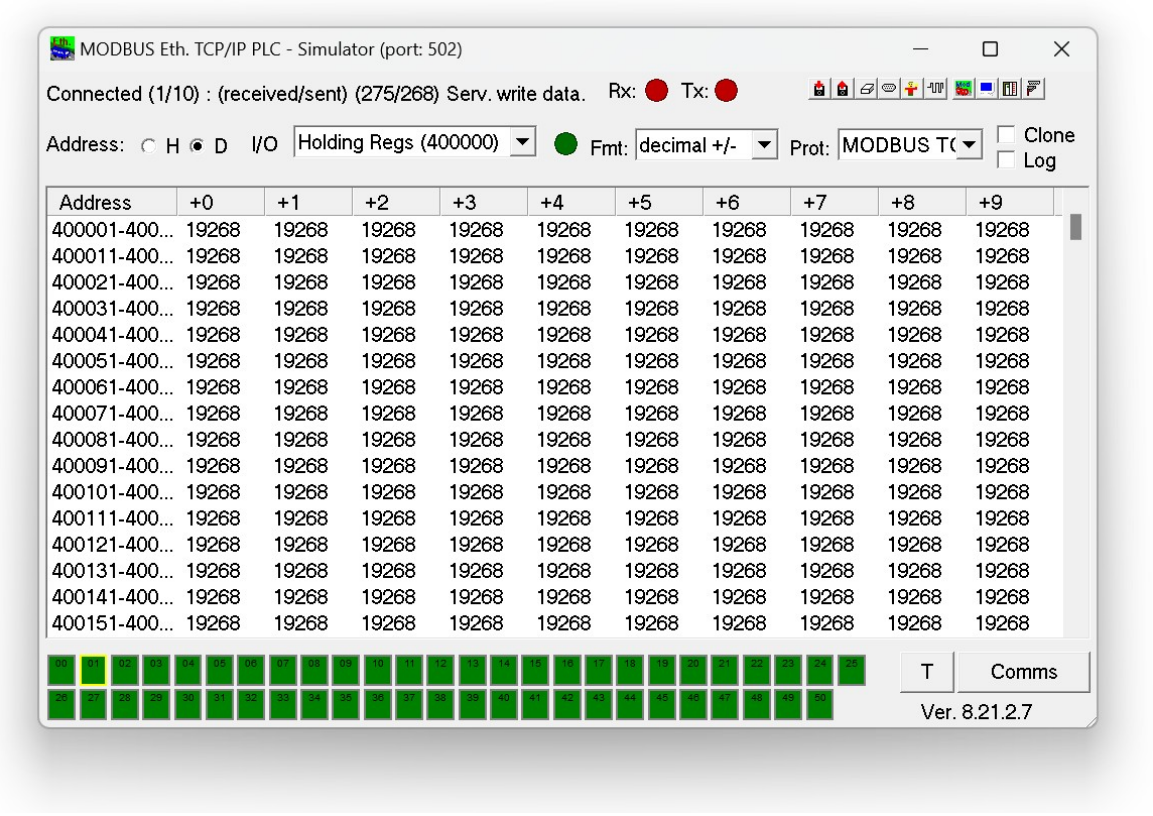
In Part 3, we talk about different types of control systems as well as different control system protocols, including but not limited to: - How a Power Plant is Built - Control System Engineering Terms - Control Systems (e.g., PLCs, HMIs, SIS, DCS, data historians) - ICS Protocols (e.g., Modbus, S7, OPC, OPC UA) - Capturing and Viewing ICS Protocols

Exercise 3.1: Installing a Modbus Server & Client

1. Download the Modbus Server (ModRSSim2) from https://sourceforge.net/projects/modrssim2/.

2. The file downloaded is a stand-alone executable and does not need to be installed to run. Run the ModRSSim2.exe file.

   You should see a screen like the following:



3. Now that the Modbus server is running, we need to install the client.

4. Download Modbus Poll from https://www.modbustools.com/download.html.

   NOTE: Modbus Poll is free to evaluate for 30 days.

5. The Modbus Poll application does need to be installed. Launch the installer file you downloaded – ModbusPollSetup64Bit.exe.

6. On the 'License Agreement" screen, review the general terms presented, check the box for "I accept the terms of the License Agreement" if you agree and click 'Next.'

7. On the “Choose Install Location” screen, accept the default by clicking ‘Next.’

8. On the “Choose Components” screen, accept the defaults by clicking ‘Next.’

9. On the second “Choose Components” screen, accept the defaults by click ‘Install.’

10. Once the installation is complete, run the Modbus Poll application.

11. When receiving the “this is an unregistered copy” message/window, click on “Register later.”

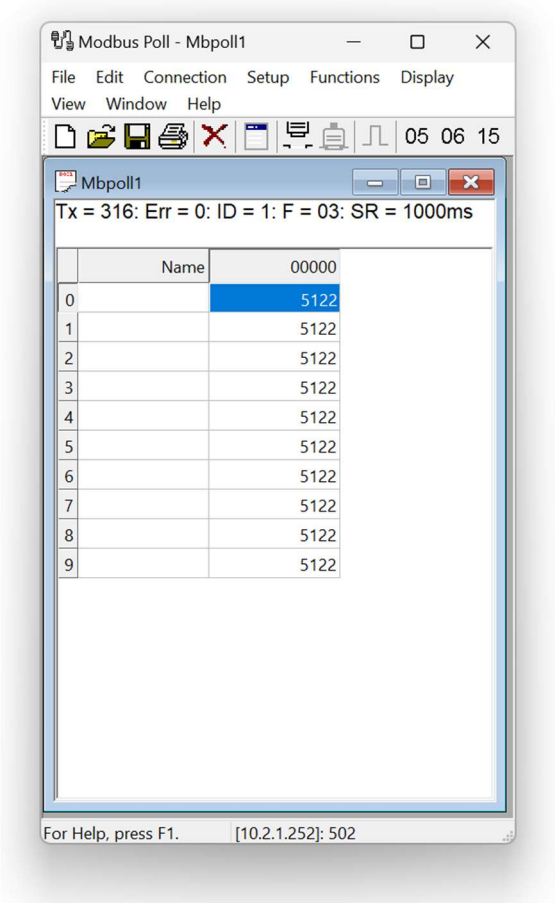
12. To connect the Modbus Poll app to the Modbus server running on your Windows system, click on the ‘Connection’ menu option and then select ‘Connect.’

13. In the ‘Connection Setup’ screen, under ‘Connection, select ‘Modbus TCP/IP.’

14. Under ‘Remote Modbus Server,’ ensure the localhost IP address of 127.0.0.1 is specified and click ‘OK.’

    NOTE: The default port for Modbus is TCP 502.

15. If connected correctly, the Modbus Poll client should be retrieving values (as seen below). These values should be continually changing and reflect the values displayed in the ModRSSim2 server.



16. The Modbus Poll client displays three columns. What are they?

17. What is particular about the second column? Why is this?

18. Leave both ModRSSim2 and Modbus Poll running to complete the next exercise.

Exercise 3.2: Installing Wireshark

1. Download Wireshark from https://www.wireshark.org/download.html.

2. Once downloaded, launch the Wireshark installation file.

3. On the 'Welcome to Wireshark x.x.x Setup' screen, click 'Next.'

4. On the 'License Agreement' screen, review the general terms presented and click Noted.'

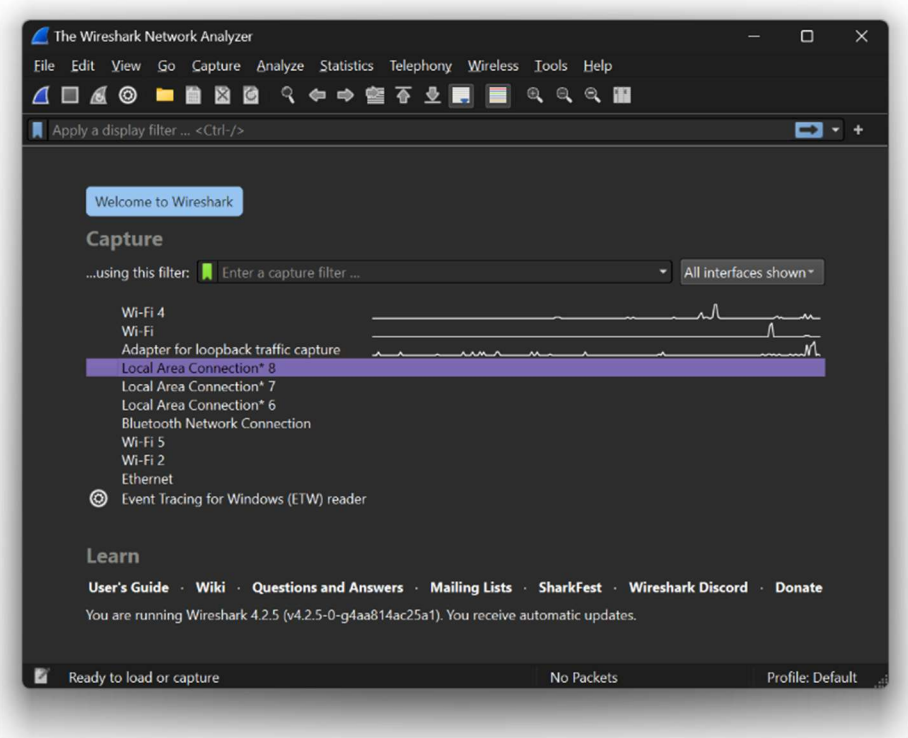
5. On the 'Your donations keep these releases coming,' screen, click 'Next.'

6. On the 'Choose Components' screen, accept the defaults and choose 'Next.'

7. On the ‘Additional Tasks’ screen, accept the defaults and choose ‘Next.’
8. On the ‘Choose Install Location’ screen, accept the defaults and choose ‘Next.’
9. On the ‘Packet Capture’ screen, accept the defaults and choose ‘Next.’
10. On the ‘USB Capture screen, accept the defaults and choose ‘Install.’
11. Once the installation completes, click ‘Next.’
12. On the ‘Completing Wireshark x.x.x Setup’ screen, click ‘Finish.’

Exercise 3.3: Capturing Network Traffic with Wireshark

1. Launch Wireshark.
2. Once Wireshark launches, you’ll see the default ‘Capture’ screen which lists each of the network interfaces in your system running Wireshark along with a line graph to note any activity on each interface.



3. Select the network interface which has visibility into the Modbus server and Modbus Poll client traffic.

   Note: This could be 'Adapter for loopback traffic capture' or another interface such as your default 'Wi-Fi' connection.

4. As the packet capture continues, if you selected the correct interface, you should not only see network packets generated, but you should see Modbus/TCP packets as seen below.

Protocol	Length	Info
Modbus/TCP	66	Query: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
Modbus/TCP	83	Response: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
Modbus/TCP	66	Query: Trans: 1; Unit: 1, Func: 3: Read Holding Registers
Modbus/TCP	83	Response: Trans: 1; Unit: 1, Func: 3: Read Holding Registers

5. If you see Modbus/TCP packets, you've selected the correct interface. Let the network capture run for at least one minute. Stop the capture by clicking the red stop button on the top menu.

   If you do not see Modbus/TCP packets, it is more than likely you've selected an incorrect interface. Close Wireshark and repeat this exercise starting at Step #1.

6. Once the capture is stopped, display only the Modbus/TCP traffic by typing in modbus in the filter bar near the top of the window and hit 'Enter.' The filter bar has what appears to be a blue bookmark on the left and buttons with an X and right arrow button on the right.

7. Select one of the packets by double clicking on it. The packet should be opened in its own window.
8. In the top half of the window, you should see lines representing the different OSI layers captured – Frame, Ethernet II, Internet Protocol, Transmission Control Protocol, Modbus/TCP and Modbus.

9. Expand the 'Frame' section.

   a. Which interface is listed?

   b. What is the frame number?

   c. What is the frame length?

10. Expand the 'Ethernet II' section.

a. What is the Destination address?

b. What is the Source address?

c. What type of addresses are the Source and Destination address?

d. What protocol is listed under Type?

11. Expand the ‘Internet Protocol’ section.

    a. What version of IP is captured?

    b. What number is listed under Protocol? What transmission protocol does this represent?

    c. What is the Destination address?

    d. What is the Source address?

    e. What type of addresses are the Source and Destination address?

12. Expand the ‘Transmission Control Protocol’ section.

    a. What is the Source Port?

    b. What is the Destination Port?

    c. Which TCP flags are set?

    d. How large is the TCP payload?

    e. What is the size of the TCP header and CRC (tail)?

       NOTE: Subtract the total length of the packet from the TCP header length.

13. Expand the ‘Modbus/TCP’ section.

    a. Which Transaction Identifier is listed?

    b. What is the Protocol Identifier for the packet?

    c. What is the Unit Identifier for the packet?

14. Expand the ‘Modbus’ section.

a. Which Modbus command is captured being issued by the Modbus client to the server?

b. How many registers are requested by the single command?

c. What is the value of one of the returned registers?

d. Is this a binary value?

Exercise 3.4: Using Wireshark Statistics

1. Open capture1.pcapng from the course files in Wireshark.
2. Use the Protocol Hierarchy from under the Statistics menu to answer the following questions.

    a. What percentage of captured packets are IPv4?

    b. What percentage of captured packets are TCP?

    c. What percentage of captured packets are UDP?

    d. What percentage of captured packets are ICMP?

    e. How many packets are DNS packets?

    f. How many packets are NTP packets?

    g. How many packets are ICMPv6 packets?

    h. How much traffic in total was captured? In Bytes? In Megabytes?

    i. How much HTTP traffic was captured? In Bytes? In Megabytes?

3. Use the Conversations option from under the Statistics menu to answer the following questions.

    a. How many TCP connections are identified in the packet capture?

    b. Which host is responsible for sending the most packets?

    c. What is the total amount of traffic sent by this host?

    d. What is the destination IP address for this traffic?

e. What is the listed duration for this traffic?

f. What is an internal IP address captured in the file?

4. Use the Resolved Addresses option from under the Statistics menu to answer the following questions.

    a. What does the IP address of 104.244.42.194 resolve to?

    b. What does the IP address of 34.198.182.201 resolve to?

    c. What does the MAC address of 01:00:1d:00:00:05 resolve to?

    d. What IP address does www.kali.org resolve to?

Exercise 3.5: Inspecting TCP/IP Traffic in Wireshark

1. Still using capture1.pcapng from the course files, use Wireshark to answer the following questions:

    a. How many packets are in the capture file?

    b. What is the source IP address of Packet #452?

    c. What is the destination IP address of Packet #452?

    d. Which IP address above is a private (internal use only) address?

    e. Which IP address above is a public (Internet-based) address?

    f. Examining the packet further, what type of packet is this? HINT: Think three-way handshake.

    g. What is the destination port for this packet? What is this connection more than likely being used for?

    h. After the connection is established, a file is accessed. What is the name of this file?

    i. What type of activity is occurring in Packet #858?

    j. What type of activity is occurring in Packet #859?

    k. What is the MAC address of the system at 192.168.32.1?

2. Open capture2.pcapng from the course files in Wireshark. Use Wireshark to answer the following questions.

    a. What application protocols make up 16.7% of the captured traffic?

    b. What is the first packet in the capture where this type of traffic starts?

    c. Right click on the packet and choose 'Follow' -> 'TCP Stream'.

    d. What type of information is displayed? What is "special" about it?

    e. How is Wireshark able to read the traffic identified in this way?

    f. Find a second session made with the same protocol. Examine it by following the TCP stream.

    g. What is the difference in this second session?

    h. What credentials are used to log on to the FTP site?

Exercise 3.6: Inspecting ICS/OT Protocols in Wireshark

1. Open 'capture3.pcap' from the course files in Wireshark.

   Which ICS/OT protocol is captured in the file?

2. Based on the queries and responses captured, what is the IP address of the PLC?

3. What is the IP address of the Engineering Workstation communicating with the PLC?

4. Which Modbus command is first sent to the PLC?

5. What is the purpose of this command?

6. Which Modbus command is sent in packet #23 to the PLC?

7. What is the purpose of this command?

8. What is the value of the coil read in Packet #51?

9. How many coils are read in Packet #54? What are their values?

10. How many registers are read in Packet #57? What are their values?

11. Which register is updated in Packet #476? What is its value?

12. What is the value of Register 198?

13. What value is written in Packet #1692? What is this in decimal? Which register is updated with his value?

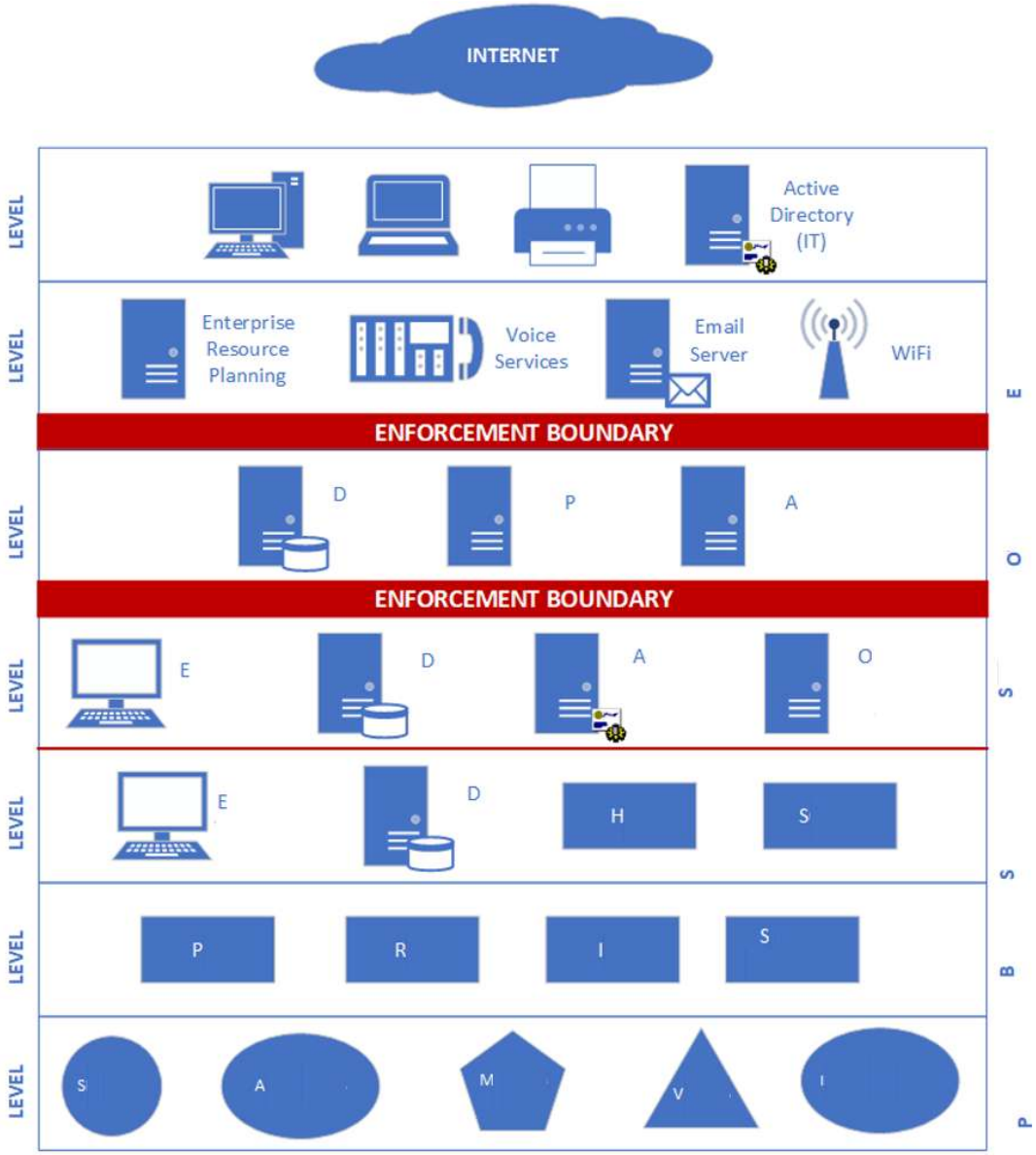
14. What is the last value written to the PLC?

Part 4: Secure Network Architecture

The most important control in reducing risk in ICS/OT networks is ensuring that that OT network (and the IT network it is connected to) have traffic properly controlled. For organizations just starting their ICS/OT cyber security journey, the expanded Purdue Model can be an excellent place to start having discussions on how to protect the OT network. This always starts with the implementation of the IT/OT DMZ which sits between the IT and OT networks. And, where possible, should not allow the IT network to originate connections into the OT network.

Exercise 4.1: The Expanded Purdue Model

Examine the diagram of the expanded Purdue Model and answer the following questions.



1. Which level of the expanded Purdue Model is connected directly to the Internet?
2. Which level of the expanded Purdue Model did not exist in the original reference model?
3. What is this level most referred to as?
4. How should traffic flow be configured for this level?
5. Which level does the OT Active Director domain controller reside on?
6. Which level is referred to as the Process level? Why?
7. At which level should the SIS be located?
8. Which network should the SIS be connected to? IT? OT?
9. Using the "one up, one down rule," which levels should Level 3 be able to communicate with?
10. At which two levels are Engineering Workstations typically used?
11. Where should the OT patching server be located for downloading patches from the IT network?
12. How should communication for the OT patching server be configured?
13. Where could data historians be located?
14. How should communication for the data historians be configured?
15. At which level of the expanded Purdue Model do actuators reside?
16. Which network should CCTV cameras be connected to? IT? OT?
17. Enforcement boundaries are implemented by using what type of appliances?
18. What is the best practice to consider when implementing these enforcement boundaries?
19. At which level should an HMI reside?
20. An HMI typically needs to be able to communicate with which other level?

Exercise 4.2: Reviewing IT/OT DMZ Access Control Lists (ACLs)

Often, the IT/OT DMZ can have its associated firewall rules misconfigured, potentially allowing attackers a route into the OT network from the back office. As the OT cyber security administrator for your plant, you're conducting a review of the firewall Access Control Lists which are configured on the external interface for the IT-to-DMZ firewall.

In your environment, it is not possible to prevent the IT network from originating connections into the OT network currently.

The Cisco firewall ACL is as follows:

```
1     permit tcp any host 10.2.1.5 eq 21
2     permit tcp any host 10.2.1.10 eq 80
3     permit tcp any host 10.2.1.10 eq 443
4     permit tcp any host 10.2.1.20 eq 3389
5     permit tcp any host 10.2.4.18 eq 502
6     permit icmp host 10.1.1.8 host 10.2.1.45
7     permit udp any host 10.2.1.66 eq 161
8     permit tcp host 10.1.1.1 any
```

After reviewing the ACL, answer the following questions to identify potential security concerns:

1. What are three potential security issues with the host at 10.2.1.5 being exposed as such?
2. What are three potential security issues with the host at 10.2.1.10 being exposed as such?
3. Which operating system is the host at 10.2.1.20 running?
4. What type of asset could the asset at 10.2.1.20 be?
5. What type of asset is the host at 10.2.4.18 more than likely?
6. What is unique about this IP address? What security considerations could it imply?
7. Why would ICMP be allowed from a particular internal IP address on the IT network?
8. What are three potential security issues with the asset at 10.2.1.66 being exposed as such?
9. Why should be concerned with the ACL listed on Line 8?
10. While not shown by default, what would Line 9 read if it was the last line of the Cisco ACL config?

Part 5: Asset Registers and Control Systems Inventory

One security control which is critical to ensuring the security of any ICS/OT network is the asset register. And yet, the importance of the asset register can often be overlooked by ICS/OT team members.

Exercise 5.1: Building an Asset Register with System Configs

1. Open the asset register file stored in the course Google Drive location. If you do not have access to Microsoft Excel, you can open the .csv version in Notepad/WordPad.

2. Review the asset register.

3. What type of environment does this appear to be an asset register for?

4. Why is it important to keep an asset register secure?

5. What vendor is listed as the manufacturer of the OT asset used to remotely control a plant process via a PLC?

6. Based on the listed MAC address, who is the associated vendor for this asset?

As an ICS/OT security analyst for your plant, you review the ARP cache on an engineering workstation in the OT network (see output below).

Use the information provided to add four additional assets to the asset register.

```
C:\Users\admin>arp -a

Interface: 192.168.1.210 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.1           00-02-fc-b0-42-77     dynamic
  192.168.1.50          00-08-06-d9-32-df     dynamic
  192.168.1.78          ac-64-17-55-8d-3e     dynamic
  192.168.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

7. Which three hosts can be found as dynamic entries in the engineering workstation's ARP cache?
8. Hosts located at .1 and .254 are usually what type of assets?
9. Which vendor manufactured the asset at 192.168.1.1?
10. Which vendor manufactured the other two "dynamic" assets?
11. Which additional host is listed?
12. How can you find the MAC address for this host?
13. Create a MAC address for this host and add it to your asset register.

Next, you review the configuration of one of your Cisco switches.

```
! EWS Subnet Switch

! Define VLANs
vlan 10
 name HOSTS_VLAN

! Interface Configuration
interface Vlan10
 ip address 192.168.1.1 255.255.255.0
 no shutdown

! Configure Access Ports
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast

interface FastEthernet0/2
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast

interface FastEthernet0/3
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast

! Assign IP Addresses to Hosts
ip dhcp pool HOST1
 network 192.168.1.0 255.255.255.0
```

```
 default-router 192.168.1.1
 host 192.168.1.230 255.255.255.0
 client-identifier 0100.1500.3c4d.5e6f

ip dhcp pool HOST2
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 host 192.168.1.231 255.255.255.0
 client-identifier 01d4.bed9.3d4e.5f6g

ip dhcp pool HOST3
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 host 192.168.1.232 255.255.255.0
 client-identifier 0100.4238.3e4f.5g6h

! Enable IP Routing
ip routing

! Configure Default Gateway
ip default-gateway 192.168.1.1
```

14. What are the IP addresses for the three new hosts discovered in the Cisco switch configuration?
15. What is “unique” about these three IP addresses?
16. Add these assets to the register. Include all relevant information.

Exercise 5.2: Building an Asset Register with Packet Captures

Using your previous Wireshark skills, examine capture4.pcap and answer the following questions.

1. What two IP addresses are discovered in the packet capture file?
2. What are the MAC addresses for these IP addresses?
3. Which vendor is associated with these MAC addresses?
4. Which port is being communicated with on the asset with the lower IP address?
5. What type of asset is this more than likely?
6. What is unique about the subnet associated with these IP addresses?
7. Which ICS/OT protocol is captured in the file? HINT: It isn't COTP.
8. Add these to your asset register with all relevant information.

One of the network administrators pings you to tell you they have the packet capture you requested from a "special" VLAN that was set up along with the OT network.

Examine capture5,pcap and answer the following questions.

9. Which two ICS/OT protocols are captured in the file?
10. What type of systems do these ICS/OT protocols typically support?
11. Are these assets typically located on the ICS/OT network or the IT network?
12. What other non-ICS/OT protocols are included in the file?
13. What is an RFC 1918 address?
14. Why is it important to note network communication with a non-RFC 1918 address?
15. Which entity is this non-RFC 1918 address associated with?
16. Who would you contact at this entity to discuss a potential cyber security attack?
17. By reviewing the who-Has packets, name three locations at the entity.
18. For more information on digging deeper into the BACnet protocol, review the following guide at

    https://guides.smartbuildingsacademy.com/definitive-guide-bacnet

Part 6: Threat & Vulnerability Management

Exercise 6.1: Building an IT Host Scanning Target

1. Download Metasploitable2 from https://sourceforge.net/projects/metasploitable/files/Metasploitable2/.

2. Unzip the downloaded file. Once unzipped, double click the Metasploitable.vmx file to have VMware Workstation automatically create a Metasploitable2 VM.

3. Run the Metasploitable2 VM by selecting “Power on this virtual machine.”

4. If you receive the "This virtual machine might have been moved or copied" message, select "I Copied It."

5. Once Metasploitable2 is up and running, login with a username and password of msfadmin.

6. Run the **`ifconfig`** command to determine which IP address was assigned to the host via DHCP. This assumes you have an available DHCP server on your network.

Exercise 6.2: Active Scanning

Active scanning is conducted when tools are used to send packets to IP addresses and ports to determine the presence of live hosts, open ports, running services and the version of those running services. While a port scanner such as Nmap would be used to do so, additional tools such as Nessus scan be used to scan specifically for vulnerabilities.

6.2.A Nmap Port Scan – Default Ports

1. To run a default Nmap scan against your target host, use the following command from a terminal window (where x.x.x.x is the target’s IP address).

```
nmap x.x.x.x
```

2. Review the output of the scan to answer the following questions.

a. How many closed ports are reported?

b. How many open ports are listed?

c. How many ports were tested?

d. Were both TCP and UDP ports tested? Or only one? If so, which?

e. How many total TCP and UDP ports exist on each system?

f. What are some of the ports that an attacker might be interested in?

g. Which is the first port listed that could be easily tested with a web browser?

h. What is the first port that we might use telnet to connect to?

i. What is the MAC address of the remote host?

j. What is the vendor associated with the MAC address?

6.2.B Nmap Port Scan – All Ports

1. Use the following command to run an nmap scan of all 65,535 TCP ports on the target system.

```
nmap x.x.x.x -p-
```

a. How many closed ports are reported?

b. How many open ports are listed?

c. How many ports were tested?

d. Were both TCP and UDP ports tested? Or only one? If so, which?

e. Would any of the newly discovered ports be of interest to an attacker? If so, which?

6.2.C Nmap Subnet Scan

1. To run a default Nmap scan against your local subnet, use the following command from a terminal window (where x.x.x.x/x is the address of your local subnet in CIDR notation).

```
nmap 192.168.1.0/24
```

2. Review the output of the scan to answer the following questions.

a. How many hosts were discovered on your local subnet?

b. How many closed ports are reported on each host?

c. How many open ports are listed on each host?

d. How many ports were tested on each host?

e. Did you discover any new ports that an attacker might be interested in?

f. What are the vendors associated with the MAC addresses of any newly discovered hosts?

3. Re-run the same scan with the switch to only display open ports. What command would you use?

4. Compare the results of the “open port” scan to the default subnet scan. What is the difference between the two?

6.2.D Nmap Service Scan

1. To run a Nmap Service scan against your target host on all ports, use the following command.

```
nmap x.x.x.x -p- -sV
```

2. Review the output of the Nmap service scan to answer the following questions.

a. How many FTP related services are on the target host? Which versions?

b. What version of OpenSSH is open?

c. What version of DNS server is running on the target?

d. What version of Apache is running on TCP 80?

e. What version of Apache is running on 8180?

f. What version of MySQL is running on the host? What port is it on?

g. What version of PostgreSQL is running on the host? What port is it on?

h. What version of VNC is available?

i. What version of SAMBA is on the host?

j. What is the Windows workgroup associated with the host?

6.2.E Nmap NSE “Script” Scan – Single Target Host

1. To run a Nmap Script scan against your target host on all ports, use the following command.

```
nmap x.x.x.x -p- -sC
```

2. Review the output to answer the following questions.

a. What type of access is available to remote users to the FTP service?

b. What is the additional information displayed for SSH?

c. What commands are supported by the default SMTP service?

d. Does the SMTP service offer encrypted email exchange?

e. What version of SSL does SMTP support?

f. What is the title page of the site running on TCP 80?

g. Based on the rpcinfo service output, what service is running on TCP 2049?

h. What is the MySQL status?

i. What is the MySQL salt?

j. What form of VNC authentication is in use?

k. What is the title of the webpage running on 8180?

l. What is the NetBIOS host name of the target host?

m. What is the system time reported on the target host?

n. Does the target host support SMB2?

Exercise 6.3: Scanning for IT Vulnerabilities

1. Download and install Tenable Nessus Professional from https://www.tenable.com/lp/campaigns/22/try-nessus-multiprdct/free-trial.

2. Once installed, login and create a new vulnerability scan by clicking on 'New Scan'.

3. On the 'Scan Templates' screen, click on 'Advanced Scan'.

4. On the 'Settings' tab, enter a name for your scan in the 'Name' field such as "Home Scan".

5. In the 'Targets' text box, enter the subnet range for your specific home network. For example, you might choose to use CIDR notation such as 192.168.1.0/24.

6. Click on the 'Discovery' selection and review the options.

7. Click on the 'Port Scanning' selection and review the options.

8. Click on the 'Plugins' tab and review the options.

9. Save your settings and run a vulnerability scan on your home network by click 'Launch'.

10. Review the results to answer all remaining questions below.

11. Reviewing the default set of 'Scan Templates' provided, what is the name of the malware that is

associated with MS17-010 vulnerability?

12. How would someone address the MS17-010 vulnerability on a vulnerable Windows host?

13. Name one other scan template you think would be of interest to a security administrator? Why did you choose this one?

14. On the 'Discovery' selection page, what does the 'ARP' option do?

15. If you wanted to ensure you scanned all available TCP ports rather than just the default set of ports,

what would you enter in the ‘Port scan range’ field?

16. On the ‘Credentials’ tab, what three options exist for supplying credentials?

17. Of the three options for supplying ‘Credentials’, which is the one that would most likely be used by

Nessus to login to a Linux-based host?

18. How many plugin checks exist to check for vulnerabilities in various DNS services?

19. How many plugin checks exist to check for vulnerabilities in Industrial Control Systems?

20. How many total plugin checks exist to search for the presence of vulnerabilities on Windows hosts?

21. Once you’ve completed the vulnerability scan of your home network including your Metasploitable2 host, provide a screenshot of the screen which shows all of your hosts and overview of the number of vulnerabilities discovered.

22. Except for the Metasploitable2 host, what is the most vulnerable host on your home

network?

23. What type of system is the most vulnerable host on your home network?

24. What is one step you can take to strengthen the security of the most vulnerable host?

25. For the Metasploitable2 host, how many vulnerabilities were discovered by Nessus?

26. What port is SSLv3 running on? What service is this port normally used for?

27. What is the password to the VNC service?

28. A backdoor was detected that was associated with what service? What port is this service running on?

29. When accessing the Bind Shell backdoor, what user name and password are required to remotely gain ‘root’ access to the host?

Part 7: OSINT for Control Systems

Exercise 7.1: Google Searches

While there are several ways to find Internet exposed PLCs, our friends at the NSA gave us a few methods for doing so in their ELITEWOLF project. While the project provided several Snort intrusion detection signatures for ICS/OT defenders to identify potentially malicious activity on their networks, the signatures also provided us with some Google searches to find PLCs.

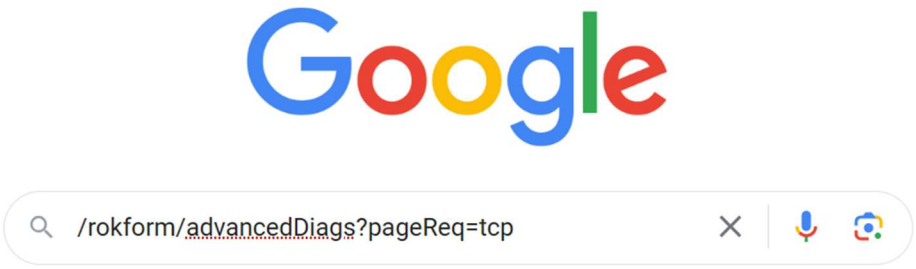
1. Access the ELITEWOLF project site at https://github.com/nsacyber/ELITEWOLF.

2. Select the 'ELITEWOLF_SNORT_AllenBradley_RockwellAutomation.txt' file.

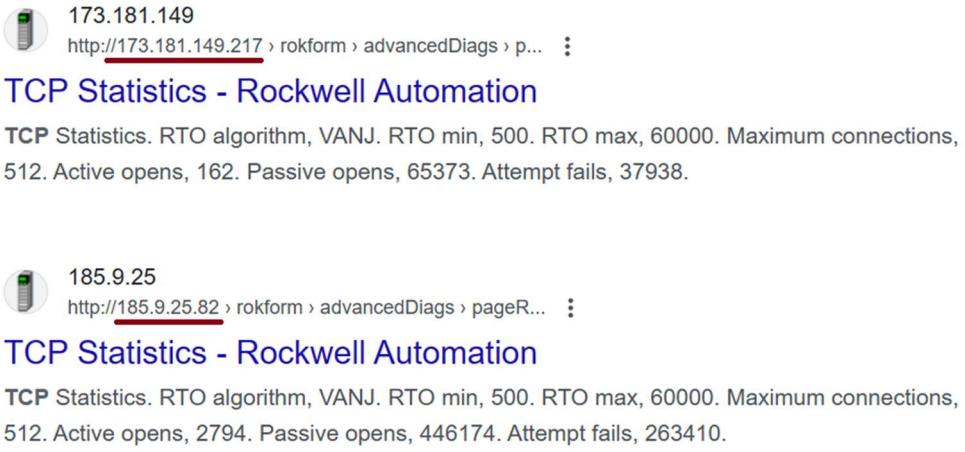
3. Looking at the last part of each Snort rule, the URL portion specified in the content: section can be used in Google to find Allen Bradley/Rockwell Automation PLCs exposed to the Internet.

```
TCP REQUEST"; content:"/rokform/advancedDiags?pageReq=tcp"; sid:1; rev:1;)
SYSTEM DATA DETAIL"; content:"/rokform/SysDataDetail?name="; sid:1; rev:1;)
UDP TABLE"; content:"/rokform/advancedDiags?pageReq=udptable"; sid:1; rev:1;)
TCP CONNECT"; content:"rokform/advancedDiags?pageReq=tcpconn"; sid:1; rev:1;)
IP ROUTE"; content:"/rokform/advancedDiags?pageReq=iproute"; sid:1; rev:1;)
GENERAL MEMORY"; content:"/rokform/advancedDiags?pageReq=genmem"; sid:1; rev:1;)
HEAP REQUEST"; content:"/rokform/advancedDiags?pageReq=heap"; sid:1; rev:1;)
ICMP REQUEST"; content:"/rokform/advancedDiags?pageReq=icmp"; sid:1; rev:1;)
ARP REQUEST"; content:"/rokform/advancedDiags?pageReq=arp"; sid:1; rev:1;)
UDP REQUEST"; content:"/rokform/advancedDiags?pageReq=udp"; sid:1; rev:1;)
IF REQUEST"; content:"/rokform/advancedDiags?pageReq=if"; sid:1; rev:1;)
IP REQUEST"; content:"/rokform/advancedDiags?pageReq=ip"; sid:1; rev:1;)
```

4. Go to Google and run a search for the first URL portion listed in the ELITEWOLF file as seen below.

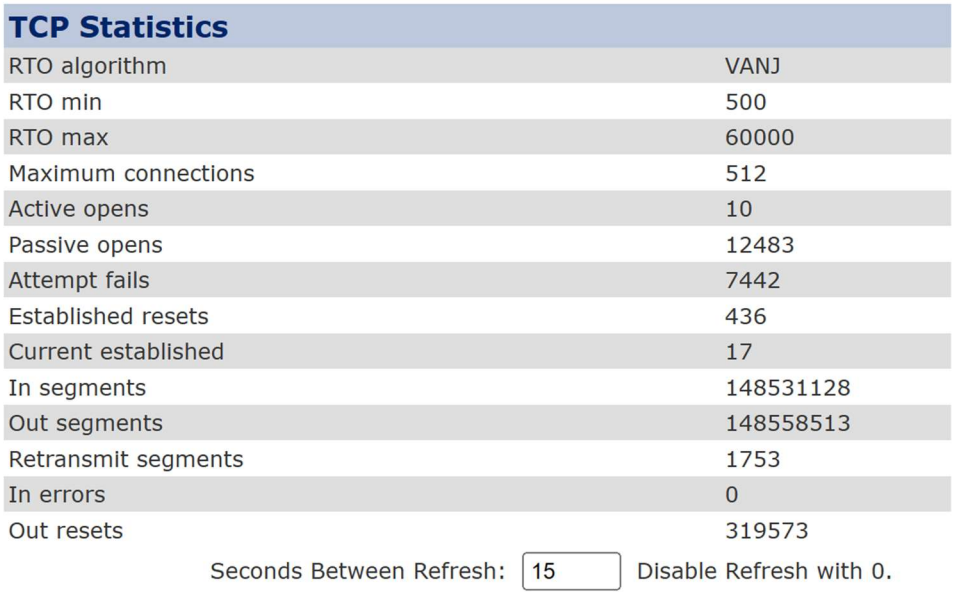


5. While some results will refer to PLC documentation and the ELITEWOLF Github page itself, most results will refer to actual PLCs exposed to the Internet. For example, my search results start with the two exposed PLCs at 173.181.149.217 and 185.9.25.82 as seen below.



As expected, based on the ELITEWOLF file we pulled the search string from, these appear to be AllenBradley/Rockwell Automation PLCs.

6. Click on one of the links for the exposed PLCs. You should see a web page that displays various statistics related to the PLC's TCP functionality such as seen below.



TCP Statistics	
RTO algorithm	VANJ
RTO min	500
RTO max	60000
Maximum connections	512
Active opens	10
Passive opens	12483
Attempt fails	7442
Established resets	436
Current established	17
In segments	148531128
Out segments	148558513
Retransmit segments	1753
In errors	0
Out resets	319573

Seconds Between Refresh: 15 Disable Refresh with 0.

7. While each of the URLs can provide interesting pieces of information, I'm always fascinated when I can see the netstat output of a remote system. Run a Google search using the partial URL of '/rokform/advancedDiags?pageReq=tcpconn'.

8. Access the URL. You should see the exposed PLCs netstat information, showing all IP addresses (external AND internal) that are communicating with the PLC.

TCP Connection Table

State	Local Address	Local Port	Remote Address	Remote Port
FIN_WAIT_2	192.168.1.100	80	60.16.221.67	58617
ESTABLISHED	192.168.1.100	80	71.85.4.152	54057
ESTABLISHED	192.168.1.100	80	71.85.4.152	54058
ESTABLISHED	192.168.1.100	80	167.94.146.53	54662
ESTABLISHED	192.168.1.100	44818	144.178.250.4	62408
ESTABLISHED	192.168.1.100	44818	192.168.1.200	49156
ESTABLISHED	192.168.1.100	44818	198.235.24.93	54495
ESTABLISHED	192.168.1.100	44818	205.210.31.145	51535
ESTABLISHED	192.168.1.100	53833	192.168.1.125	44818
ESTABLISHED	192.168.1.100	53835	192.168.1.123	44818
ESTABLISHED	192.168.1.100	53837	192.168.1.121	44818

9. In the previous example, there are several items of note:

   - The internal IP address of the PLC is 192.168.1.100.
   - The public IP address is the same as the IP in the URL.
   - The PLC is communicating with multiple internal AND external IP addresses over HTTP (TCP port 80) and EthernetIP (TCP port 44818).

10. If you look up the GeoIP information for the public IP addresses found on the **tcpconn** page you had visited., you can find a lot of interesting items of note.

```
IP address found: 60.16.221.67 - Location: Shenyang, Liaoning, CN
IP address found: 192.168.1.130 - Location: Private IP Address - No Location
IP address found: 192.168.1.131 - Location: Private IP Address - No Location
IP address found: 192.168.1.127 - Location: Private IP Address - No Location
IP address found: 71.85.4.152 - Location: Simpsonville, South Carolina, US
IP address found: 192.168.1.100 - Location: Private IP Address - No Location
IP address found: 192.168.1.122 - Location: Private IP Address - No Location
IP address found: 205.210.31.145 - Location: São Paulo, São Paulo, BR
IP address found: 192.168.1.125 - Location: Private IP Address - No Location
IP address found: 144.178.250.4 - Location: Brussels, Brussels Capital, BE
```

In the sample above, we can note that:

   - The PLC is being remotely accessed from Shenyang in China, Sao Paulo in Brazil, Brussels in Germany and (of course) Simpsonville, South Carolina, United States.
   - Internal hosts communicating with the PLC include 192.1168.1.100,192.168.1.122,192.168.1.125, 192.168.1.127,192.168.1.130 and 192.168.1.131.

So it appears we are not the only external visitors to the PLC's web interface. Not only that, but we have also enumerated more than a few internal hosts on the PLCs ICS/OT network.

Exercise 7.2: Using WHOIS for OSINT

1. Use the dnslytics.com site to perform the following research and answer the associated question.

2. In the search field, supply the IP address of 98.99.252.118 and click the magnifying glass icon to run your search.

3. On the next screen, select 'IP Report 98.99.252.118.'

4. Based on the provided description, which company is the IP address associated with?

   NOTE: I'm sitting in one of their stores right now as I write this lab. 😊

5. What complete IP range is associated with this IP address?

6. What is the Autonomous System (AS) Number associated with this IP address?

7. Does this IP address appear on any of the 28 DNS blacklists tracked by DNSlytics?

8. When was the associated domain name for this IP address registered?

9. When was the associated registration information last updated?

10. Which physical address is associated with the owner for this IP address?

11. What is unique about this physical address?

12. Which Starbucks employee is associated with the domain registration?

13. Which contact information of theirs is listed?

    NOTE: Keep this information handy as we'll be using it in the next exercise.

14. Which email address would you send an email to about a suspected cyber-attack coming from that IP address?

Exercise 7.3: Using DNS for OSINT

1. Use the dnsdumpster.com site to perform the following research and answer the associated question.

2. In the search field, supply the domain name of panerabread.com and run a search.

3. Which DNS servers are associated with this domain?

4. What are the IP addresses of the mail servers for panerabread.com?

5. Based on the associated TXT records, what would be one item of interest to attackers related to the domain?

6. How many host ('A') records are returned by DNSdumpster?

7. Based on the host record names, which of these hosts might be of interest to an attacker?

8. The last column represents the Autonomous System (AS) Number and associated name for each IP range. What are some of the different entities listed?

9. What could the information in Question #8 above be used to deduce about each system?

10. Based on that information, which host might be of interest to an attacker wanting a foothold on the company's internal corporate network?

Exercise 7.4: Using LinkedIn for OSINT

1. Use LinkedIn to perform the following research and answer the associated question.

2. Using the employee's name found in Exercise 7.2, run a LinkedIn search for this person.

   NOTE: To help, use only their first name, last name and company name for your search.

3. How long has this person been with the company?

4. What is this person's current job title?

5. When were they promoted into this position?

6. What was this person's original job title when they started with the company?

7. Which web conferencing and instant messaging platform does this company use?

8. Which IPAM solution did this company use 13 years ago (and maybe today)?

9. What was this person's first job according to LinkedIn?

10. Which company did this person work for?

11. When was this person's last post on LinkedIn?

12. Would this person be considered an active participant on LinkedIn?

13. What sensitive information could be exposed by someone's LinkedIn 'Projects' section?

14. What LinkedIn groups is this person a member of?

Exercise 7.5: Using Shodan for OSINT

NOTE: Depending on when you are performing this lab, the results might not matched based on the answers as the systems in question might have changed.

1. Use Shodan (shodan.io) to perform the following research and answer the associated question.

   NOTE: Shodan free accounts are limited to two pages of results and do not have access to some features.

2. Once logged in, click 'Explore' in the upper left corner of the main page.

3. Next, click 'Industrial Control Systems.' You'll be presented with a list of commonly seen ICS/OT protocols on the Internet.

4. Click 'EXPLORE MODBUS.'

5. What search string does Shodan use to look for hosts running Modbus?

6. What is the default TCP port number associated with Modbus?

7. Why is this not necessarily accurate in finding hosts running Modbus exposed to the Internet?

8. Run a Shodan search on the IP address 109.95.176.245 which has the default Modbus port exposed.

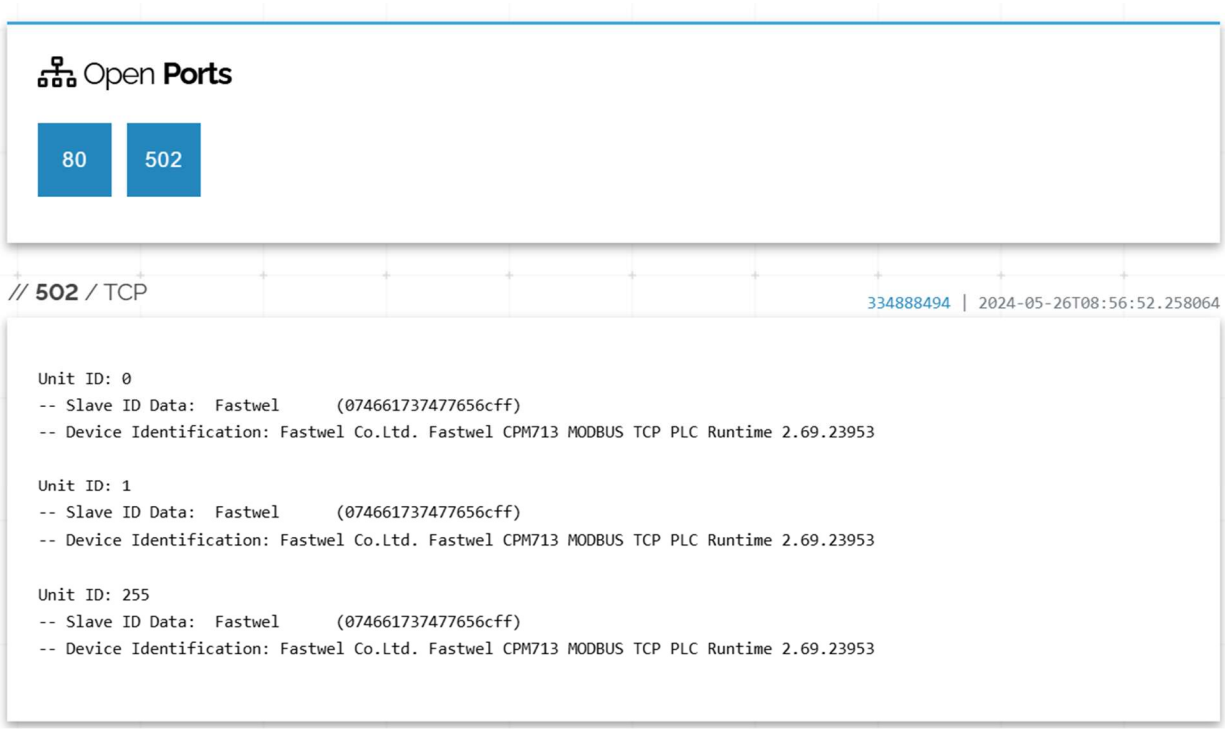
   Rather than Modbus, what service is running on this host? What is it used for?

9. Run a Shodan search for 'port:502 modbus.' You should now receive a number of more relevant hits such as the one seen below.

10. Click on the IP address for the host running Modbus you identified.

11. What other ports are running on the host?

    For example, the host seen above not only has the Modbus service running, but also appears to have a web server listening on TCP port 80.



12. Based on the information presented in the example above, what type of ICS/OT asset is this?

13. What is the assets model type?

14. Find a picture of this type of ICS/OT asset.

15. What are some of the security risks associated with exposing an ICS/OT protocol like Modbus to the Internet?

16. What are some of the security risks associated with exposing a web service on this device to the Internet?

17. Another way to find ICS/OT assets on the Internet is to run a search for common ICS/OT vendor names.

    Run a new Shodan search for “Schneider Electric”.

    Most of the devices returned should be Schneider Electric PLCs that are exposed to the Internet.

18. How many assets which advertise “Schneider Electric” as part of their service banner do you see exposed to the Internet?

19. One other way covered during the course was to run Shodan searches for the actual names for ICS/OT assets.

    Run a new Shodan search for “Programmable Logic Controller”.

20. Now how many hosts do you see through Shodan?

21. What other brands of PLCs do you see exposed to the Internet besides the earlier Schneider Electric ones?

Part 8: Incident Detection & Response

Exercise 8.1: Backdoors & Breaches (ICS OT Core Deck)

1. Access the Backdoors & Breaches site to play online at https://play.backdoorsandbreaches.com/.

2. Click on the link for "ICS OT Core Deck." This will load a new B&B game to play.

   To learn how to play B&B, watch this YouTube video with one of its creators, Jason Blanchard, explaining the game play - https://www.youtube.com/watch?v=pMY2HXUrKsg.

3. You can either play the online version as explained in the YouTube video or simply take a look at the select cards.

4. Having been developed primarily by Dragos, these cards reflect real world scenarios that you would see when responding to different ICS/OT cyber security incidents.

5. Be sure to cycle through as many of the card types to get a good feel for how various ICS/OT incidents occur.
   a. Initial Compromise
   b. Pivot and Escalate
   c. C2 and Exfil
   d. Persistence

   Don't forget the various procedures which you could emulate in your environment and then injects which can be good for a laugh here or there!

Part 9: Industry Standards & Regulations

There are no labs for this part currently.

Part 10: Introduction to ICS/OT Penetration Testing

There are no labs for this part currently.

Appendix A: Answer Key

Part 1: Course Introduction

There are no questions and answers for this part.

Part 2: ICS/OT Cybersecurity Overview

Exercise 2.1: Top Critical Controls for ICS/OT Cyber Security

1. Secure Network Architecture
2. IT/OT Partnership
3. Secure Network Architecture
4. IT/OT Partnership
5. Conducting Risk Assessments
6. Backup & Recovery
7. Secure Network Architecture
8. Asset Inventory (Hardware, Software & Firmware)
9. Network Security Monitoring
10. Secure Remote Access
11. Secure Network Architecture
12. Employee Education & Awareness (as well as IT/OT Partnership)
13. Continuous Vulnerability Management

Part 3: Control Systems & Protocols

Exercise 3.1: Installing a Modbus Server & Client

16. Row Identifier, Name and Value
17. The second column is blank. The Modbus server does not provide this information.

Exercise 3.2: Installing Wireshark

There are no questions and answers for this exercise.

Exercise 3.3: Capturing Network Traffic with Wireshark

9a. Answers will vary. The network interface card should be listed with the term 'interface.'

9b. Answers will vary.

9c. Answers will vary.

10a. Answers will vary. You're looking for a MAC address such as a1-b2-c3-d4-e4-f6.

10b. Answers will vary. You're looking for a MAC address such as a1-b2-c3-d4-e4-f6.

10c. MAC addresses

10d. IPv4 (0x0800)

11a. IPv4

11b. 6

11c. 127.0.0.1 (or your specific IP address)

11d. 127.0.0.1 (or your specific IP address)

11e. Local addresses

12a. Answers will vary. This should be seen as a high order random port.

12b. TCP 502

12c. Answers will vary.

12d. Answers will vary.

12e. Answers will vary.

13a. Answers will vary.

13b. Answers will vary.

13c. Answers will vary.

14a. Read Holding Registers

14b. 10

14c. Answers will vary.

14d. No

Exercise 3.4: Using Wireshark Statistics

2a. 98.2%

2b. 86.5%

2c. 8.7%

2d. 2.9%

2e. 518

2f. 10

2g. 8

2h. 8,238,801 Bytes / 7.8 MB

2i. 1,664,406 Bytes / 1.6 MB

3a. 30

3b. 192.168.33.95

3c. 920 bytes

3d. 38.229.71.1

3e. 18481.4411

3f. Any address which begins with 192.168.33.

4a. api.twitter.com

4b. www.nethunter.com

4c. Cabletron-PVST-BPDU

4d. 192.124.249.10

Exercise 3.5: Inspecting TCP/IP Traffic in Wireshark

1a. 6,085

1b. 192.168.33.95

1c. 209.190.218.107

1d. 192.168.33.95

1e. 209.190.218.107

1f. SYN packet

1g. TCP port 80; more than likely the packet is being used to establish a connection with a web server.

1h. success.txt

1i. DNS lookup/name resolution for an IPv4 address

1j. DNS lookup/name resolution for an IPv6 address

1k. a0:36:9f:92:ca:70

2a. File Transfer Protocol (FTP)

2b. Packet #38

2d. The cleartext communication over FTP.

2e. FTP traffic is unencrypted by default.

2g. In the first session, the user is unable to login with the credentials provided. In the second session, the user is able to login.

2h. Username: joseph / Password: StarWars@123

Exercise 3.6: Inspecting ICS/OT Protocols in Wireshark

1. Modbus (Modbus/TCP)

2. 10.0.0.3

3. 10.0.0.57

4. Force Listen Only Mode

5.

6. Clear Counters and Diagnostic Register

7.

8. 1

9. 2 (0 & 0)

10. 2 (9 & 24)

11. 101 (0000)

12. 0

13. 003c / 60 / 502

14. 0000

Part 4: Secure Network Architecture

Exercise 4.1: The Expanded Purdue Model

1. Level 5

2. Level 3.5

3. IT/OT DMZ

4. Only traffic from the IT/OT DMZ to IT should be allowed. IT should not be allowed to make connections into the IT/OT DMZ.

5. Level 3

6. Level 0. This is where the Process takes place where the physical systems in the real world operate.

7. Level 2

8. None. It should be airgapped.

9. Levels 2 and 3.5

10. Levels 2 and 3

11. Level 3.5

12. An OT patching server on the OT network at Level 3 should pull patches from the patching server in the IT/OT DMZ (Level 3.5) which pulls the patches from the IT network.

13. Typically on levels 2, 3 and 3.5 (as well as potentially in the IT network).

14. Traffic is only sent up through the Purdue Model layers towards IT, never down.

15. Level 0

16. CCTV cameras should not be on either the IT or OT network. If you had to choose, CCTV cameras should reside on the IT network.

17. Firewalls

18. Consider using two physical firewalls from two different vendors.

19. Level 2

20. Level 1 (where the PLCs it controls reside)

Exercise 4.2: Reviewing IT/OT DMZ Access Control Lists (ACLs)

1. TCP port 21 is normally associated with FTP which can have several security issues including that FTP is an unencrypted protocol, the FTP service could have software vulnerabilities and FTP credentials could be easily guessed.

2. TCP port 80 and 443 are normally associated with website access which can have several security issues including HTTP traffic over TCP port 80 is unencrypted, the associated web services could have software vulnerabilities and the web application could have its own vulnerabilities.

3. Windows

4. A Windows workstation or server (e.g., data historian, domain controller)

5. PLC

6. The IP address for the PLC is on another subnet from the other hosts.

7. The single source IP address could be used for monitoring uptime of specific hosts.

8. UDP port 161 is normally associated with SNMP which can have several security issues including that older versions of SNMP are unencrypted, most SNMP services are implemented with the default community string (a.k.a. password) and provide relevant information about the host that could be used by attackers.

9. The ACL allows the host at 10.1.1.1 to access ALL hosts on ALL ports.

10. deny ip any any

Part 5: Asset Registers and Control Systems Inventory

Exercise 5.1: Building an Asset Register with System Configs

3. A power plant

4. The asset register could aid attackers into compromising the environment.

5. Schneider Electric

6. Siemens AG

7. 192.168.1.1, 192.168.1.50 and 192.168.1.78

8. Routers (or switches acting as routers)

9. Cisco Systems, Inc.

10. Siemens AG

11. 192.168.1.210

12. ipconfig /all

13. No answer required.

14. 192.168.1.230, 192.168.1.231, 192.168.1.232

15. These are dynamic IP addresses assigned to specific hosts by the switch via DHCP. These hosts are identified by their MAC addresses.

Exercise 5.2: Building an Asset Register with Packet Captures

1. 192.168.25.131, 192.168.25.177

2. 192.168.25.131 = 00:1c:06:0f:bd:e5, 192.168.25.177 = 00:50:56:2b:5c:65

3. 192.168.25.131 = Siemens, 192.168.25.177 = VMware

4. TCP port 102

5. PLC

6. It is different than the other subnets found in the asset registry.

7. Siemens' S7

8. No answer required.

9. BACnet-APDU and BVLC

10. Building Automation Controls

11. Typically located on the IT network.

12. HTTP

13. An RFC 1918 address is one that is reserved for private internal use and is not directly routable on the Internet.

14. Communication with a non-RFC 1918 address, otherwise referred to as a public or Internet address, would typically indicate the ICS/OT network has active communication with a host on the Internet.

15. Florida International University

16. David Rotella

17. Valid locations would include FIU-SOUTH-NAE35, FIU-SOUT-NAE36 and FIU-SOUTH-NAE27.

Part 6: Threat & Vulnerability Management

Exercise 6.1: Building an IT Host Scanning Target

No answers required for this exercise.

Exercise 6.2: Active Scanning

6.2.A Nmap Port Scan - Default Ports

1. No answer required.

2a. 977 closed ports

2b. 23

2c. 1,000

2d. Only TCP ports

2e. 65,535 TCP ports and 65,535 UDP ports

2f. Any port could be of interest to an attacker, particularly those associated with known services that are typically vulnerable such as FTP and Telnet.

2g. TCP port 80

2h. TCP port 21

2i. Answer will vary.

2j. Answer will vary. Should be the vendor of your virtualization platform.

6.2.B Nmap Port Scan - All Ports

1a. 65,505 closed ports

1b. 30 open ports

1c. 65,5345

1d. Only TCP ports

1e. Any perhaps though we'll have more context after we perform service/script scans.

6.2.C Nmap Subnet Scan

1. No answer required.

2a. Answer will vary.

2b. Answer will vary.

2c. Answer will vary.

2d. Answer will vary.

2e. Answer will vary.

2f. Answer will vary.

3. Answer will vary.

4. Answer will vary.

6.2.D Nmap Service Scan

1. No answer required.

2a. 2

2b. OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

2c. ISC BIND 9.4.2

2d. Apache httpd 2.2.8 ((Ubuntu) DAV/2)

2e. Apache Tomcat/Coyote JSP engine 1.1

2f. MySQL 5.0.51a-3ubuntu5 on TCP 3306

2g. PostgreSQL DB 8.3.0 - 8.3.7 on TCP 5432

2h. VNC (protocol 3.3)

2i. Samba smbd 3.X - 4.X

2j. Workgroup

6.2.E Nmap NSE "Script" Scan - Single Target Host

1. No answer required.

2a. Anonymous access

2b. Public SSH keys

2c. PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

2d. Yes

2e. SSLv2

2f. Metasploitable2 - Linux

2g. NFS

2h. Autocommit

2i. /WF8(\wcknf4pYNZY1(p

2j. VNC Authentication (2)

2k. Apache Tomcat/5.5

2l. metasploitable

2m. Answer will vary.

2n. No

Appendix B: List of Resources (Books)

1. "Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers" by Andy Greenberg

An incredible introduction to the world of ICS/OT cyber security and why it is needed in protecting the world around us! It becomes even more important in helping explain the geopolitical considerations of cyber security.

2. "Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions" by Clint Bodungen, Stephen Hilt, Aaron Shbeeb, Bryan Singer and Kyle Wilhoit

Who doesn't love to learn about how to break into ICS/OT networks?

3. "Practical Industrial Cyber Security: ICS, Industry 4.0 & IIoT" by Charles J. Brooks and Philip A. Craig, Jr.

Written as a study guide for the GICSP exam, the book provides an excellent overview of industrial cyber security with some great practical examples.

4. "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapons" by Kim Zetter

For many of us, Stuxnet is where it all begins. Similar to Sandworm, this is a great book that's an easy read to get lost in.

5. "Industrial Automation and Control Systems Security Principles" by Dr. Ronald Krutz

The "official" ICS/OT cyber security guide sponsored by ISA and provided during the ISA/IEC 62443 certification courses.

6. "Industrial Cybersecurity"* by Pascal Ackerman

While there are different "editions" of the book, each is really a completely different book.

Each is a monster in their own right but definitely references you want to have on hand if you're on-site and have no Internet access for research!

7. "Engineering-Grade OT Security: A Manager's Guide" by Andrew Ginter

Be sure to check out his other two books as well! I'm just starting this new release!

8. Implementing IEC 62443 - A Pragmatic Approach to Cybersecurity by Michael D. Medoff and Patrick C. O'Brien

Understanding how to implement ISA/IEC 62443 can be daunting at first, but it doesn't have to be.

9. Industrial Cybersecurity: Case Studies and Best Practices by Steve Mustard

Real world examples and case studies can often be the best way to learn!

10. "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems" by Eric D. Knapp.