University of South Brittany

Subject : Pentesting

ICS Pentesting Report

MASTER 1 CYBERUS

Accomplished by:

- Karels, Anthony
- Ali-Khodja, Myriam
- Bouta, Ali
- Benali, Mohammed Yacine

Assignment requested by the professors :

O. Mawloud and S. Bouchelaghem

School Year 2023-2024

Contents

List of Figures

Introduction

In today's technological landscape, Industrial Control Systems (ICS) are the backbone of worldwide critical infrastructure. These systems, vital for the operation of energy, water, transportation sectors, and more, are integrating increasingly advanced and connected technologies. However, this evolution leads to a heightened exposure to cyber risks and vulnerabilities, underscoring the critical importance of security within these environments.

This project aims to provide a general overview of ICS/OT by defining its nature, role, and the scope they encompass. We will explore a few communication protocols specific to ICS, which often differ from those used in traditional IT networks, to grasp their peculiarities and the security challenges they present. Subsequently, we will discuss some of the methods of pentesting tailored to ICS, a critical practice for identifying security flaws without compromising the stability or safety of these vital systems. This exploration will include an analysis of some of the tools, techniques, and strategies used for pentesting in this specific context. Therefore, this project will provide a demonstration concerning the practical application of these methods through a concrete demonstration, highlighting some key vulnerabilities within ICS.

Chapter 1

Introduction to Industrial Control Systems

Industrial Control Systems (ICS) are specialized frameworks used to control industrial processes, machinery, and infrastructure. These systems play a critical role in the automation of manufacturing plants, power generation and distribution, water treatment facilities, and other essential services that maintain the infrastructure of modern society. The evolution of ICS from mechanical and analog controls to digital, computer-based technology has significantly enhanced their efficiency, reliability, and the precision of industrial operations.

1.1 Operational vs Information Technology

The convergence of Operational Technology (OT) and Information Technology (IT) security is blurring as OT systems incorporate connected devices and the rise of the Internet of Things (IoT) and Industrial IoT (IIoT) facilitates real-time data sharing. While OT and IT security systems protect different environments and have distinct vulnerabilities, their integration is increasingly necessary. OT systems, traditionally isolated and run on proprietary software, contrast with the interconnected and standard-operating-system-dependent IT environments. OT security, focused on physical system integrity and continuous operation, contrasts with IT's emphasis on data confidentiality. However, both face the challenge of securing systems against highly disruptive events and frequent cyber threats. Despite OT's historically infrequent updates leading to potential vulnerabilities, the growing connectivity demands alignment with IT's regular patching and security policies to mitigate risks. This evolving landscape underscores the importance of IT/OT collaboration to enhance productivity and security in the face of sophisticated cyber threats.

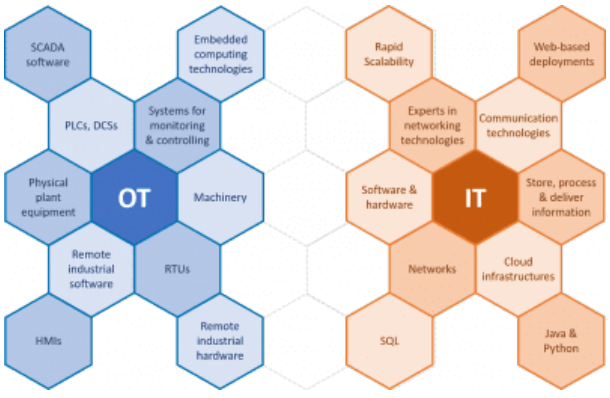

Figure 1.1: IT/OT Convergence

1.2 The Importance of ICS

The functionality and stability of ICS are vital for economic stability, national security, and public safety. Any disruptions in these systems can lead to significant impacts, including economic losses, environmental disasters, and compromises in public health and safety. The critical nature of these systems makes them a target for cyberattacks, underscoring the importance of cybersecurity measures in the industrial sector.

1.3 History and Evolution of ICS

The history of ICS can be traced back to mechanical systems used in the early 20th century. The development of electronic devices and later, computer technology, revolutionized these control systems. The introduction of Programmable Logic Controllers (PLC) in the 1960s marked a significant milestone, enabling more sophisticated control and automation of industrial processes. The advent of the Internet and advancements in communication technologies have further evolved ICS into highly interconnected and complex systems capable of remote monitoring and control.

1.4 Types of Industrial Control Systems

1.4.1 SCADA Systems - Supervisory Control and Data Acquisition

These systems are designed to collect data from various sensors at a facility or in remote locations, then send this data to a central computer system for monitoring and control purposes. SCADA is widely used in industries where automation is spread over large distances, such as water treatment and distribution.

1.4.2 Distributed Control Systems - DCS

DCS are used to control industrial processes such as chemical plants, oil and gas refineries, and pharmaceutical manufacturing. These systems distribute control elements close to the plant processes they manage, offering a high level of reliability and process availability.

1.4.3 Programmable Logic Controllers - PLC

PLCs are computer-based, solid-state devices that control industrial processes and machinery. They are known for their ruggedness, ease of programming, and ability to withstand harsh industrial environments.

1.5 Role of ICS in Critical Infrastructure

ICS are the backbone of critical infrastructure, ensuring the seamless operation of services that society relies upon. They enable the automation and control of processes across various sectors, including energy, water management, transportation, and manufacturing. The efficiency and safety of these sectors heavily depend on the reliability and security of ICS.

1.6 Challenges and Considerations

Industrial Control Systems (ICS) are pivotal to the functionality of modern infrastructure, playing a crucial role in managing essential services across 16 critical infrastructure sectors identified by the US Department of Homeland Security. These sectors, including energy, water, healthcare, and transportation, rely heavily on ICS for daily operations, such as regulating flow rates, monitoring temperatures, and controlling production processes. The ubiquity and importance of these systems make them prime targets for cyber-attacks, with potential motives ranging from intellectual property theft to causing widespread disruption. High-profile cyber incidents, like the 2015 electricity outage in Ukraine and attacks on US water systems, highlight the vulnerabilities and consequences of such security breaches. Despite their critical role, many utilities, especially in rural areas, face budget constraints that limit their cybersecurity capabilities, exposing them to increased risk of cyber threats.

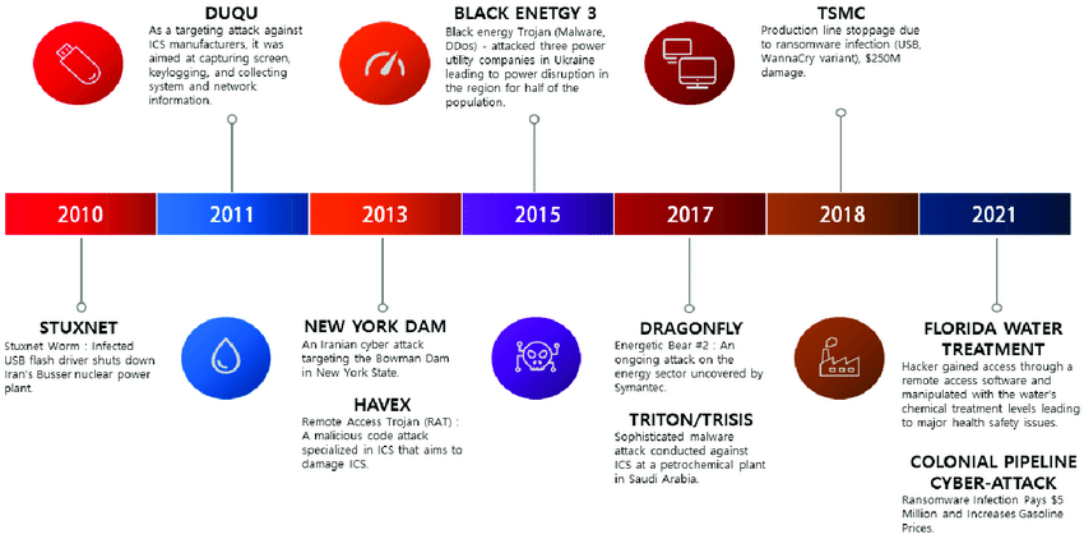

Figure 1.2: History and timeline of international industrial control system ICS cyberattacks

Chapter 2

Components of ICS

2.1 Introduction

The architecture of Industrial Control Systems is comprised of multiple layers, each with its specialized components and functionalities. At the core of any ICS are the following critical components.

- Field Devices: These include sensors and actuators deployed across industrial environments. Sensors collect data about process parameters (e.g., temperature, pressure), while actuators perform actions based on commands (e.g., opening a valve, starting a motor).
- Programmable Logic Controllers (PLCs): PLCs are ruggedized computers that execute control functions based on pre-programmed logic. They act as the brain within the ICS, processing data from field devices and issuing control commands.
- Human-Machine Interfaces (HMIs): HMIs provide a graphical overview of the industrial process, allowing operators to interact with the system, monitor operational data, and manually control processes when needed.
- Communication Networks: These networks facilitate data transmission between the different components of the ICS. They can be wired or wireless and must be designed to ensure reliable and secure communication.
- Control Servers: Control servers host the software applications that perform data analysis, process visualization, and sometimes, advanced control algorithms. They serve as a central point for data aggregation and decision-making.
- Data Historians: Data historians collect and store data over time from various parts of the ICS. This data is crucial for trend analysis, performance monitoring, and regulatory compliance.

2.2 Hierarchical Structure and Functionality

The architecture of ICS typically follows a hierarchical model that organizes the system into multiple levels:

- Field Level: The lowest level, consisting of field devices that directly interact with the physical process.
- Control Level: This level includes PLCs and other control devices that execute automation tasks by processing inputs from field devices.
- Supervision Level: The supervision layer features HMIs and control servers that provide a comprehensive view of the process and enable operator interaction.

- Enterprise Level: At the top of the hierarchy, the enterprise level integrates ICS data with business systems, facilitating decision-making and strategic planning.

This hierarchical structure ensures organized data flow, decision-making processes, and a clear separation of concerns, enhancing both operational efficiency and security.

2.3 Interconnectivity within ICS

Interconnectivity is a defining feature of modern ICS, allowing for seamless communication between components and levels within the architecture. This interconnectivity enables real-time data acquisition and control, which are essential for efficient and automated industrial operations. However, it also introduces challenges related to cybersecurity, as the integration of IT and operational technology (OT) environments expands the attack surface.

To address these challenges, ICS architectures incorporate advanced security measures, such as firewalls, intrusion detection systems, and secure communication protocols. Additionally, redundancy and failover mechanisms are implemented to ensure system resilience and continuity of operations in the event of failures or cyberattacks.

Chapter 3

The Perdue Model

The Purdue Model, also known as the Purdue Enterprise Reference Architecture (PERA), is a seminal framework in industrial control systems. Developed in the 1990s, it provides a structured approach to understanding and organizing the layers of a manufacturing system, from physical equipment to enterprise-level planning. The model is widely revered for its clear representation of industrial network security layers, making it a foundational tool in designing and securing industrial control systems. [1]

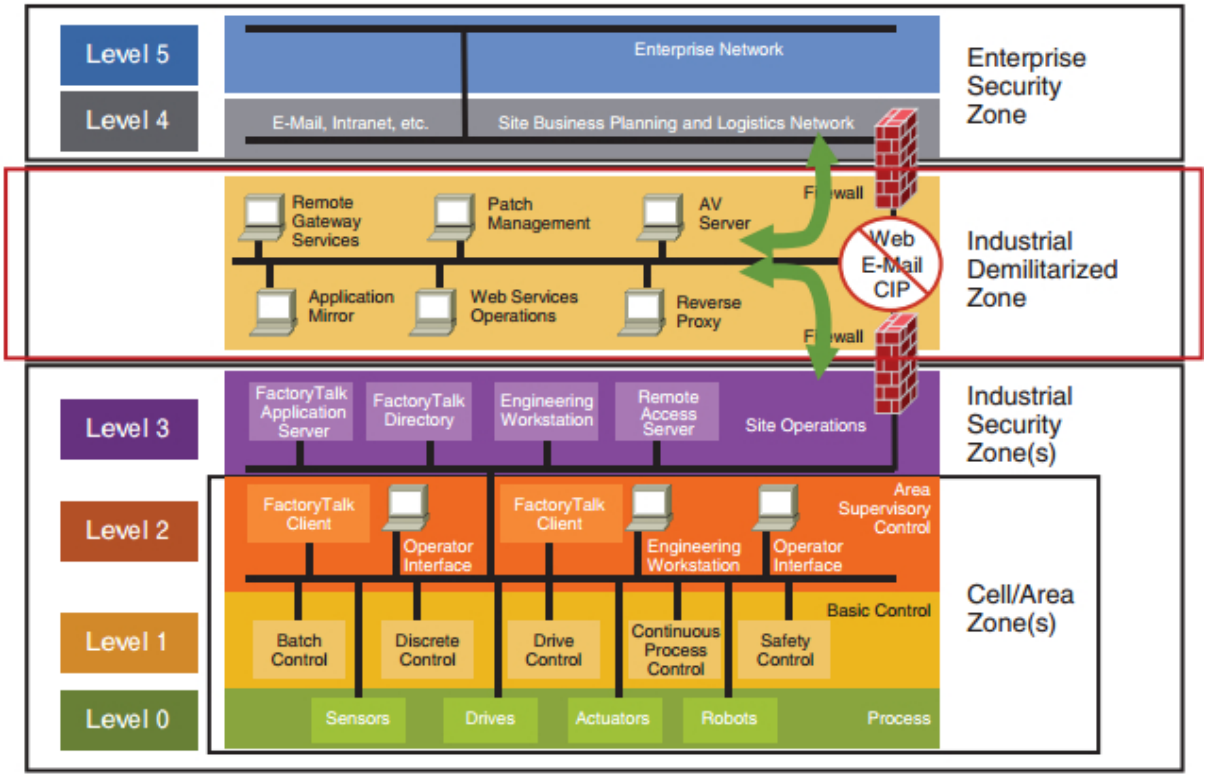

Figure 3.1: The Perdue Model

Here's a breakdown of each level as seen in the image [2]:

- **Level 0**: This is the physical process level where actual physical processes take place.It includes sensors that measure and collect data, drives that power machines, actuators that move components, robots for automation, and the actual process or physical operation being controlled or monitored.
- **Level 1**: This level comprises the direct control layer. Here, you will find controllers that directly manage the process, such as Batch Control for batch processes, Discrete Control for on/off control processes, and Safety Control systems that ensure the safe operation of the plant.

- **Level 2**: The supervisory control level, where operators interface with the system. Operator Interface Terminals or Human Machine Interfaces (HMIs) allow personnel to interact with control systems. Engineering Workstation allows for system setup and programming.
- **Level 3**: The site operations level, which involves overseeing the operation of multiple control systems. This level includes servers that provide services such as data collection (historians), system management, and possibly access to the enterprise levels.
- **Industrial Demilitarized Zone (IDMZ)**: This serves as a buffer between the enterprise network and the industrial network. It typically contains services that need to be accessed from both networks, like web services, patch management, and remote gateway services. The presence of firewalls indicates the use of network segmentation to protect different parts of the system. it also acts as information sharing layer between the business or IT systems in levels 4 and 5 and the production or OT systems in levels 3 and lower.
- **Level 4**: The site business and logistics level where enterprise management systems reside. This could involve business planning, logistics,ERP software, and other corporate-level functions.
- **Level 5**: The enterprise network level which includes the corporate network where business functions such as email and internet access occur.

Chapter 4

Common ICS Protocols

In this chapter, we discuss common Industrial Control Systems (ICS) protocols, focusing on Modbus, and mentioning HART, and WirelessHART. These protocols form the backbone of modern ICS communications, enabling efficient and secure interactions between various devices and systems. Understanding their functions, strengths, and limitations is crucial for anyone involved in with industrial automation systems. This discussion aims to provide a broad overview of these protocols, highlighting their security aspect.

4.1 ModBus

4.1.1 Introduction

Modbus stands as one of the oldest and most universally adopted protocols in Industrial Control Systems (ICS). Originating in 1979, it was initially developed for effective communication with Programmable Logic Controllers (PLCs). The protocol, created by Modicon, now a part of Schneider Electric, has stood the test of time, proving its durability and relevance in the field.

4.1.2 Key Features

The enduring popularity of Modbus can be attributed to its core features:

- **Simplicity**: Its straightforward structure simplifies deployment and maintenance. Employing a master-slave architecture, Modbus allows a master device, such as a PLC, to send requests to slave devices like sensors or actuators, which subsequently respond. This clear communication model enhances ease of understanding and implementation.
- **Open Protocol**: Modbus is distinguished by its publicly available specification, ensuring that it is not controlled by any single company.
- **Versatility**: The protocol supports various communication methods, including serial and TCP/IP, and can operate over traditional serial lines like RS-232 or RS-485. [3]

4.1.3 Operational Modes

Modbus functions in several modes to suit different applications [5] [4]:

- **Modbus ASCII**: This mode, featuring a human-readable format, is particularly useful for debugging and diagnostics.
- **Modbus RTU** (Remote Terminal Unit): Utilizes a more compact, binary data representation and is commonly employed in industrial applications for its efficiency.
- **Modbus TCP/IP**: Adapted for Ethernet networks, this mode facilitates integration with modern network infrastructure, enhancing its applicability in contemporary settings.

4.1.4 Common Uses in ICS

In the realm of industrial control and data acquisition, Modbus is extensively utilized for interfacing with various ICS components such as sensors, actuators, and industrial machines. It finds application in systems like HVAC, building automation, and power systems. For instance, in HVAC systems, Modbus is instrumental in connecting devices like thermostats, air handlers, and chillers to central control systems, thus enabling automated temperature control and efficient energy management.

4.1.5 Security Considerations

Initially designed without encryption or authentication mechanisms, Modbus necessitates the use of secure networks to safeguard communications. In modern applications, it is advisable to pair Modbus with secure gateways, firewalls, and other security measures to mitigate potential vulnerabilities.

4.1.6 Modbus Today

Despite its age, Modbus continues to be a cornerstone in ICS due to its ease of use, widespread support, and adaptability to contemporary network technologies. Its ability to evolve and integrate with modern systems underscores its relevance in the field of industrial automation.

4.2 HART: Highway Addressable Remote Transducer

4.2.1 Overview

HART is also a prevalent communication protocol in industrial automation, combining analog and digital communication in a hybrid format. This protocol is akin to a smartphone's ability to handle both voice calls (analog) and digital messages, merging the reliability of analog signaling with the advanced features of digital communication.

4.2.2 Functionality and Features

The HART protocol facilitates two-way digital communication alongside traditional 4–20 mA analog signals [6], using the same wiring. This feature enables the transmission of detailed digital data without interrupting the analog signal flow, therefore not changing the existing communication infrastructure.

4.2.3 Components and Communication

The system involves two key components: a HART-enabled device (such as a sensor or valve) and a controller or monitoring system. Communication follows the same master/slave format [7], with the master (control system) initiating interactions and the slave (field device) responding.

4.2.4 Security Aspects

Although HART traditionally lacked robust security features, recent advancements have introduced enhancements to protect against unauthorized access and ensure data integrity, addressing its primary security concerns.

4.3 WirelessHART : A Concise Overview

4.3.1 Introduction

WirelessHART, an extension of the established HART protocol, represents a significant advancement in industrial automation by adapting the protocol for wireless communication. This innovation was introduced in 2007 to fulfill the growing demands for wireless communication capabilities in process automation settings.

4.3.2 Key Features

WirelessHART is distinguished by its ability to establish a mesh network for communication. In this network, each device can function as a router for others, thereby enhancing the reliability and range of the network. This feature significantly simplifies the process of adding, removing, or relocating devices, as it eliminates the need for altering physical wiring configurations[8].

4.3.3 Security

Since this protocol was created in 2007 it places a strong emphasis on security, incorporating comprehensive measures like encryption, key management, and device authentication. These security features are designed to safeguard against unauthorized access and ensure reliable operation in challenging industrial environments. Additionally, WirelessHART includes specialized mechanisms to manage interference and data retransmission, further bolstering its robustness and suitability for industrial applications.

Chapter 5

ICS Pentesting

5.1 Challenges in ICS Security

In the realm of Industrial Control Systems (ICS), several unique concerns must be addressed. One of the primary concerns is the safety of personnel, the environment, and the industrial processes themselves. Industries may deliberately use clear-text protocols and insecure applications for various reasons. For instance, they might opt for clear-text protocols to eliminate potential delays in information transfer between devices that could occur if more complex protocols were used. Similarly, they might use applications without encryption to expedite processes.

Another significant concern is the sustainability, availability, and integrity of the industrial processes. Many industries require continuous operation, often 24/7, and any interruption could disrupt the supply chain, leading to substantial financial losses.

Regulatory compliance is another aspect that can pose challenges in ICS environments. Some critical infrastructures may already have security regulations in place, which can guide and simplify the penetration tester's task. However, other industries, such as a tuna factory, may not have such stringent regulations. Their regulations might primarily focus on cleanliness and hygiene, leaving a gap in the cybersecurity aspect. This lack of specific cybersecurity regulations represents a significant concern for ICS environments.

In addition to these points, it's also crucial to consider the legacy nature of many ICS. These systems were often designed and implemented before the advent of modern cybersecurity threats, making them particularly vulnerable. Furthermore, the convergence of Information Technology (IT) and Operational Technology (OT) in ICS environments introduces additional complexities and challenges for penetration testing.

Lastly, the potential impact of a successful cyberattack on an ICS can be far more severe than in other sectors. Disruptions can lead to physical damage, environmental disasters, and even loss of life, making the stakes incredibly high. Therefore, the importance of thorough and careful penetration testing in ICS environments cannot be overstated. It's not just about protecting data - it's about ensuring the safe and reliable operation of critical infrastructure upon which society depends.

5.2 ICS Penetration Testing Methodology

Penetration testing in ICS environments largely follows the same steps and methodology as conventional penetration testing. However, there are some key differences due to the unique nature of ICS. The methodology for conventional penetration testing is well-established and effective, typically involving Planning and Reconnaissance, Scanning and Enumeration, Gaining Access, Post-Exploitation and Maintaining Access, and Analysis and Reporting.

In contrast, penetration testing in ICS environments must be conducted in a way that yields useful and impactful results without disrupting the industry's workflow. This involves several unique steps:

- **Architecture Review:** The penetration tester begins by reviewing the architecture on

paper to gain a comprehensive overview of the ICS before proceeding with any active testing.

- **Boundary Assessment:** This involves assessing the segmentation controls and boundary defenses that form the core of the ICS security strategy. Since ICS devices were not designed with security in mind, a robust boundary is necessary to protect them. Penetration testing of the boundary is a crucial step to determine how secure a boundary control actually is.
- **Device Assessment:** In some cases, a penetration tester will assess what an attacker could do if they gain access to an ICS network. This is generally done in a lab or a testing environment to isolate its effect from the production environment.

By following this methodology, it is possible to test the security controls in the ICS environment and strengthen the system against attacks while maintaining the required uptime and continuity of the system.

Furthermore, it's important to note that ICS penetration testing should also include a Vulnerability Assessment phase, where potential vulnerabilities in the ICS environment are identified. This could involve using automated vulnerability scanners, manual testing, and researching known vulnerabilities for the identified systems and services.

Lastly, the Analysis and Reporting phase is crucial in ICS penetration testing. This is where the findings are analyzed, vulnerabilities and exploits are documented, and recommendations for mitigation are provided. The report should be clear, concise, and actionable, providing value to the ICS operators. It's not just about identifying vulnerabilities - it's about providing practical solutions to improve the security posture of the ICS environment.

5.3 What to 'Get Over' in ICS Pentesting

Penetration testers may encounter several challenges when conducting penetration testing in ICS environments. These challenges often stem from the unique operational requirements and constraints of these environments.

One such challenge is network scanning. Some industries, particularly those requiring continuous uptime, may restrict or even prohibit network scanning. This is because network scanning can potentially cause network congestion or even outages, disrupting the industrial processes. For instance, there have been cases where aggressive network scans have caused network subnets to go down for weeks.

Another challenge is the modification of the system. Any changes to the system, even seemingly innocuous ones like creating a file, can be seen as altering the system. OT teams are often very cautious about changes due to the potential risks to the system's stability and reliability. In fact, any changes to an ICS system often require rigorous and expensive testing, and unauthorized changes could void maintenance agreements.

Working with OT teams can also be challenging. OT teams often have different operational goals than IT teams, focusing more on system availability, safety, and process integrity. This can sometimes lead to misunderstandings or conflicts. However, effective communication and collaboration between IT and OT teams are crucial for successful ICS security.

These challenges may seem illogical from a traditional IT perspective, but they exist for valid reasons. The stakes in ICS environments are incredibly high, and the potential impacts of a security incident can be severe. Therefore, it's crucial for penetration testers to understand these challenges and adapt their methodologies accordingly. This often involves taking a more

cautious approach, coordinating closely with the OT teams, and always prioritizing the safety and reliability of the industrial processes.

5.4 ICS Pentesting Tools

5.4.1 ControlThings.io

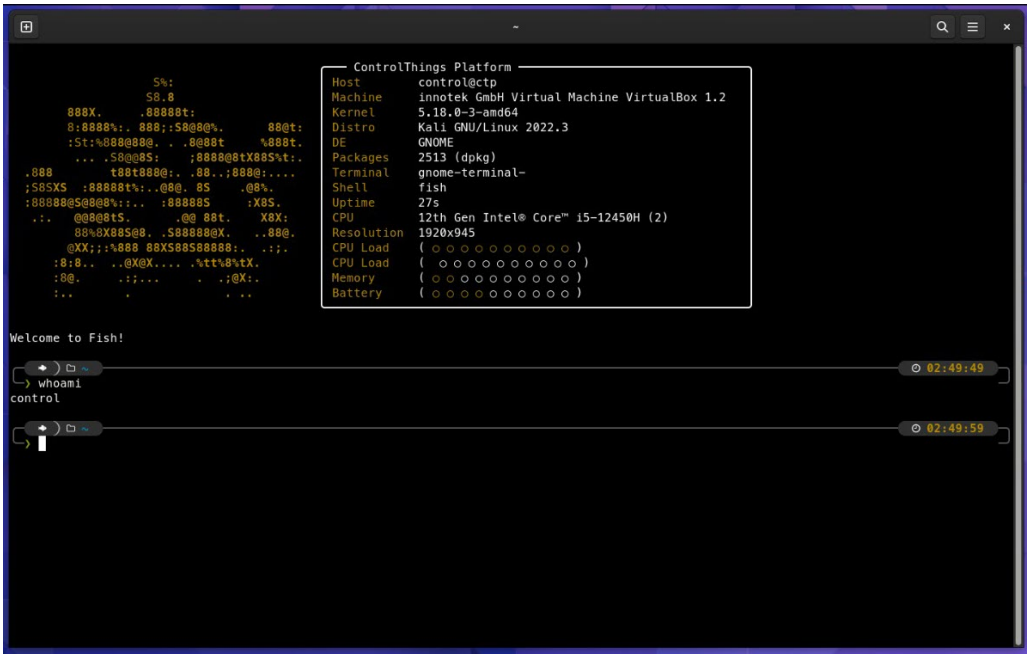

Figure 5.1: ControlThings.io Linux shell welcome page.

Controlthings.io is a specialized Linux distribution designed specifically for Industrial Control System (ICS) penetration testing. It's tailored to meet the unique challenges of assessing the security of industrial environments, where traditional cybersecurity approaches may not suffice. Here's an overview of ControlThings and some of the supplementary tools it provides:

1. **Customized Linux Environment**: ControlThings offers a customized Linux environment optimized for ICS penetration testing. It comes pre-configured with a range of tools and utilities necessary for assessing the security of industrial systems.

2. **ICS-Specific Penetration Testing Tools**: The distribution includes a comprehensive suite of ICS-specific penetration testing tools. These tools are specifically designed to identify vulnerabilities, assess system configurations, and test the resilience of industrial control networks against cyber threats.

3. **Protocol Analysis and Exploitation**: ControlThings provides tools for analyzing and exploiting industrial protocols commonly used in ICS environments. This includes protocols such as Modbus, DNP3, OPC, and others. By analyzing these protocols, testers can identify potential attack vectors and vulnerabilities.

4. **SCADA System Assessment**: The distribution includes tools for assessing Supervisory Control and Data Acquisition (SCADA) systems, which are central to many industrial control processes. Testers can use these tools to evaluate the security of SCADA systems and identify weaknesses that could be exploited by malicious actors.

5. **Simulation Environments**: ControlThings also include simulation environments for emulating industrial control systems. These environments allow testers to conduct realistic assessments in a controlled setting, without risking damage to operational systems.

6. **Documentation and Reporting Tools**: To facilitate thorough testing and analysis, ControlThings comes with documentation and reporting tools. These tools help testers document their findings, generate reports, and communicate vulnerabilities to stakeholders effectively.

7. **Support for Hardware Testing**: ControlThings also includes support for hardware testing, allowing testers to assess the security of physical devices commonly found in industrial environments. This could include PLCs (Programmable Logic Controllers), RTUs (Remote Terminal Units), and other industrial control hardware.

5.4.2 ControlThings Tools

ControlThings also offers a suite of specialized assessment tools tailored for Industrial Control System (ICS) penetration testing. These tools include **ControlThings Serial**, designed for interacting with binary serial devices to emulate ICS vendor tools for impersonation purposes. **ControlThings Modbus** facilitates communication with Modbus devices, supporting both TCP/UDP and serial (RTU/ASCII) connections. For assessing embedded chips, ControlThings provides SPI and I2C tools, enabling interaction with EEPROMs, Flash chips, and other embedded components using the Serial Peripheral Interface (SPI) and Inter-Integrated Circuit (I2C) protocols, respectively. **ControlThings Velocio** is dedicated to interacting with Velocio PLCs, showcasing the potential for similar tools planned for other vendors. Underpinning these tools is **ControlThings UI**, a freely available library empowering users to build their own assessment tools leveraging its capabilities.

5.5 Metasploit

5.5.1 ICS Exploitation Framework

trial environments, identifying weaknesses and assessing the resilience of control systems againstThe ICS Exploitation Framework (IEF) within Metasploit is a specialized module designed to assess the security of Industrial Control Systems (ICS). It offers a comprehensive suite of exploits and payloads specifically tailored for targeting vulnerabilities in ICS devices and networks. Leveraging the IEF module, penetration testers can simulate real-world cyber attacks on industrial environments, identifying weaknesses and assessing the resilience of control systems against malicious intrusions. By exploiting known vulnerabilities, IEF enables testers to uncover potential risks and vulnerabilities within ICS infrastructures, ultimately aiding in the development of robust security measures to protect critical industrial assets from cyber threats.

Chapter 6

PLC Hacking Demonstration

This chapter presents a detailed overview of a PLC hacking demonstration, including the hardware and software components, their configuration, and a potential attack scenario. There were several objectives in mind when planning this demonstration, firstly, showcasing some hardware which could simulate a real-world industrial control system environment. With the hope of obtaining a real PLC, ACE Automation (aceautomation.eu) in France was contacted to inquire if they could loan a device, however they were unable to assist with the request. Since this project does not include a budget, it was opted to improvise by using an available Raspberry Pi in conjunction with the OpenPLC suite.

Additionally, the demonstration served to gain insights into the function of PLCs, circuit design, ladder logic and their roles in industrial automation processes. Furthermore, this setup allowed for an examination of the Modbus TCP protocol through understanding its vulnerabilities and potential security risks. Lastly, the demonstration was designed to be visually engaging, providing an immersive experience for viewers to see the concepts and processes involved in industrial control systems in action.

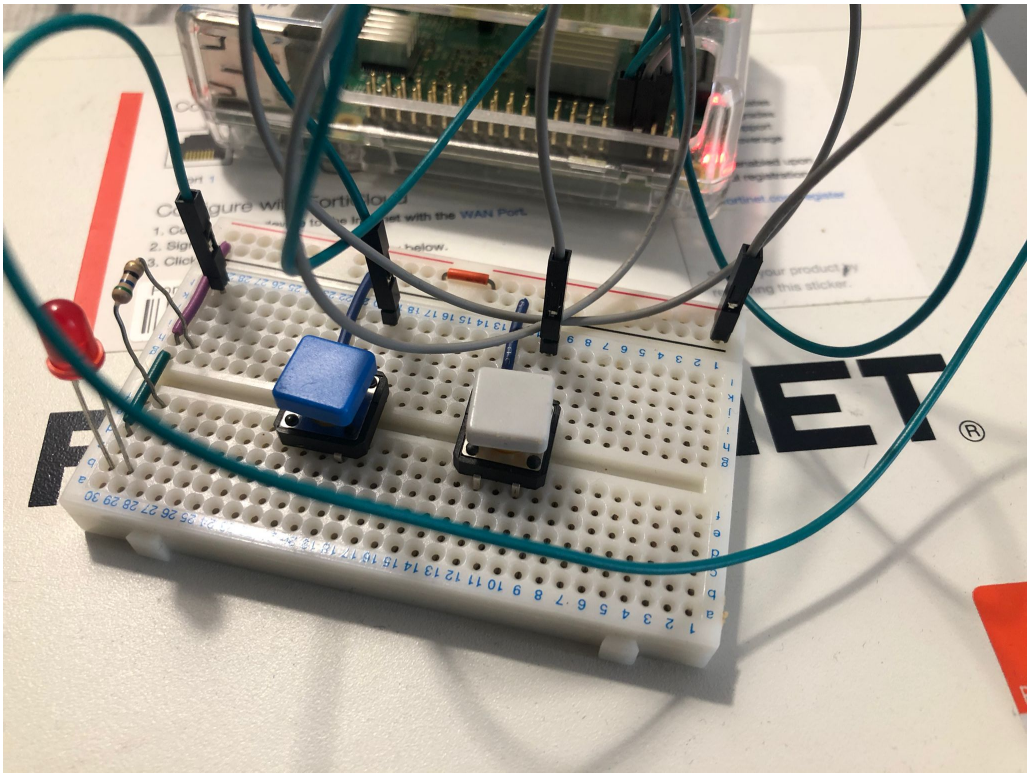

Figure 6.1: Simple circuit constructed on a breadboard.

6.1 Hardware Itemization

6.1.1 Raspberry Pi 2 B

This is the main computing platform used for running scripts and acting as a PLC by interfacing with external components via it's GPIO pins.

6.1.2 Electronic Components

LEDs, switches, resistors, leads, and a breadboard were used to design a circuit which simulates the physical inputs and outputs of the PLC system.

6.1.3 FortiGate 60E Firewall

This firewall device provides network security, SSL VPN, and also acts as a network switch.

6.1.4 TP-Link TL-WR902AC Router

Small travel router which is used to bridge a wireless hot-spot to the firewall's WAN port.

6.1.5 iPhone 8

Used solely for its wireless hot-spot feature to provide an internet connection when a wired connection was not available.

6.1.6 Attacker Laptop

A Windows 10 laptop employed to carry out the demonstration, making use of several different applications.

6.2 Software Itemization

6.2.1 Raspbian GNU/Linux

This is the operating system (version 11 - bullseye) installed on the Raspberry Pi 2 B, providing the platform for running software and scripts.

6.2.2 OpenPLC Suite

The OpenPLC suite is an open source multi-hardware PLC solution created by Autonomy which consists of two separate parts: the runtime, and the IDE.

6.2.3 Qbee.io Platform

This platform allows for the deployment and remote management of IoT devices, including pushing scripts, software installations, device metrics, remote access, port forwarding, and much more.

6.2.4 Radzio! Modbus Master Simulator

Software tool used for simulating Modbus communication for testing and development purposes.

6.3 Configuration

6.3.1 Creating a PLC

Configuring the Raspberry Pi to act as a PLC required some initial steps before it could be utilized. To start, a brand-new installation of Raspbian was written to an SD card used to boot the Pi. During the search for options to use the Pi as a PLC, the **qbee.io** platform was discovered. Determining it would be useful for the demonstration, a free account was registered which could manage up to 2 devices. Adding new devices to the platform only required the execution of a single a bash command using the account API key:

Listing 6.1: Bootstrap Install Script

```
1  wget -qO - https://raw.githubusercontent.com/qbee-io/qbee-agent-
       installers/main/qbee-agent installer.sh | sudo bash -s -- --
       bootstrap-key <key>
```

With the Pi connected to a home router via Ethernet, the command was used to successfully bootstrap the device into the **qbee.io** device manager. A few moments later the device appeared in the online portal and it was possible to observe and monitor the device, and also easily deploy additional software packages such as 'git.' The OpenPLC runtime package was next installed on the Pi by pushing a script which automated its deployment. On a side note, this is one aspect of the platform which really shines if you intend to deploy multiple devices, as the newly bootstrapped device will automatically install the provided configuration.

The OpenPLC runtime uses a web application front-end to configure hardware drivers, slave devices, protocols, and programs. After logging into the front-end for the first time, the hardware drivers need to be configured for Raspberry Pi and the default login password changed. The Modbus TCP protocol was also enabled on port 502 to allow control of the device over a network. Programs are then created with the additional tool **OpenPLC Editor**, and are uploaded via the website, compiled, and started when ready for deployment.

6.3.2 Circuit Design

The circuit was constructed on a breadboard using two momentary switches and an LED with a corresponding pull-up resistor. The operation was such that one switch (grey) would signal to turn the LED *on* while the other switch (blue) would signal to turn the LED *off*. The breadboard was then connected to the Pi's GPIO pins using four leads, one for ground (pin 6), one for the LED (pin 8), and two others (pins 3 and 5) for the momentary switches. (Figure 6.1)

The corresponding ladder logic was diagrammed in the IDE before uploading into OpenPLC. The logic contained two methods to operate the LED, first through the use of the physical switches, and additionally through the use of *soft* switches which were internal to the device. The logic was also able to be checked via the interface, which presented a green line where current was flowing through the circuit. It also had the ability to force the switches (actuators) *on* or *off* to observe the logic. While performing this testing, it was noticed that an effect of the design allowed for the soft switches to override the physical switches, a behavior which will be covered in more detail later. (Figure 6.2)

Having uploaded the designed logic and starting it, the status of the switches and LED could be examined on the **Monitoring** page. This display is similar to how an HMI may look, since it provides visual feedback for each device defined in the ladder logic. One curiosity of note is the inverse values displayed for the physical buttons (*PHYS1 and PHYS2*), which occurs due to the internal pull-up resistors on the Raspberry Pi's GPIO pins. The circuit worked as expected

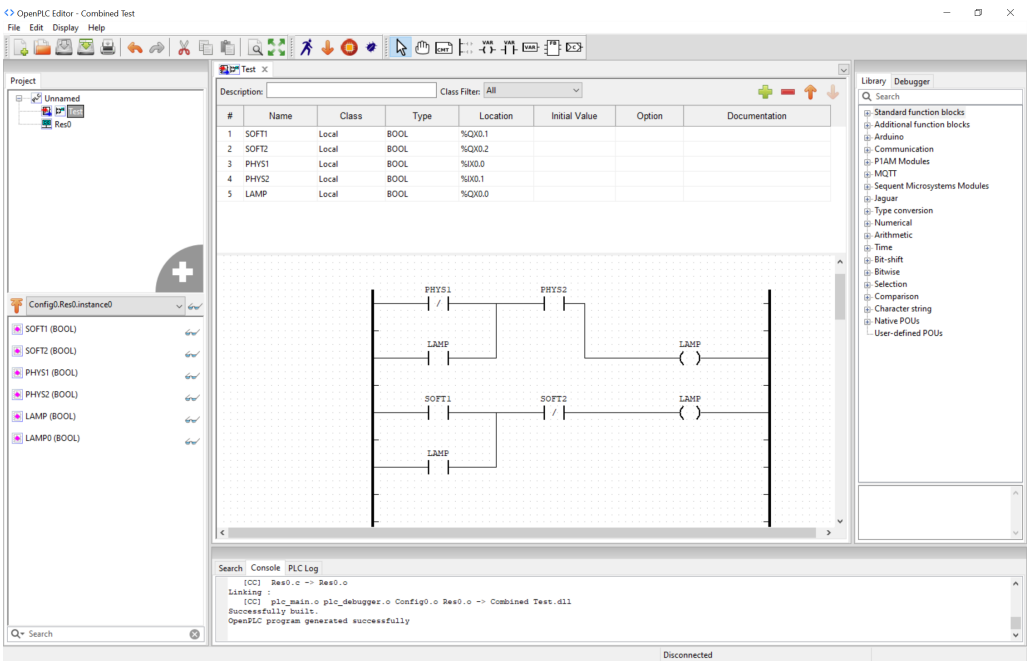

Figure 6.2: The OpenPLC IDE and circuit ladder logic.

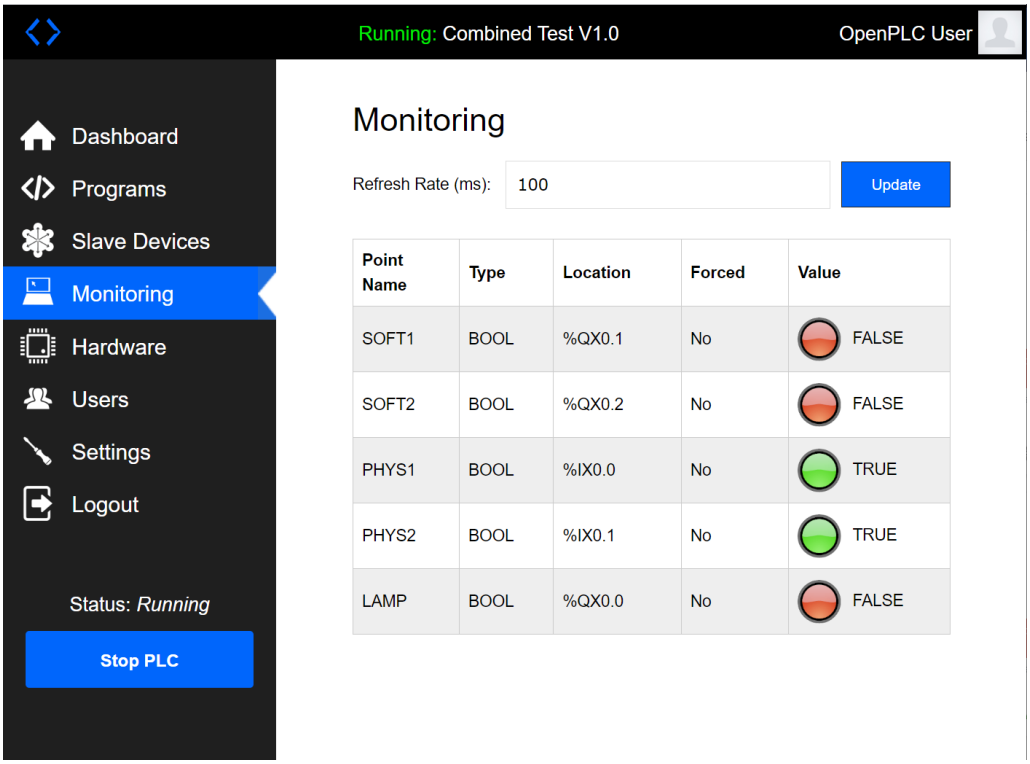

Figure 6.3: OpenPLC web interface monitoring page.

however, and the values on the web monitoring page were also updating in real-time to show which buttons were pressed along with the current state of the LED. (Figure 6.3)

6.3.3 Network

The Pi is connected via Ethernet to an open port on the firewall, which would typically be placed on Perdue level 3 to segregate the industrial security zone from the DMZ. While working in a home lab, the network configuration is slightly easier to contend with compared to the network at the university. The firewall can be directly connected to the home router to provide internet connectivity, typically a dangerous setup - but necessary for the demonstration to function. With this configuration, it was possible to VPN into the firewall to access the Pi/PLC's functionality on the internal network.

A slight change was however required to provide network access during the live demonstration at the university due to the complexities and security of their LAN. Using a travel router, it was possible to bridge a hot-spot created on an iPhone and provide internet access to the firewall via the WAN interface. This presented another challenge because most mobile hot-spots do not allow NAT via their APNs, thus making it impossible to connect to the VPN over this type of connection. The difficulty was overcome with the help of the **qbee.io-connect** application which is able to forward ports from the Pi to the localhost. With this setup it was only necessary to *pretend* a VPN connection was used, though it was still possible to perform the demonstration over the internet instead of locally.

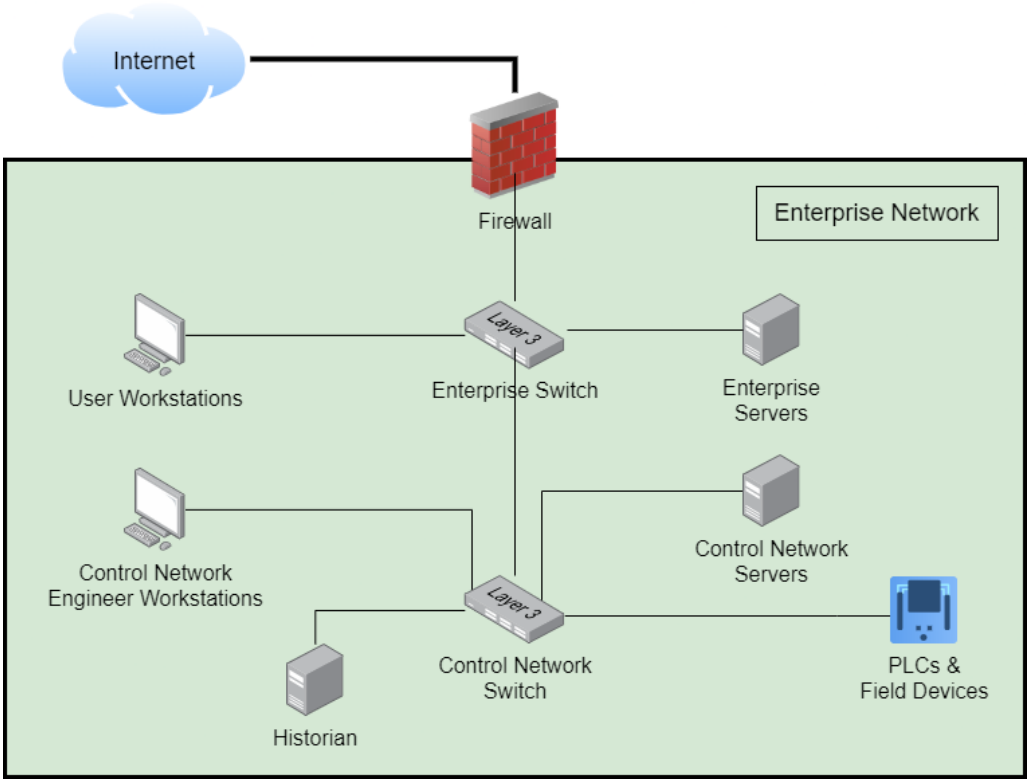

Figure 6.4: ICS Network: The worst case scenario.

6.4 Attack Scenario

The attack scenario suggests that the configuration of the ICS network is of the "worst case scenario" with only a firewall between the internet and the enterprise network. Additionally, the enterprise network and control networks are connected via switches without a second firewall. (Figure 6.4)

6.4.1 Vulnerability

It is also assumed that an attacker took advantage of one of the recent vulnerabilities affecting the FortiGate line of firewalls. One such vulnerability was **CVE-2018-13382** [9] which affected numerous FortiNet firewall products running a vulnerable version of the firmware. Due to a bug in a feature intended only for a specific client, it was discovered that a VPN user's password could be updated by an unauthenticated attacker. Normally this would only pose an issue for the single client, however this feature was accidentally built into the release version of the firmware and disseminated to the general public.

6.4.2 Modbus TCP is Cleartext

With these assumptions, it can be concluded than an attacker would have access to the entire ICS network including PLCs should they exploit the vulnerability and be able to connect to the firewall's VPN. Once inside the network, the attacker would perform scans and network packet captures to search for potential targets. Should the attacker discover the PLC devices are running the Modbus TCP protocol for communication, it would be possible for them to have direct control the inputs and outputs of the device using an application like **Radzio! Modbus Master Simulator**. (Figure 6.5)

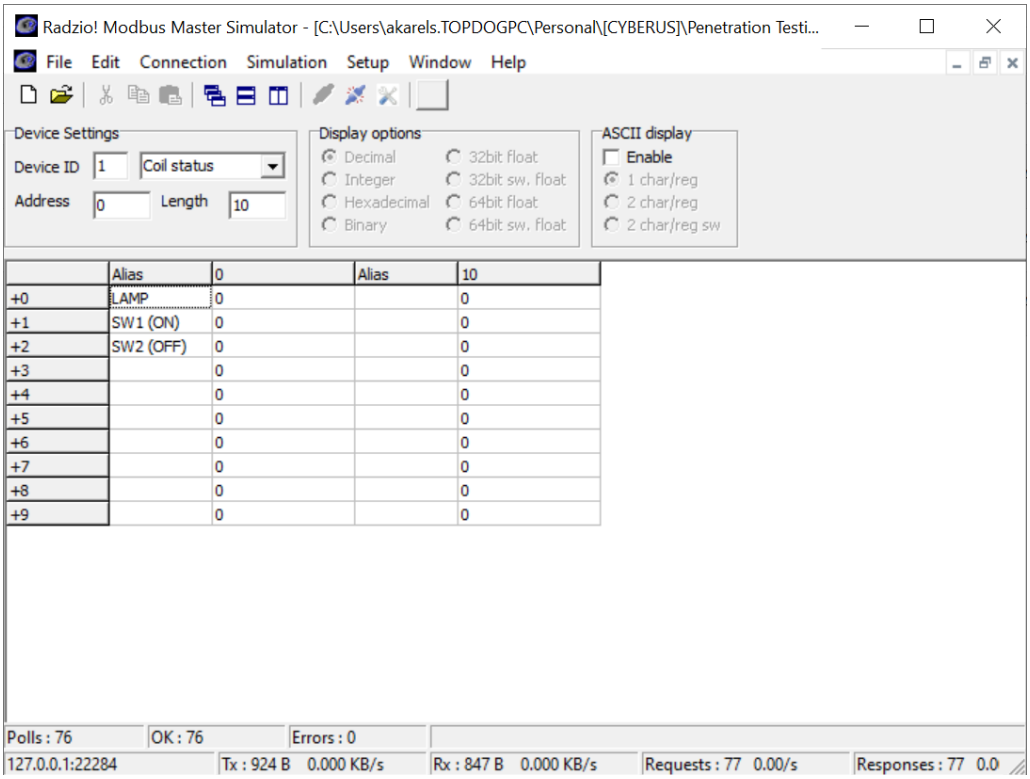

Figure 6.5: Radzio! Modbus Master Simulator

Using the Radzio! application the PLC device can have its control inputs and outputs mapped, as can be seen in figure 6.5 for *LAMP* and *SW1* and *SW2*. Commands to update the values from on/off can be sent to the PLC by simply connecting to the Modbus TCP service on the specified port (502), or simply observe the current state (0 or 1). This is possible because the Modbus protocol does not use any sort of encryption or authentication, completely trusting whatever commands it is sent. This may be the preferred behavior should timing be of key importance, but additional layers of security would be required (strict adherence to the Perdue model).

6.5 Outcomes

The demonstration was not only able to show how Modbus TCP was insecure, but also how functions could be *locked out* by writing directly to the **ON** or **OFF** soft switches, effectively stopping the device from changing state using the physical controls. With this much power over the operation of the PLC, an attacker could create dangerous situations which could potentially be deadly. For instance, an attacker could lock-out the **emergency stop** button, while simultaneously disabling any **warning** lights or alarms. This scenario begs the question if similar tactics were used for the Stuxnet attack.

Overall, the demonstration provided an effective platform to explore the basics of PLC operation and vulnerabilities, and served as a sufficient platform for learning about PLC operation and control. Through hands-on interaction with the hardware and software components, insight was gained into how industrial control systems work, and the potential risks associated with insecure configurations. The vulnerabilities of the Modbus protocol underscores the critical importance of implementing proper ICS security such as the Perdue Model in industrial environments to mitigate the risk of unauthorized access and manipulation.

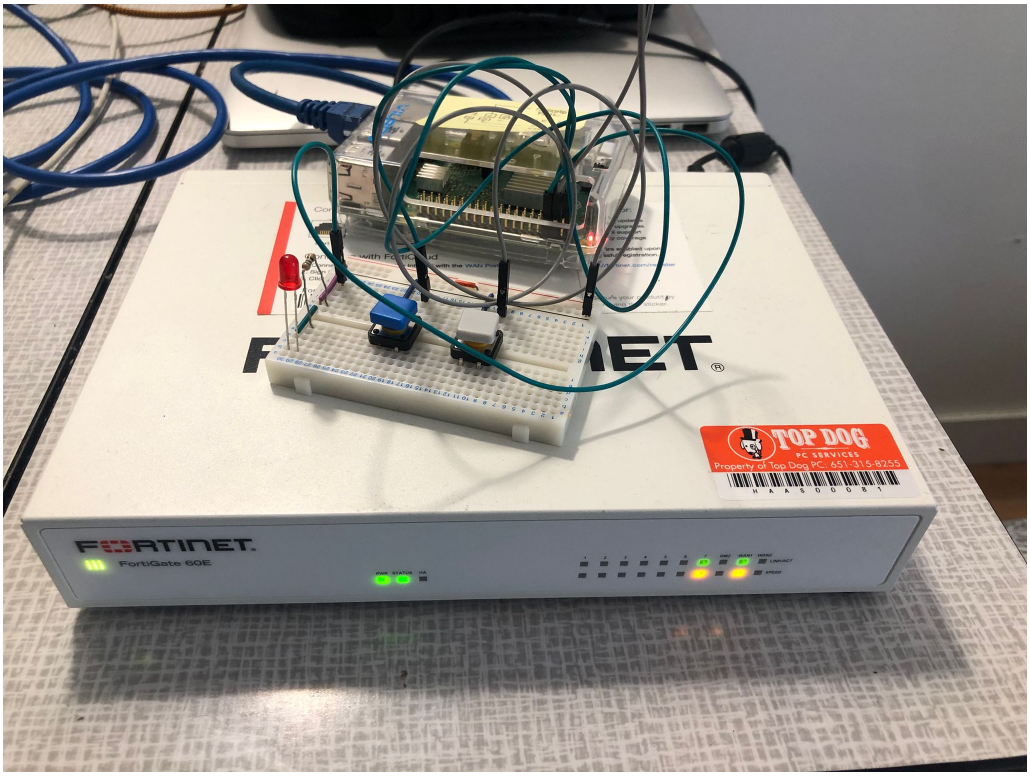

Figure 6.6: Complete setup with firewall, Pi, and components.

Chapter 7

Conclusion

Due to its specialized focus on critical infrastructure, operational processes, and safety systems, ICS penetration testing requires expertise in industrial protocols and specialized tools tailored to these environments. Its importance lies in safeguarding essential services, protecting against cyber threats, and ensuring the resilience and reliability of critical infrastructure. By identifying and addressing vulnerabilities proactively, ICS penetration testing plays a crucial role in mitigating risks and maintaining operational continuity.

Furthermore, ICS penetration testing can instill confidence in manufacturers whose equipment is not currently not networked due to security concerns. During our first semester in Cyberus, we had an opportunity to visit a robotics facility which possessed many high-tech pieces of machinery for their manufacturing process. We were told that although this equipment had the capability for remote control and monitoring, they were purposely kept offline to protect against potential cyber threats. As the company grows it is likely they will want to utilize these advanced time saving features of their equipment, and a proper ICS penetration test will allow them to alleviate their apprehensiveness in networking their industrial equipment.

Figure 7.1: Cyberus visit to Avel Rrobotics in Lorient, France.

Chapter 8

Bibliography

[1] Wikipedia. *Purdue Enterprise Reference Architecture*. Available: https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture.

[2] U.S. Department of Energy. *PURDUE MODEL FRAMEWORK FOR INDUSTRIAL CONTROL SYSTEMS & CYBERSECURITY SEGMENTATION*. Available: https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.energy.gov%2Fsites%2Fdefault%2Ffiles%2F2022.

[3] Modbus. *Modbus Protocol Reference Guide*. Available: https://modbus.org/docs/PI_MBUS_300.pdf#:~:text=URL%3A%20https%3A%2F%2Fmodbus.org%2Fdocs%2FPI_MBUS_300.pdf%0AVisible%3A%200%25%20.

[4] Modbus. *Modbus Application Protocol Specification*. Available: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf#:~:text=URL%3A%20https%3A%2F%2Fmodbus.org%2Fdocs%2FModbus_Application_Protocol_V1_1b.pdf%0AVisible%3A%200%25%20.

[5] National Instruments. *Modbus Protocol Overview*. Available: https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/the-modbus-protocol-in-depth.html.

[6] , Introduction to HART – Highway Addressable Remote Transducer Communication Protocol, Available = https://circuitdigest.com/article/introduction-to-hart-highway-addressable-remote-transducer-communication-protocol,

[7] What is the HART protocol? (Highway Addressable Remote Transducer), Available = https://automationforum.co/what-is-hart-protocol/,

[8] Wireless HART Communication Protocol Overview, Available = https://instrumentationtools.com/wireless-hart-communication-protocol-overview//,

[9] Unauthenticated SSL VPN users password modification, Available = https://www.fortiguard.com/psirt/FG-IR-18-389