DESIGN OF A NOVEL MANUAL AND AUTOMATED PENETRATION TESTING FRAMEWORK FOR CONNECTED INDUSTRIAL CONTROL SYSTEMS (ICS)

by

Rafat Rajab Elsharef

A Dissertation Submitted in

Partial Fulfillment of the

Requirements of the Degree of

Doctor of Philosophy

in Engineering

at

The University of Wisconsin-Milwaukee

May 2021

ABSTRACT

DESIGN OF A NOVEL MANUAL AND AUTOMATED PENETRATION TESTING FRAMEWORK FOR CONNECTED INDUSTRIAL CONTROL SYSTEMS(ICS)

by

Rafat Elsharef

The University of Wisconsin-Milwaukee, 2021
Under the Supervision of Professor Wilkistar Otieno

This research presents the design of new framework—a manually executed and an automated penetration testing process for Connected Industrial Control Systems (ICS). Both frameworks were built using open-source security software and ICS equipment currently used in critical infrastructure, manufacturing companies, and other institutions in the United States and around the world. Existing penetration testing frameworks have largely been focused on manual testing and are specific to Information Technology (IT). In addition, a new severity scoring system framework, called Common Vulnerability Scoring System for Industrial Control Systems (CVSS-ICS), was recommended for calculating the severity score in Industrial Control Systems (ICS).The broader goal of this research is to build penetration frameworks, both manual and automated, for Operations Technology (OT). Four objectives were used to achieve this goal. First, an OT-based testbed was built comprised of PLCs (Programmable Logic Controllers), HMIs (Human Machine Interfaces), a motor drive, and the expected embedded network devices that enable connectivity to emulate a real manufacturing environment. In addition, special security VMs (Virtual Machines) were created and used in the OT testbed. Second, this research ran a manual process of penetration testing against the ICS network using

open-source tools that are used by many IT security professionals and hackers; the data was then collected and analyzed manually. Third, a software program was created using python programming language to automate the above manual process. In addition, the program automates data acquisition, generates security analyses, and makes recommendations. Fourth, a recommended framework of a new severity scoring system, Common Vulnerability Scoring System for Industrial Control Systems (CVSS-ICS), takes into account the importance of safety as a key metric in addition to confidentiality, integrity, and availability in calculating the severity of a single vulnerability, an individual ICS device, or the entire ICS system.

The test results revealed several vulnerabilities related to safety, confidentiality, integrity, and availability of ICS devices used in this testbed. It is recommended to run additional future testing and apply control measures to automate penetration testing in the ICS environment to ensure that the process does not get out of hand in such in an environment, where safety is of concern.

To

my parents

Rajab Ismail Elsharef and Fatima Hossein Elsharef

my wife Reem

and

my kids

Muhammed, Yusef, Isra, Ahmad, Rajab, Sana, Saja, Ismail, and Sama

Thank you for all your support, encouragement, patience, and smiles!

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACHKNOWLEDGMENTS

I would like to acknowledge my advisor Professor Wilkistar Otieno for her support, guidance, patience and encouragement. Also, I would like to acknowledge members of my Ph.D. committee: Professor Hossein Hosseini, Professor Hamed Seifoddini, Professor Matthew Petering , Professor Abdelshakour Abuzneid (Bridgeport University), and Dr. Maryam Hashemian (Rockwell Automation) for their time, support, and feedback.

I would like to acknowledge my colleague Professor Tom Heraly from Milwaukee Area Technical College for providing the testbed equipment, support, and encouragement.

1 Introduction

1.1 Background of Industrial Control Systems (ICS):

The term Industrial Control Systems (ICS) refers to the collection of components that are responsible for controlling and monitoring critical infrastructures such as advanced manufacturing, electrical power grids, water supply, wastewater collection and treatment systems, natural gas pipelines, railroad and transportation networks, air traffic control, and operations in chemical plants and the pharmaceutical and food and beverage industries.

ICSs have been in use for many institutions; they are expected to stay operational after installation for many years, providing high availability [1]. ICSs consist of main components such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Servo Drives (SD), and Human Machine Interfaces (HMIs).

The ICS network is the heart of the new industrial revolution; it has been and remains a key part of Operational Technology (OT). For many years, ICSs ran with no fear of interruptions because such control systems were completely isolated from the rest of the information technology (IT). Such isolation gave OT a sense of security that prevented any threat to disrupt its operation. There were no advantages or needs for IT and OT to be connected or to converge—that is, before the era of cyber-physical systems. This isolation is no longer valid, with the explosion of the Internet, and the availability and advantages of the Connected Enterprise (CE), where systems and devices are connected to and through the Internet.

The great benefits and values of having a connected enterprise are driving many companies and institutions to be part of this network of academics and industry practitioners working on the emerging areas of enabling the OT-IT convergence. The connected enterprise empowers companies to gain valuable benefits such as quality, standardization, scalability, reliability, usability, and integration [2]. The increasing demand for collecting real-time data that enables decision-makers to apply faster and better business decisions, as well as utilize new techniques such as artificial intelligence (AI), machine learning (ML), data analytics, real-time monitoring, and remote configuration and control, has left companies with no choice but to digitize and be part of a connected enterprise(CE). According to Rockwell Automation, "Smart manufacturing and industrial operations embrace a new way forward. This new direction is highly connected, so devices and processes can be continually monitored and optimized [3]."

1.2 The Connected Enterprise (CE)

The connected enterprise (CE) is the idea of connecting companies, people, processes, and equipment together. Such connectivity is vital to deepening the understanding of events and optimizing decision-making [4]. CE brings IT and OT into a single architecture to capitalize on business data and improve the enterprise, operation, and supply chain performance. According to a white paper by Fujitsu titled "The Connected Enterprise: Making the industrial IoT Happen-Right Here, and Right Now [5]," "The advantages of being connected are priceless to companies and vital to their existence. Manufacturing and energy companies have a strong desire to adopt digital technology. The reason for this is clear: automated routines, asset optimization, operating efficiencies, and central manufacturing concerns are all key aspects of being

connected. Indeed, the Industrial Internet of Things (IoT), and connected technologies will have the biggest economic impact: up to $ 3.7 trillion by 2025 [5]."

1.3 Industrial Control Systems' (ICS) Main Components Overview

ICS consists of many components that make up the control systems [6]. These ICS components will be covered in the next subsections.

1.3.1 System Control and Data Acquisition Systems (SCADA):

SCADA is the management component in the ICS system, usually a server with specialized software that can monitor, configure, and troubleshoot ICS devices. A SCADA system allows operators to control distributed control systems located within a Local Area Network (LAN) or a Wide Area Network (WAN) from a centralized location.

1.3.2 Programmable Logic Controllers (PLC):

This is a small industrial computer with limited memory and limited processor power that is designed to perform logic functions that usually are performed by electrical hardware such as relays, switches, mechanical counters, and timers.

1.3.3 Remote Terminal Units (RTU):

These are field devices. Some PLCs serve as a field device and are often referred to as RTUs.

1.3.4 Human Machine Interface (HMI):

HMIs are devices that are generally placed close to production lines. The location, platform, and interface may vary. Some HMIs could be dedicated platforms in a computer room, while others may use a laptop, a browser, or dedicated hardware and software. HMIs are used to display process status information, historical information, and reports. They also allow human

operators to monitor the state of a process under control, modify control settings to change control objectives, and manually override automatic control operations in the event of an emergency.

1.3.5 Servo Drives (SD):

Servo drives are sometimes called amplifiers because they take the control signal from the controller and amplify it to deliver a specific amount of voltage and current to the motor. They also can control torque, velocity, or position of the servo motor. Current servo drives are network aware and have their own IP address that enables them to communicate with the rest of the ICS devices.

1.3.6 Sensors and Actuators

ICS may include different sensors that are used for measurements as well as controlled actuators that include devices such as valves, breaks, switches, and motors.

1.4 ICS Operation:

An ICS operation is enabled by three features, as shown in Figure 1-1. It consists of the following key aspects [6]:

1.4.1 Control loop

Controlled variables are sent from the sensors to the controllers; the controller manipulates the variables according to set points and sends action signals to the actuators that control the process and use the sensors again to relay the change in a feedback loop.

1.4.2 Human-Machine Interface (HMI)

HMIs are used by operators and engineers to monitor, configure, and control PLCs. They are also used to display process status for data visualization and to convey historic information.

1.4.3 Remote Diagnostics and Maintenance Utilities (RDMU)

These are used to identify, prevent, and recover from failure or unexpected operation.

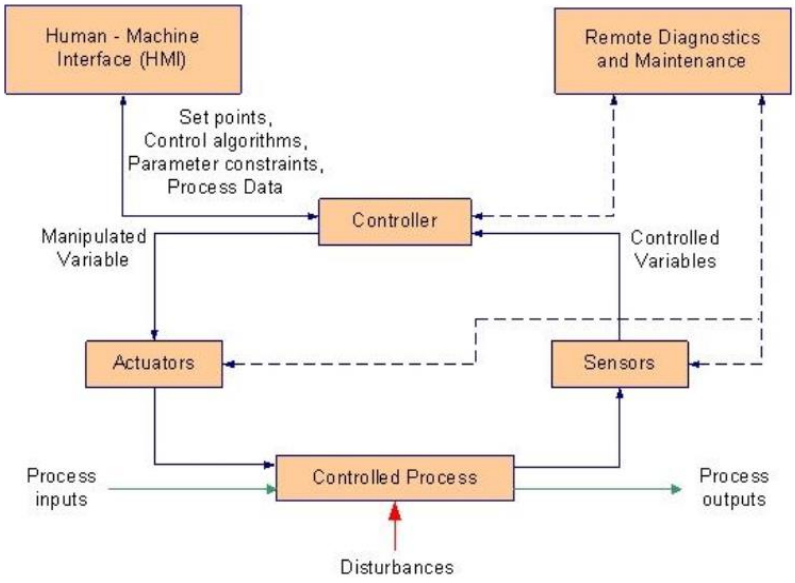


Figure 1-1. ICS operation [6]

1.5 The Purdue Model for Control Hierarchy

The Purdue model is considered as a reference for designing Industrial Control Systems architecture, as shown in Figure 1-2. It is divided into levels of operations that are separated into different zones and isolated by using an industrial demilitarized zone (DMZ).

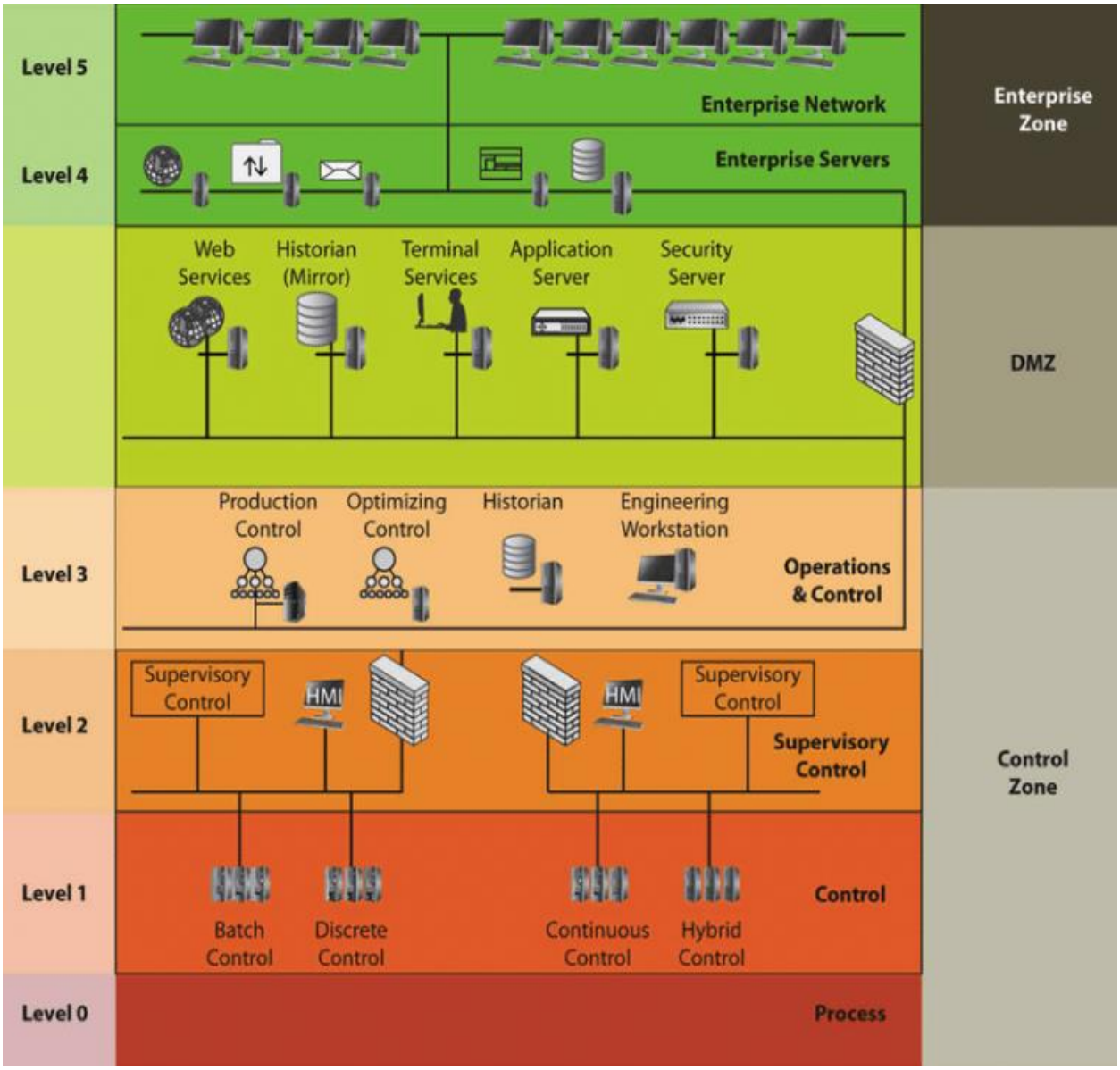


Figure 1-2. The Purdue Model [7]

The Purdue model identifies five recommended levels in this architecture, categorized into three zones, as follows: [8]

- **Enterprise Zone**
    - Level 5: Enterprise network: corporate applications
    - Level 4: Enterprise servers: IT services

- **Demilitarized Zone (DMZ):**
    - These devices can access and be accessed by both the enterprise security zone and the operational zone; it acts like a buffer zone or airgap.
- **Control zone**
    - Level 3: Operations and control.
    - Level 2: Supervisory control: communications to level 1 such as PLC and HMI.
    - Level 1: Basic control: PLC and HMI communicate with level 0 and with each other.
    - Level 0: Process: this level includes sensors, actuators, drives, and motors that communicate with level 1.

1.5.1 Distributed Control Systems (DCS) Implementation Example

Different topologies support DCS. Figure 1-3 [6] shows a basic example of a DCS network topology, where IT and OT networks are shown, including field-controlled devices such as SCADA, PLC, HMI, Servo Drives, and Motors.

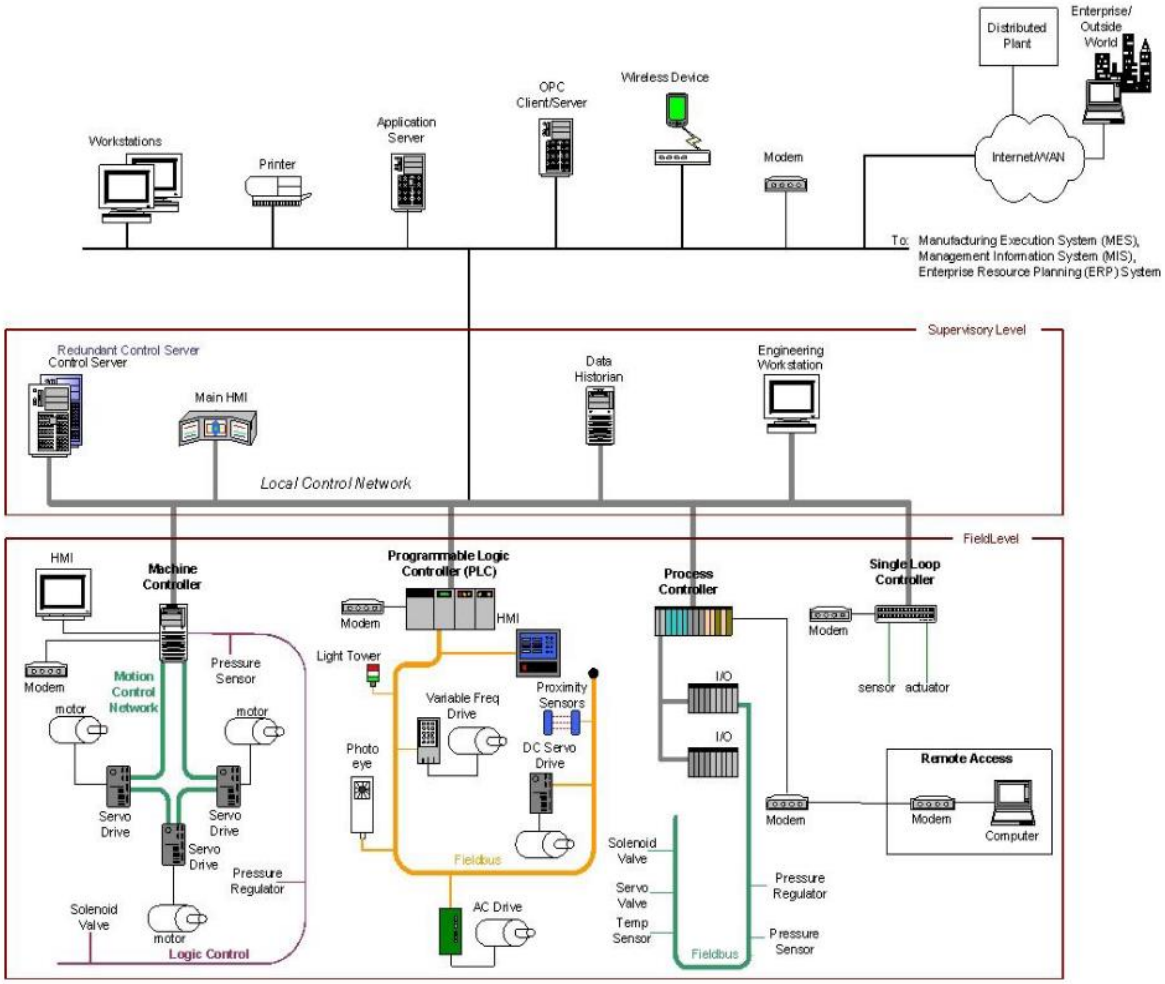


Figure 1-3. DCS implementation example

Figure 1-4 shows a diagram of a PLC controlling a manufacturing process using a fieldbus network. The figure also shows the connections between PLCs, servo drives, and motors [6].

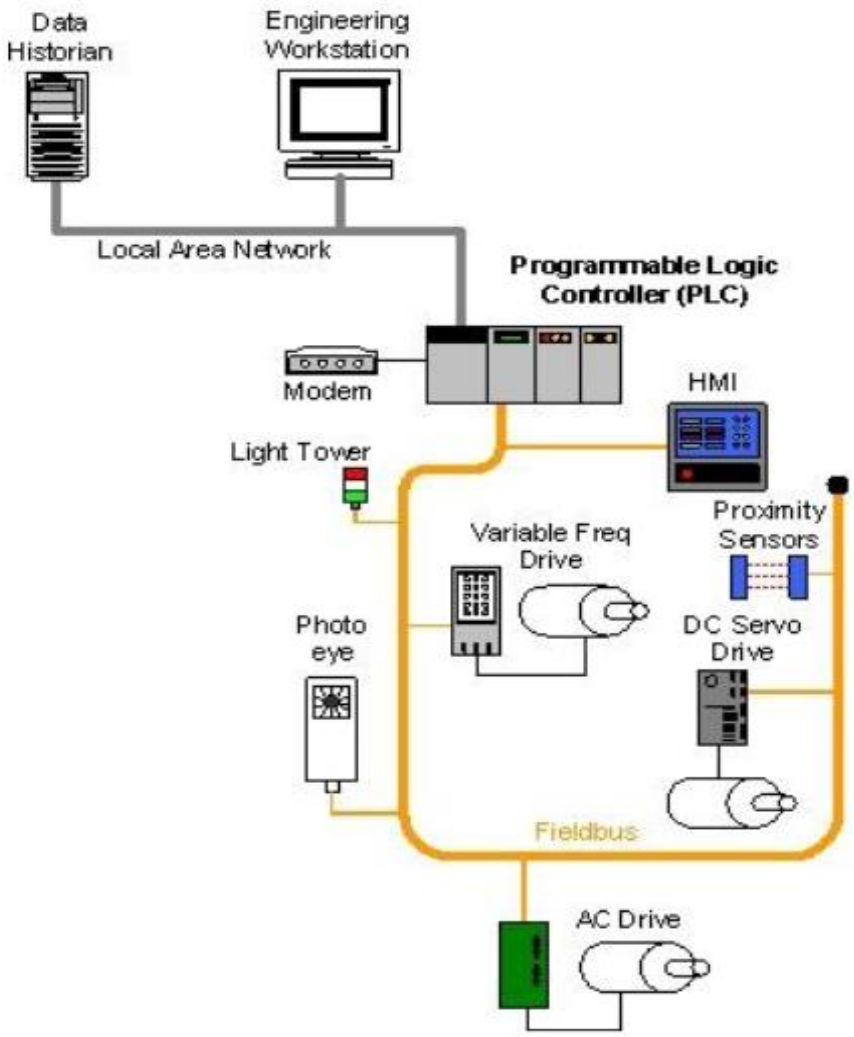


Figure 1-4. PLC control system implementation [6]

Another example of ICS architecture is shown in Figure 1-5, in which the architecture shows the segmentation of the whole network into four areas. First, the corporate local area network (LAN) connects to SCADA via a firewall to isolate both IT and OT. Second, an independent control network communicates with SCADA network via a wide area network (WAN). Finally, the link between SCADA network and field devices connects via a communication link, as shown in Figure 1-5.

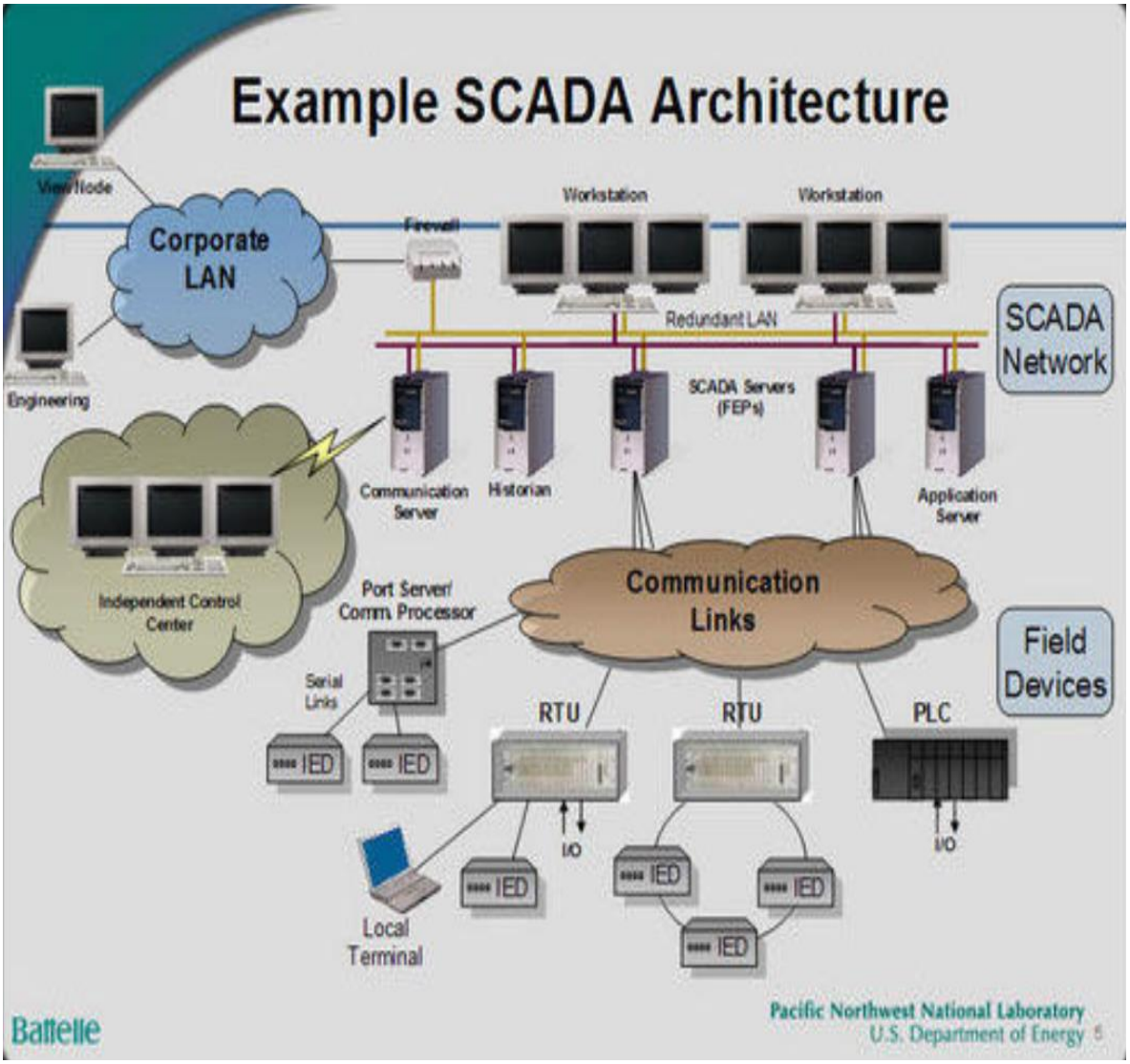


Figure 1-5. Example of SCADA architecture [8]

1.5.2 History of SCADA Architectures

SCADA architecture went through four different generations; early ones were very limited and completely isolated with very specific tasks, whereas the current generation is fully connected and remotely monitored and configured. The four different types of SCADA include [9]:

1. Monolithic (first generation) SCADA systems

These systems were developed when common network services were not available. They function as a standalone system. The first-generation architecture consists of a SCADA master controlling multiple remote terminal units (RTU), as shown in Figure 1-6 below. These early systems were limited to monitoring sensors and sending alerts in case of emergency.

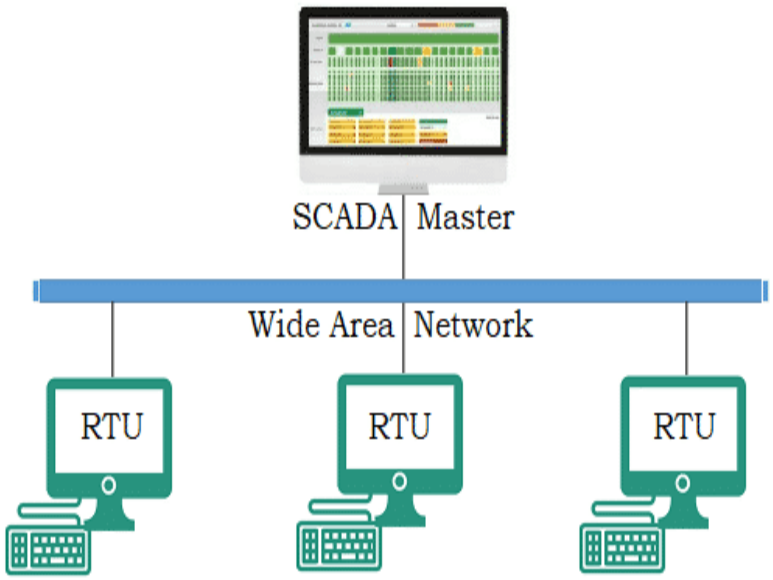


Figure 1-6. Monolithic or early SCADA systems [9]

2. Distributed SCADA systems

This is the second-generation SCADA, where control functions are distributed across several SCADA systems connected via a LAN, as shown in Figure 1-7.

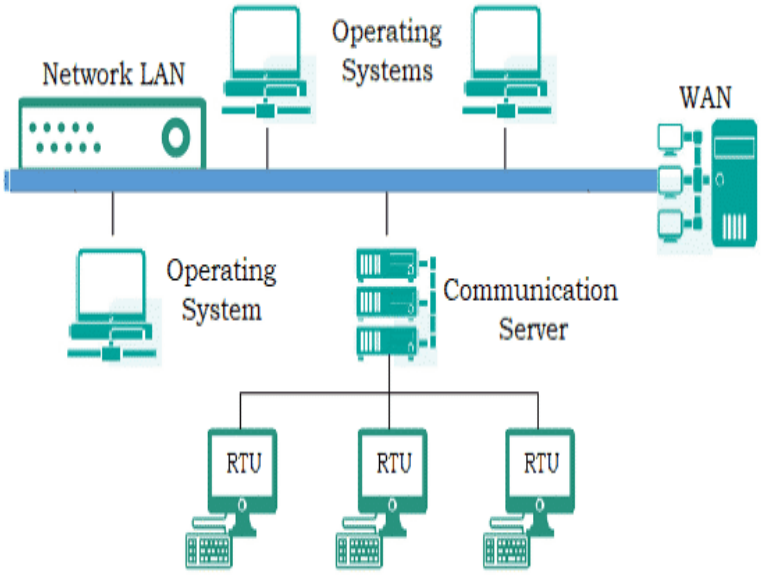


Figure 1-7. Distributed SCADA systems [9]

3. Networked SCADA systems

This type of networked system is considered the third generation of SCADA architecture. These systems use PLCs for controlling operations. SCADA is networked and able to communicate over a WAN through telephone or data lines, as shown in Figure 1-8.

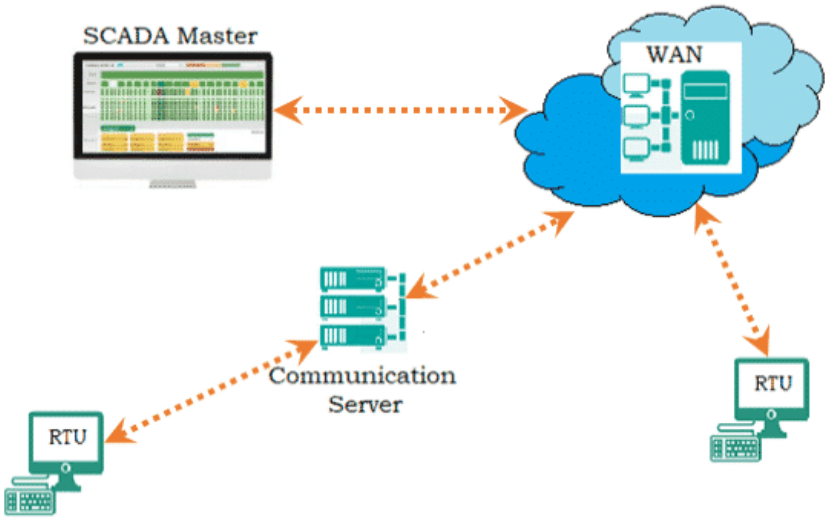


Figure 1-8. Networked SCADA systems [8]

1.5.3 Advantages of ICS/SCADA Systems Implementation

Some of the advantages gained by implementing ICS/SCADA systems include [9]:

- Reduction in cost
- Reduction in manpower
- Minimizing downtime
- Improving the quality of service
- Improving reliability
- Realtime monitoring
- Realtime information on demand
- Value-added services

2 Research Motivation

2.1 Motivating Cases of Cyberattacks

Cyberattacks against critical infrastructure, ICS, and manufacturing environments pose a real threat to the safety, productivity, and quality of operations. Cyber incidents can affect the operator's ability to view, monitor, or control the processes. Some examples of these incidents that had national and international impact include Stuxnet, the Ukraine attacks, and the Triton/Trisis attack, as described below.

2.1.1 Stuxnet

Stuxnet is a computer worm that was originally aimed at Iran's nuclear plant facilities. It was first released in June 2009. Stuxnet has since mutated and spread to other industrial and

energy-producing facilities. The Stuxnet attack was different from other known IT cyberattacks in that instead of stealing sensitive data or damaging computer data, it damaged devices that were controlled by these computers. For example, an early version of the attack targeted the valves on the centrifuges at the Iranian nuclear plant, where the goal was to increase the pressure inside the centrifuges and damage them as well as the enrichment process.

In January 2010, a year after the malware targeted the nuclear plant, inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment plant in Iran noticed that centrifuges used to enrich uranium were failing at unprecedented rates without any clear reason. “The cause was a complete mystery for both the Iranian technicians replacing the centrifuges, and the inspectors observing them [10].” A computer security firm in Belarus was called in to troubleshoot another problem, in which computers were crashing and rebooting constantly, but again, the investigators were not able to identify the cause of the problem [9].

Later, researchers found a small number of malicious files on one of the systems, which led to the discovery of the first digital weapon targeting physical systems such as PLCs. Stuxnet targeted the Step 7 software that is used to program the German-made Siemens S7-400 PLCs. Stuxnet was a targeted cybersecurity attack that was designed to only affect a specific controller. Despite its ability to spread and infect many computers, it does no harm, unless that infected device is involved in uranium enrichment and connected to specific models of programmable logic controllers that are manufactured by Siemens.

Siemens PLCs control and monitor the speed of the centrifuges in the nuclear plant. To secure these controllers from any outside attack, the plant network was air-gapped, which means there is no physical connection between IT and OT. To reach the OT network and deliver the payload inside that isolated network, the attackers first infected the computers of a few support companies that work on installing and programming industrial control and automation systems for the plant. They used an infected USB flash drive and windows autorun feature or through the print spooler that Kaspersky Lab and Symantec later found in the code [9]. The attack generated media attention when it was discovered in 2010, since "it was the first known virus that was able to cripple industrial control systems [10]."

2.1.2 Ukraine Attack

This cyberattack, which occurred on December 23, 2015, was the first known successful cyberattack on a power grid. "According to results from an extensive investigation of the attack, attackers were skilled and stealthy, they carefully planned their hack over many months, first doing the reconnaissance to study the IT and OT networks and siphon operator credentials, then launched a synchronized assault in a well-choreographed dance," according to an article by *Wired* magazine [11]. Attackers were able to control the SCADA systems, resulting in seven 110 KV and twenty three 35 KV substations to be disconnected for three hours, an outage that caused about 225,000 customers to lose power across various locations in Ukraine [11].

Many U.S. experts say that despite the successful attack on Ukraine's power plant, the control systems in Ukraine were surprisingly more secure than some in the U.S. Ukraine's network was well-segmented from the control center business networks with robust firewalls. But they were not secure enough in implementing remote login to control the SCADA network that controls

the power grid, and there were no requirements for employees to use two-factor authentication.

One-factor authentication made it easier for the attackers to hijack their credentials and gain access to their SCADA networks and control the breakers [10]. The attackers spent many months inside the Ukraine network conducting extensive reconnaissance, exploring, and mapping both IT and OT key network nodes and getting access to Windows domain controllers and administrator credentials. These included virtual private network (VPN) logins and passwords that are used remotely to log in and manage the SCADA networks.

2.1.3 Triton/TRISIS Attack

According to Julian Gutmanis, who was involved with an oil and gas organization in Saudi Arabia at the time of the attack, "The publicly revealed attack on August 7, 2017, was not the first incident suffered by the victim at the hands of the Triton/Trisis attacks" [12]. He also indicated that the organization that was affected was a petrochemical plant owned by Tasnee in Saudi Arabia. The attack started earlier in June 2017 when the attackers managed to shut down an emergency plant processor. According to Schneider Electric, the petrochemical's vendor that manufactures Triconex Emergency Shut Down (ESD), the initial investigation of the shutdown was not identified as an attack, as they examined the Triconex ESDs equipment offline and found no indication that there were any problems with it. So, they returned it to the organization.

As a result of this attack, six infected Triconex ESDs machines triggered an unexplained shutdown. "The June investigation by Schneider Electric was insufficient, Schneider attributing

the attack to a mechanical failure of the ESD system rather than a cyberattack," said Gutmanis. "They should have investigated what occurred in the plant" [12]. As a result, the attackers remained unnoticed in the plant network, and it was not until the second attack in August 2017 that it becomes clear that the attackers were inside the network.

According to Gutmanis' team, there were some clues of a spreading attack, including Remote Desktop Protocol (RDP) sessions to the plant's engineering workstations from within the IT network and a poorly configured demilitarized zone (DMZ) infrastructure that led the attackers to compromise the DMZ located between IT and OT. In addition, the VPN network was compromised and infiltrated [12]. As a further result of the attack, the organization suffered multiple outages for at least one full week per attacked plant within the site, but no catastrophic physical disaster occurred. As a clear lesson from the Triton/Trisis attack, according to Phil Neray, Vice President of Industrial Cybersecurity at CyberX, the lack of communication between the organization's IT and OT network operators and the unclear definitions of which team was responsible for ensuring that security controls had been properly implemented were the major contributing factors for such an attack.

2.1.4 Probing the Networks of Electric Utility Organizations in the U.S.

A destructive Advanced Persistent Threat (APT) called XENOTIME, linked to Russian hackers who were behind the TRISIS industrial control system (ICS) attack, had been seen probing electric companies. According to Sergio Caltagirone, Vice President of Threat Intelligence at Dragos, a well-known ICS cyber security consulting company "Offensive government programs worldwide are placing more emphasis and resources into attacking and disrupting industrial processes like oil, power, and water. This means more attacks are coming and people will die,

we just do not know when. XENOTIME is the most dangerous cyber threat in the world, it provides a prime example of threat proliferation in ICS [13]."

2.1.5 Other Related Attacks

"Back in late August 2019, FortiGuard Labs discovered a Malspam campaign that had targeted a large U.S. manufacturing company with malware, a variant of the LokiBot infostealer family. In another incident, Bloomberg reported on the efforts of bad adversaries targeting Airbus by infiltrating its suppliers' networks [14]. Airbus is considered by the National Security Agency as one of the vital companies in the country; they may have created a vulnerability that hackers used by failing to ensure that their suppliers have good security measures in place [14].

2.2 The Need for ICS Cybersecurity

In September 2019, a survey was conducted by Dimensional Research that surveyed 263 ICS professionals. All participants had direct responsibility for securing the ICS system at energy, manufacturing, chemical, dams, nuclear, water, food, automotive, or transportation companies. The survey asked them about their concerns regarding cyberattacks on their organizations' infrastructure and the effect of such attacks. Figure 2-1 [15] shows the distribution of responsibility, job level, and region of the respondents who participated in this research survey.

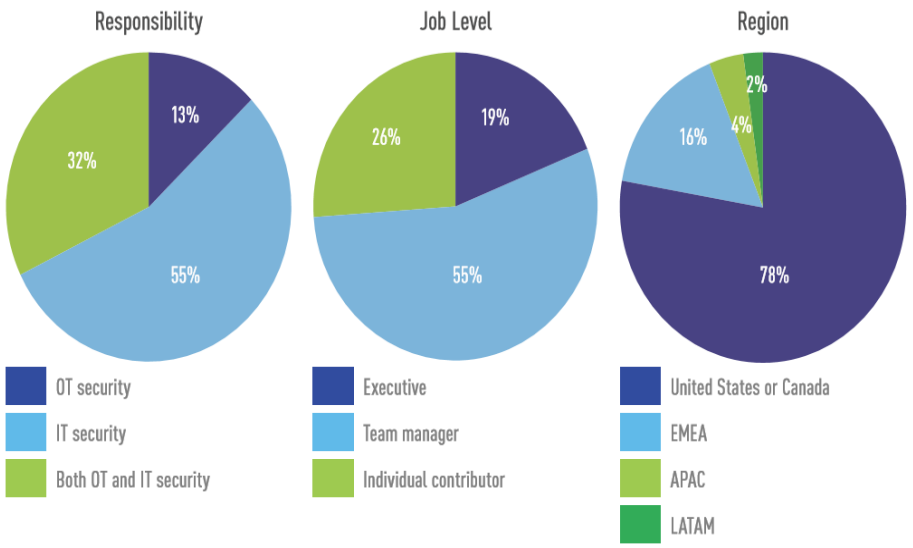


Figure 2-1. Distribution of responsibility, job level, and region of professionals who participated in the research

Figure 2-2 shows the company size and distribution by type for those who participated in the survey [15].

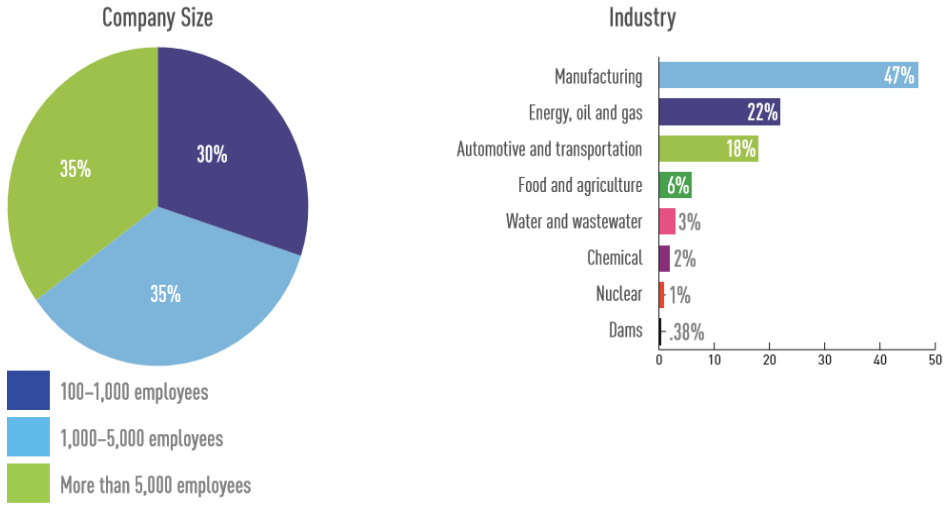


Figure 2-2. Company size and distribution by industry type

Figure 2-3 shows an answer to the survey question: Is your company worried about the risk of cybersecurity attacks on your ICS? The answers according to the research showed very clearly

the concern of these professionals about the status of their ICS security. Of the respondents, 88 percent said yes, and 12 percent said no. Of those who responded yes, 82 percent were in the automotive and transportation sectors, 89 percent were in manufacturing, and 97 percent were in the energy, oil, and gas sectors. Cyberattacks, to these industries, may lead to shutdowns and unplanned downtime, low quality of production, lost reputation, and data exfiltration.

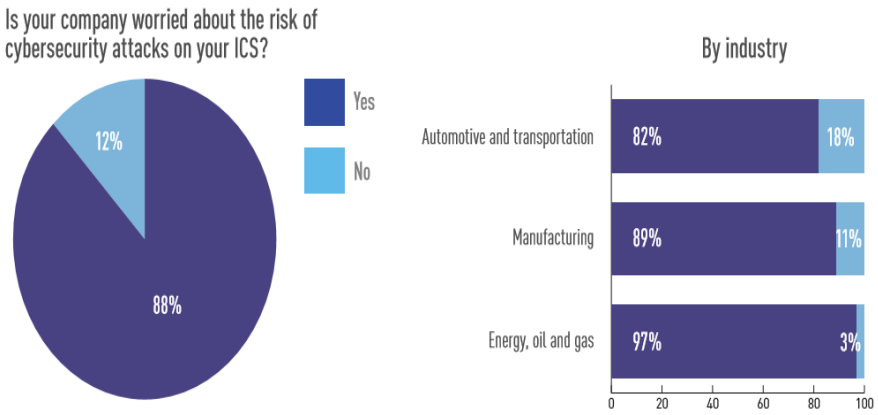


Figure 2-3. The percentage of answers about the risk of cybersecurity attacks on ICS

Security assessments are usually a good starting point for building a cybersecurity program, as they provide an organization with a comprehensive understanding of its security vulnerabilities and risks. According to the research from Tripwire [15], only a third of the organizations that were surveyed (34 percent) had an industrial security assessment, but more than half (55 percent) were thinking about having one; see Figure 2-4.

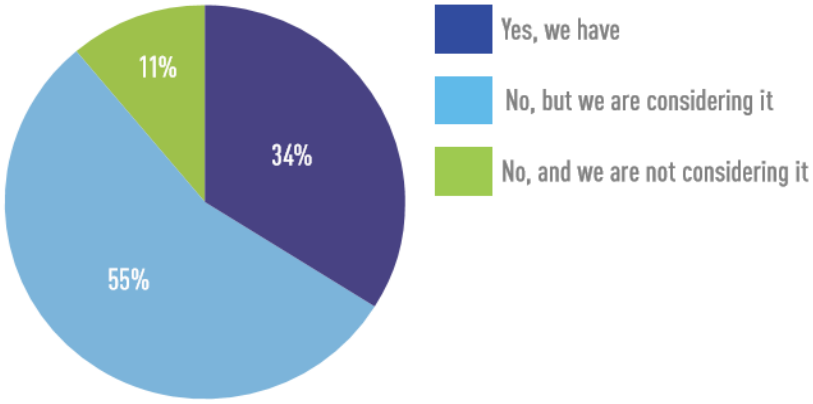


Figure 2-4. This figure shows the answer to whether the organization had a security assessment.

2.3 Information Technology (IT) Versus Operational Technology (OT)

2.3.1 Information Technology (IT)

The building blocks of Information technology (IT) include devices such as routers, switches, firewalls, protocols, and end nodes. Transmission control protocol/internet protocol (TCP/IP), the main protocol used on the Internet, is a collection of communication protocols required to communicate over an Ethernet. The three most important protocols are: (1) Internet protocol (IP), which is responsible for moving packets between source and destination; (2) transmission control protocol (TCP), which is a connection-oriented protocol responsible for managing and maintaining a reliable connection between source and destination; and (3) user datagram protocol (UDP), a connectionless protocol responsible for sending data between source and destination nodes using less overhead and faster transmission compared with TCP.

Transmission Control Protocol/Internet Protocol (TCP/IP) is the most famous and widely used protocol in IT. There are two main models in IT that are used as reference models, namely,

Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). These two models are used to show how communications are done in various network stages.

Data gets encapsulated at the source node as it leaves the application layer, going through multiple layers until it reaches the physical layer, where data is converted into signals represented by ones and zeros. Then signals are transferred through the connected media and any connected network devices until they reach their destination. There, the process of encapsulation is reversed, reaching the target application at the destination node. The OSI reference model consists of seven layers, starting with the application layer at the top, followed by presentation, session, transport, network, data link, and, finally, the physical layer, as shown in Figure 2-5 [16].

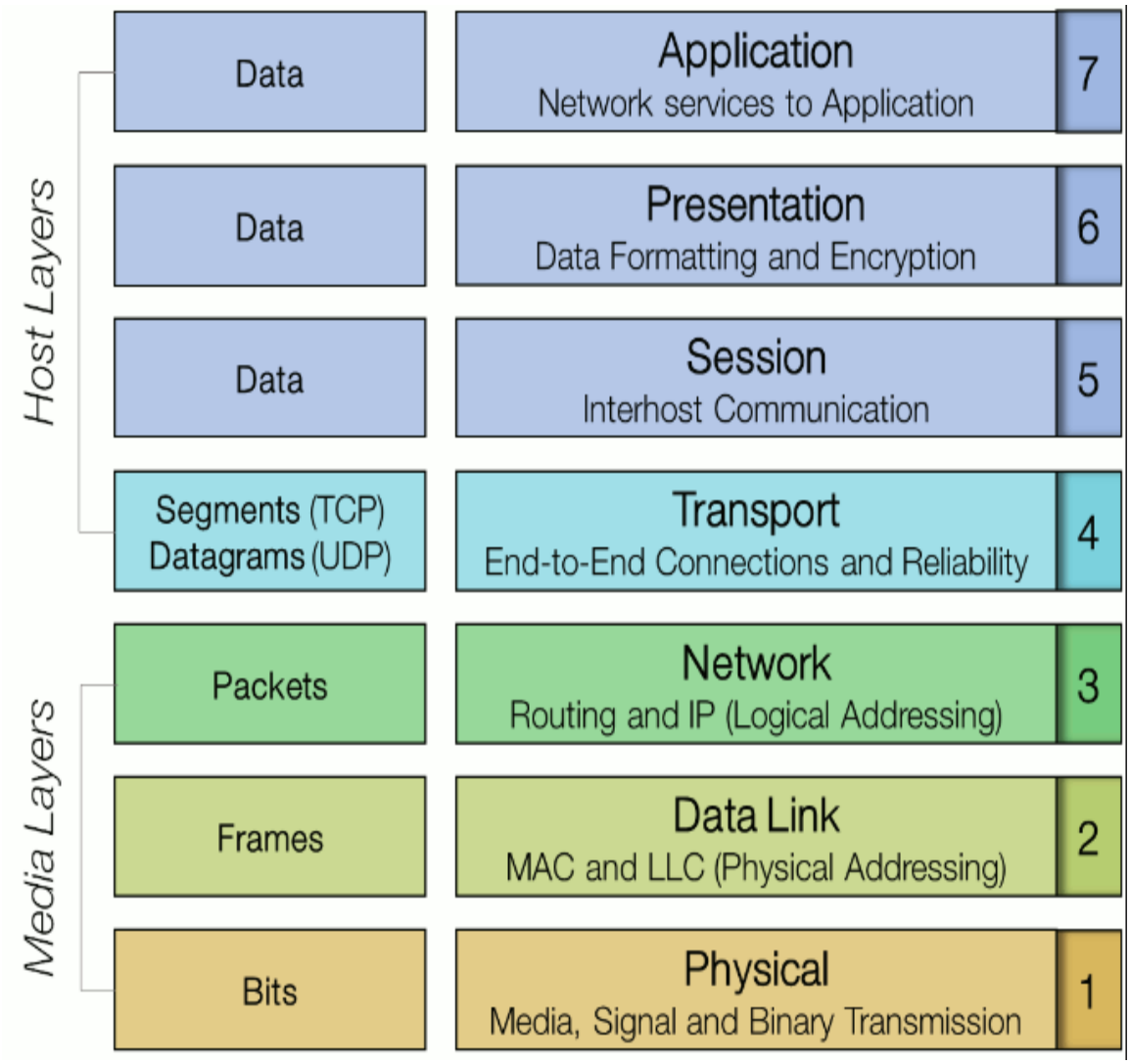


Figure 2-5. OSI model with list functions and protocols in each layer

The Transmission Control Protocol/Internet Protocol (TCP/IP) Model consists of four layers, with the application layer on top, then the transport Internet and the network access layer, shown in Figure 2-6 [17].

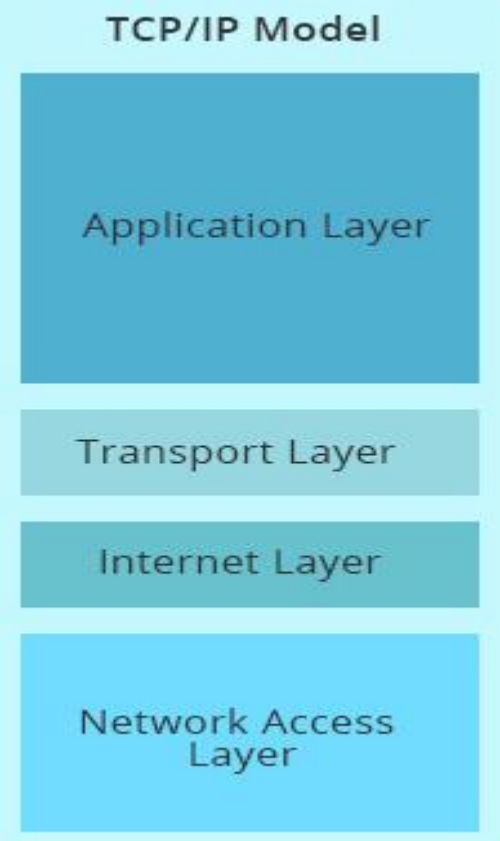


Figure 2-6. TCP/IP model with list functions and protocols in each layer

IT Communication Protocols

Protocols are the rules that allow devices to connect to the network and be able to communicate with reliability and integrity. Modern protocols generally use packet switching for communication. Each packet has a header with multiple fields, including addressing, that are used to assist devices to move packets from source to destination through the network.

Three types of addressing are needed for IT communications:

1. Media Access Control (MAC) addresses

MAC addresses are typically assigned by vendors who created the network interface card (NIC); MAC addresses belong to layer 2 of the OSI model. Each MAC address consists of 12

hexadecimal numbers that are unique. Each node may have one or multiple MAC addresses depending on the number of NIC cards installed in that device.

2. IPv4 /IPv6 addressing

IPv4/IPv6 addresses are needed for each node to join the network. IPv4 can belong to one of five different classes of IP addresses, A, B, C, D, and E, as shown in Figure 2-7. The first three classes are used in an IPv4 addressing assignment, class D is used for multicast, and class E is reserved for research and development purposes.

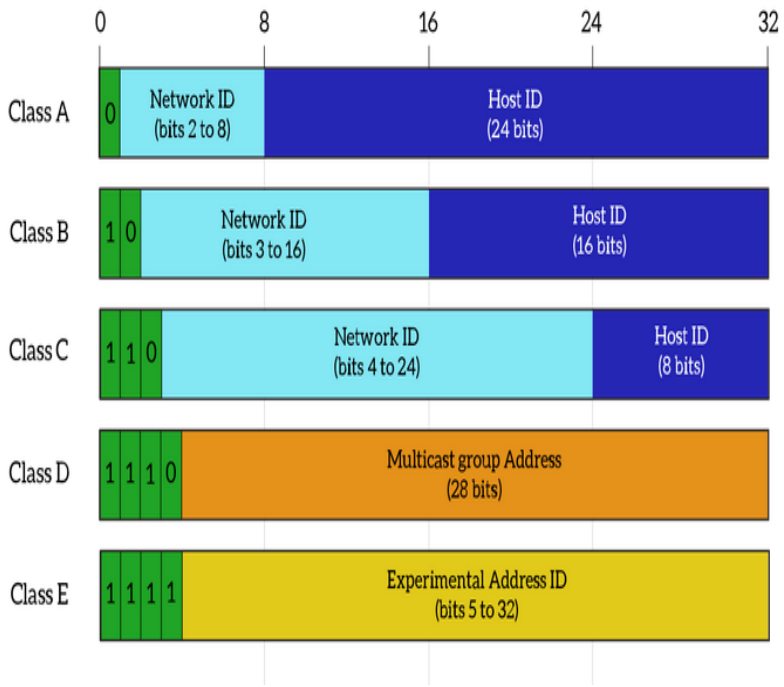


Figure 2-7. Five classes of IPv4 addressing [18]

An IPv4 address consists of 32 bits or four bytes. It is usually represented in four octets using decimal notation. IP addresses are divided into two groups; the first group, called public IP

addresses, are routable across the Internet. There are three classes of public IP addresses, class A, class B, and class C.

The second group of IP addresses is called private IP addresses, which are a list of IP addresses allocated by the network information center (InterNIC). They exist behind routers that are using network address translation (NAT) and are not publicly routable on the global Internet. According to standards set forth by the Internet Engineering Task Force (IETF), the following addresses shown in Table 2-1 are IPv4 address ranges that are reserved for private internets.

Table 2-1: List of reserved private IP addresses

IP Addresses	Range
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

IPv4 packet, Figure 2-8 [18], has many fields in the header that are needed for communication between nodes. Source and destination IP addresses are part of the 20-byte IP header in addition to other fields needed for communications on the network.

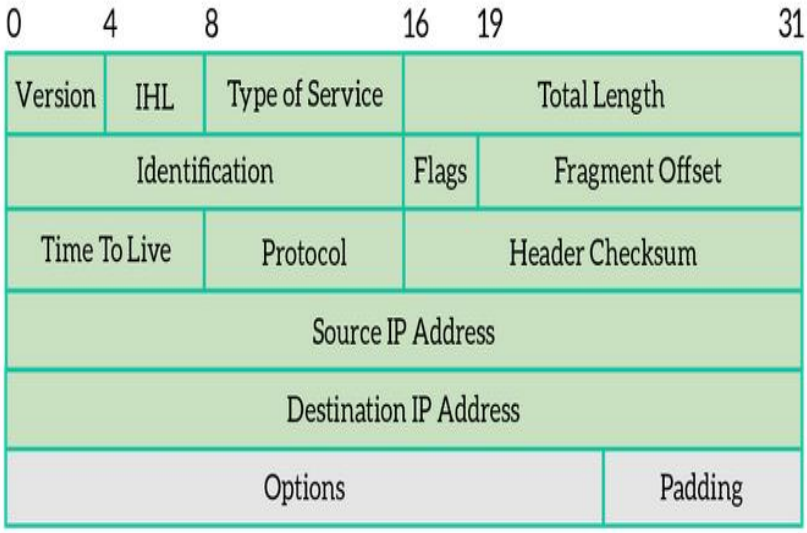


Figure 2-8. IPv4 header

IPv6 addresses are 128-bit numbers and expressed using hexadecimal string notation; No IP version 6 were detected on any of the ICS devices used in this testbed.

3. Port numbers

In networking, port numbers range from 0 to 65535. Port numbers identify a specific connection on the client or a specific service that is running on the server. These port numbers either relate to Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) traffic, as shown in Figure 2-9.

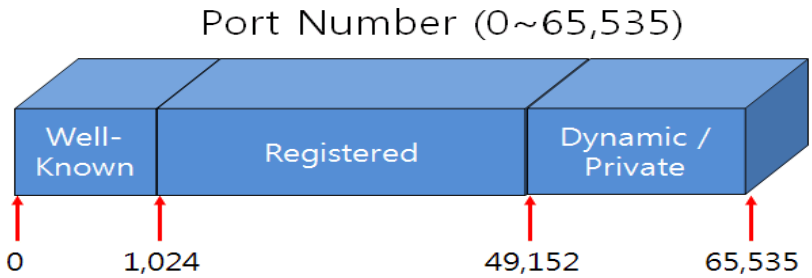


Figure 2-9. Three types of port numbers [18]

There are three ranges of port numbers:

1. Ports 0 to 1023: this range referred to as “well-known ports” that are assigned to specific services by the Internet Assigned Numbers Authority (IANA). An example would be port 80, which is assigned to hypertext transfer protocol (HTTP) or port 123, which is assigned to network time protocol (NTP).
2. Ports 1024 to 49151: these are ports that organizations can register with IANA to be used for specific applications.
3. Ports 49152 to 65535: these are used by client programs; for example, when a client visits a website, the browser will assign the session a port part of this range.

2.3.2 Operation Technology (OT)

Operation technology is referred to as both the SCADA and field devices that are connected to the SCADA using network devices and protocols designed specifically to work for OT. The most used protocol is Ethernet/IP (Ethernet/Industrial Protocol) (EIP), which is the implementation of the Common Industrial Protocol (CIP) over an Ethernet. This research will use Ethernet/IP to communicate between field devices [19].

ICS Standards:

1. International Society of Automation (ISA)99

The International Society of Automation (ISA) 99 standards development committee is responsible for developing ISA standards on industrial automation and control systems security to ensure that industrial and critical infrastructure are secure. The standard addresses issues related to [20] include the following:

- Safety for public and employees

- Loss of public confidence
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Economic loss
- Impact on national security.

In addition, ISA 99 addresses manufacturing and control systems areas such as:

- Networking, monitoring, and diagnostics of DCS, PLC, SCADA and its related hardware and software.
- Human Machine Interface (HMI) that provides control or safety and manufacturing operations functionality to continuous or discreet processes.

2. International Society of Automation (ISA)/International Electrotechnical Commission (IEC) (ISA/IEC 62443)

The ISA/IEC 62443 is a series of standards that were developed by the ISA 99 committee and adopted by the International Electrotechnical Commission (IEC). These standards are specifically designed to address and mitigate current and future security vulnerabilities in ICS. The standards see cybersecurity as an ongoing process and not as a goal that must be reached. The key standards in the IEC 62443 series are the following [20]:

- IEC 62443-2-4, a standard that covers the policies and practices for system integration
- IEC 62443-4-1, a standard that covers the secure development lifecycle requirements
- IEC 62443-4-2, a standard that covers the IACS components security specifications
- IEC 62443-3-3, a standard that covers the security requirements and security levels.

ICS Communication Protocols

There are many communications protocols that are used in SCADA/ICS in comparison with IT protocols. Different vendors may use standard SCADA/ICS protocols or may develop their own proprietary protocols. This is a list of some major manufacturers of SCADA/ICS:

- Rockwell Automation
- Siemens
- Schneider Electric
- Honeywell
- General Electric
- Toshiba
- Mitsubishi

Each of one these companies make different products that use different protocols, some of which are proprietary. Proprietary protocols may add some sense of security, as attackers are unfamiliar with the structure and weaknesses of these protocols. The major disadvantage of proprietary protocols is the lack of ability to integrate with other devices in the network. Integration of these proprietary protocols with other products from other vendors becomes a big challenge. Many SCADA/ICS protocols work and behave differently from each other, and that by itself creates a big challenge to integrators and security professionals. A few examples of the many communications protocols are Modbus, DNP3, Common Industry protocol ((CIP) — CompoNet, DeviceNet, ControlNet, Ethernet/IP), and Profibus.

The common industry protocol (CIP)

CIP is a mechanism for organizing and sharing data in industrial devices [21]. It is the core technology behind ControlNet, DeviceNet, and Ethernet/IP (EIP), and it organizes data objects with data elements called attributes. Figure 2-10 illustrates how ControlNet, DeviceNet, and Ethernet/IP share the CIP common layers.

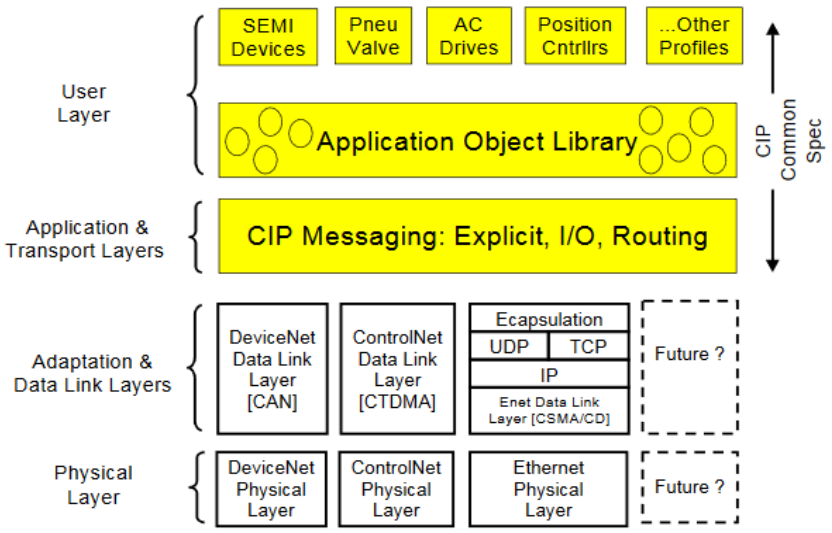


Figure 2-10. CIP common overview

CIP defines two classes of objects that are used with the protocol. The first class of objects is referred to as the required objects that are present in every CIP device. One example of a required object is the identity object that includes vendor, catalog number, and revision number. All information related to this object can be accessed via a CIP read attribute message.

The second class of objects is referred to as application objects, which reflect how the device vendor would like to show the application data. The protocol uses two types of messages. Explicit messages are asynchronous messages using TCP protocol to ensure reliability. An example would be changing the operational setpoint. Implicit messages, on the other hand, are

synchronous messages using UDP protocol where another message will be transferred in the next cycle of communication if a message fails.

Ethernet/IP (EIP)

Ethernet/IP (Ethernet/Industrial Protocol) is a communication protocol that is designed to be used in an industrial environment to allow industrial devices to exchange time-critical application information. An example of such devices are the complex control devices, which are programmable logic controllers, robots, welders, and process controllers. Ethernet/IP uses the implementation of CIP over an Ethernet, which is built on top of TCP/IP protocol to transport CIP messages over an Ethernet [21].

The major advantages of Ethernet/IP include interoperability and the support of plug and play between different devices from multiple vendors, which enables the connections of complex devices such as drives, robot controllers, bar code readers, and weigh scales without custom software. Such interoperability results in faster startups and superior diagnostics, as shown in Figure 2-11, where Ethernet/IP uses a common application layer protocol and shares a common object library, a common device profile, and a common routing with other protocols.

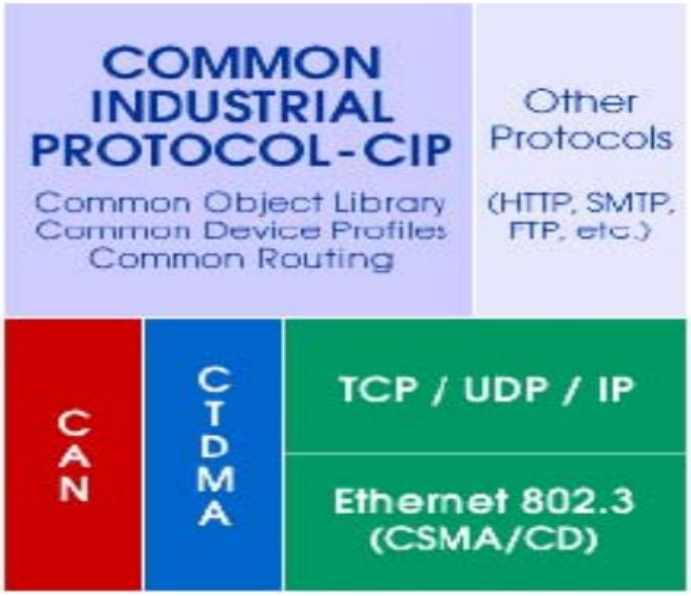


Figure 2-11. Ethernet/IP benefits [21]

Ethernet/IP has two types of messaging connections between nodes: explicit messaging with point-to-point relationships and used to facilitate request-response transaction, and implicit connections that are used to move applications-specific input/output (I/O) data between one-to-one or one-to-many relationships.

Ethernet/IP can provide one-to-many communication for the exchange of real-time critical data such as control data. For example, an Ethernet/IP device can send the same application information to multiple devices at the same time. It accomplishes this by making use of a CIP network and transport layers along with IP multicast capabilities.

2.4 The Need for Security

Due to the important role that ICS plays in controlling critical infrastructure processes, manufacturing companies, and other institutions, there is a great need to secure such devices and ensure that they run without any interruption. One way to test the systems' weaknesses

and finding vulnerabilities is through penetration testing. These tests identify vulnerabilities in the ICS network and enable us to apply fixes to ensure that IT/OT environments are cyber safe [22].

2.4.1 CIA Triad of Information Security

The confidentiality, integrity, and availability (CIA) triad model was created to be used as the baseline standard for any implementation of security systems regardless of the underlying infrastructure or organization. These three elements are considered the most important in ensuring security [33], as shown in Figure 2-12 [23].

Figure 2-12. CIA triad of information security

1. Confidentiality

Confidentiality is the principle that controls access to information. It is the ability to hide data from unauthorized users. Different available algorithms are used to scramble data to allow only authorized users to access it. An example of confidentiality implementation is in the use of data encryption. There are two types of encryption algorithms: symmetric ones that allow encryption and decryption of data using the same key, and asymmetric ones that have two

keys, a public one that can be used by anyone to encrypt data, and a private one that only authorized users have and can be used to decrypt data that was encrypted using the paired public key. Examples of the symmetric algorithms are data encryption standard (DES), triple data encryption standard (3DES), and advanced encryption standards (AES). Asymmetric encryption is used to transfer keys.

2. Integrity

Integrity is the protection of data from unauthorized modification, to ensure consistency, accuracy, and trustworthiness of information that should be sustained over its life cycle. To achieve integrity in data communication, a hash is calculated and added to a packet. This can be achieved by using hashing algorithms such as MD5, SHA-1, and SHA-2, among others.

3. Availability

Availability ensures that resources, devices, and information are available to authorized users when needed. Redundancy, failover, RAID, and clustering are different measures to ensure the availability of data when needed.

In addition to the CIA triad, other areas that are related to security may be as important as the CIA triad. These areas are authenticity, nonrepudiation, and privacy. In the area of ICS, human safety is paramount [45].

Authenticity

This is the process of identification and authentication of users or processes that are trying to access the network resources.

Nonrepudiation

This is the ability to ensure that the originator of a communication or message is the true sender and owner of the message by using a digital signature that identifies the sender.

Safety

Safety ensures that the controlled process is safe when it starts, as it is working, and when it is terminated.

2.5 Penetration Testing

Penetration Testing is an action done by security professionals, who are sometimes called ethical hackers, to identify strengths and weaknesses in the system and exploit vulnerabilities and loopholes. Security professionals use tools and methods to mimic real hackers' actions to test the system. The outcome is a report detailing their findings and their recommendation to harden the system and make it more cyber secure.

2.5.1 Information Technology (IT) versus Operation Technology (OT) Penetration Testing

Usually in an IT environment, the goal of a penetration tester would be to accomplish three tasks [13]:

1. Identify hosts, nodes, and networks.
2. Identify services available such as operating systems and applications related and found in # 1 above.
3. Identify possible vulnerabilities for services found in # 2 above.

On the other hand, in an OT network, in addition to being able to run the penetration testing and accomplish the above-listed tasks, safety, confidentiality, integrity, and availability of ICS are considered top priorities

Each step listed above has an action plan, scope, tools, and results that are associated with it. Due to the critical nature of running such tools in production ICS compared with IT, it is preferred to use passive tools instead of active tools when dealing with production ICS. Table 2-2 shows a list of tools that can be used in penetration testing of both IT and OT, and the recommended actions that can be used [24].

Table 2-2: The difference in actions performed for IT and ICS by penetration testing professionals

Activity	Usual Actions related to IT	Preferred Actions for Production ICS
Identification of hosts, nodes, and networks	Ping Sweep (e.g., Angry IP, Nmap)	1. Examine CAM tables on switches.
		2. Examine router configuration files or route tables
		3. Physical verification (checking physical cable)
		4. Passive listening or IDS (snort, Burp Suite) on network
Identification of services	Port scan (Nmap)	1. Local port verification (e.g. netstat)
		2. Port scan of a duplicate, development or test system.
Identification of vulnerabilities within a service	Vulnerability scan (e.g., Nessus, ISS)	None

2.5.2 The Five Phases of Penetration Testing

Phase 1: Planning and Reconnaissance

The planning and reconnaissance phase is the longest phase; it sometimes may last for weeks or months. The first step in the planning phase is defining the scope and goals of the attack, including the systems to be attacked and the best methods to be used to get the most results. The second step is to gather intelligence (e.g., type of network and type of hardware and software used) and may involve Internet searches, social engineering, dumpster diving, domain name management, search services, and nonintrusive network scanning. Some measures that can be taken to mitigate the impact of this phase are [25]:

- Prevent the leak of information about the system's hardware and software used.
- Ensure proper disposal of printed information related to systems used.
- Install and configure the proper local area network (LAN) and wide area network (WAN) security devices such as firewalls and intrusion detection systems (IPS) that monitor and deny any scanning attempts of the internal network.

Phase 2: Scanning

Attackers move to this phase once they have enough information from phase 1. Such valuable information will enable attackers to select the right tools and to work with the given environment. In this phase, different tools can be used to enable penetration testers to have a more in-depth understanding of the network, devices (hardware and software), operating systems and applications used, open port numbers, and any vulnerabilities associated with all findings. A list of valuable information can be gained in this phase such as:

- Hardware used
- List of open ports
- List of open services and revision number.
- Different applications and version number depending on the tool used
- Operating systems and version used
- Capturing of data in transit and the ability to capture unencrypted information.

Phase 3: Gaining Access

In this phase, weaknesses found in phase 2 are exploited to gain access to systems.

Phase 4: Maintaining Access

After access, usually attackers will leave a backdoor or a rootkit to maintain access and be able to get back in again.

Phase 5: Analysis / Covering Tracks

This is the last phase; in this phase, penetration testing professionals write a report with an analysis of their findings and recommendations to prevent such attacks. In the case of hackers, usually this is the time to clean logs and cover their tracks.

2.5.3 Incidents Due to Penetration Testing

Performing penetration testing on the ICS production system is very dangerous and should not be taken lightly. ICS devices were designed, built, and put into production to perform real-time commands that control real-world processes and equipment. Penetration testing performed on ICS may affect such a system, giving the wrong commands that, in turn, may cause the process

or equipment being controlled to perform incorrectly, causing equipment damage, life-threatening injury, or death.

Some examples of real-life incidents related to penetration testing that show the need for a testbed penetration testing rather than using the real production network directly for such testing include [26]:

First Incident:

The first incident happened while scanning an active SCADA network that controlled a 9-foot robotic arm using a ping sweep. It was noticed that the arm became active and swung around 180 degrees. The controllers of the robot arm were in standby mode before the ping sweep. Fortunately, the person who was in the room at that time was outside the reach of the robot arm.

Second Incident:

The second incident happened when a ping sweep was used on the IT network to identify all hosts connected to the company's network for inventory purposes. The ping sweep reached the OT network and end up bringing the systems that controlled the creation of integrated circuits in the fabrication plant to halt. The outcome was the destruction of wafers worth $50K [26].

Third Incident:

The third incident occurred when a gas utility hired a penetration testing company to conduct a penetration test on the corporate IT Network [26]. The penetration testing tools were able to reach the OT network affecting the SCADA system. As a result, SCADA systems were locked up,

and the gas utility company was not able to send gas through its pipelines for four hours, with a loss of service to customers.

3 Literature Review and Previous Work

To compare our research with other studies that have been published, we looked at seven areas:

1. **IT/ICS:** Was the penetration testing done in IT or OT?
2. **Testbed:** Did the research use a testbed, and what type of vendors and devices were used?
3. **Protocol:** What protocols were used in the research (IT and OT protocols)?
4. **List of tools:** What penetration testing tools were used?
5. **Open-source tools:** Were the tools used open-source, commercial, or both?
6. **Manual/Automated:** Was the penetration testing done manually, automated, or both?
7. **Severity score used for ICS:** was there any Severity score used for ICS?

3.1 Current Solutions

This section lists the current literature and publications related to manual and automated ICS penetration testing and how those studies compare with the manual and automated penetration testing proposed by our research.

3.1.1 SCADA Testbed for Vulnerability Assessments, Penetration Testing, and Incident Forensics

This published research [27] shows a testbed used as an industrial cybersecurity lab at the Department of Computer Science of Sam Houston State University. It is designed to simulate a

near-world industrial setting for industrial cybersecurity to address three areas: penetration testing, vulnerability analysis, and incident forensics, as shown below in Figure 3-1.

Figure 3-1. Original lab setup (left) and current lab setup of systems and network (center and right)

The lab is used as a testbed for students and researchers interested in ICS security and incident forensics. A summary comparison between the above research testbed lab and the testbed used in our research is listed in Table 3-1.

Table 3-1: Comparison of ICS cybersecurity lab at Sam Houston State University and our research

Components	The above research	Our Research
IT/ICS	ICS	ICS
Testbed	EATON (PLC, HMI)	Rockwell Automation PLC, HMI and ABB Drive
Protocol	TCP/IP, MODBUS/ Distributed Network Protocol 3(DNP3)	TCP/IP, CIP, Ethernet/IP
List of Tools	Kali, Wireshark, Nmap, Metasploit, Forensics software such as FTK)	Kali, Nmap, Wireshark, Tshark, TCPdump, Arp-scan.
Open-Source Tools	Open-source and commercial	Only open-source tools
Manual/Automated	Manual attack only	Manual and Automated attack
Severity score used for ICS	None	Recommendation of a new framework that include Safety (SAF) Metric and equations to calculating ICS Severity CVSS-ICS for Vulnerabilities (V), devices (D), and entire system (ENV).

3.1.2 A Cybersecurity Analysis of a SCADA System under the Current Standards, Client Requisites, and Penetration Testing

The aim of the research [28] was to provide guidance by example on how to evaluate and improve the security of SCADA systems, following both a theoretical and practical approach. In the theoretical approach, the research addressed four main areas. First, it analyzed and highlighted standards related to SCADA systems. Second, it suggested and demonstrated an approach on how to perform an analysis of a generic client's cybersecurity requisites. Third was a practical approach that presented a methodology to establish a threat model to help identify common entry points, desired assists on SCADA systems, and possible attack vectors that could

allow access to such assets. Finally, the research proposed a penetration testing methodology that will help validate the attack vector of the threat model. A comparison between the research mentioned above and our research is summarized in Table 3-2 below.

Table 3-2: Summary comparison between this research and our research

Components	This research	Our Research
IT/ICS	ICS	ICS
Testbed	Not listed	Rockwell Automation PLC, HMI and ABB Drive
Protocol	TCP/IP, Distributed Network Protocol 3(DNP3)	TCP/IP, CIP, Ethernet/IP
Tools	Kali, Wireshark, Nmap, Ettercap, Metasploit	Kali, Nmap, Wireshark, Tshark, TCPdump, Arp-scan.
Open-Source Tools	Only open-source	Only open-source
Manual/Automated	Manual attack	Manual and Automated attack
Severity score used for ICS	None	Recommendation of a new framework that include Safety (SAF) Metric and equations to calculating ICS Severity CVSS-ICS for Vulnerabilities (V), devices (D), and entire system (ENV).

3.1.3 Automated Penetration Testing Master's Thesis

This research was done as part of the Master of Science requirements [29]. The researcher automated a testing application that covers attacks based on IT services such as HTTP, SIP, and TCP/IP. The objective was to offer a fast, reliable, and automated testing tool for IT services. A summary of comparison between the above research and our research is shown in Table 3-3.

Table 3-3: Summary comparison between this research and our research

Components	This research	Our Research
IT/ICS	IT	ICS
Testbed	IT services	Rockwell Automation PLC, HMI and ABB Drive
Protocol	TCP/IP	TCP/IP, CIP, Ethernet/IP
Tools	Nmap, Hping	Kali, Nmap, Wireshark, Tshark, TCPdump, Arp-scan.
Open-Source Tools	Only open-source	Only open-source
Manual/Automated	Automated attack (Java)	Manual and Automated attack (python)
Severity score used for ICS	None	Recommendation of a new framework that include Safety (SAF) Metric and equations to calculating ICS Severity CVSS-ICS for Vulnerabilities (V), devices (D), and entire system (ENV).

3.1.4 ICS/SCADA Security Analysis of a Beckhoff CX5020 PLC

The research [30] addressed security analysis of a Beckhoff CX5020 PLC. Beckhoff CS5020 is a PLC manufactured by Beckhoff Automation GmbH, a German automation manufacturer. The PLC runs a Windows CE 6.0 and open standard communication protocols. The research presents the vulnerabilities of this specific PLC and shows ways to achieve rights to control the PLC program. A summary of comparison between the Beckhoff CS5020 research and our research is shown below in Table 3-4.

Table 3-4: Summary comparison between the Beckhoff CS5020 research and our research

Components	Beckhoff CS5020 research	Our Research
IT/ICS	ICS	ICS
Testbed	Beckhoff CS5020	Rockwell Automation PLC, HMI and ABB Drive
Protocol	TCP/IP	TCP/IP, CIP, Ethernet/IP
Tools	Nmap, OpenVAS	Kali, Nmap, Wireshark, Tshark, TCPdump, Arp-scan.
Open-Source Tools	Only open-source	Only open-source
Manual/Automated	Manual attack	Manual and Automated attack (python)
Severity score used for ICS	None	Recommendation of a new framework that include Safety (SAF) Metric and equations to calculating ICS Severity CVSS-ICS for Vulnerabilities (V), devices (D), and entire system (ENV).

Table 3-5 below is a list of literature reviews that were found directly related to IT security, OT security, manual automating penetration testing, and automated penetration testing. Most of the literature is related to automating penetration testing in the Information Technology (IT) environment only. Manual penetration testing tools were found in the operational technology (OT) environment due to safety and availability concerns in such an environment.

Table 3-5: List of some related literature part 1

Author(s), Title, Journal	Year	IT-PenTest	OT-PenTest	OT-Manual	IT-Auto	OT-Auto	Problem Description
S. Krishnan and M. Wei, "SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757543.	2019	N	Y	Y	N	N	Proposed a manual penetration testing using a testbed in a lab environment
G. Bonney, H. Höfken, B. Paffen and M. Schuba, "ICS/SCADA security analysis of a Beckhoff CX5020 PLC," *International Conference on Information Systems Security and Privacy (ICISSP)*, Angers, 2015, pp. 1-6	2015	N	Y	Y	N	N	Proposed a manual Security analysis of a CS5020 PLC made by Beckhoff Automation a German manufacturing company. The paper presents vulnerabilities in this PLC and ways to achieve rights to control the PLC program and operation system itself.
M. Zineddine, "The dilemma of securing industrial control systems: UAE context" 2016 International Conference on Information Technology for Organizations Development (IT4OD), Fez, 2016, pp. 1-6	2016	Y	Y	N	N	N	The proposed solution addresses IT vs. OT. A study that shows the different perception of IT and non-IT staff to ICS security, and how the resistance of non-IT staff impacts the level of coordination in case of cyber war.
Alisherov, F. A., & Sattarova, F. Y. (2009, June). Methodology for Penetration Testing. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.386.7412&rep=rep1&type=pdf	2019	Y	N	Y	N	N	Proposing a penetration testing methodology and the importance of a policy that should be followed by both the tester and the client to reduce financial and confidential disparities.
Duggan, D. (2005). Penetration Testing of Industrial Control Systems. Retrieved September 23, 2019 from https://energy.sandia.gov/wp-content/gallery/uploads/sand_2005_2846p.	2005	N	Y	Y	N	N	The research introduces a list of penetration testing tools and discussion of active vs passive scanning in penetration testing

Table 3-6: List of some related literature part 2

Author(s), Title, Journal	Year	IT-PenTest	OT-PenTest	OT-Manual	IT-Auto	OT-Auto	Problem Description
K. P. Haubris and J. J. Pauli, "Improving the Efficiency and Effectiveness of Penetration Test Automation," *2013 10th International Conference on Information Technology: New Generations*, Las Vegas, NV, 2013, pp. 387-391.	2013	Y	N	N	Y	N	The study addresses automation in an information Technology (IT) environment only
N. Antunes and M. Vieira, "Comparing the Effectiveness of Penetration Testing and Static Code Analysis on the Detection of SQL Injection Vulnerabilities in Web Services," *2009 15th IEEE Pacific Rim International Symposium on Dependable Computing*, Shanghai, 2009, pp. 301-306	2009	Y	N	N	Y	N	The automation in this study is only discussing IT environment with penetration testing against webservices
Y. Stefinko, A. Piskozub and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," *2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, Lviv, 2016, pp. 488-491	2016	Y	N	N	Y	N	The research discusses benefits and drawback of automating penetration testing as it relates to IT environment
J. Zhao, W. Shang, M. Wan and P. Zeng, "Penetration testing automation assessment method based on rule tree," *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, Shenyang, 2015, pp. 1829-1833	2015	Y	N	Y	N	N	Developing a method to improve the accuracy and effectiveness of security assessment in general
N. A. Almubairik and G. Wills, "Automated penetration testing based on a threat model," *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Barcelona, 2016, pp. 413-414	2016	Y	N	N	Y	N	Suggesting a methodology to automate penetration testing based on a threat model as it relates to IT

3.2 Conclusion of the Literature Review and Proposed Solution

None of the solutions in the literature addressed the automation part of penetration testing. A list of areas that were addressed in our research makes it unique and distinguishes it from other studies that have been done so far in the area of ICS penetration testing. These areas are:

1. Both manual and automated processes of penetration testing were conducted against ICS testbed.
2. Penetration testing targeted three areas: the operating system, services, and protocols used on the following specific devices:
    a. PLCS: CompactLogix L30ERM
    b. HMI: Rockwell Panel View 7
    c. Drives: ABB Drive AC350
3. Created a program in Python to automate penetration testing using the following open-source tools: ARP-scan, Nmap, Wireshark, Tshark, TCPdump..
4. Conducted scanning of devices for vulnerabilities, captured and analyzed data, analyzed protocols output, and attacked ICS devices using passive and active man-in-the-middle attack (MITM).
5. Created a new framework (CVSS-ICS) by adding safety as a key metric to calculate severity scoring for vulnerabilities, devices, and the entire ICS system.

4 Research Goals and Objectives

Motivated by the need to secure ICS systems, and performing cybersecurity analysis using penetration testing on such devices, the broader goal of this research to build penetration testing frameworks, both manual and automated and recommend a new framework for calculating the severity score for ICS vulnerabilities, devices, and the whole ICS system Four objectives were used to achieve this goal.

Objective 1: An OT-based testbed of PLCs (Programmable Logic Controllers), HMIs (Human Machine Interfaces), motor drives, and the expected embedded network devices that enable connectivity was built to emulate a real manufacturing environment. In addition, special security VMs (Virtual Machines) will be included in the OT testbed.

Objective 2: Manual penetration testing was done against the ICS network using the open-source tools that are used by many IT security professionals and hackers.

Objective 3: Software was created to automate the manual production testing process. In addition to automating the process of sequential security tool implementation at the end-device level, the processes of security data acquisition, analysis, and security report generation will also be automated.

Objective 4: A recommended framework of a new severity scoring system: Common Vulnerability Scoring System for Industrial Control System (CVSS-ICS), which takes into account the importance of safety as a key metric in addition to confidentiality, integrity, and availability in calculating the severity of a single vulnerability, an individual ICS device, or the entire ICS system.

Due to the sensitivity and sometimes unpredictable results of using penetration tools to test critically connected ICS devices in manufacturing environments, this research built, configured, and analyzed the validity of the proposed frameworks on an isolated testbed as opposed to a real manufacturing environment.

5 Research Methodology

The list of devices to be used in this research are:

1. Rockwell Automation Programmable Logic Controller (PLC): MicroLogix – 1769 - L30ERM/A
2. Rockwell Automation Human Machine Interface (HMI): PanelView Plus 7 1000 DLR
3. ABB Industrial Systems AC Drive: AC350

A Python program was developed to automate the penetration testing process using open-source tools (scanning, capturing, and vulnerability assessment).

5.1 Configuration of the Manual and Automated Penetration Testing

5.1.1 List of Hardware Devices Used

As shown below in Figure 5-1 to 5-9, the ICS testbed consists of the following devices:

1. The main laptop, IP address 192.168.1.109, has a connection to the Internet and running VirtualBox [31]; the virtual machine (VM) software needed to create the attack virtual machine.
2. An attack VM, a specialized Linux machine with open-source tools called Kali [32]. The IP address for this machine is 192.168.0.15

3. A Windows 10 operating system with an IP address of 192.168.0.30.
4. An Ubuntu Linux machine with an IP address of 192.168.0.25
5. Rockwell CompactLogix L30ERM PLC with an IP address of 192.168.0.110
6. Rockwell PanelView Plus 7 (HMI) with an IP address of 192.168.0.120
7. ABB drive AC350 with an IP address of 192.168.0.100
8. Netgear HUB that connects all devices using an Ethernet cable.

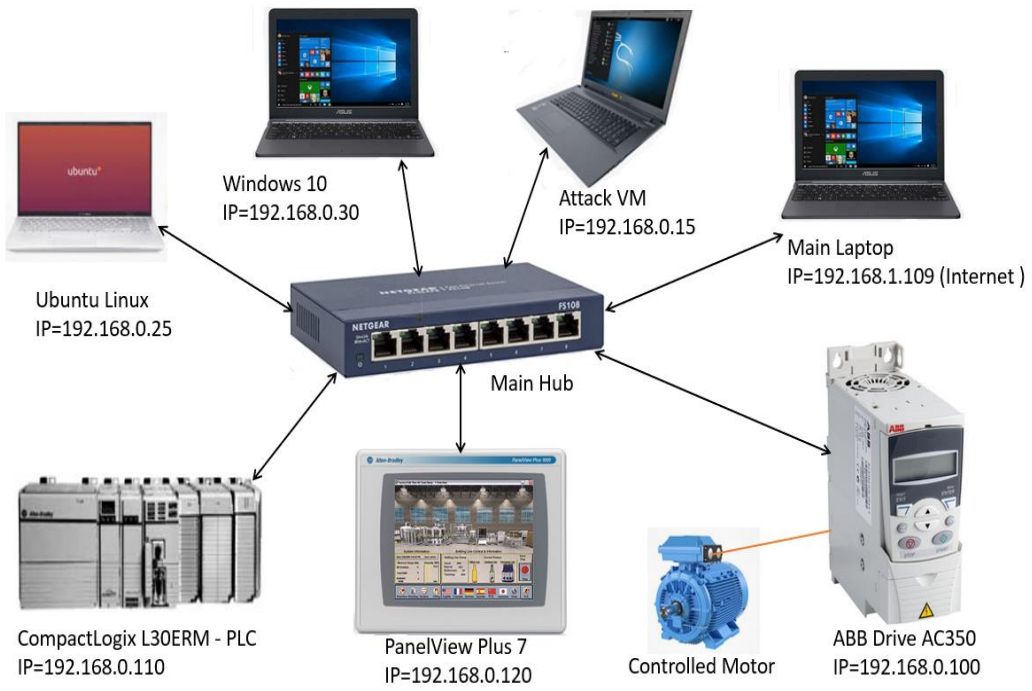


Figure 5-1. ICS testbed with the devices used and their assigned IP addresses

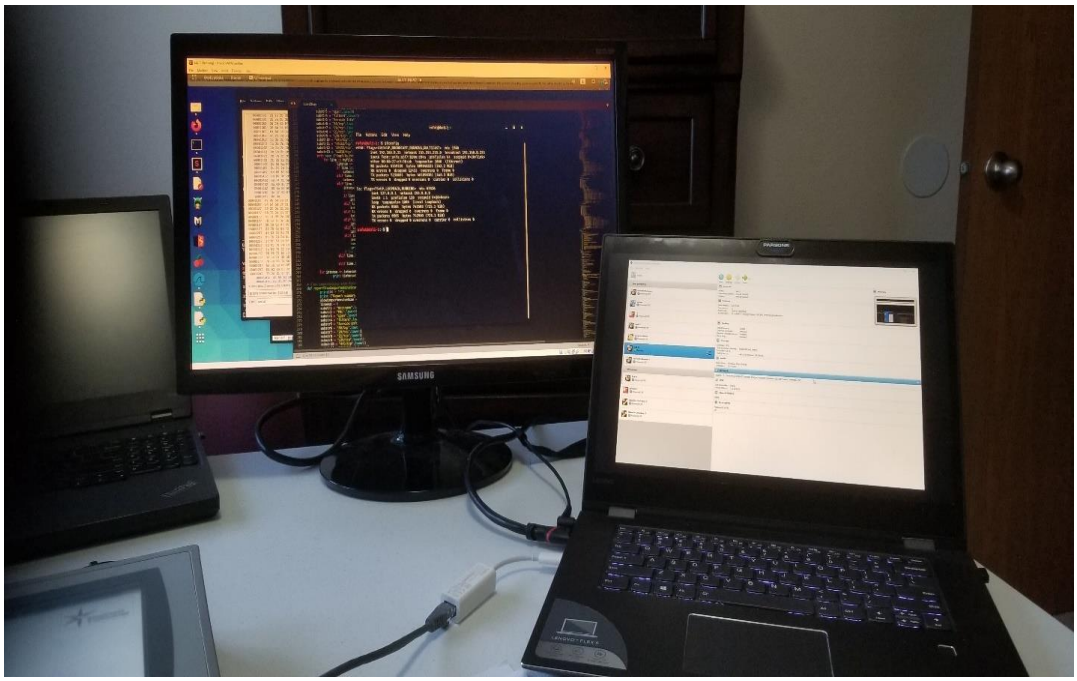


Figure 5-2. Main laptop and Kali VM used to scan, capture, and run the penetration testing program

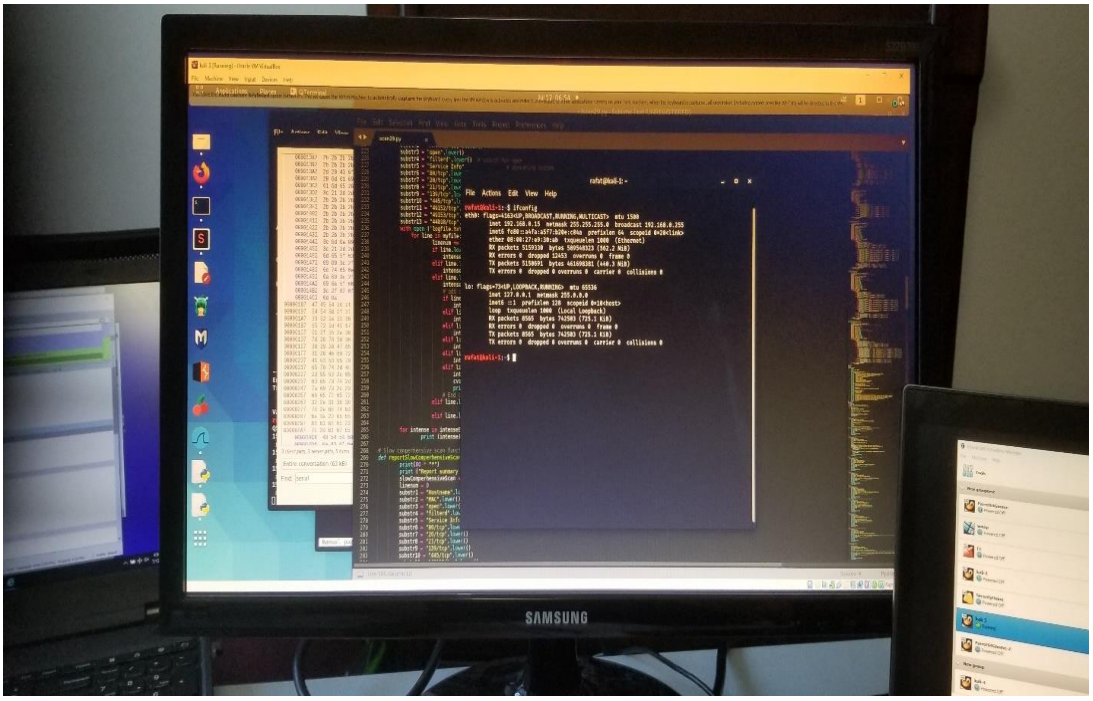


Figure 5-3. Shows the IP address of the Kali virtual machine

Figure 5-4. ICS testbed, including PLC, HMI, ABB drive, laptops including Kali VM

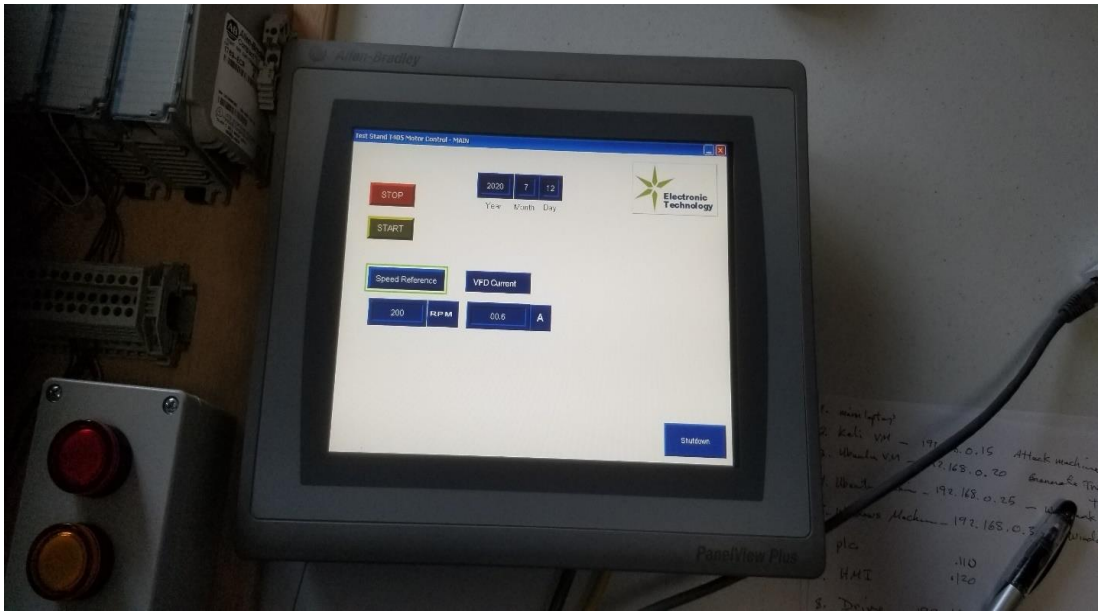


Figure 5-5. Rockwell HMI panel view plus 7

Figure 5-6. Rockwell CompactLogix L30ERM

Figure 5-7. ICS testbed showing connection to the rest of the devices

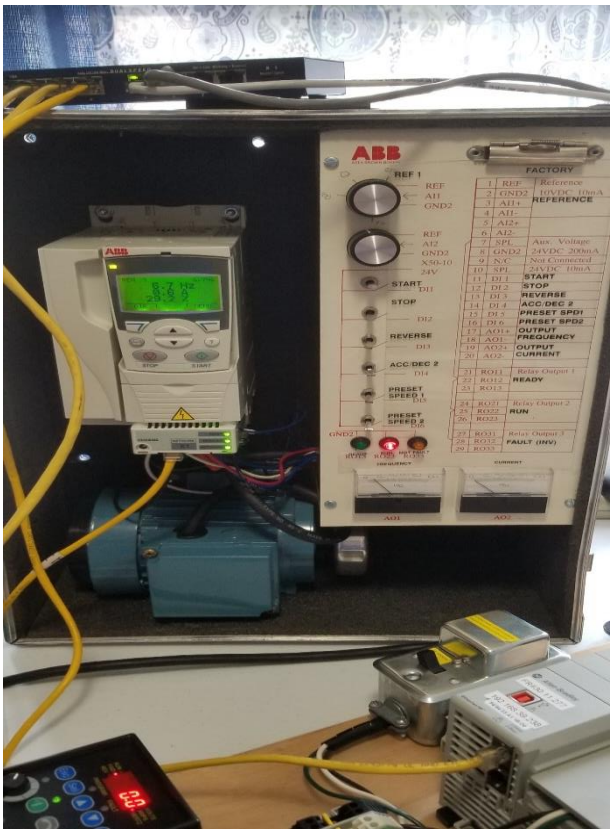


Figure 5-8. ABB drive

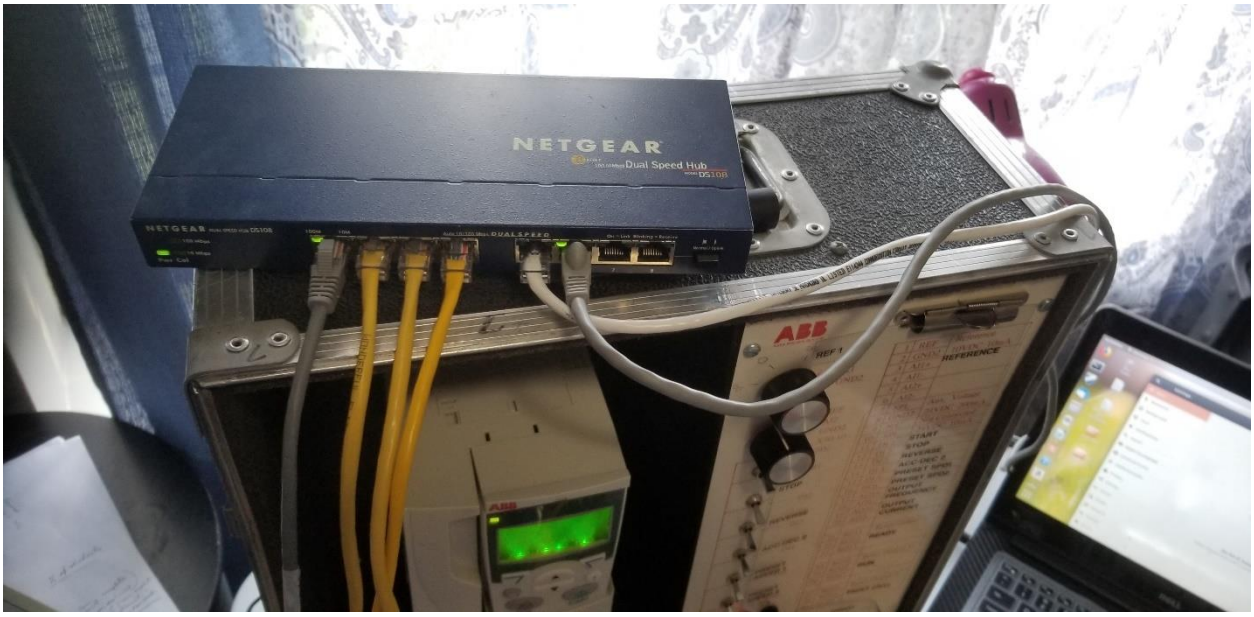


Figure 5-9. Netgear HUB that connects the ICS testbed

5.1.2 Penetration Testing Tools Used

1. **ARP-scan**

Address resolution protocol (ARP) is a protocol that is used in networking to map MAC addresses to IP addresses. ARP-scan uses the ARP protocol, which is used as a penetration testing tool. ARP-scan is an open-source tool that was developed by Roy Hills. The tool needs to access the network at layer 2 (link layer) to extract and display information about the network devices that are connected to the network. To run the ARP-scan command, root privilege is needed. Users either need to log in as root or use the “sudo” command to be able to run the command successfully. The tool sends ARP packets to the hosts on the same local area network and collects and displays their related IP addresses, media access control (MAC) addresses, and vendor name. The tool was very helpful in our research in performing the initial reconnaissance of all LAN attached devices and finding out the vendor to which they belong. Some of the tags used with the ARP-scan are shown in Table 5-1 below.

Table 5-1: List of tags used in the ARP-scan command line

Tag	Description
-i	Network interface to use
--localnet or -l	Find list of targets from the outgoing interface address and netmask
-rtt or -D	Display the packet round-trip time
-verbose or -v	Display extra debugging information

1. **Nmap**

   Nmap is an open-source powerful scanning tool used for network discovery and security auditing. It is mostly used by network and security professionals, as well as hackers [33]. Nmap is designed for an IT environment but also can be used for OT with caution. It uses raw IP packets to determine what hosts exist on the network, what services are running on the hosts, and what operating systems are used.

2. **Tcpdump**

   Tcpdump is a command-line packet capture utility that is included with most UNIX and Linux operating system distributions [34]. It has a limitless possibility with capture and display filter expressions. An example list of flags that are used with the tcpdump command line is shown in Table 5-2 below.

Table 5-2: Commonly used tcpdump flags

Flags	Description
-I <interface>	Listen on <interface> . example -i eth0
-n	Do not perform reverse DNS resolution on IP addresses
-w <filename>	Save capture in pcap format to < filename>
-s	Snap length: Amount of data to be captured from each frame
-c <# of packets>	Exit after receiving a specific number of packets
-p	Do not put the interface in promiscuous mode
-v	Verbose output
-e	Display source and destination MAC addresses and VLAN tags

3. Wireshark/Tshark

Wireshark/Tshark is an open-source traffic analyzer. An essential tool for any network or security professional, it is used to capture traffic and troubleshoot problems related to data communication. Wireshark is the graphical application, whereas Tshark is the command line application. Both Wireshark and Tshark were used in this research to capture and display unencrypted traffic used by ICS devices [35].

4. Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a list of entries that contains an identification number, a rank of impact, a description, and at least a one public reference [36]. A copy of a CVE database was downloaded and used in this research to look up vulnerabilities related to ICS scans during the automated penetration testing process.

5. Automated Program

A Python program was written to automate the penetration testing process. Appendix C shows the code of the program. The program flowchart is shown Appendix A and consists of the following sections:

1. The main program that has the main menu and all the 18 options that can be divided into the following main topics:
    a. Simple scan
    b. Advanced scan
    c. CVE database lookup
    d. Hardware information
    e. Traffic capturing
2. Function ReportSummaryOpenPort()

A function that scans open ports and reports any unsecured ports to be added to the recommendations.

3. Function Report SummaryServices()

   A function that scans all nodes, and identifies all services running, including name, version, and port to be used as the CVE database is searched for vulnerabilities.

4. Function ReportSummaryOS()

   A function that scans all nodes and identifies operating systems used including version number to be used against the CVE database.

5. Function ReportSummaryIntenseScan()

   A function that scans all nodes, including all 655235 ports; it will use Nmap to scan for all TCP, UDP, and OS for information.

6. Function ReportSummaryLowComperhensive()

   A function that scans all nodes, including all 655235 ports; it will use Nmap to scan for all TCP, UDP, and OS, including different scripts and Internet information to find out more information.

7. Function HardwareInfo()

   A function that detects information related to ICS hardware used such as: Type, vendor, product name, serial number, product code, and revision.

8. Function ReportSummaryOfCapturedTraffic()

A function that will list specific information related to captured packets such as: source and destination MAC, IP, and port number.

9. CVE database

The testbed in this research is isolated from the Internet, so a local copy of the CVE database was imported in json format from a CVE website [36], to be used by the automated program. The automated program was designed to search for vulnerabilities using any name, number, or a string and extract related information from the database, such as CVE ID, severity, impact, and description of the vulnerability. The results of searching the CVE database were used to create the final recommendation given by the automated program.

5.1.3 Manual Penetration Testing Flowchart

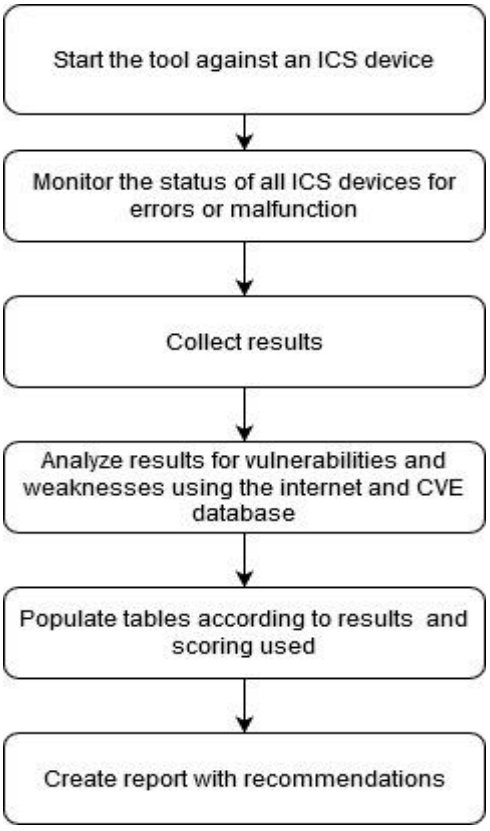


Figure 5-10. Manual penetration testing flowchart

5.1.4 Automated Penetration Testing Flowchart

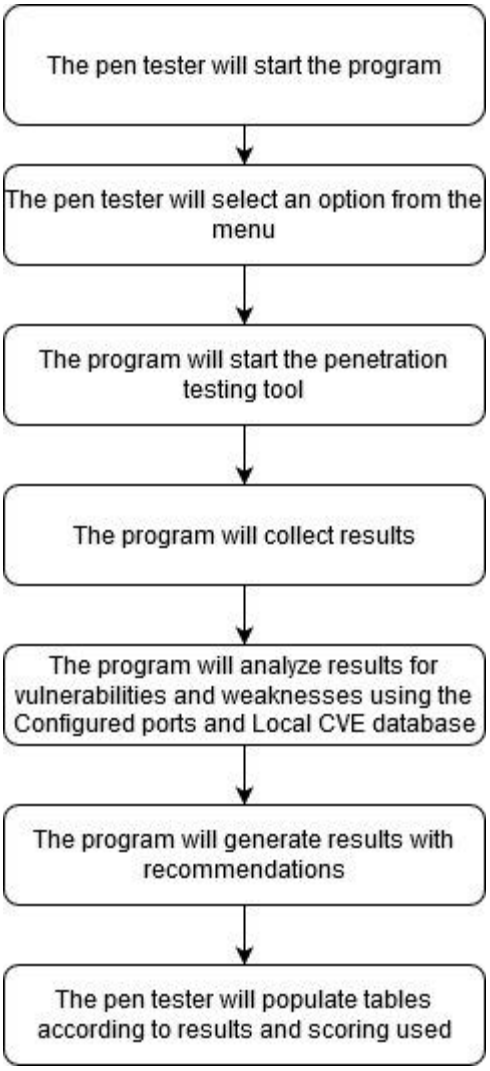


Figure 5-11. Automated penetration testing flowchart

5.2 Manual Penetration Testing Results and Analysis

Steps taken to conduct manual penetration testing:

1. Launched the tool against each device in the ICS testbed.
2. Collected screenshot output from the tool.
3. Continuously monitored the status of the ICS system.

4. Analyzed data for vulnerabilities and weaknesses.
5. Data was collected for the following two areas and tables were created:
    a. ICS: (safety, confidentiality, integrity, and availability)
    b. Process: (efficiency, effectiveness)
6. Report recommendations were made regarding the output.

In the manual process, ran 15 tests were run. Data from each test were collected in addition to screenshots of results, as shown in Figures 5-11 to 5-48. Listed in these figures are the type of penetration testing done, commands used, the output from each command, and an analysis of each output.

5.2.1 Network Scan

Using the ARP-scan tool, the resulting scan is shown in Figure 5-12 below. The output shows the following information:

a. The IP address of the attacking device; in this case, it is the kali machine using ARP-scan.
b. The output of all existing devices on the network, including their version 4 IP addresses, MAC addresses, and the list of vendors that manufactured these devices, such as ABB and Rockwell.

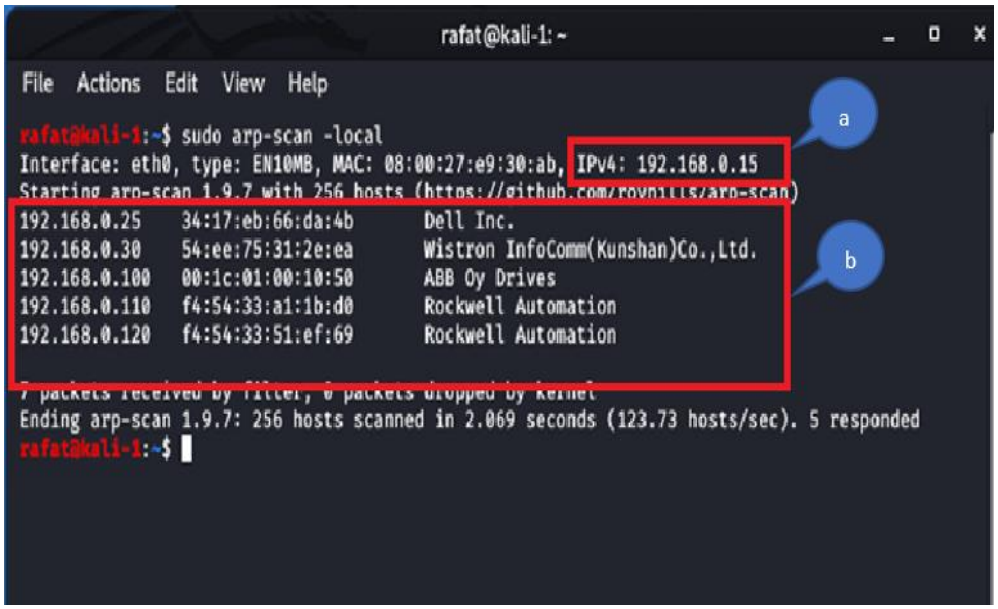


Figure 5-12. Result of ARP-scan

5.2.2 The Output of a Fast Scan

The fast scan of the ICS system using Nmap is shown in Figure 5-13 below. The output shows the following information:

a. The command used to perform the fast scan on the ICS system.

b. The IP address of the target device, which in this case is the ABB drive with an IP address of 192.168.0.100.

c. The only port that shows as open using this scan is TCP port 80 (HTTP), which is a nonsecure port. This port allows a client to connect to the ABB drive over non-secure communication.

d. The IP address of this machine is 192.168.0.110, which is the Rockwell PLC.

e. The IP address of this machine is 192.168.0.120, which is the Rockwell HMI.

f. The list of ports that shows open using this scan is TCP port 80 (HTTP), which is not secure; TCP port 21 (FTP), which is not secure; TCP port 443 (HTTPS), which is a secure port; and port TCP 631 (IPP), Internet printing protocol (IPP) [37].

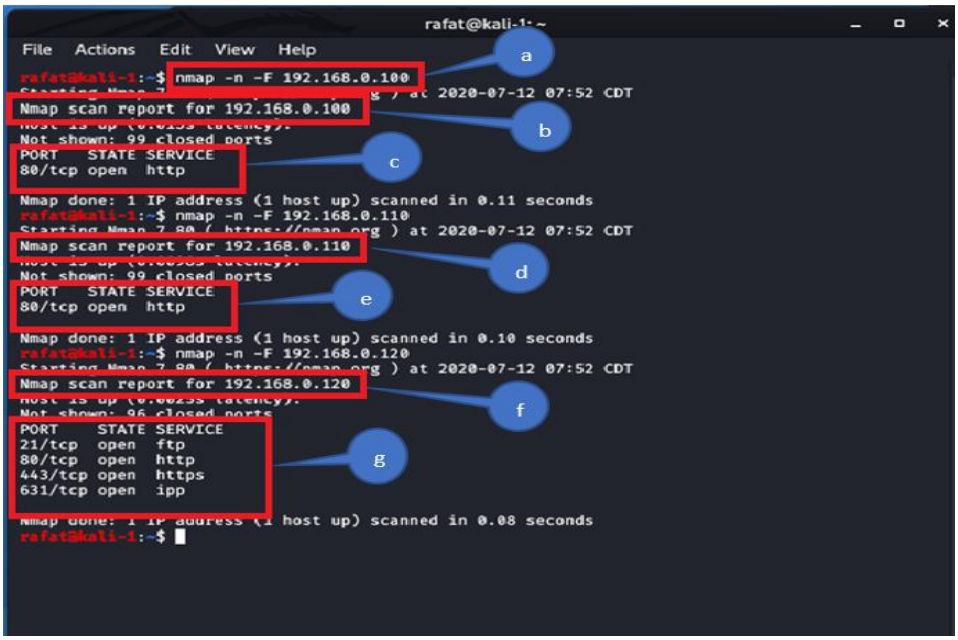


Figure 5-13. Result of a fast scan using Nmap

5.2.3 The Output of the Host/Port Individual Scan

The output of scanning the ICS system using Nmap is shown in Figure 5-14. The command can be used to include the target IP address and the specific port number to be tested. The output shows the following information:

a. The tool and command used to perform the specific scan. In this case, we are targeting the PLC and port 80.

b. Result shows that port 80 is open.

c. Scanning the HMI and port 80.

d. Result shows that port 80 is open.

e. Scanning the ABB drive and port 80.

f. Result shows that port 80 is open.

g. Scanning the ABB drive and port 21.

h. Result shows that port 21(FTP) is closed.

i. Scanning the HMI and port 21.

j. Result shows that port 21(FTP) is open.

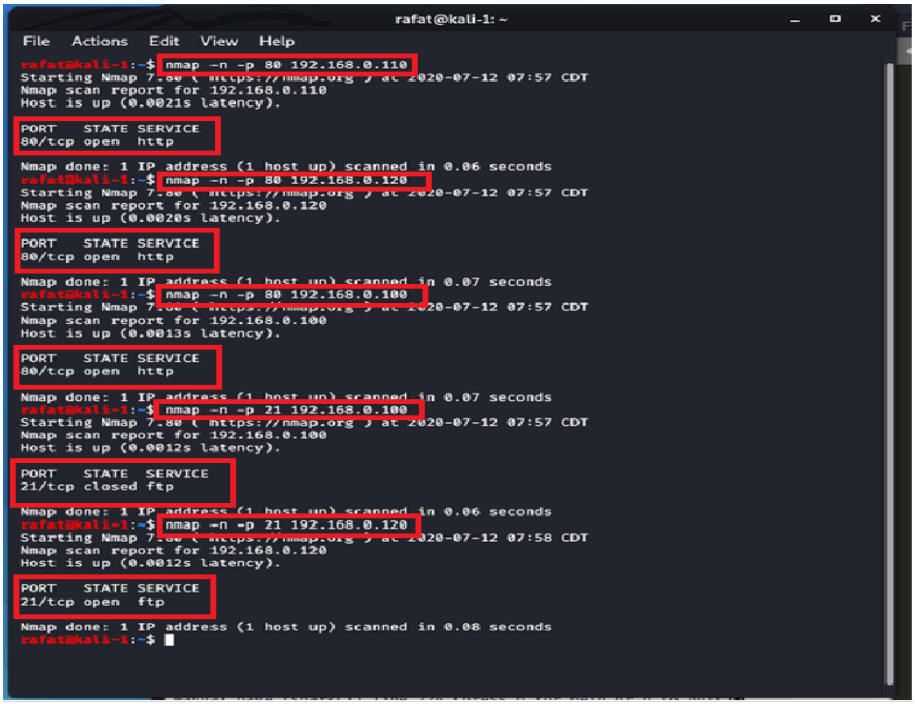


Figure 5-14. Result of selected scan using Nmap

5.2.4 The Output of the TCP Scan

The output of scanning the PLC for all TCP ports (1 – 65535) using Nmap is shown in Figure 5-15 below. The output of the scan is:

a. The Nmap command that is used to scan TCP ports on the PLC.

b. The scan is going through all 65535 TCP ports to find out which port is open.

c. The output shows two ports that are open on the PLC using this scan: Port 80 (HTTP) and port 44818 (Ethernet/IP), used for communication by the PLC and other ICS devices on the network.

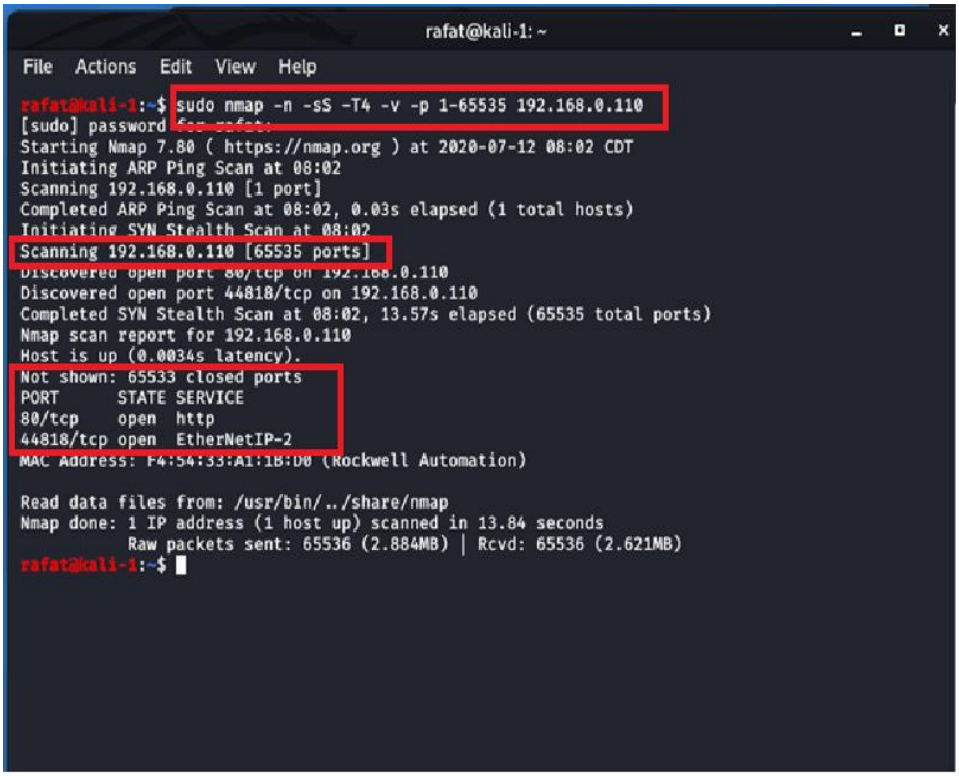


Figure 5-15. Results of all TCP ports scan for the PLC

The output of scanning the HMI for all TCP ports (1 – 65535) using Nmap is shown in Figure 11-16 below. The output of the scan is:

a. The Nmap command that is used to scan TCP ports on the HMI.

b. The scan is going through all 65535 TCP ports to find out which port is open.

c. The output shows seven ports that are open on the HMI using this scan. In addition to ports shown in previous scans, such as port 21(FTP), port 80 (HTTP), port 443 hypertext transfer protocol(HTTPS), port 631(IPP), and port 44818(Ethernet/IP), the TCP scan discovers two new ports that are open. The first one is port TCP 5120, which, according to the IANA website [58], is called Barracuda Backup protocol. The second open port is TCP 5241, a port for which Nmap could not find the service it belongs to. No reference to this port is on the Internet.

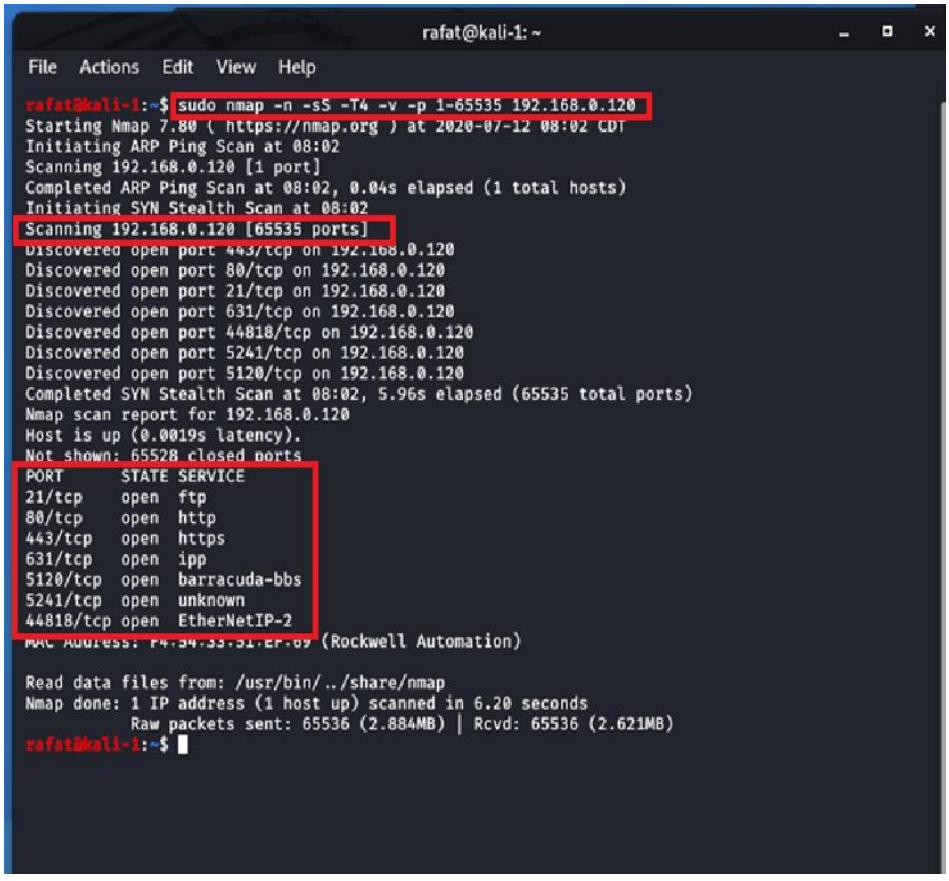


Figure 5-16. Results of all TCP ports scan for the HMI

The output of scanning the ABB Drive for all TCP ports (1 – 65535) using Nmap is shown in Figure 5-17 below. The output of the scan is:

a. The Nmap command that is used to scan TCP ports on ABB drive.

b. The scan is going through all 65535 TCP ports to find out which port is open.

c. Two ports were found open, port 80 and 4818, the same as previous in scans.

As a result of the TCP scan, the ABB drive completely stopped with message Fault-28; as a result, the motor stopped running.

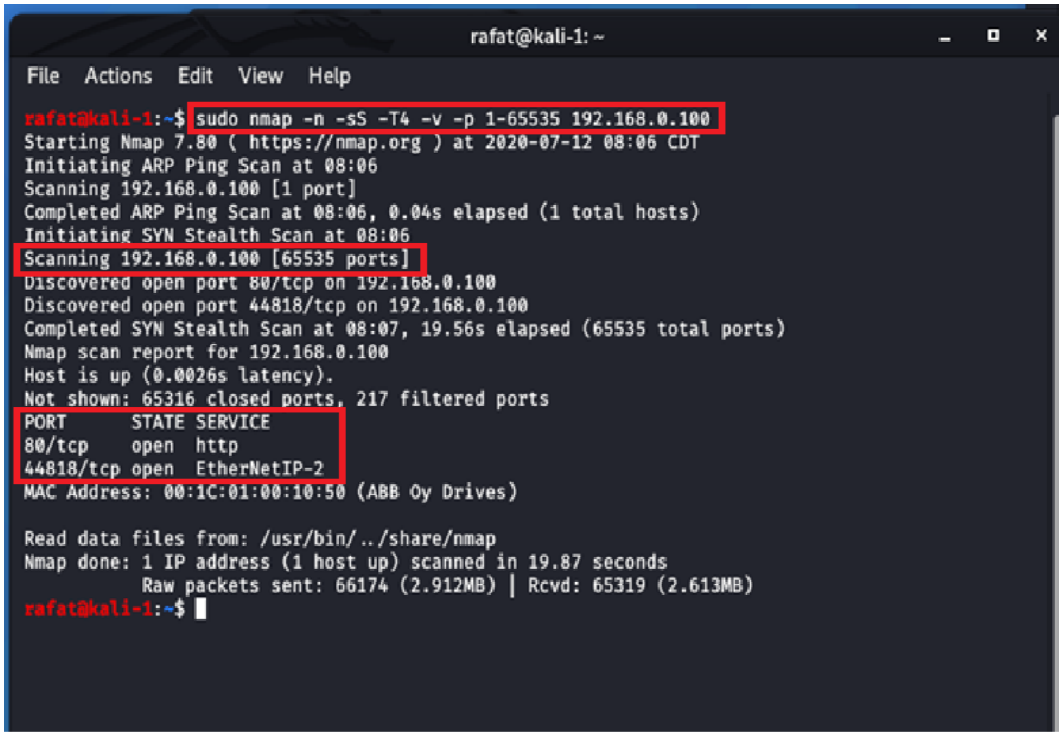


Figure 5-17. Results of all TCP ports scan for the ABB drive

The ABB drive failed, as shown in Figure 5-18 and Figure 5-19 below:

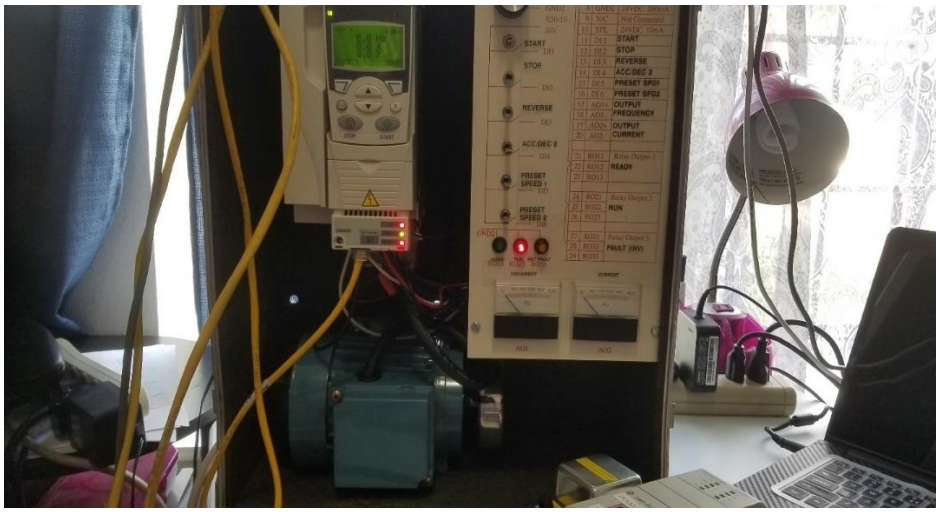


Figure 5-18. ABB drive failed, and the motor completely stopped as a result of the TCP scan

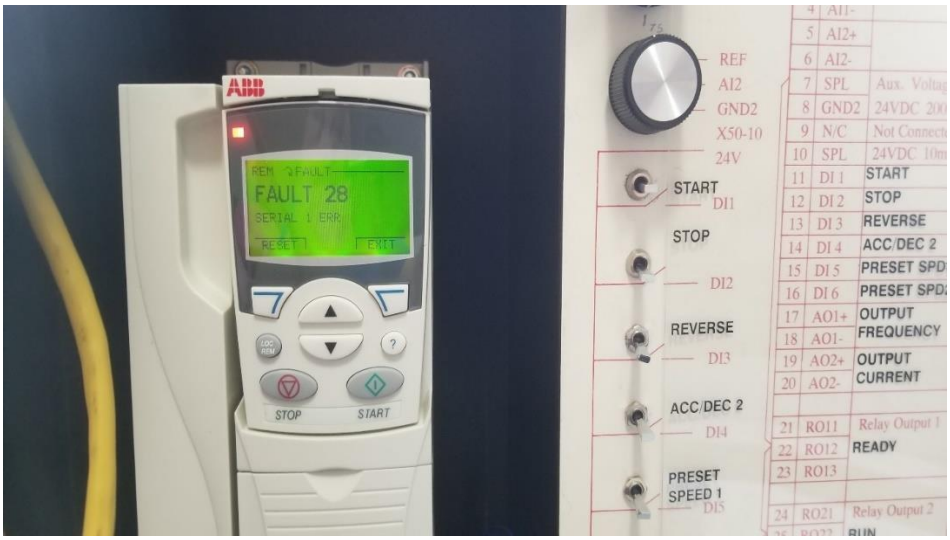


Figure 5-19. ABB drive error with “FAULT 28”

5.2.5 The Output of the UDP Scan

The output of scanning the PLC for all UDP ports (1 – 65535) using Nmap is shown in Figure 5-20 below. The Nmap command is used to scan all 65535 UDP on the PLC. The output shows six UDP ports that were not shown before using previous scans.

a. Port 68/udp (dhcpc) belongs to a service bootpclient. This is a bootstrap protocol client used by a client to obtain dynamic IP addressing information from a DHCP server. There is no need for this port to be open, and it should be disabled, as all PLCs should have static IP assignments.
b. Port 161/udp (SNMP) is used by simple network management protocol (SNMP) and is used by various network devices and applications to communicate management and logging information. SNMP v3 uses encrypted communication, where SNMP v1 and v2 are clear text and should not be used.
c. Port 319/udp (ptp event message) using Precision Time Protocol (PTP) and Port 320/usp (general message) are both used to synchronize the clock of a network client with a server similar to network time protocol (NTP), but PTP is mainly used in LAN with devices that require precision timing more than NTP, usually in the range of tens of microseconds to tens of nanoseconds and explained in the specification IEEE 1588 [38].
d. Port 2222/udp (msantipiracy): the port name is Rockwell csp2; AB/Ethernet is a legacy protocol that only works on non-CIP messaging.
e. Port 44818/Ethernet/IP-2 is used for Ethernet/IP messaging between ICS devices. Communication for this port is in clear text.

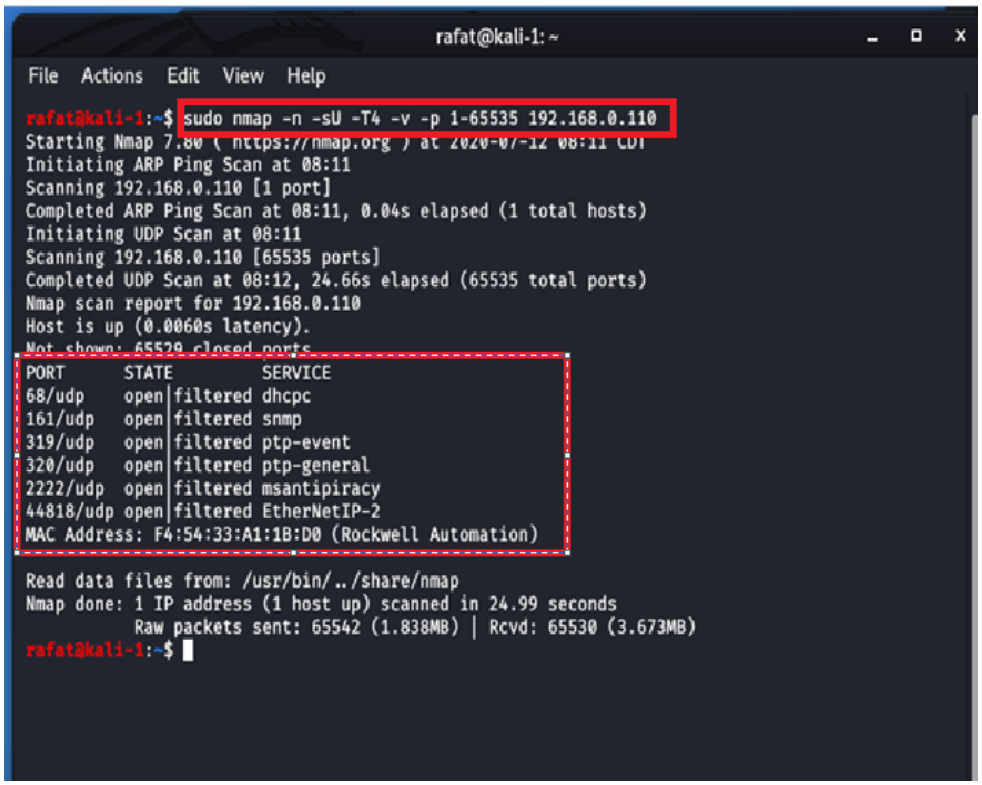


Figure 5-20. UDP scan of PLC shows all UDP ports found

The output of scanning the HMI for all UDP ports (1 – 65535) using Nmap is shown in Figure 5-21 below. Nmap command was used to scan all 65535 UDP on the HMI. The output shows three UDP ports that were not shown before using previous scans in addition to port 44818/udp(Ethernet/IP). A list of ports discovered is:

a. Port 137/udp (NetBIOS-ns) is Windows NetBIOS name service. udp NetBIOS name query packets are sent to this port to ask for NetBIOS name. This port usually runs on a Windows machine or systems running Samba (SMB).

b. Port 138 / udp (NetBios-dgm) report open or filtered is Windows NetBIOS datagram service. It allows datagrams to be exchanged between machines, which allows access to

shared resources such as files and printers. This port usually runs on a Windows machine or systems running Samba server message block protocol (SMB).

c. Port 1900/udp upnp, universal plug and play, is used by Microsoft simple service discovery protocol (SSDP) to enable discovery of UPNP devices. It runs by default on WinXP and creates an immediately exploitable security vulnerability for any network-connected system. The status for this port is open/ filtered to prevent any security issues.

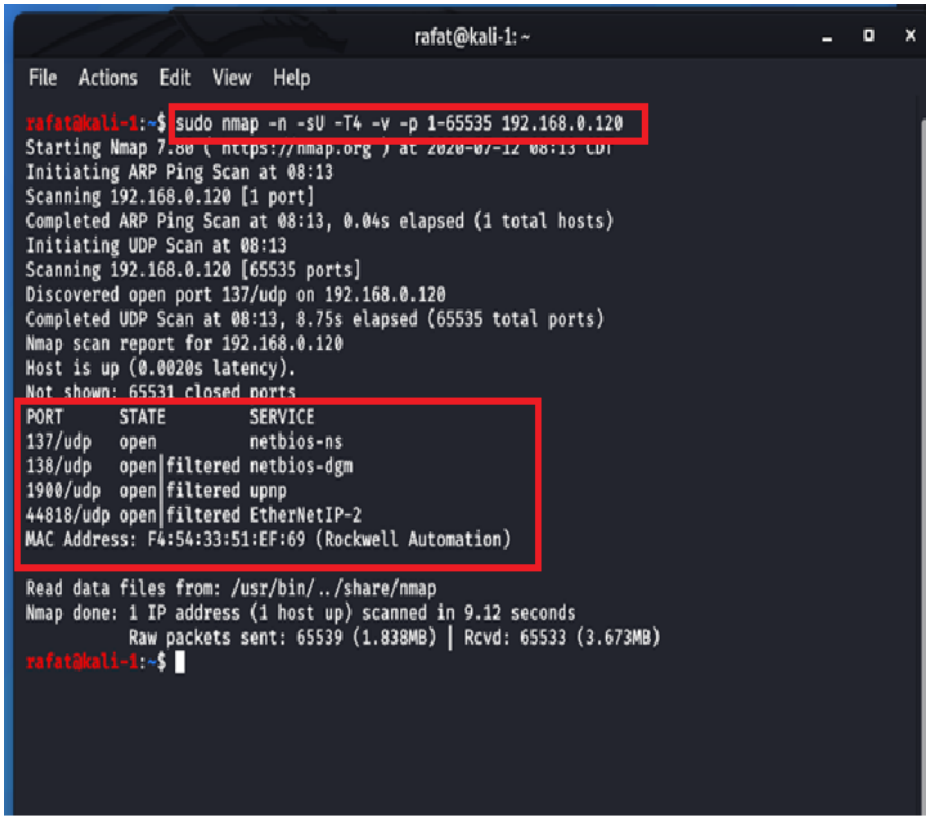


Figure 5-21. UDP scan of HMI

The output of scanning the ABB drive for all UDP ports (1 – 65535) using Nmap is shown in Figure 5-22 below.

a. The Nmap command scanned all 65535 UDP of the ABB drive.

b. The output shows that all UDP ports are closed on the drive.

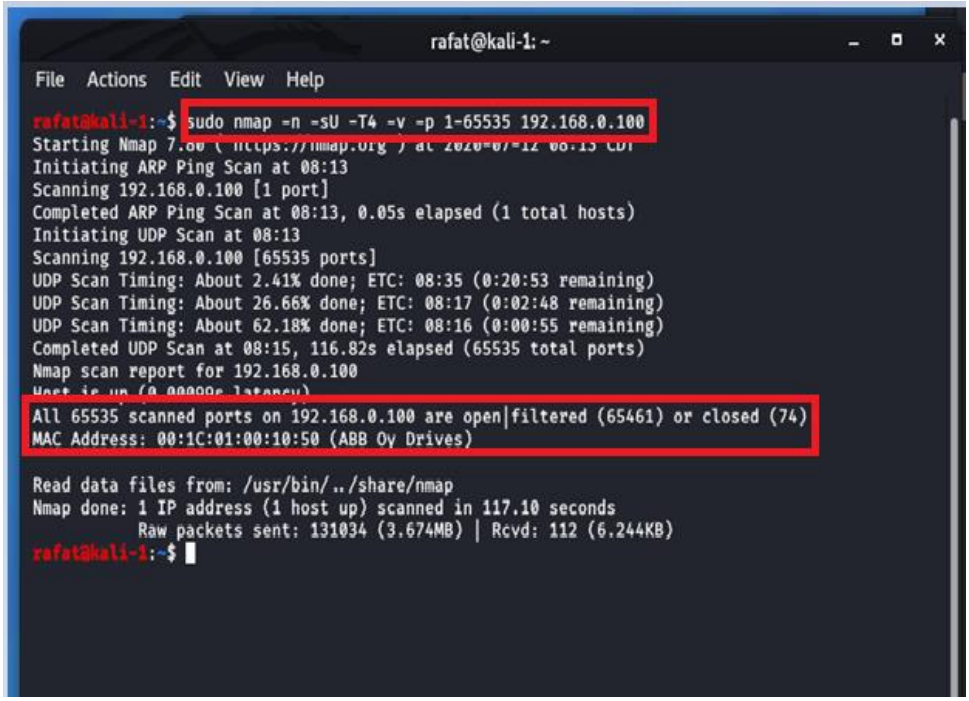


Figure 5-22. UDP scan of ABB Drive

The rest of all manual penetration testing results can be found in appendix B.

5.3 Automated Penetration Testing Results and Analysis

Since the same commands were used, the results below shown in Figures 5-23 to 5-36 gave the same output as the manual one. The main differences that were found in the automated process over the manual process are the following:

a. Ease of use in executing the automated process.

b. Very efficient in selecting the option and executing the desired task.

c. Safety, by eliminating human errors in typing the long commands.

d. The ability to link automatically to the vulnerability database and retrieve the result.

e. Automated penetration testing is much faster and more accurate in finding what we are searching for compared with humans in large data files, such as log or output of a scan files.

f. We ran the automated program 15 times and collected screenshots and needed data.

This is the list of steps taken to run the automated penetration testing process:

1. Start the program.
2. Select the option of choice.
3. Continuously monitor the status of the ICS system.
4. Collect screenshot output from the tool.
5. The program will analyze data for vulnerabilities and weaknesses.
6. A recommendation will be generated automatically at the end of the scan.

Starting the automated program displayed the main menu, as shown below. The program has five main areas: simple scan, advanced scan, CVE database, hardware information, and traffic analysis, as shown in Figure 5-23 below.

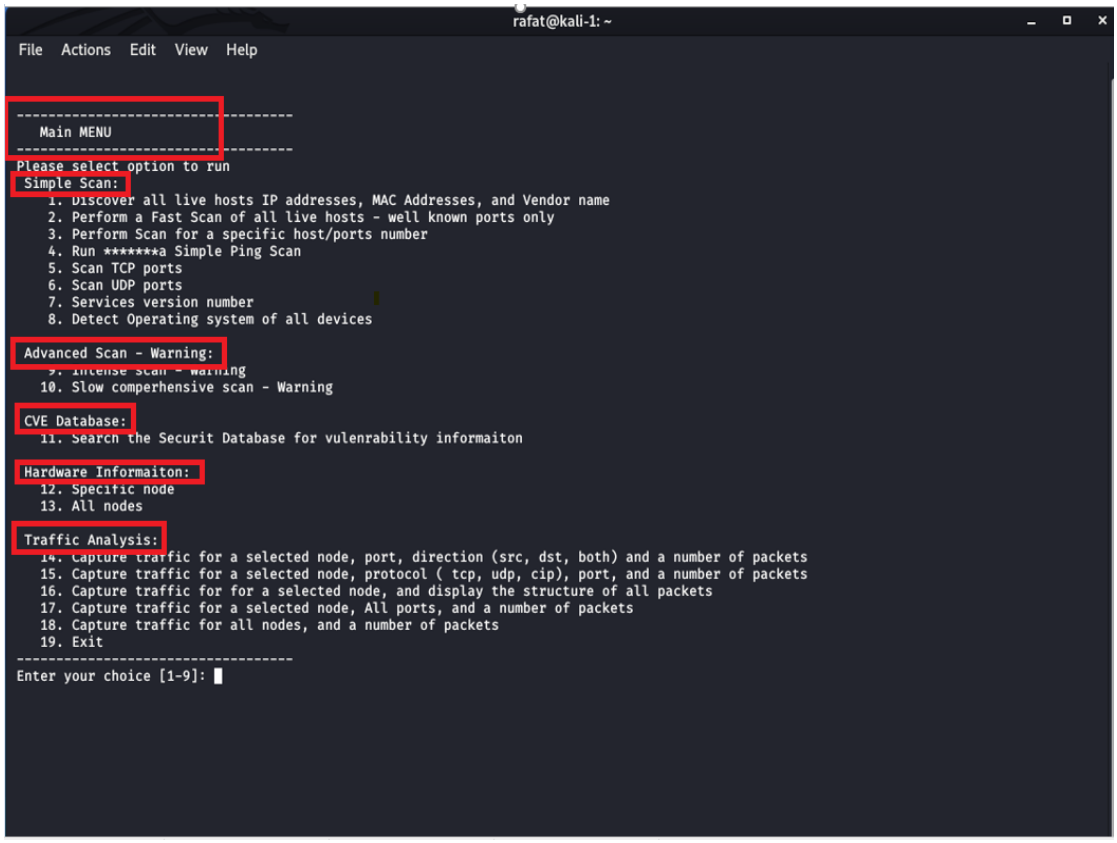


Figure 5-23. Program main menu

5.3.1 Option 1: Scan All Available Nodes

We started by selecting option 1 to discover all hosts on the network as part of the reconnaissance process. The output showed all nodes on the network with their related IP, MAC, and vendor name, as shown in Figure 5-24 below:

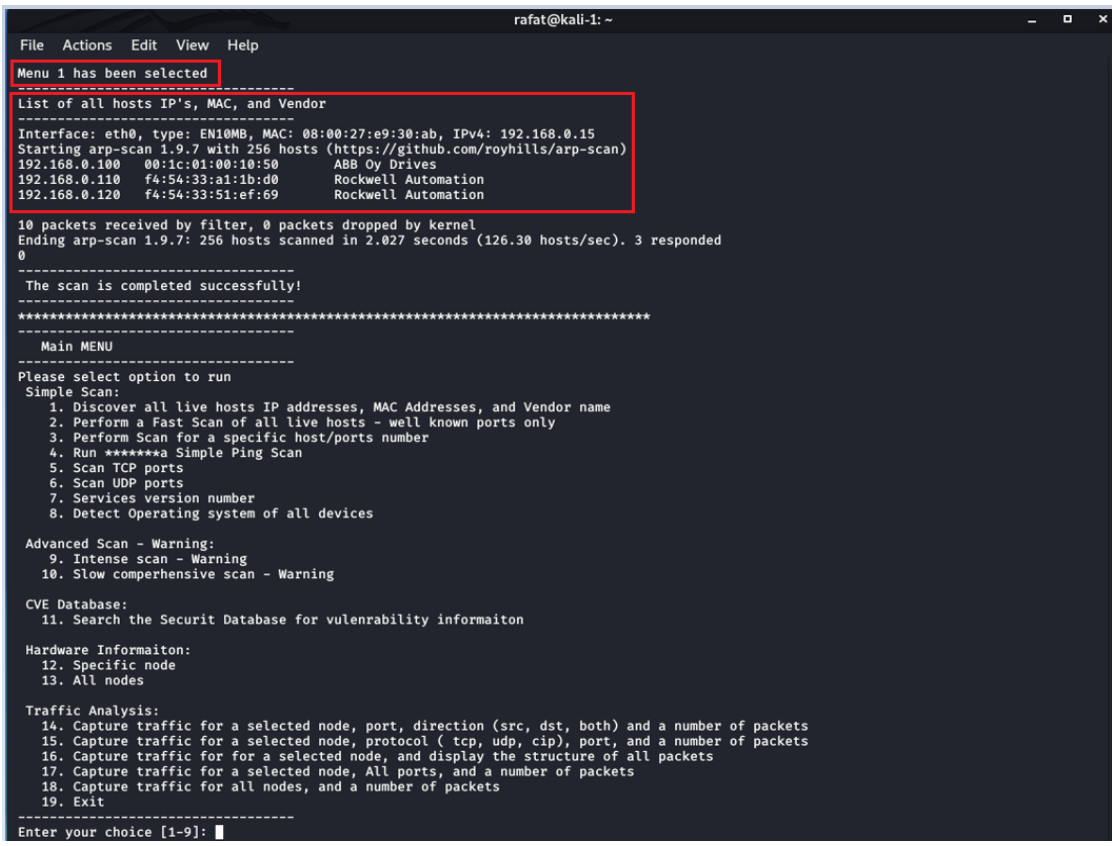


Figure 5-24. Selecting option 1 in the program

5.3.2 Option 2: Perform Fast Scan

Option 2 was selected from the main menu, which gave us a fast scan of all nodes on the network, as shown in Figure 5-68 and Figure 5-25 below.

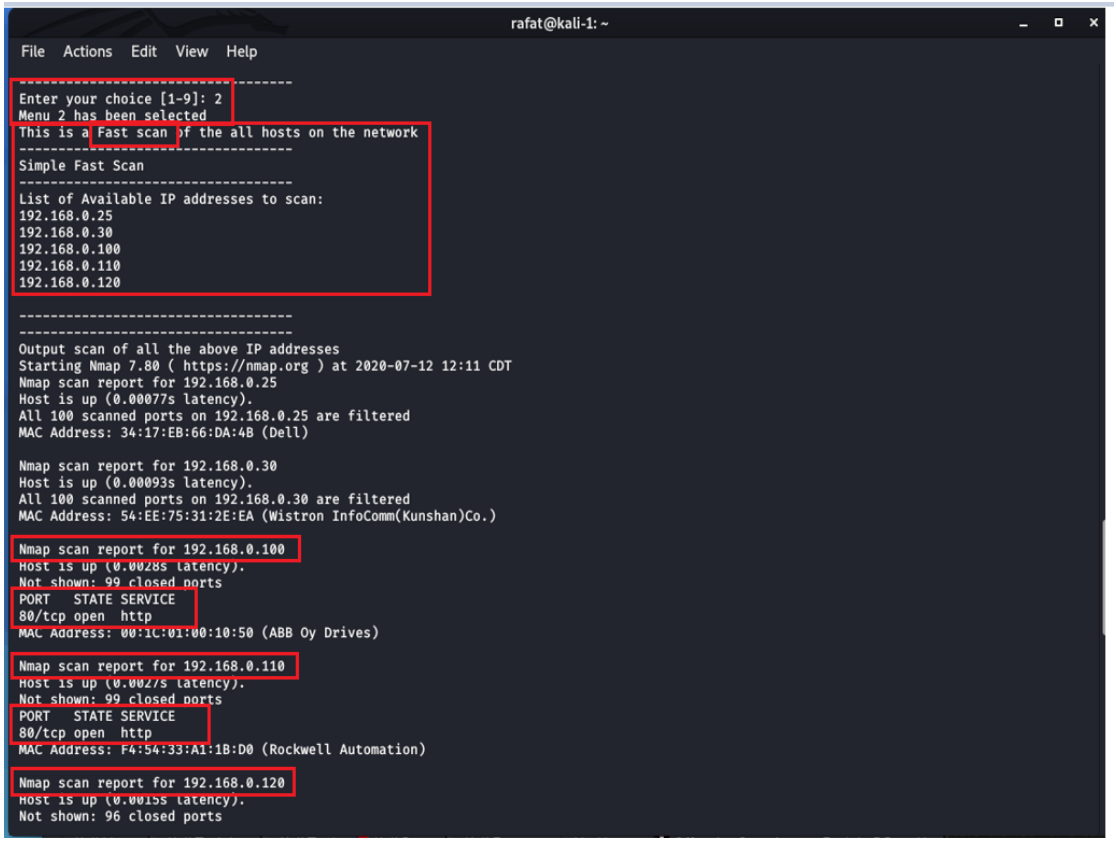


Figure 5-25. Selecting option 2 from main menu

The remainder of the scan is shown in Figure 5-26 below, including a recommendation report that shows a warning for any use of nonsecure ports.

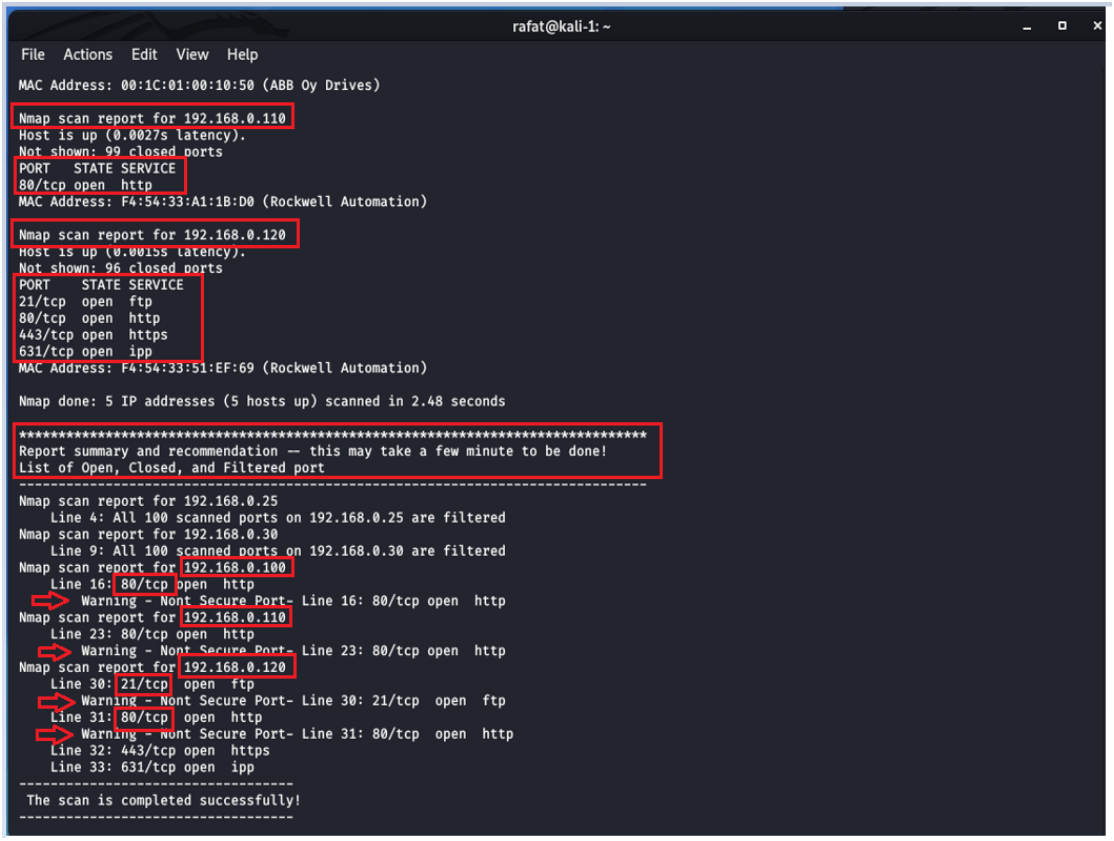


Figure 5-26. Output of the automated scan including a recommendation report

5.3.3 Option 3: Scan Specific Host/Port

Option 3 allowed us to select the IP address and port number to be scanned. A recommendation was reported as a warning at the end of the scan in Figure 5-27, as shown below, where HTTP (80) is not a secure port.

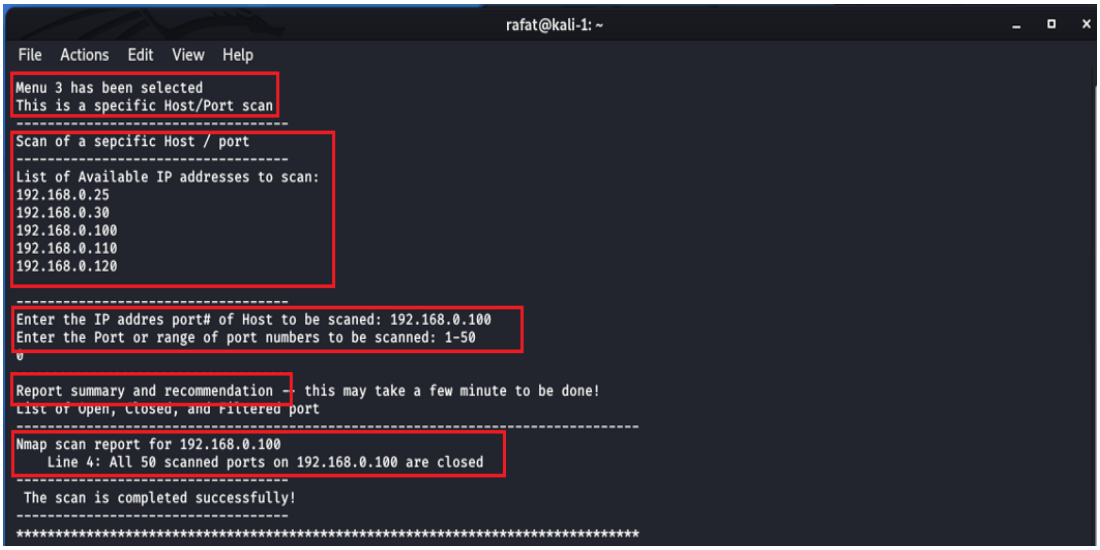


Figure 5-27. Option 3 allowing scanning specific host and port

5.3.4 Option 4: Perform Simple Ping Scan

The output is very similar to option 2, scans all well-known ports.

5.4.5 Option 5: Perform TCP Port Scan

By using TCP scan, we were able to find information regarding ports on the ICS devices, very similar to the manual scan, as we started the TCP scan. As a result of the TCP scan, the ABB drive completely stopped with message “fault-28”; as a result, the motor stopped running.

By selecting TCP scan, we got the output shown in Figure 5-28, Figure 5-29, and Figure 5-30. All open TCP ports for each device are shown with a warning message regarding each port that is not secure.

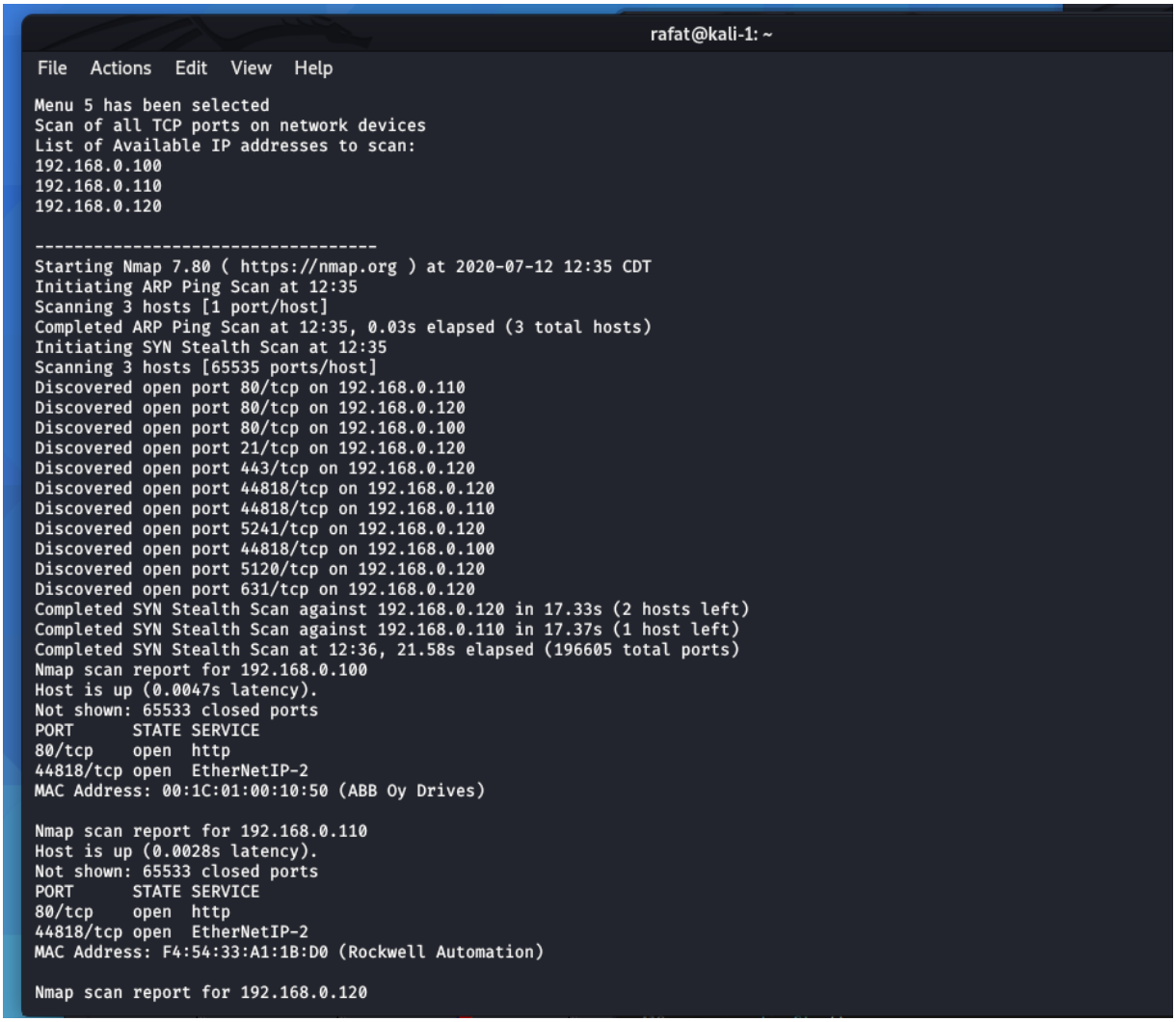


Figure 5-28. Option 5 to scan all TCP ports for all nodes

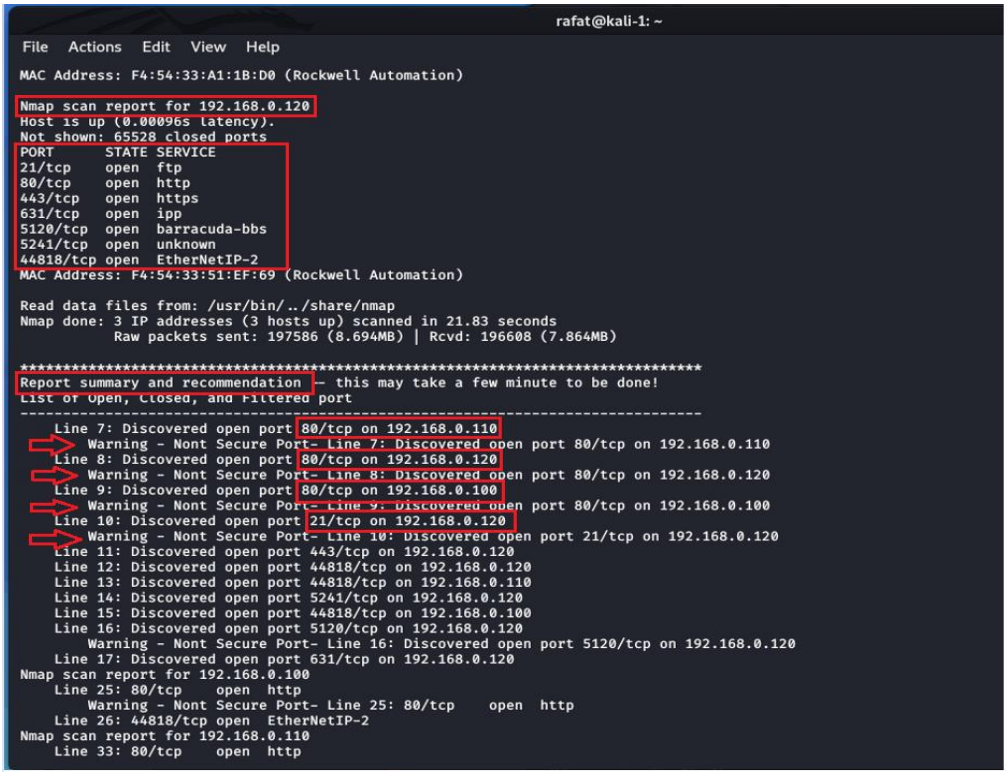


Figure 5-29. Option 5 to scan all TCP ports for all nodes

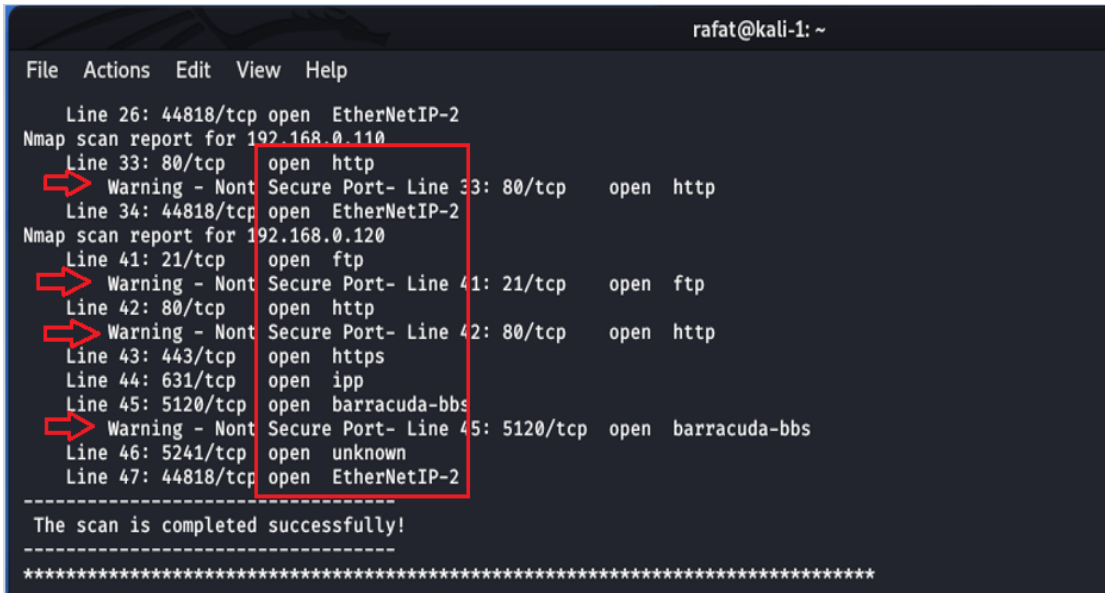


Figure 5-30. Option 5 to scan all TCP ports for all nodes and recommendations

5.3.6 Option 6: Perform UDP Scan

This option scanned all UDP ports on all ICS devices, as shown in Figures 5- 31 and 5-32. A report summary and recommendation were generated with a warning identifying any nonsecure ports.

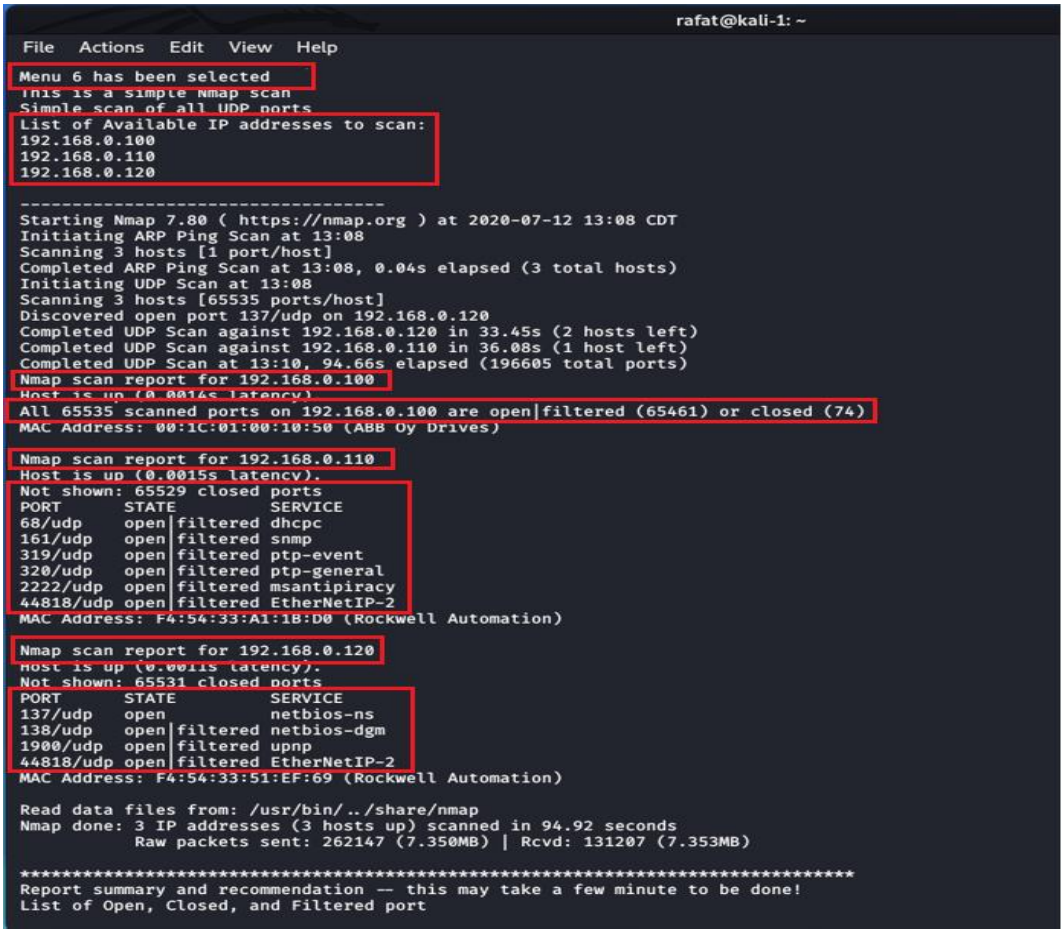


Figure 5-31. Option 6 to scan all UDP ports for all nodes

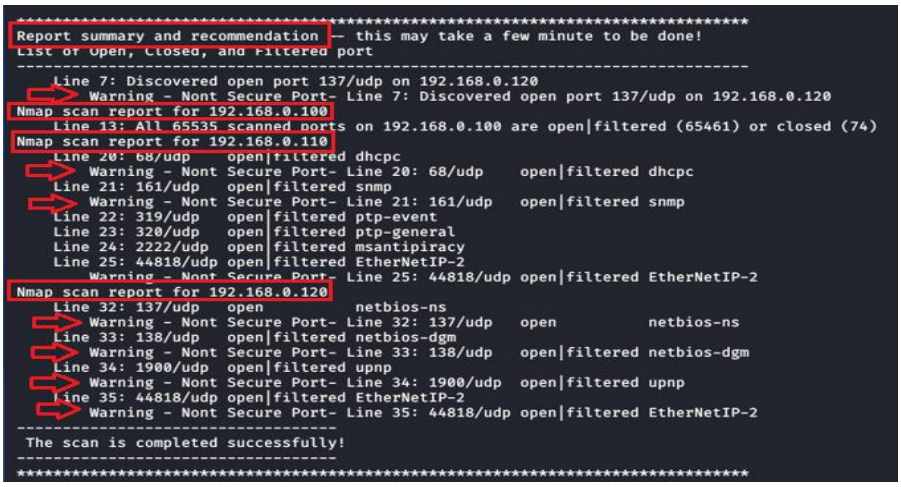


Figure 5-32. Option 6 to scan report recommendation of all UDP ports for all nodes

5.3.7 Option 7: Detect Services Running on ICS Devices

Option 7 is detecting service names that are running on ICS devices, as shown in Figure 5-33, and Figure 5-34.

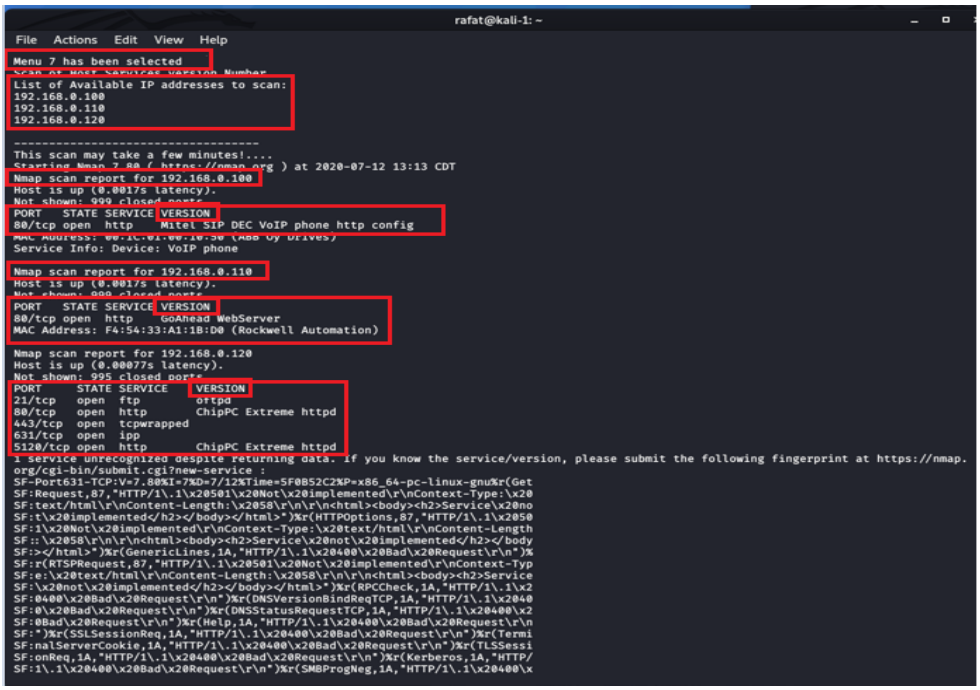


Figure 5-33. Option 7 to scan all UDP ports for all nodes

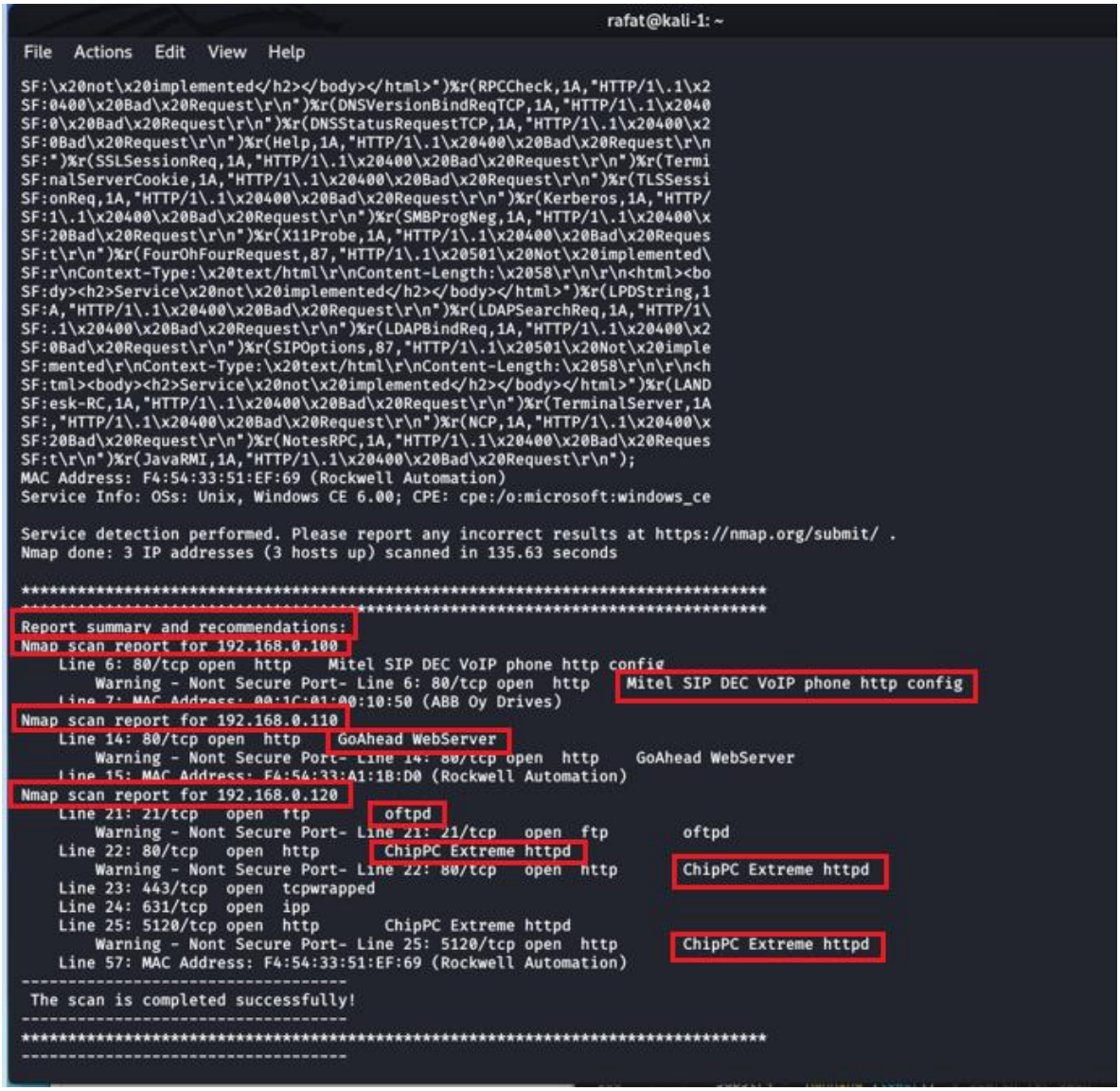


Figure 5-34. Option 7 to scan all UDP ports for all nodes

5.3.8 Option 8: Detect Operating Systems

We selected option 8 to try to detect the type of operating system running on the ICS devices, as shown in Figure 5-35 and Figure 5-36. The scan failed to detect the correct operating system for both the PLC and the ABB drive, both of which use embedded firmware. In the case of the HMI, the scan was successful in detecting that the operating system is Windows CE 5.0/ or 6.0.

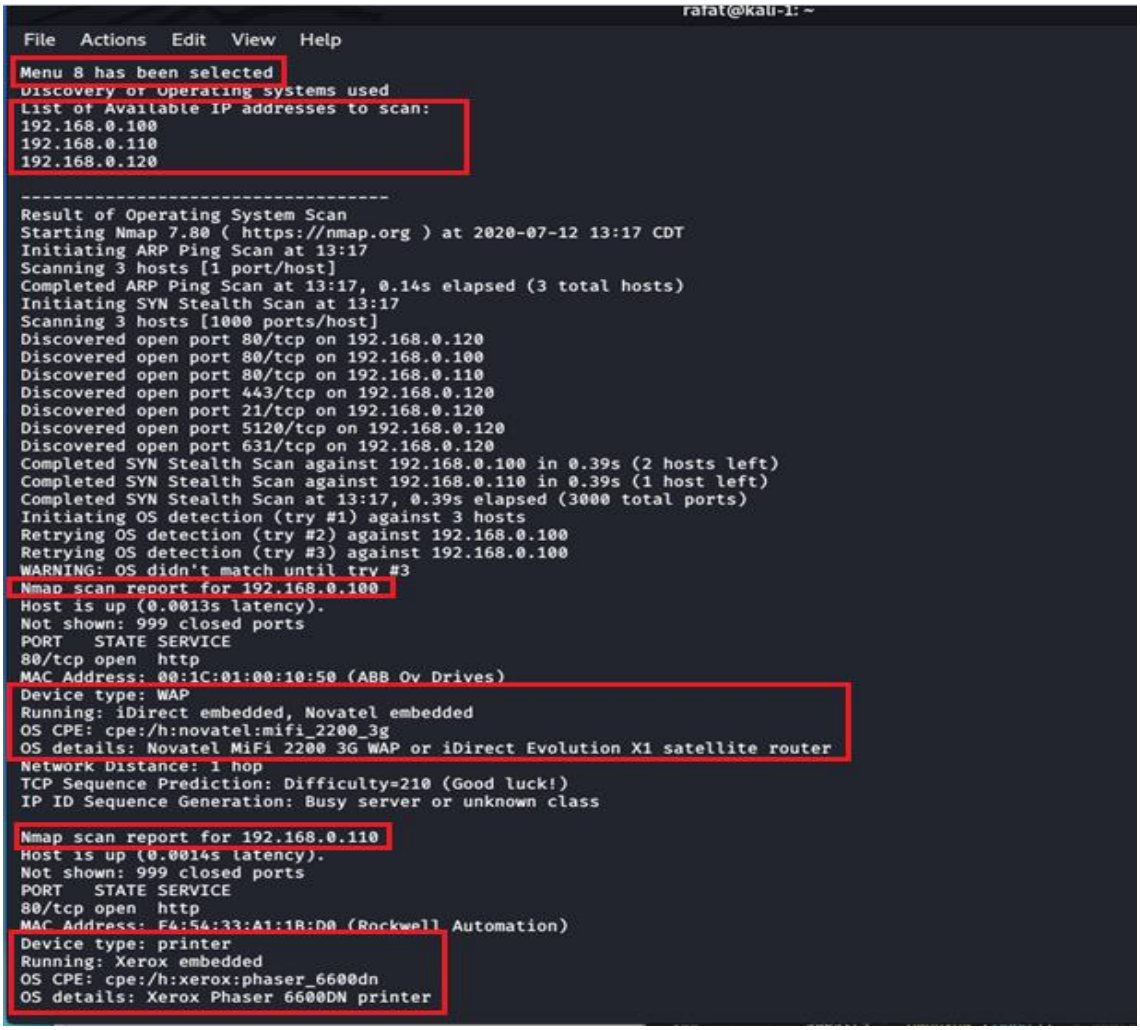


Figure 5-35. Option 8: Scan results of ABB drive and PLC operating system

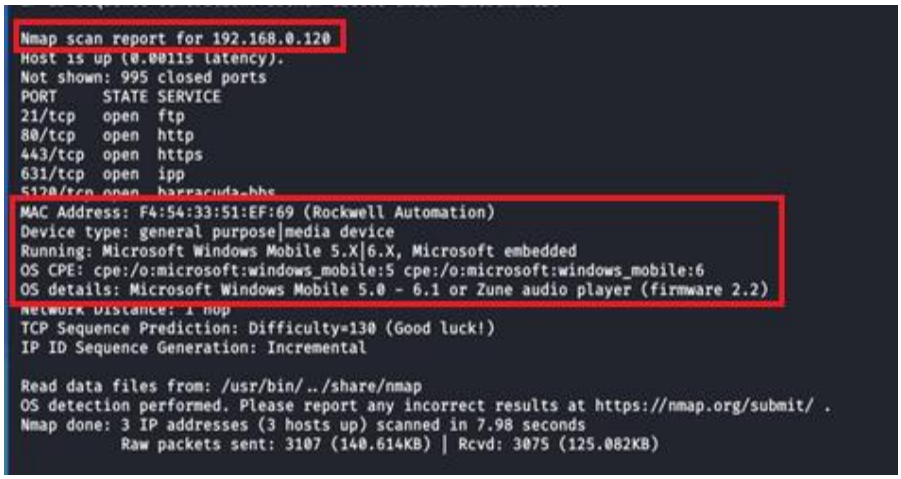


Figure 5-36. Option 8: Scan results of HMI operating system

The resto of automated penetration testing results can be found in appendix C.

5.4 Summary of Results from Manual and Automated Penetration Testing

a. Port 80(HTTP) is open on all three devices.

b. Port 21 is open on the HMI with anonymous login.

c. Port 44818, clear text on all three devices.

d. Port 631/TCP is open on the HMI.

   This port is called Internet Printing Protocol (IPP)[38]. If a port is open, anyone can anonymously log in, and attackers can abuse such devices for information disclosure, including potential access to and manipulation of data.

e. Port TCP 5120 is open on HMI, and, according to IANA, it is called Barracuda Backup

f. Port TCP 5241 is open on HMI; no information found on this port.

g. As a result of the TCP scan, the ABB drive completely stopped, with error message "fault-28," and the motor stopped running.

h. Nmap was able to identify the HMI operating system as Windows CE 5.0/6.0.

i. Nmap failed to identify the correct operating system-embedded devices such as the PLC and the ABB drive; the reported operating system was incorrect.

j. Since all HTTP, FTP, and protocol communications were not encrypted, when traffic was captured using Wireshark, Tshark, and Tcpdump, we were able to capture and identify all ICS-related device information.

k. Using port 44818 (Ethernet/IP), the scan was able to identify more information regarding the PLC, such as type of device, vendor, product name, serial number, product code, revision, status, and state. This is considered very valuable information in the penetration testing reconnaissance phase

l. Port UDP 161/SNMPv1 is open on the PLC– simple network management protocol (SNMP); version 1 and v2 uses clear-text in its communication. It is recommended to use SMPv3, which is more secure, and use encrypted communication.

6 Existing and Recommended Scoring Metrics

6.1 Overview of the Common Vulnerability Scoring System (CVSS) Framework

Common Vulnerability Scoring System (CVSS) is an open framework scoring system, introduced in 2005, that is used for evaluating the characteristics and impacts of software and hardware security vulnerabilities. It helps organizations understand the severity of the threat and determine their response. The forum of Incident Response and Security Teams (FIRST) is the organization responsible for maintaining and developing the CVSS framework. On July 12, 2019, FIRST announced the latest version of the publication, CVSS version 3.1[42].

CVSS was designed for IT, but some experts believe that CVSS can still work for ICS scoring with the understanding that the scores are adapted accordingly and not used alone. According to David Atch, Vice President of Research at CyberX, an IoT and ICS security company, “The optimal approach is using a risk-based rating that takes into account the potential impact of a compromise as well as the ease of exploitation. How critical is the device to the ICS environment? Could the vulnerability be exploited in a chain of compromises resulting in a major safety or environmental issues or costly downtime? [43].”

6.1.1 Metric Groups

CVSS consists of three different metric groups, as shown in Figure 6-1:

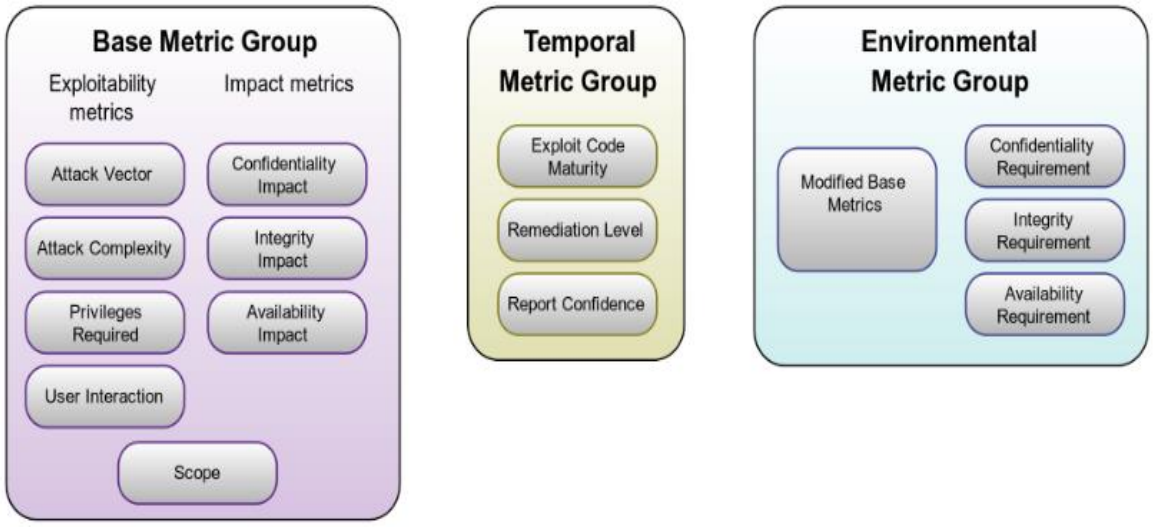


Figure 6-1. CVSS Metric Groups

- Base metrics group

Base metrics group represents the characteristics of a vulnerability that is independent of time and place and has three sub-score elements: Exploitability, Scope, and Impact.

- Exploitability: Exploitability metrics are made up of four components and addresses the question of how difficult it is to exploit the vulnerability from a technical point view. The four metrics are:
    - Attack Vector (AC):

      This metric relates to the settings by which the vulnerability exploitation is possible. The score for this metric is dependent on the level of access required to exploit a vulnerability. The score is higher if the access level is executed remotely or from a network outside of the corporate network and lowest if the attacker has physical access to the equipment. A list of possible values that can be used is presented in Table 6-1.

      Table 6-1: Attack vector possible values for Attack Vector (AV)

Metric Value	Description
Network (N)	The vulnerability is remotely exploitable.
Adjacent (A)	Attack is launched from the same physical or logical network.
Local (L)	Attacker exploit vulnerability by accessing the target system locally or relies on another user interaction.
Physical (P)	The attacker has physical access to the vulnerable component.

    - Attack Complexity (AC)

      To carry the attack successfully, the attacker is required to expend a lot of effort. The base score is highest for the low complexity attack. A list of possible values is shown in Table 6-2.

Table 6-2: Attack vector possible values for Attack Complexity (AC)

Metric Value	Description
Low (L)	No special access conditions are required
High (H)	Conditions beyond attackers' control is needed to carry a successful attack

- Privileges Required (PR)

This metric describes the level of privileges required before the attacker is successfully able to exploit the vulnerability. The base score is highest if no privileges required to exploit the vulnerability. A list of possible values is shown in Table 6-3.

Table 6-3: Attack vector possible values for Privileges Required (PR)

Metric Value	Description
None (N)	No privileges are required to carry out an attack successfully.
Low(L)	Th attacker requires basic user privileges to be able to carry the attack
High (H)	The attacker requires administrative privileges to be able to carry the attack successfully.

- User Interaction (UI)

This metric determines the requirement for a human to participate in carrying out a successful exploit on a vulnerable component. The base score is highest when no user interaction is required to carry out the attack successfully. A list of possible values is shown in Table 6-4.

Table 6-4: Attack vector possible values for User Interaction (UI)

Metric Value	Description
None (N)	No human interaction is required to carry out an attack successfully.
Required (R)	Human interaction is required to carry out an attack successfully.

- Scope Metric

The scope metric addresses the concern of whether a vulnerability of one component impacts other components outside of its security range. The base score is highest when the change of scope occurs. A list of possible values is shown in Table 6-5.

Table 6-5: Attack vector possible values for Scope(S)

Metric Value	Description
Unchanged (U)	The component that has the vulnerability is the only component that is effect by it.
Changed (C)	The component that has the vulnerability will have effect on other components.

- Impact Metrics:

This metric captures the effects of a successfully exploited vulnerability by the attacker on a component.

  - Confidentiality (C)

Confidentiality refers to limiting information access to only authorized users; the possible values according to CVSS calculations are listed in Table 6-6. When the loss of the impacted component is highest, the base score is greatest [44].

Table 6-6: Attack vector possible values for Confidentiality (C)

Metric Value	Description
High (H)	Total loss of confidentiality, attacker has or information to potentially able access to all resources.
Low(L)	Some loss of confidentiality, but no control over the information or resources.
None(N)	No loss of confidentiality related to the impacted component.

- Integrity (I)

Integrity metric measures refer to the trustworthiness of the information. They measure the impact on integrity of a vulnerability that has been successfully exploited by the attack. The list of possible values is presented in Table 6-7. The base score is greatest when the result of the affected component is highest.

Table 6-7: Attack vector possible values for Integrity (I)

Metric Value	Description
High (H)	Total loss of Integrity or protection where attacker can modify any or all files on the effected component.
Low (L)	Modification of data is possible, but attacker has limited ability of modifying any or all files on the effected component.
None (N)	There is no loss of integrity of related component

- Availability (A)

Availability is the measurement of the availability of the affected component as a result of exploiting the vulnerability successfully. The base score is greatest when the result to the impacted component is highest. A list of metric values used is shown in Table 6-8.

Table 6-8: Attack vector possible values for Availability (A)

Metric Value	Description
High (H)	Total loss of availability as a result of total control of the attacker to the effected component whether during or after the attack. And the component became unavailable or malfunction as a result of the attack
Low (L)	Noncritical components were affected and availability to critical components is not affected
None (N)	No impact to availability on the effected component.

The CVSS base score is modified by the next set of optional metrics called Temporal Metrics and Environmental Metrics, as shown in Figure 6-2.

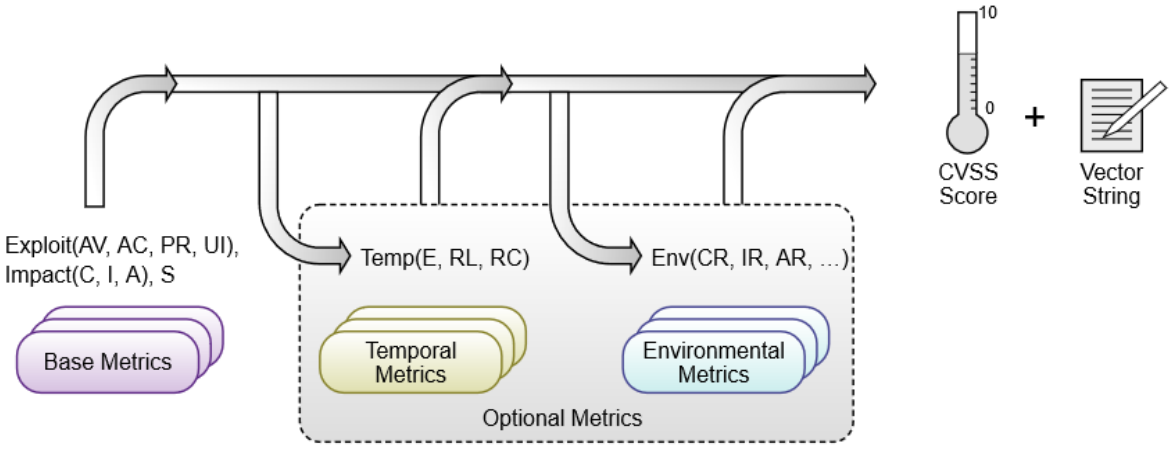


Figure 6-2. CVSS Base Metrics and Optional Metrics

- Temporal metrics group (optional)

This group represents the characteristics of a vulnerability that are based on the current situation, for example, is there a work-around available? Three metrics are used: Exploit Code Maturity (E), Remediation Level (RL), and Report Confidence (RC).

- Environmental metrics group (optional)

This group represents the characteristics of a vulnerability that are relevant to a user's unique environment, for example, how the software or hardware is deployed in the environment. Eleven metrics are used: Confidentiality Requirements (CR), Integrity Requirements (IR) Availability Requirements (AR) Modified Attack Vector (MAV), Modified Attack Complexity (MAC), Modified Privileges Required (MPR), Modified User Interaction (MUI), Modified Scope (MS), Modified Confidentiality (MC), Modified Integrity (MI), and Modified Availability (MA).

We will not use Both Temporal and Environmental metrics in calculations for this research, as both metrics are rarely used and the published CVSS scores are typically composed of Base metrics only [44].

6.1.2 Qualitative Severity Rating Scale

CVSS uses a numeric representation for its textual rating representation of the final rating severity scale. The scale ranges from 0.0, which represents no severity, to 10.0, which represents Critical severity, as shown in Table 6-9. According FIRST, "The use of these qualitative severity ratings is optional, and there is no requirement to include them when publishing CVSS scores. They are intended to help organizations properly assess and prioritize their vulnerability management process [44]."

Table 6-9: Qualitative severity rating scale

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

CVSS uses several equations and a scoring system for each of the metrics used to calculate the final severity score. According to FIRST, "To produce the CVSS v3.1 formula, the CVSS Special Interest Group (SIG) framed the lookup table by assigning metric values to real vulnerabilities, and a severity group (low, medium, high, critical). Having defined the acceptable numeric ranges for each severity level, the SIG then collaborated with Deloitte & Touche LLP to adjust formula parameters in order to align the metric combinations to the SIG's proposed severity ratings [44]."

6.1.3 CVSS v3.1 Equations

CVSS v 3.1 equations were created by FIRST to help organizations calculate the severity score for vulnerabilities. CVSS equations provide a mathematical approximation of all possible metric combinations, which were ranked in order of severity, as shown in Table 6-10 [44].

Table 6-10: Metric Values for base score according to CVSS v3.1

Metric	Metric Value	Numerical Value
Attack Vector (AV)	Network	0.85
	Adjacent	0.62
	Local	0.55
	Physical	0.2
Attack Complexity (AC)	Low	0.77
	High	0.44
Privileges Required (PR)	None	0.85
	Low	0.62 (or 0.68 if Scope changed)
	High	0.27 (or 0.5 if Scope changed)
User Interaction	None	0.85
	Required	0.62
Confidentiality / Integrity / Availability	High	0.56
	Low	0.22
	None	0

According to CVSS version 3.1 framework, this is the list of equations that are used to calculate the CVSS base score for a vulnerability:

Impact Sub-Score (ISS) = 1-[(1-confedentiality) * (1-Integrity) * (1-Availability)] (6.1)

Impact = (6.2)

If Scope is Unchanged, Impact = 6.42 * ISS

If Scope is changed, Impact = 7.52 * (ISS – 0.029) – 3.25 * (ISS – 0.02)[15]

Exploitability = 8.22 * AttackVector (AV) * AttackComplexity (AC) * PrivilegesRequired (PR) * UserInteraction (UI) (6.3)

CVSS) BaseScore = (6.4)

If Impact <= 0, BaseScore = 0, else

If Scope is Unchanged, Roundup (minimum [Impact + Exploitability), 10])

If Scope is Changed, Roundup (minimum [1.08 *(Impact + Exploitability), 10])

6.2 Recommended Vulnerability Scoring System-ICS (CVSS-ICS) Framework

The impact of the severity of Safety (SAF) metric is paramount in calculating the final severity score in ICS. According a report titled "Examining the Industrial Control System Cyber Risk Gap — The missing link that may put your organization in jeopardy," published by Deloitte, a consulting company specializing in security. When it comes to ICS security, human safety is paramount, as shown in Figure 6-3 [45].

Table 1

Category	Business system security	ICS security
Risk management requirements	• Data confidentiality and integrity are paramount • Fault tolerance is less important; momentary downtime is not typically a major risk • Major risk impact is delay of business operations and financial reporting	• Human safety is paramount, followed by protection of the process • Fault tolerance is essential; even momentary downtime may not be acceptable • Major risks can include loss of life, production interruption, product integrity and safety, equipment damage or loss

Figure 6-3. Impact of Safety in ICS [from above]

Also according to a survey titled "Some ICS Security Incidents Resulted in Injury, Loss of Life: Survey," published in October 2019 by *Security Week*, an Internet and Enterprise Security News, Insights, and Analysis magazine, safety is a key metric in an ICS environment [46].

The new modified CVSS-ICS base score equation is designed to take into account the criticality of the Safety (SAF) metric by using the existing CVSS base score framework and adding the impact of the safety metric as a result of a successful attack to come up with the final CVSS-ICS base score.

6.2.1 Recommended Safety Metric (SAF):

Safety Metric (SAF) is the measure of the impact of vulnerability or the attack on safety in an ICS environment. The impact of a cyber-physical attack may add the risk of injury, including but not limited to, death [47]. Current CVSS scoring does not include the safety metric as a factor in calculating CVSS severity, which makes CVSS not accurate when it comes to ICS scoring. The misleading CVSS scores can have a negative impact on industrial organizations [43]. A list of recommended safety metric values that are going to be used in by the equations to calculate the CVSS-ICS are shown in Table 6-11. The score for safety severity is greatest when the impact on safety is highest.

Table 6-11: Recommended Safety Metric (SAF) values

Metric Value	Description
High (H = 1)	Not safe, component was halted or malfunctioned during scans /attacks
None (N = 0)	Safe, component was not impacted by the scans/attacks and no safety issues reported.

The new CVSS-ICS framework consists of three types of recommended calculations:

- Common Vulnerability Scoring System for individual vulnerabilities in ICS (CVSS-ICS(V)).
- Common Vulnerability Scoring System for individual devices in ICS (CVSS-ICS(D)).

- Common Vulnerability Scoring System for the whole ICS environment (CVSS-ICS(ENV).

6.2.2 Recommended Equations to Calculate CVSS-ICS(V) for Individual Vulnerability (V) in ICS

To calculate the proposed CVSS-ICS base score framework for individual vulnerability in an ICS environment, we use the original CVSS equations (6.1 to 6.4), then we use the new recommended CVSS-ICS equation (6.5):

In addition to the above equations from the CVSS v3.1 framework, we added the following formula to come up with the final CVSS-ICS severity score for an individual vulnerability in an ICS environment.

CVSS-ICS(V) = (CVSS) Base Score + Safety (SAF) (6.5)

Where:

SAF = Severity impact due to safety

By using the CVSS-ICS equation (6.5), we were able to calculate the severity score of each vulnerability (V) in each ICS device. As a result of our manual and automated penetration testing, vulnerabilities that were discovered in the PLC are shown in Table 6-12. The results of calculating the severity score for each one of these vulnerabilities are shown in Table 6-13. A noticeable result of this calculation is that when there is no safety impact, then CVSS-ICS severity score=CVSS severity score.

Table 6-12: List of vulnerabilities found in PLC

Device name	Operating system	Port	Protocol	Service Name	state	Encryption	name	version	Description
PLC:192.168.1.110	Printer, Xerax Phaser 6600DN	80	tcp		open	no		GoAhead	
		68	udp	dhcpc	open|filtered	no			DHCP/Bootp, client only
		161	udp	snmp	open|filtered	no			the port is filterd, but it uses snmpv1
		319	udp	ptp-event	open|filtered	no			Precision Time Protocol
		320	udp	ptp-general	open|filtered	no			Precision Time Protocol
		2222	udp	msantipiracy	open|filtered	no			Name: Rockwell-csp2, unreg-ab2, Allen-Bradley unregistered port, I/O communications used only by products that support I/O over EtherNet/IP
		44818	udp	EthernetIP-2	open|filtered	no			

Table 6-13: Result of calculating both CVSS and CVSS-ICS for each vulnerability (V) in PLC

Vulnerability \ Metric	Confidentiality	Integrity	Availability	CVSS(V)	Safety	CVSS-ICS(V)
Port 80	H	H	N	7.1	0	7.1
Port 68	H	H	N	7.1	0	7.1
Port 161	H	H	N	7.1	0	7.1
Port 319	H	H	N	7.1	0	7.1
Port 320	H	H	N	7.1	0	7.1
Port 2222	H	H	N	7.1	0	7.1
Port 44818	H	H	N	7.1	0	7.1
Scan / Attack	H	H	N	7.1	0	7.1

Table 6-14 shows the list of discovered vulnerabilities as a result of the manual and automated penetration testing. Table 6-15 shows the result of calculating the severity of each one of these vulnerabilities using the recommended CVSS-ICS formula. As a result of our calculation for HMI, we noticed that when there is no safety impact, then CVSS-ICS severity score=CVSS severity score.

Table 6-14: List of vulnerabilities found in HMI

Device name	Operating system	Port	Protocol	Service Name	state	Encryption	name	version	Description
HMI:192.168.0.120	Microsoft Windows Mobile 5.0 or Zune audio player (firmware 2.2), Windows CE 6.0	80	tcp	http	open	no		ChipPC Extreme	
		21	tcp	ftp	open	no		oftpd	
		443	tcp	https	open-TCPwrapped	yes			
		631	tcp	ipp	open	no			Internet Printing Protocol
		44818	tcp	EthernetIP-2	open				
		5241	tcp	unknown	open				
		5120	tcp	barracuda-bbs	open			ChipPC Extreme	
		137	udp	netbios-ns	open	no			UDP NetBIOS name query packets are sent to this port, usually of Windows machines but also of any other system running Samba (SMB), to ask the receiving machine to disclose and return its current set of NetBIOS names.
		138	udp	netbios-dgm	open|filtered	no			UDP NetBIOS datagrams packets are exchanged over this port, usually with Windows machines but also with any other system running Samba (SMB). These UDP NetBIOS datagrams support non-connection oriented file sharing activities.
		1900	udp	upnp	open|filtered	no			
		44818	udp	EthernetIP-2	open|filtered	no			

Table 6-15: Results of calculating both CVSS and CVSS-ICS for each vulnerability (V) in HMI

Vulnerability \ Metric	Confidentiality	Integrity	Availability	CVSS(V)	Safety	CVSS-ICS(V)
Port 21	H	H	N	7.1	0	7.1
Port 80	H	H	N	7.1	0	7.1
Port 137	H	H	N	7.1	0	7.1
Port 138	H	H	N	7.1	0	7.1
Port 1900	H	H	N	7.1	0	7.1
Port 631	H	H	N	7.1	0	7.1
Port 2222	H	H	N	7.1	0	7.1
Port 44818	H	H	N	7.1	0	7.1
Scan / attack	H	H	N	7.1	0	7.1

Table 6-16 shows the list of discovered vulnerabilities as a result of the manual and automated penetration testing. Table 6-17 shows the result of calculating the severity of each one of these vulnerabilities using the recommended CVSS-ICS formula. As a result of our calculations for ABB drive, severity of CVSS -ICS (V) is higher than CVSS(V) when the safety metric is high.

Table 6-16: List of vulnerabilities found in ABB drive

Device name	Operating system	Port	Protocol	Service Name	state	Encryption	name	version	Description
ABB: 192.168.1.100	VoIP phone ??	80	tcp	http	open	no		Mitel SIP DEC VoIP phone http config	
		44818	tcp	EthernetIP	open	no	EthernetIP-2		Rockwell Encapsulation, IANA registered for EtherNet/IP messaging
	Novatel MiFi 2200 3G WAP or Idirect evolution XL satellite router								

Table 6-17: Result of calculating both CVSS and CVSS-ICS for each vulnerability (V) in ABB drive

Vulnerability \ Metric	Confidentiality	Integrity	Availability	CVSS(V)	Safety	CVSS-ICS(V)
Port 80	H	H	N	7.1	0	7.1
Port 44818	H	H	N	7.1	0	7.1
Scan / attack	H	H	H	7.8	1	8.8

6.2.3 Recommended Equations to Calculate CVSS-ICS(V) for Each Device (D) in ICS

The recommended equation for calculating the severity score for a single ICS device is CVSS-ICS(D) as shown in equation (6.6):

$$\text{CVSS-ICS (D)} = \frac{1}{n}\sum_{i=1}^{n} CVSS - ICS(V_i) \qquad \text{where i = 1, ... n.} \tag{6.6}$$

Where:

SAF = Metric assigned to safety of the device D

CVSS-ICS (D) = Severity score of an ICS device D.

CVSS-ICS (V_i) = Severity score for each ICS vulnerability (V_i) in device (D_i).

Table 6-18 shows the results of calculating CVSS-ICS(D) for the PLC. CVSS-ICS (D) was calculated as the average of all CVSS-ICS(V_i) that were discovered as a result of the manual and automated penetration testing of the PLC.

Table 6-18: Result of calculating both CVSS and CVSS-ICS for PLC

Vulnerability \ Metric	Confidentiality	Integrity	Availability	CVSS(V)	Safety	CVSS-ICS(V)
Port 80	H	H	N	7.1	0	7.1
Port 68	H	H	N	7.1	0	7.1
Port 161	H	H	N	7.1	0	7.1
Port 319	H	H	N	7.1	0	7.1
Port 320	H	H	N	7.1	0	7.1
Port 2222	H	H	N	7.1	0	7.1
Port 44818	H	H	N	7.1	0	7.1
Scan / attack	H	H	N	7.1	0	7.1
CVSS (PLC)				7.1		
CVSS-ICS (PLC)						7.1

Table 6-19 shows the average of all CVSS-ICS(V_i) that were discovered as a result of the manual and automated penetration testing of the HMI.

Table 6-19 shows the results of calculating CVSS-ICS(D) for the HMI. CVSS-ICS (D) was calculated using equation (6.6).

Table 6-19: Result of calculating both CVSS and CVSS-ICS for HMI

Vulnerability \ Metric	Confidentiality	Integrity	Availability	CVSS(V)	Safety	CVSS-ICS(V)
Port 21	H	H	N	7.1	0	7.1
Port 80	H	H	N	7.1	0	7.1
Port 137	H	H	N	7.1	0	7.1
Port 138	H	H	N	7.1	0	7.1
Port 1900	H	H	N	7.1	0	7.1
Port 631	H	H	N	7.1	0	7.1
Port 2222	H	H	N	7.1	0	7.1
Port 44818	H	H	N	7.1	0	7.1
Scan / attack	H	H	N	7.1	0	7.1
CVSS (HMI)				7.1		
CVSS-ICS (HMI)						7.1

Table 6-20 shows the results of calculating CVSS-ICS(D) for the ABB drive. CVSS-ICS (D) was calculated using equation (6.6). Since the ABB drive malfunctioned as a result of the attack, the

safety metric was high. As a result of including safety as a metric for calculating CVSS-ICS, the recommended severity score CVSS-ICS(D) is higher than the existing severity score CVSS.

Table 6-20: Result of calculating both CVSS and CVSS-ICS for ABB drive

Vulnerability \ Metric	Confidentiality	Integrity	Availability	CVSS(V)	Safety	CVSS-ICS(V)
Port 80	H	H	N	7.1	0	7.1
Port 44818	H	H	N	7.1	0	7.1
Scan / attack	H	H	H	7.8	1	8.8
CVSS (ABB-Drive)				7.33		
CVSS-ICS (ABB-Drive)						7.67

6.2.4 Recommended Equations to Calculate CVSS-ICS(V) for the Whole Environment in ICS

It is common for an ICS environment to have multiple devices, including many PLCs, HMIs, and drives. To come up with a severity score for the entire ICS environment as one system; the recommendation is to use either equation (6.7) or (6.8), depending on the criticality of the individual devices:

1. If all ICS devices (D) that exist in the ICS environment are treated equally critical, then we use equation (6.7).

$$\text{CVSS-ICS (ENV)} = \frac{1}{n}\sum_{i=1}^{n} CVSS - ICS\,(D_i) \quad \text{, where i = 1, ... n} \tag{6.7}$$

Where:

n = Total number of devices (D)

Table 6-21 shows the results of calculating severity score for an entire environment using the existing CVSS and the recommended CVSS-ICS, with the assumptions that all devices in ICS are critically equal using equation (6.7). The recommended CVSS-ICS(ENV) is higher than the existing CVSS, which reflects a more accurate severity when it comes to scoring the ICS environment due to the importance of the safety metric.

Table 6-21: Result of calculating both CVSS and CVSS-ICS(ENV) when all devices are critically equal.

Vulnerability \ Metric	CVSS(V)	CVSS-ICS(V)
CVSS-ICS (PLC)	7.1	7.1
CVSS-ICS (HMI)	7.1	7.1
CVSS-ICS (ABB-Drive)	7.33	7.67
CVSS (ENV)	7.18	
CVSS-ICS (ENV)		7.29

2. If all ICS devices (D) that exist in the ICS environment are not treated equally critical, then we use equation (6.8).

The Weight of criticality is (W), the higher the wight the higher the criticality of the device to the environment. The criticality weight ranges from low = 1 to high = 10.

$$\text{CVSS-ICS (ENV)} = \frac{\sum_{i=1}^{n} CVSS{-}ICS(D_i) * W_i}{\sum_{j=1}^{n} W_i} \quad (6.8)$$

Where:

i = 1, ... n.

W = Weight of criticality for each device (D) (Low =1, high=10)

n = Total number of devices (D) in an ICS environment

In order for us to show the result of the severity of the environment when all devices are not critically equal, we assumed the criticality of the devices (W) are as follows:

W_{PLC} = 110, W_{HMI} = 5, and W_{ABB} = 7

Table 6-22 shows the assumptions of the weight of criticality of each device used in this research, the result of calculating the severity score for an entire environment using the existing CVSS, and the recommended CVSS-ICS with the assumptions that all devices in ICS are not critically equal using equation (6.8). The recommended CVSS-ICS(ENV) result was higher than the existing CVSS, which reflects a more accurate severity when it comes to scoring the ICS environment due the safety metric that was included in our calculations.

Table 6-22: Result of calculating both CVSS and CVSS-ICS(ENV) when all devices are not critically equal.

Vulnerability \ Metric	CVSS(V)	CVSS-ICS(V)	W	CVSS-ICS(D)
CVSS-ICS (PLC)	7.1	7.1	10	71
CVSS-ICS (HMI)	7.1	7.1	5	35.5
CVSS-ICS (ABB-Drive)	7.33	7.67	7	53.69
CVSS (ENV)	7.18			
CVSS-ICS(ENV)				7.28

7. Summary of Contributions, Recommendations, and Future Work

This research presents the design of new framework—a manually executed and automated penetration testing process for Connected Industrial Control Systems (CICS). Both frameworks were built using open-source security software and controls equipment currently used in critical infrastructure, manufacturing companies, and other institutions in the United States and around the world. Existing penetration testing frameworks have largely been focused on manual testing and are specific to Information Technology (IT). In addition, a new severity scoring system framework, called Common Vulnerability Scoring System for Industrial Control Systems (CVSS-ICS), was recommended for calculating the severity score in Industrial Control Systems (ICS).The broader goal of this research is to build penetration frameworks, both manual and automated, for Operations Technology (OT).

7.1 Contributions of This Research

First, an OT-based testbed was built comprised of PLCs (Programmable Logic Controllers), HMIs (Human Machine Interfaces), a motor drive, and the expected embedded network devices that enable connectivity to emulate a real manufacturing environment. In addition, special security VMs (Virtual Machines) were used in the OT testbed. Second, this research ran a manual process of penetration testing against the ICS network using open-source tools that are used by many IT security professionals and hackers; the data was then collected and analyzed manually. Third, a software program was created using Python programming language to automate the above manual process. In addition, the program automates data acquisition, generates security analyses, and makes recommendations. Fourth, a new severity scoring framework for ICS,

Common Vulnerability Scoring System for Industrial Control Systems (CVSS-ICS), takes into account the importance of safety as a key metric in addition to confidentiality, integrity, and availability in calculating the severity of a single vulnerability, an individual ICS device, or the entire ICS system. The recommended CVSS-ICS calculations presented the importance of adding safety metrics to the existing CVSS 3.1 calculations when it comes to calculating severity scores in ICS.

The test results revealed several vulnerabilities related to safety, confidentiality, integrity, and availability of ICS devices used in this testbed. Since we are dealing with critical ICS devices, it is recommended to run additional future testing and apply control measures to automate penetration testing when applied in an ICS environment to ensure that the process does not get out of hand in such an environment, where safety is always a big concern.

Due to the sensitivity and sometimes unpredictable results of using penetration tools to test critically connected ICSs in manufacturing environments, this research output, analysis, and results are limited by the equipment used in the testbed. To get more accurate results, testing of both the recommended manual and automated penetration testing process should be done in a larger and more diverse controlled production environment.

7.2 Conclusion and Recommendations

This conclusion is related to research conducted on equipment used in this testbed and may differ from other devices. If given the chance, the researcher would test it in a larger environment with a busier network to get more accurate results. As a result of this research, these are some of the conclusions and recommendations:

1. Nmap was very effective in identifying TCP and UDP port numbers that are open, closed, or filtered on all devices.
2. The TCP scan of devices beyond the well-known ports (1-1023) caused the ABB drive to stop working; the only way to recover was to reset the drive. More testing can be done to find the cause and develop a solution, as this can be used as a DoS attack.
3. The UDP scan beyond the well-known ports (1-1023) did not affect any of the ICS devices.
4. Using Nmap to scan and identify operating systems running on these devices seems to be not accurate, and the output reported the wrong operating system when it tried to identify an embedded operating system. The researcher used other tools such as Wireshark and MITM to identify the ICS operating system.
5. Both Rockwell Automation and ABB are using one or more non-secure services such as HTTP, FTP, and SNMPv1. These protocols are communicating in a clear text, and the vendor should phase these non-secure protocols out and replace them with secure ones such as HTTPS, sftp, and SNMPv3.
6. All devices used in this testbed are dependent on CIP and Ethernet/IP (port 44818) for their communications. This CIP protocol is using a clear text, and the recommendation is to use encrypted communication protocols. This could be a challenge, as ICS devices may not be able to handle encryption due to CPU and memory limitations. As technology advances, future ICS devices may become capable of handling encrypted communications.

7. Using different open-source penetration testing tools was very effective, as each tool has its own strength and weaknesses.
8. The automated penetration testing program can be packaged as an open-source tool that is freely available to be used by ICS companies to ensure that ICS devices were deployed with "Good Security Practices".

7.3 Future Work

This is a list of future work that can be done in addition to this research:

1. More accurate results can be obtained if both manual and automated penetration testing are conducted in either a real production ICS environment (with safety measures) or using a similar testbed with more devices and simulated traffic using a traffic generator to add more stress on the ICS devices and emulate a real ICS environment.
2. It is recommended to use both a manual and an automated program to test as many devices as we can to create a baseline for ICS devices. The same vendor may apply or configure devices differently, which may lead to a different outcome.
3. Nmap had difficulty identifying the operating system of the embedded firmware. Therefore, more work can be done in this area to make sure that Nmap is more effective and accurate in identifying the operating system of embedded firmware devices.
4. Additional attacks may be tested against ICS, such as replay attacks, distributed denial of service attack (DDoS), and using scapy (security tool) to manipulate packets received by ICS devices.
5. The automated program can be easily modified to be used in testing other ICS devices and sensors, including Industrial Internet of Things (IIoT) devices to make it more robust and secure.

References

[1] Kostas Mathioudakis, Nick Frangiadakis, Andreas Merentitis, and Vangelis Gazis. Towards generic SCADA simulators: A survey of existing multi-purpose co-simulation platforms, best practices and use-cases. AGT Group (R&D), 2013.

[2] Sajid Nazir, Shushma Patel, and Dilip Patel. Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & Security, 70:436–454, 2017.

[3] Rockwell Automation, Smart Manufacturing, https://www.rockwellautomation.com/en_NA/capabilities/connected-enterprise/overview.page. Accessed October 20, 2019.

[4] The Connected Enterprise, Bringing people, processes and technology together, https://literature.rockwellautomation.com/idc/groups/literature/documents/br/cie-br001_-en-p.pdf. Accessed October 21, 2019.

[5] Fujitsu.com, the connected Enterprise: Making the Industrial IoT Happen – Right Here, Right Now, https://www.fujitsu.com/fi/Images/wp-fujitsu-connected-enterprise.pdf. Accessed October 21, 2019.

[6] NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems(ICS) Security: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf. Accessed October 17, 2019.

[7] Wei Xu, Experience and Lessons in Building an ICS Security Testbed, University of Science and Technology of China, July 2019.

[8] Cisco and Rockwell Automation, Deploying Network Security within a Converged Plantwide Ethernet Architecture: Design and Implementation Guide: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf. Accessed December 2018.

[9] Nandini Raghvendra, SCADA Systems – Components, hardware & software architecture, types: https://electricalfundablog.com/SCADA-system-components-architecture/. Accessed October 25, 2019.

[10] Kim Zetter: An Unprecedented look at Stuxnet, the World's First Digital Weapon: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. Accessed January 20, 2020.

[11] Kim Zetter: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Accessed January 23, 2020.

[12] Kelly Jackson Higgins, Triton/Trisis Attack was more widespread than publicly known: https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661. Accessed February 25, 2020.

[13] Tara Seals, June 14, 2019, Trisis group, known for physical destruction, targets U.S. Electric companies. Accessed January 26, 2020.

[14] B.D. Katz and H. Fouquet, September 26, 2019, Airbus Counters Cyber Attacks Targeting Suppliers, https://www.bloomberg.com/news/articles/2019-09-26/airbus-takes-steps-to-counter-cyber-attacks-targeting-suppliers. Accessed November 20, 2019.

[15] Dimensional Research in September 2019, Tripwire State of Industrial Cybersecurity Report, October 2019, https://www.tripwire.com/solutions/industrial-control-systems/industrial-cybersecurity-report/ . Accessed December 28, 2019.

[16] The OSI Model: https://www.coengoedegebure.com/osi-model/, accessed October 14, 2019.

[17] Software Testing Help, TCP/IP Model With different Layers, https://www.softwaretestinghelp.com/tcp-ip-model-layers/ Accessed October 14, 2019.

[18] IANA Service Name and Transport Protocol Port Number Registry: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?skey=4&page=15. Accessed June 15, 2020.

[19] ODVA : https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf. Accessed September 5, 2019.

[20] Anastasios Arampatzis, what is the ISA/IEC 62443 framework? https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/. Accessed March 27, 2020.

[21] Paul Brooks, Ethernet/IP: Industrial Protocol White Paper: https://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp001_-en-p.pdf. Accessed March 30, 2020.

[22] Fady Bashay, What is the CIA triangle and why is it important for cybersecurity management?: https://www.difenda.com/blog/what-is-the-cia-triangle-and-why-is-it-important-for-cybersecurity-management. Accessed March 2nd, 2020.

[23] Hayro, august 27, 2019: The three goals of cyber security-CIA triad defined: https://www.preferreditgroup.com/2019/08/27/the-three-goals-of-cyber-security-cia-triad-defined/. Accessed, March 2nd, 2020.

[24] Software Testing Help, 7 Layers Of The OSI Model, https://www.softwaretestinghelp.com/osi-model-layers/ . Accessed October 14, 2019.

[25] https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/ Accessed October 20, 2019.

[26] David P. Duggan, Sandia Report, Penetration of Testing of Industrial Control Systems: https://energy.sandia.gov/wp-content/gallery/uploads/sand_2005_2846p.pdf, March, 2005.

[27] S. Krishnan and M. Wei, "SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics," *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757543.

[28] Filipe Rocha, CyberSecurity analysis of a SCADA system under current standards, client requisites, and penetration testing: https://repositorio-aberto.up.pt/bitstream/10216/119066/2/315683.pdf. Accessed October 20, 2019.

[29] Samant, Neha, "AUTOMATED PENETRATION TESTING" (2011).Master's Projects. 180. DOI: https://doi.org/10.31979/etd.fxpj-pt6k https://scholarworks.sjsu.edu/etd_projects/180. Accessed January 14, 2020.

[30] Bonney, Gregor, & Hoefken, Hans & Paffen, Benedikt & Schuba, Marko. (2015). ICS/SCADA Security Analysis of a Beckhoff CX5020 PLC. Accessed December 1st, 2019.

[31] Oracle VirtualBox: https://www.virtualbox.org/. Accessed October 10, 2019.

[32] Kali, https://www.kali.org/. Accessed May 10, 2019.

[33] Nmap, https://nmap.org/. Accessed May 10, 2019.

[34] TCPdump: https://www.tcpdump.org/. Accessed May 10, 2019.

[35] Wireshark: https://www.wireshark.org/. Accessed June 15, 2019.

[36] CVE Common Vulnerabilities and Exposures, http://cve.mitre.org. Accessed January 20, 2020.

[37] Rockwell TCP and UDP Port Configuration: https://literature.rockwellautomation.com/idc/groups/literature/documents/qr/comm-qr001_-en-e.pdf. Accessed April 15, 2020.

[38] Precise Time Protocol (PTP), https://wiki.wireshark.org/Protocols/ptp. Accessed July 7, 2020.

[39] CVE Details: https://www.cvedetails.com/vulnerability-list/vendor_id-1641/product_id-2833/Goahead-Goahead-Webserver.html. Accessed July 1, 2020.

[40] FTP server response codes: The first dig, https://www.smartfile.com/blog/big-list-ftp-server-response-codes/. Accessed July 10, 2020.

[41] National Institute of Standards and Technology vulnerability database: https://www.nist.gov/. Accessed July 10, 2020.

[42] Eduard Kovacs: CVSS Scores often misleading for ICS vulnerabilities: Experts: https://www.securityweek.com/cvss-scores-often-misleading-ics-vulnerabilities-experts. Accessed November 16, 2018.

[43] CVSS Common Vulnerability Scoring System version 3.1 specification document Revision 1: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf. Accessed September 2020.

[44] Common Vulnerability Scoring System Version 3.1 Calculator: https://www.first.org/cvss/calculator/3.1. Accessed September 2020.

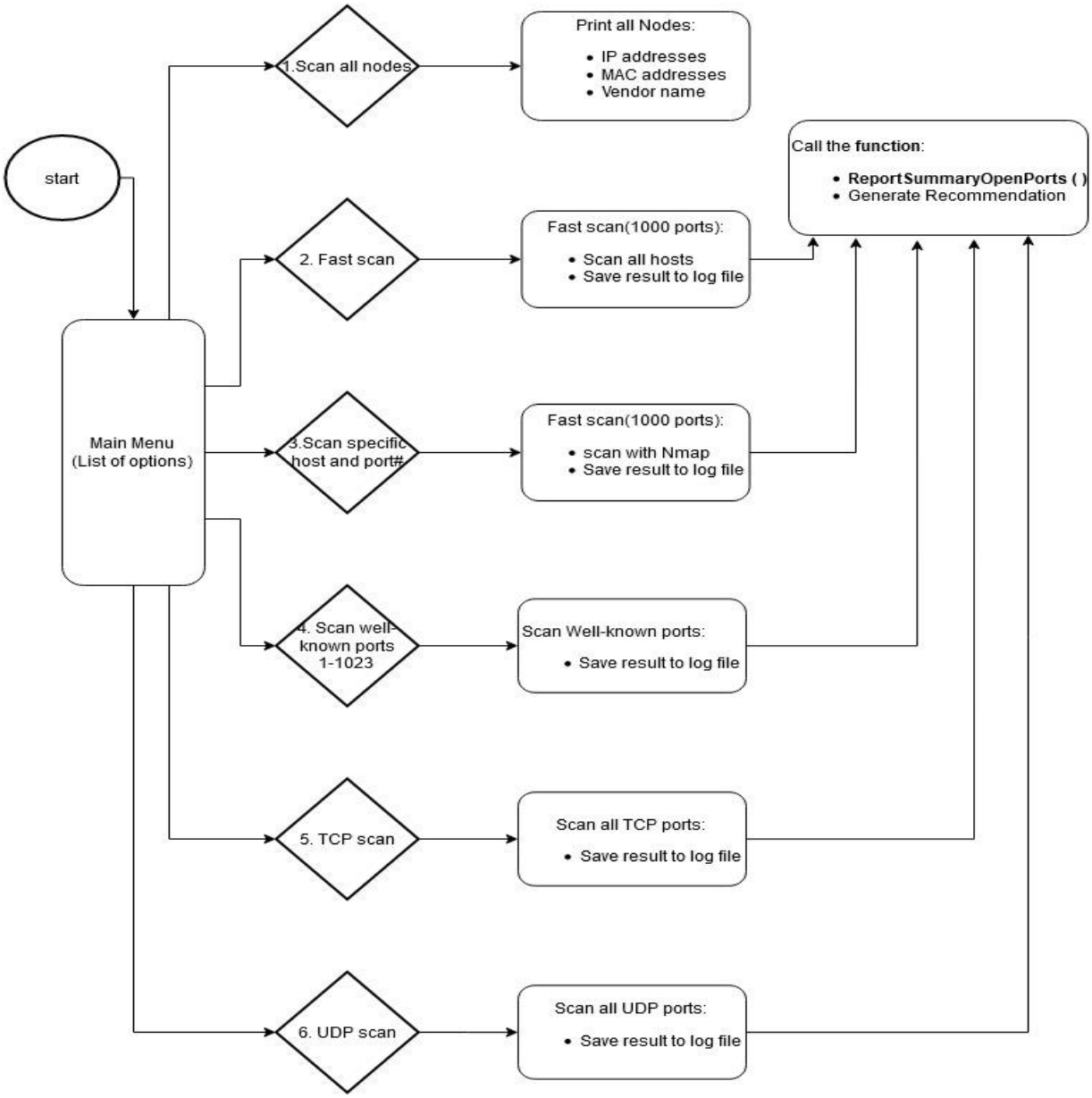
[45] Deloitte, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ics-white-paper.pdf. October 2015. Accessed October 2020.

[46] Security Week: https://www.securityweek.com/some-ics-security-incidents-resulted-injury-loss-life-survey, October 24, 2019. Accessed November 2019.

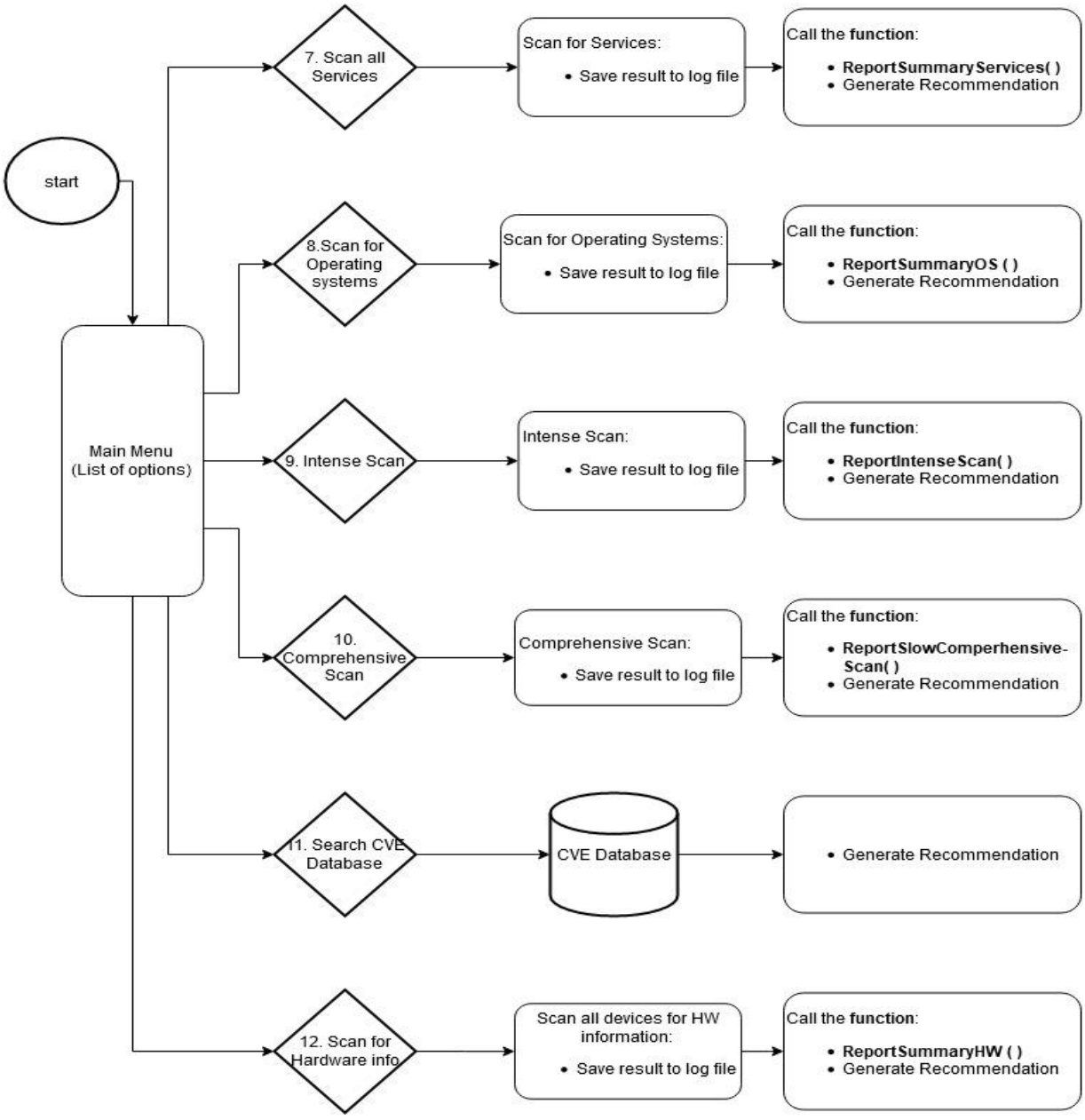
[47] Low.com https://www.law.com/thelegalintelligencer/2020/08/21/when-cyber-attacks-result-in-physical-damage-important-insurance-considerations/. August 2020. Accessed November 2020.

Appendix A: Flow Chart of The Automated Program

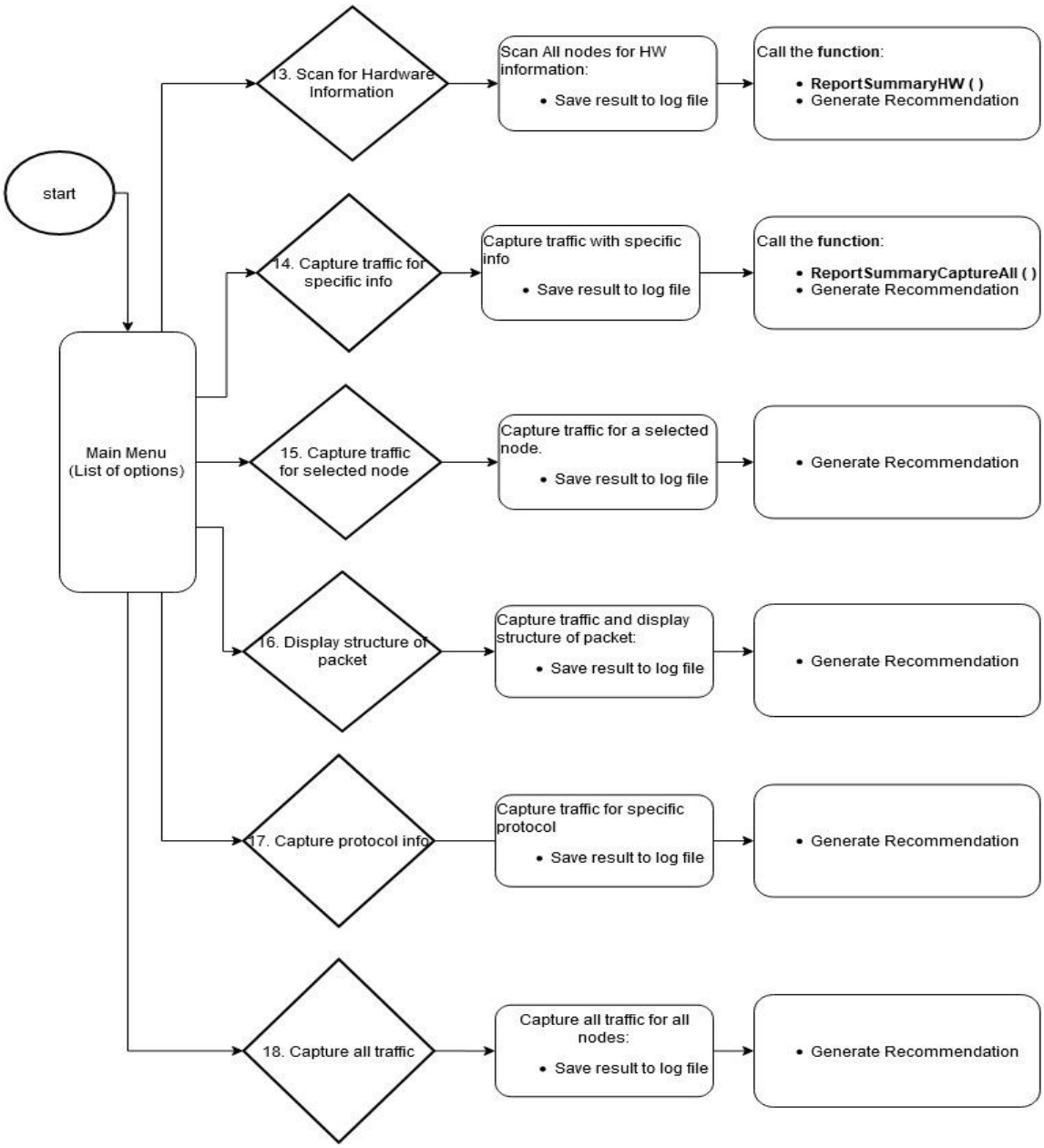
Flow Chart – Part 1



Flow Chart – Part 2



Flow Chart – Part 3



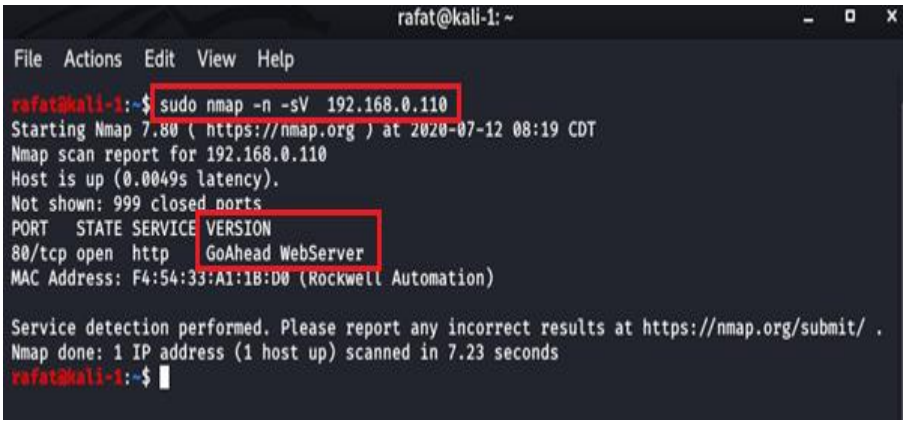
Appendix B: Output of Manual Penetration Testing

Results of Scanning for Available Services

Results of scan for running services on the PLC:

a. The Nmap command scans the name and version of available services.

b. The output of the scan revealed the name of the service used to run the HTTP server. The PLC is using the GoAhead webserver running on port 80. Vulnerabilities dating back to 2011 were found for the GoAhead webserver such CVE-2011-4273, which would allow an attacker to execute multiple cross-site scripting (XSS), and CVE-2009-5111, which would allow a remote attacker to cause a denial of service attack via partial HTTP requests [39].



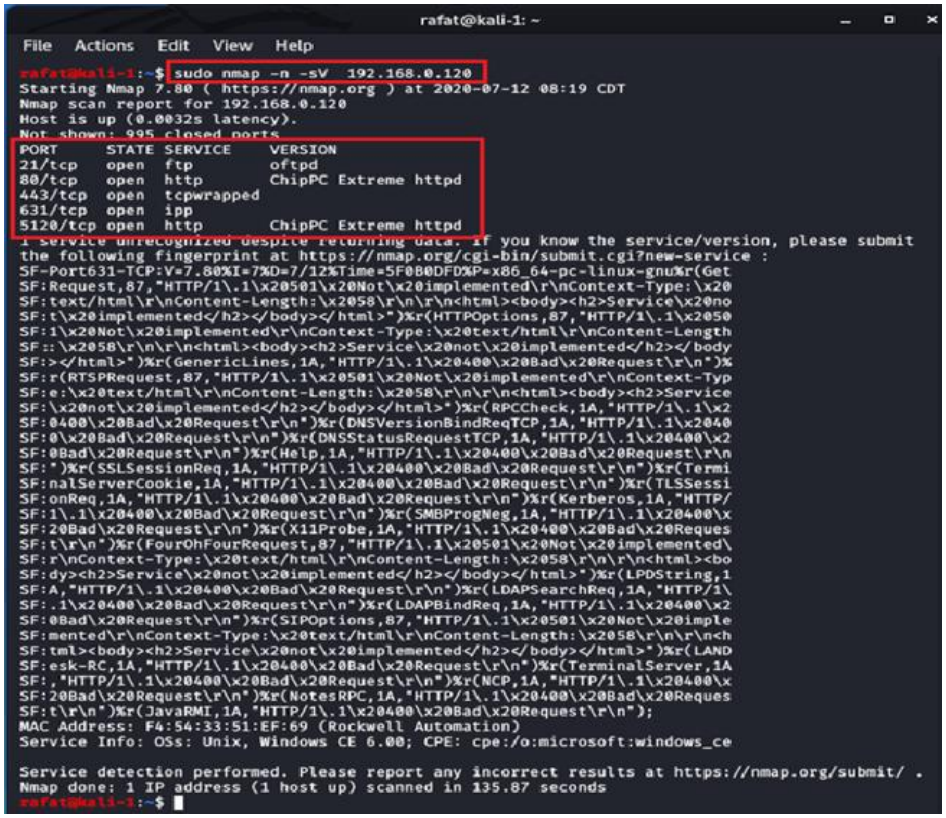
Services running on the PLC

Results of scan for running services on the HMI:

a. Using Nmap to scan for services.

b. The output identified two services running on the HMI. First, with oftpd that runs the ftp server on port 21, searching the CVE database [39], we found vulnerability with versions

before 0.3.7 that allows remote attackers to cause a denial of service, with a high warning score. Second was ChipPC Extreme httpd, running on both port 80 and port 5120/tcp. With no version number reported with this scan, also no information was found on this service using the CVE database.



Results of Nmap scan for services running on HMI

Results of scan for running services on the ABB drive:

a. Using Nmap to scan for services.

b. The output shows one service Mitel SIP DEC VoIP phone running on port 80. The Nmap scan failed to identify the type of webserver running on the ABB drive.

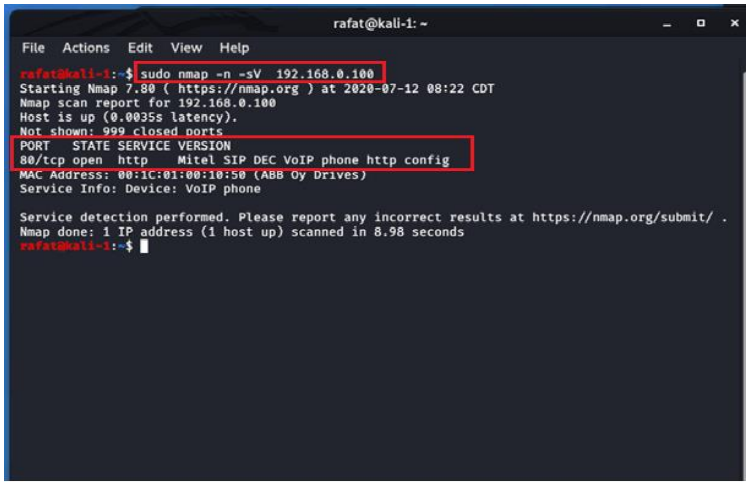


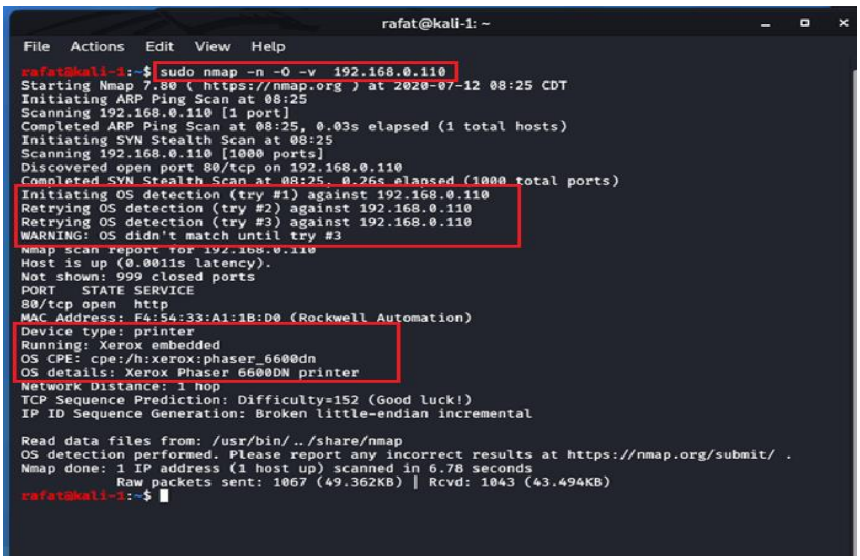
ABB drive scan for services identification

Results of Scanning for Identifying Operating Systems (OS)

Results of scan for OS on the PLC :

a. Shows the Nmap command used to scan for OS.

b. Nmap failed to identify the correct OS running on the PLC; the result of the scan is a Xerox phaser 6600DN printer running an embedded operating system.

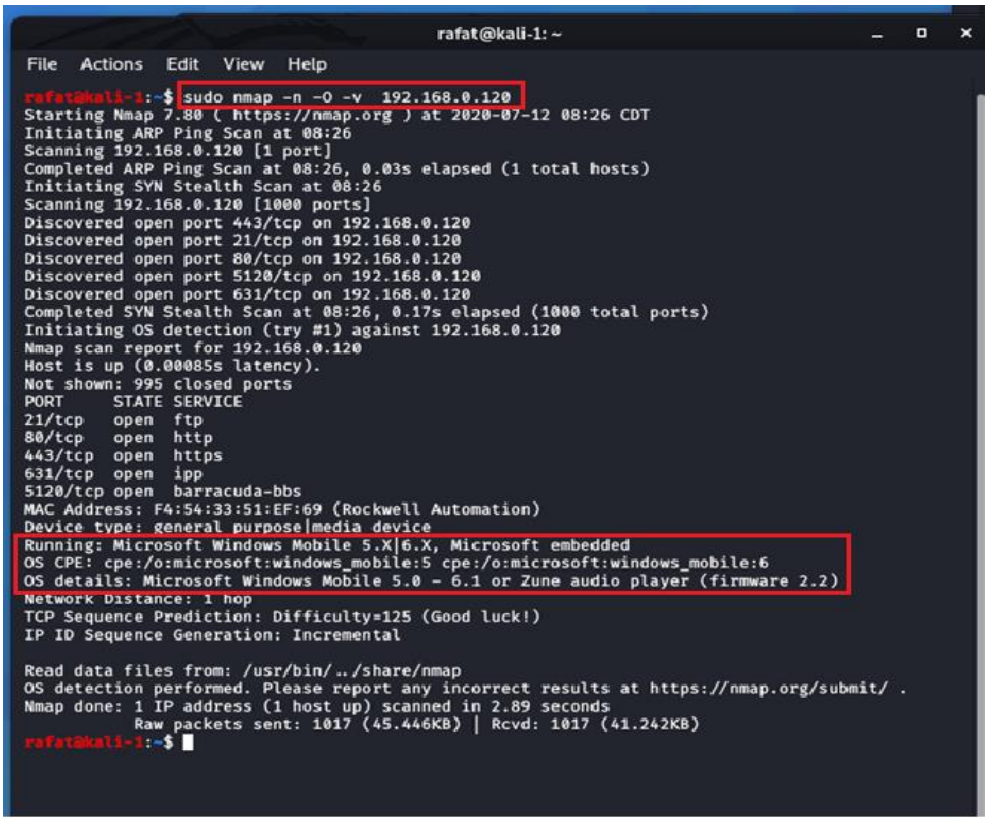


Results of Nmap scan to identify PLC OS.

Results of scan for OS on the HMI:

a. Shows the Nmap command used to scan for OS.

b. The output of the Nmap scan identified the OS for the HMI as Microsoft Windows mobile 5.x/6.x Microsoft embedded.

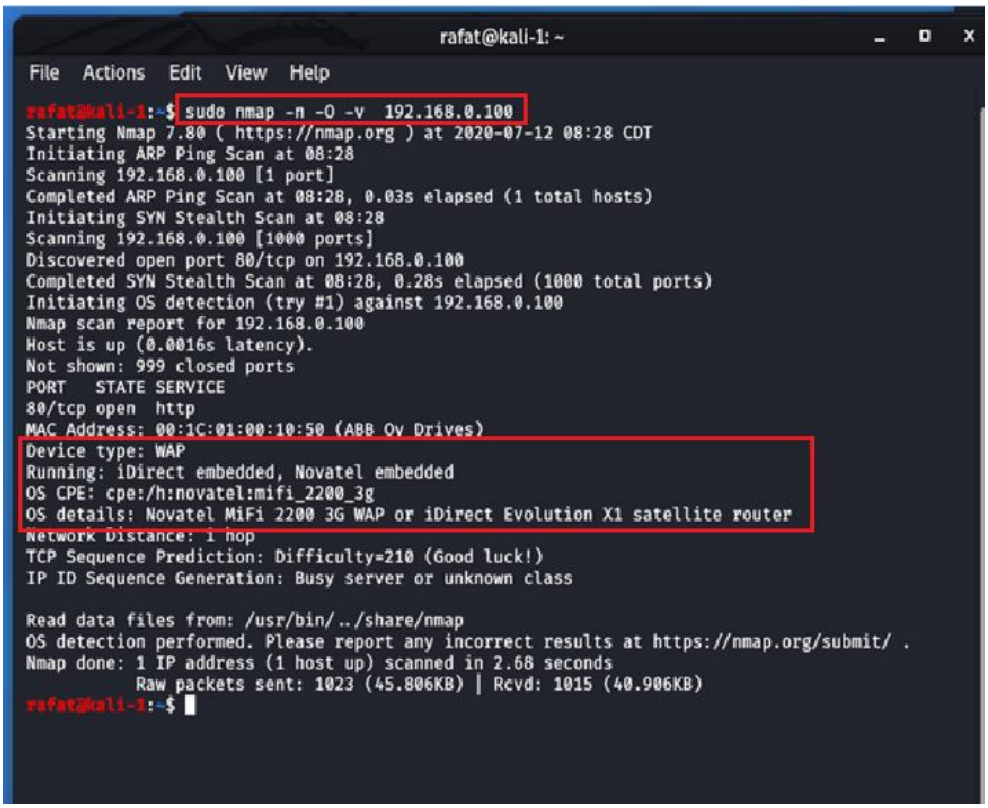


Nmap was able to identify HMI OS as Windows mobile 5.x/6.x

Results of scan for OS on the ABB drive:

a. Shows the Nmap command used to scan for OS.

b. Nmap scan failed to identify ABB drive OS. The scan output shows the OS as Novatel MiFi 2200 3G WAP or Idirect evolution XL satellite router, which may have simmilar OS signature as the ABB drive.



Output of ABB drive

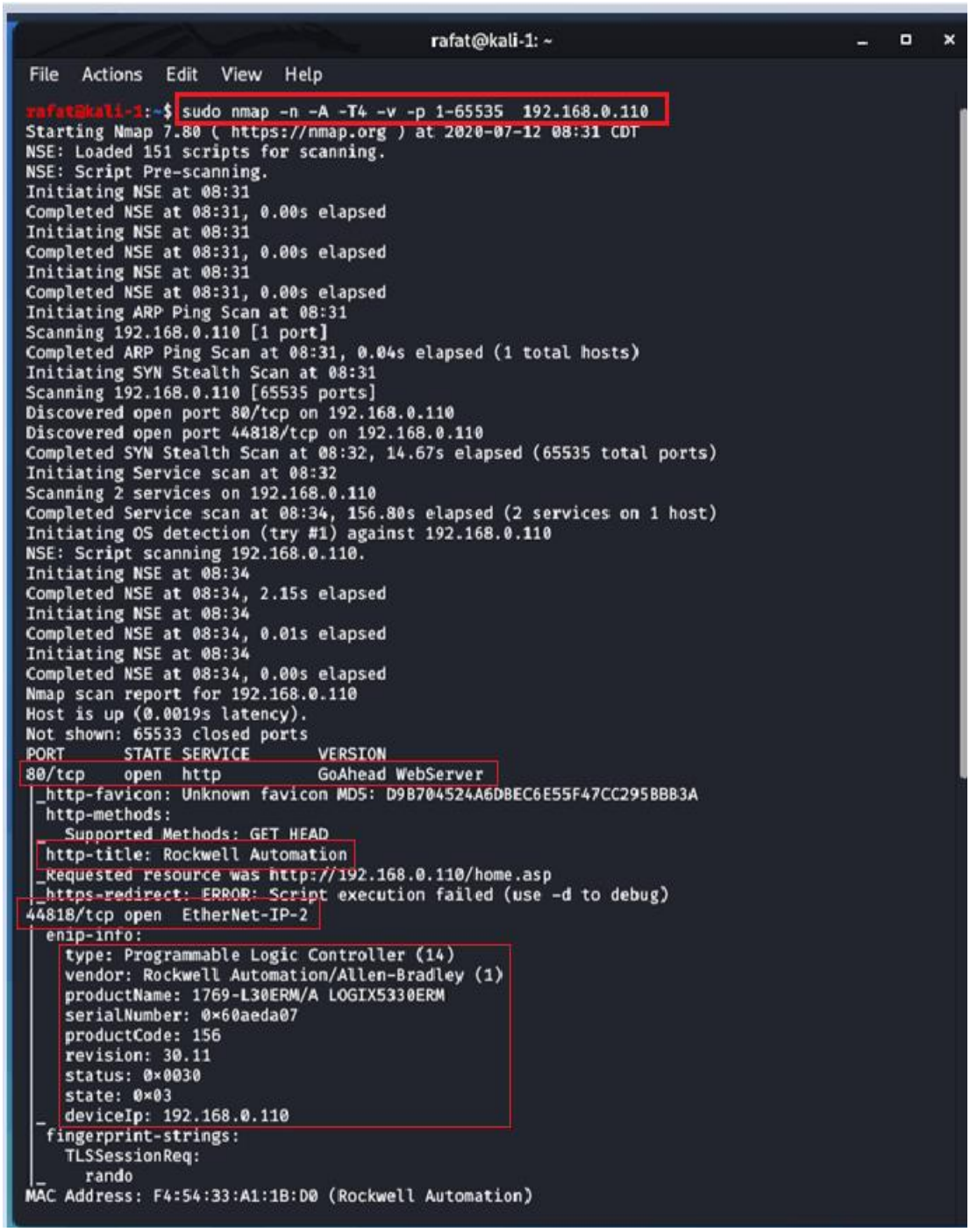
Results of Intense Scan – Warning

Results of intense scan of the PLC :

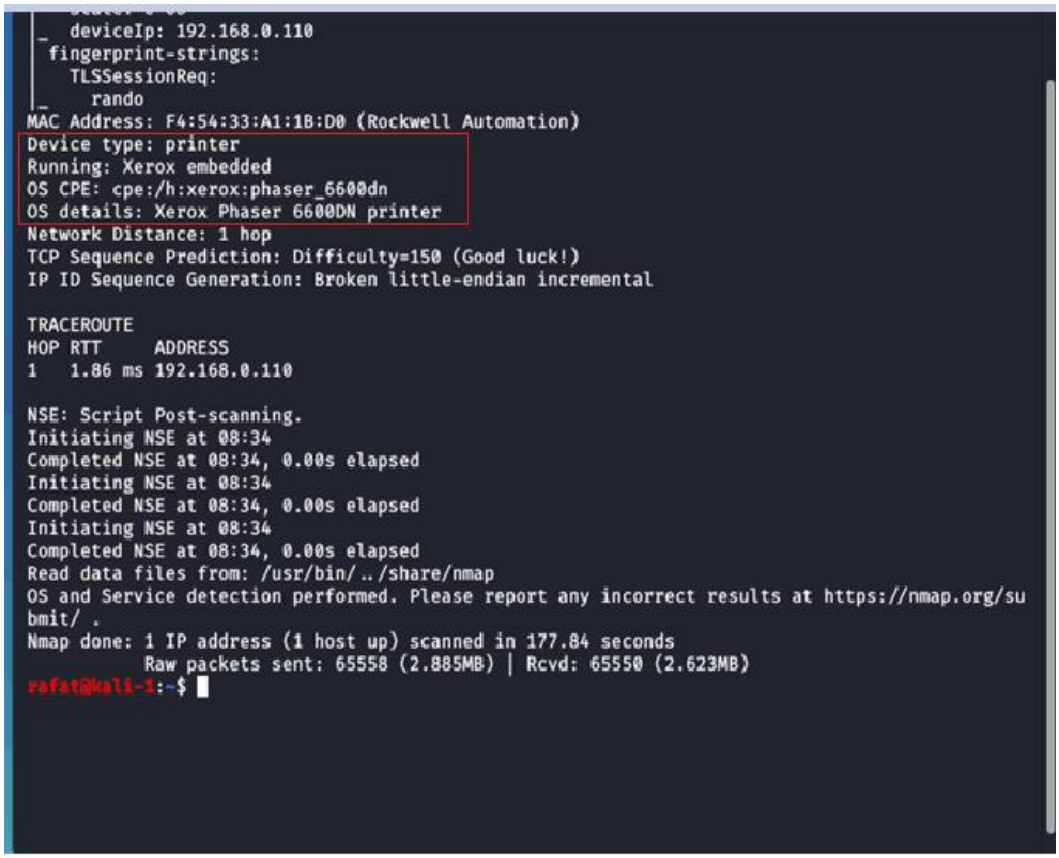
a. Shows the Nmap intense scan command.

b. This scan identified all the information found earlier such as port numbers, different services, and OS. This scan, similar to previous ones, failed to identify the OS that the PLC is using.

c. Using port 44818 (Ethernet/IP) and Ethernet/IP script, the scan was able to identify more information regarding the PLC, such as the type of device, vendor, product name, serial number, product code, revision, status, and state. This output is considered very valuable information in the penetration testing reconnaissance phase.



Results of intense scan on the PLC — Part 1



Results of intense scan on the PLC — Part 2

Results of intense scan of the HMI**:**

a. The Nmap intense scan command.

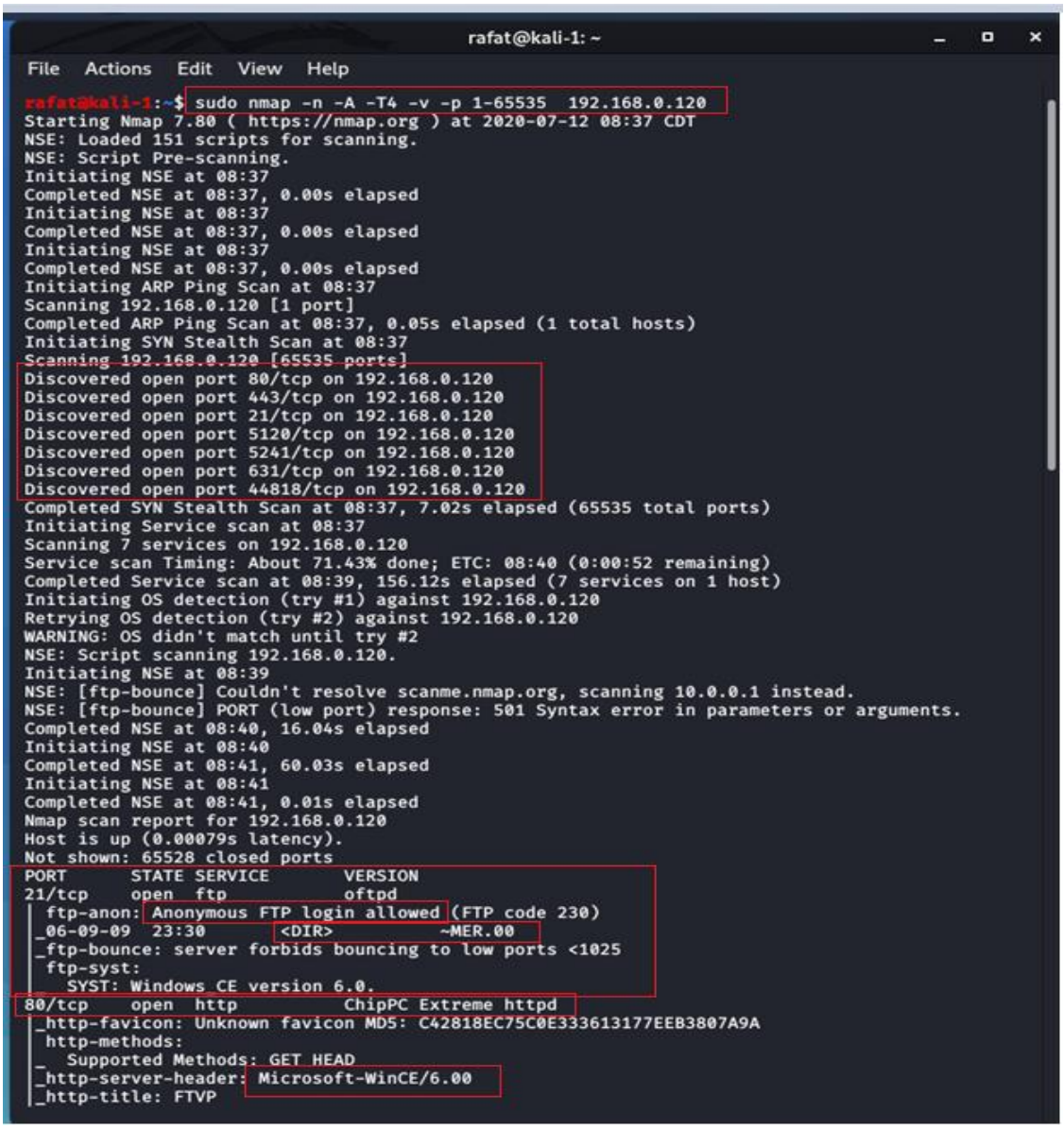
b. Shows all open ports.

c. The intense scan successfully logged into the ftp server (ftp code 230) using an anonymous username [40] and was able to display the directory on the server with the name: MER.000.

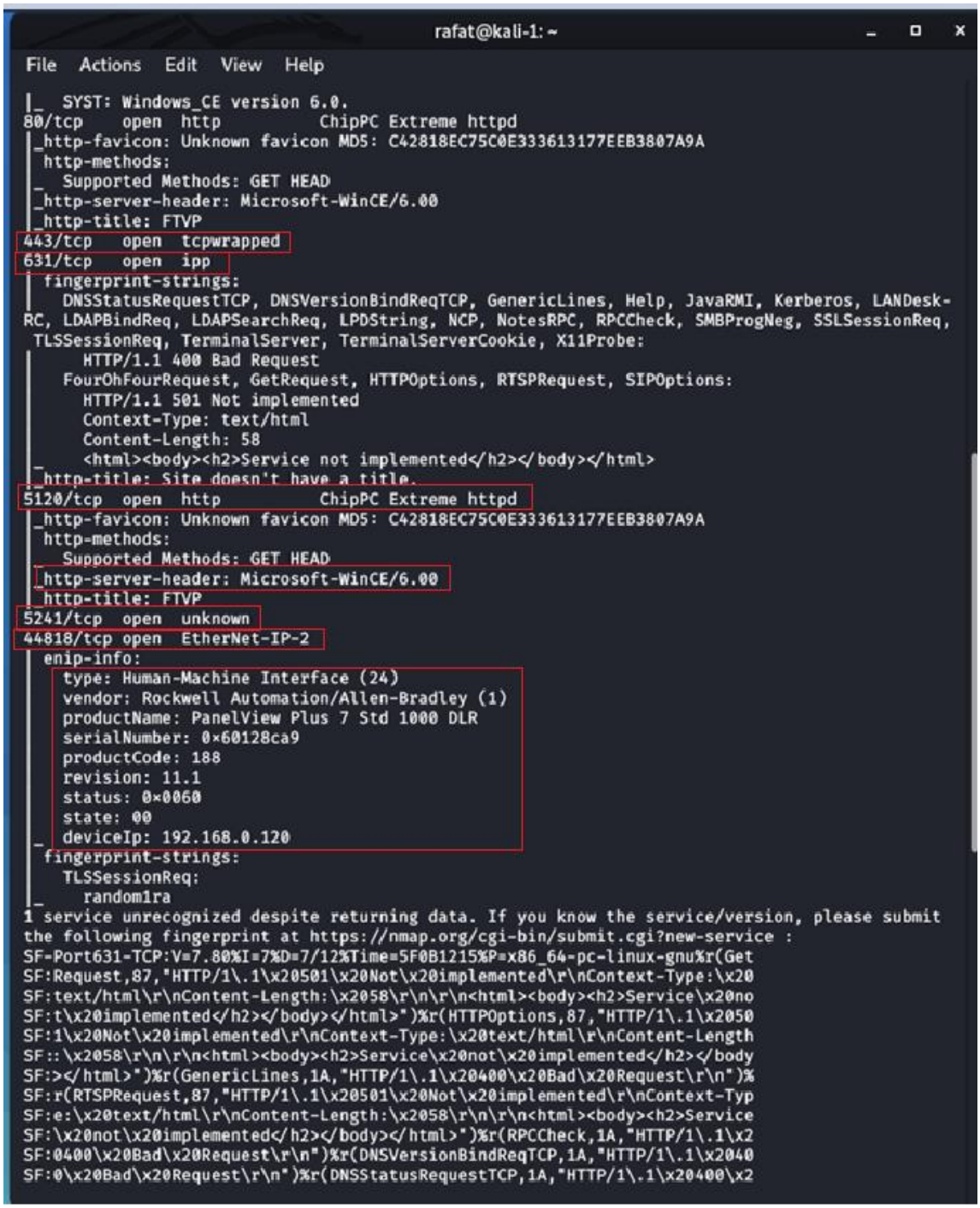
d. This scan identified all the information found earlier such as port numbers and different services, including the OS as Windows CE 6.0.

e. Using port 44818 (Ethernet/IP) and Ethernet/IP script, the scan was able to identify more information regarding the HMI, such as the type of device, vendor, product name, serial number, product code, revision, status, and state. This is considered very valuable information in the penetration testing reconnaissance phase.

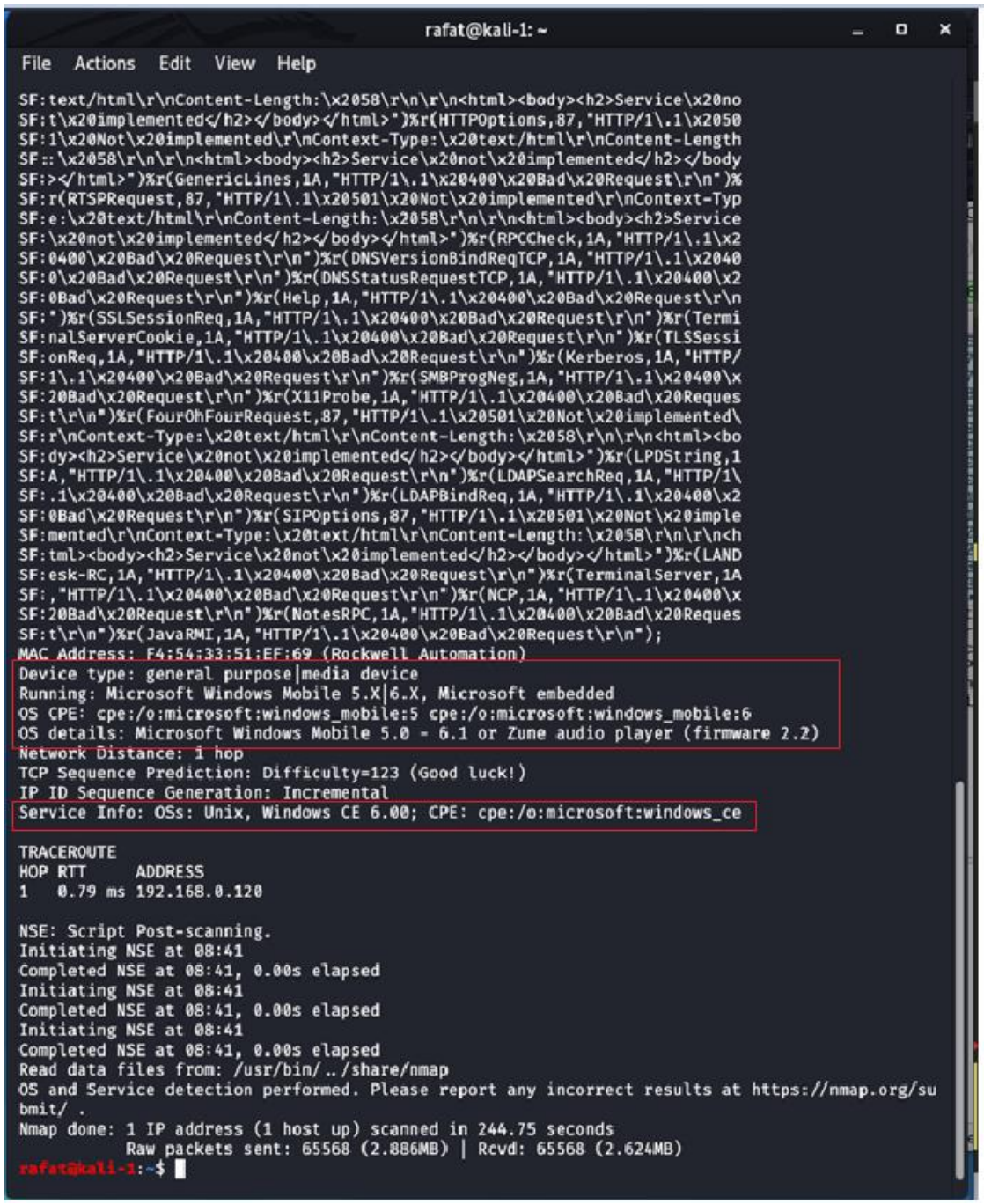
f. The scan took about 4 minutes to complete, a longer time than previous commands.



Intense scan of HMI — Part 1



Intense scan of HMI — Part 2



Intense scan of HMI — Part 3

Results of intense scan of the HMI:

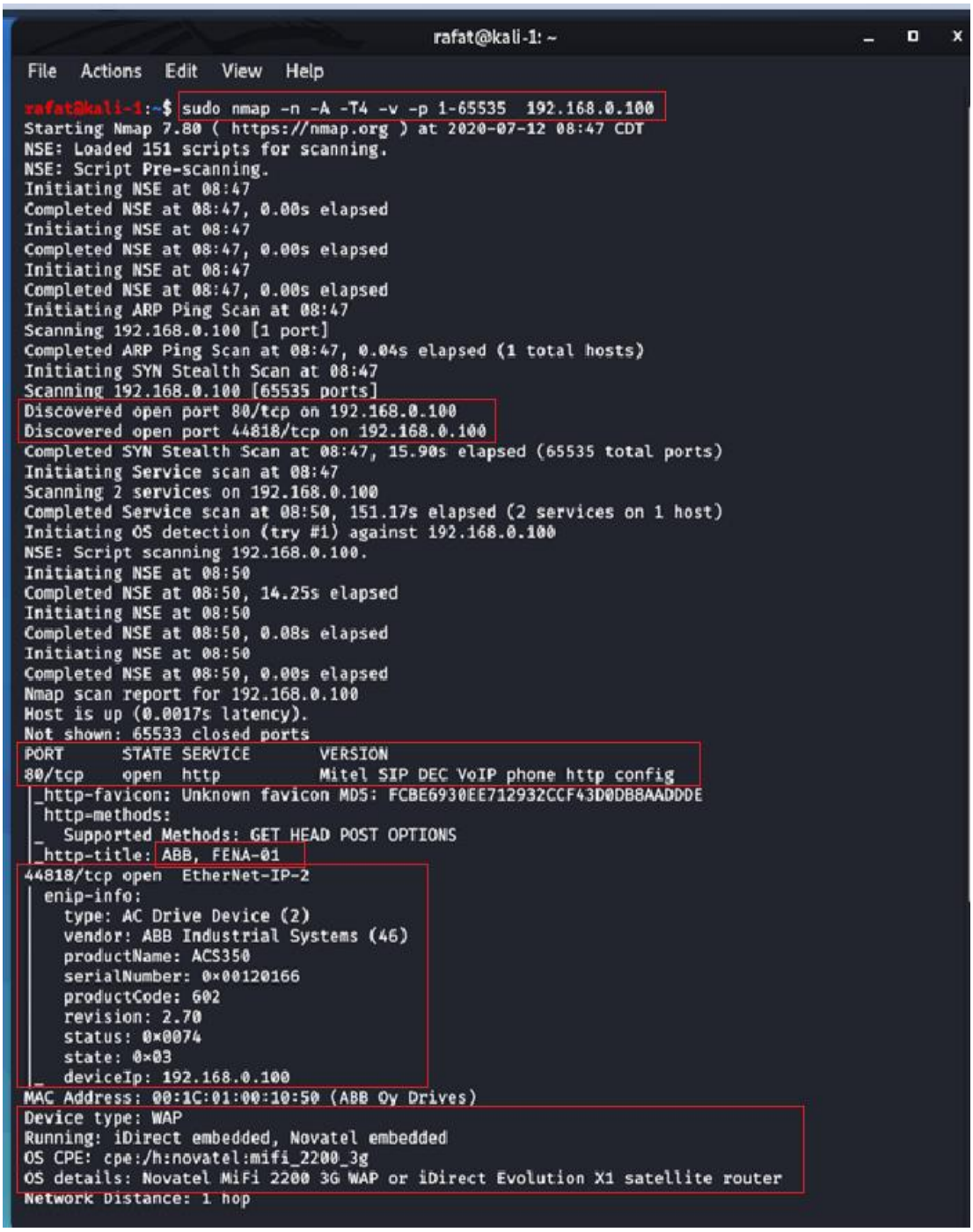
a. Shows the Nmap intense scan command.

b. Shows two ports open, similar to the previous scan.

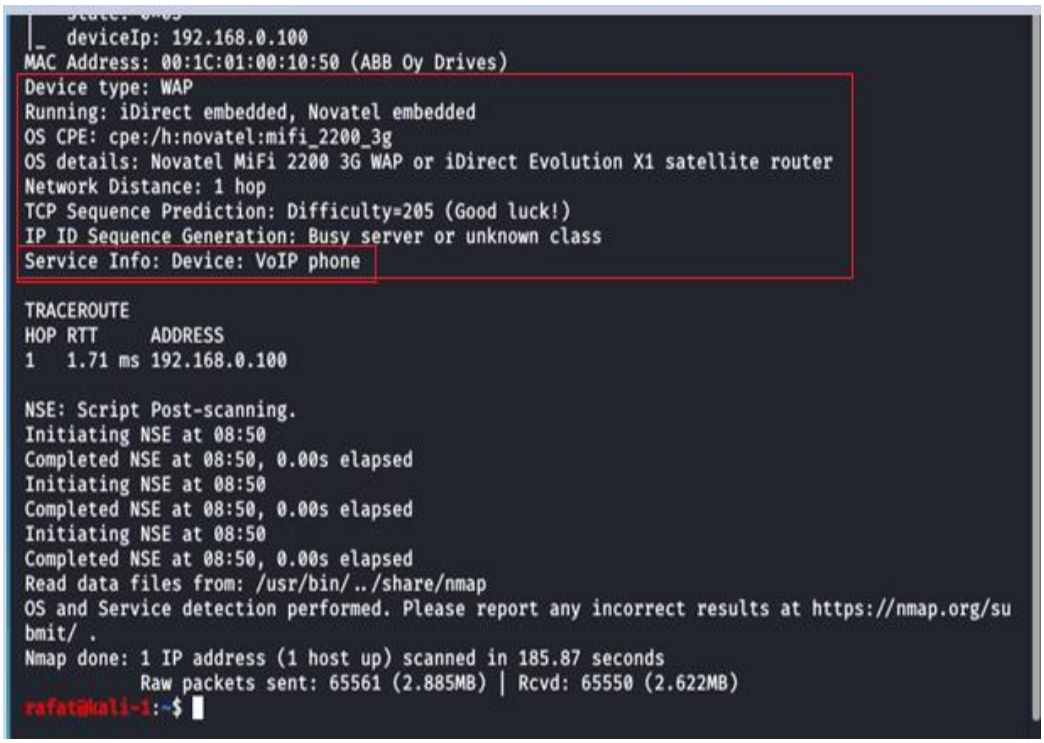
c. The scan failed to identify the type of webserver running on port 80.

d. Using port 44818 (Ethernet/IP) and Ethernet/IP script, the scan was able to identify more information regarding the ABB drive, such as the type of device, vendor, product name, serial number, product code, revision, status, and state. This is considered a very valuable information in the penetration testing reconnaissance phase.

e. The scan failed to identify the correct device and OS using Nmap.



Intense scan of ABB drive — Part 1



Intense scan of ABB drive — Part 2

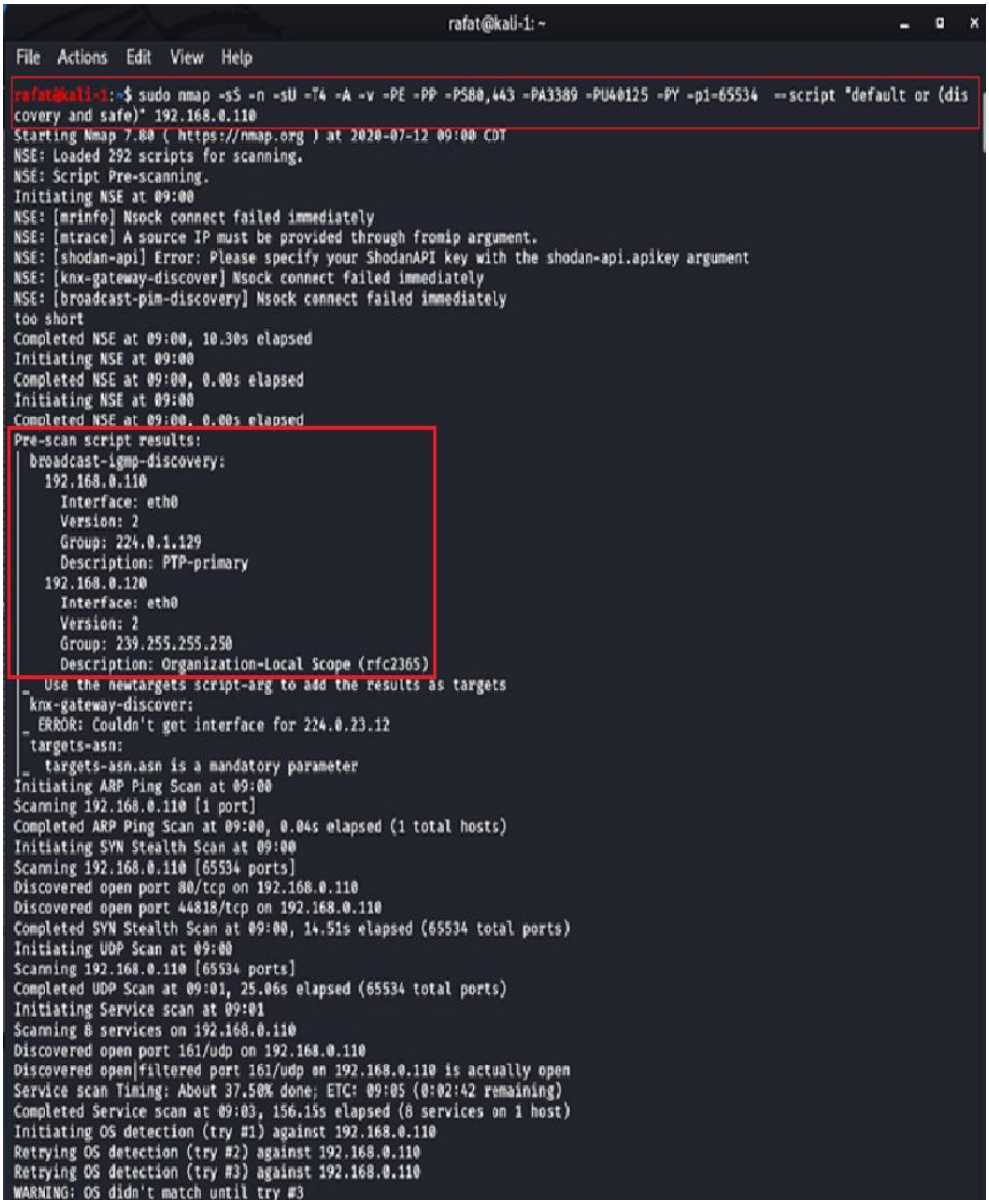
Results of Slow-Comprehensive Scan – Warning

The results of the slow comprehensive scan of the PLC**:**

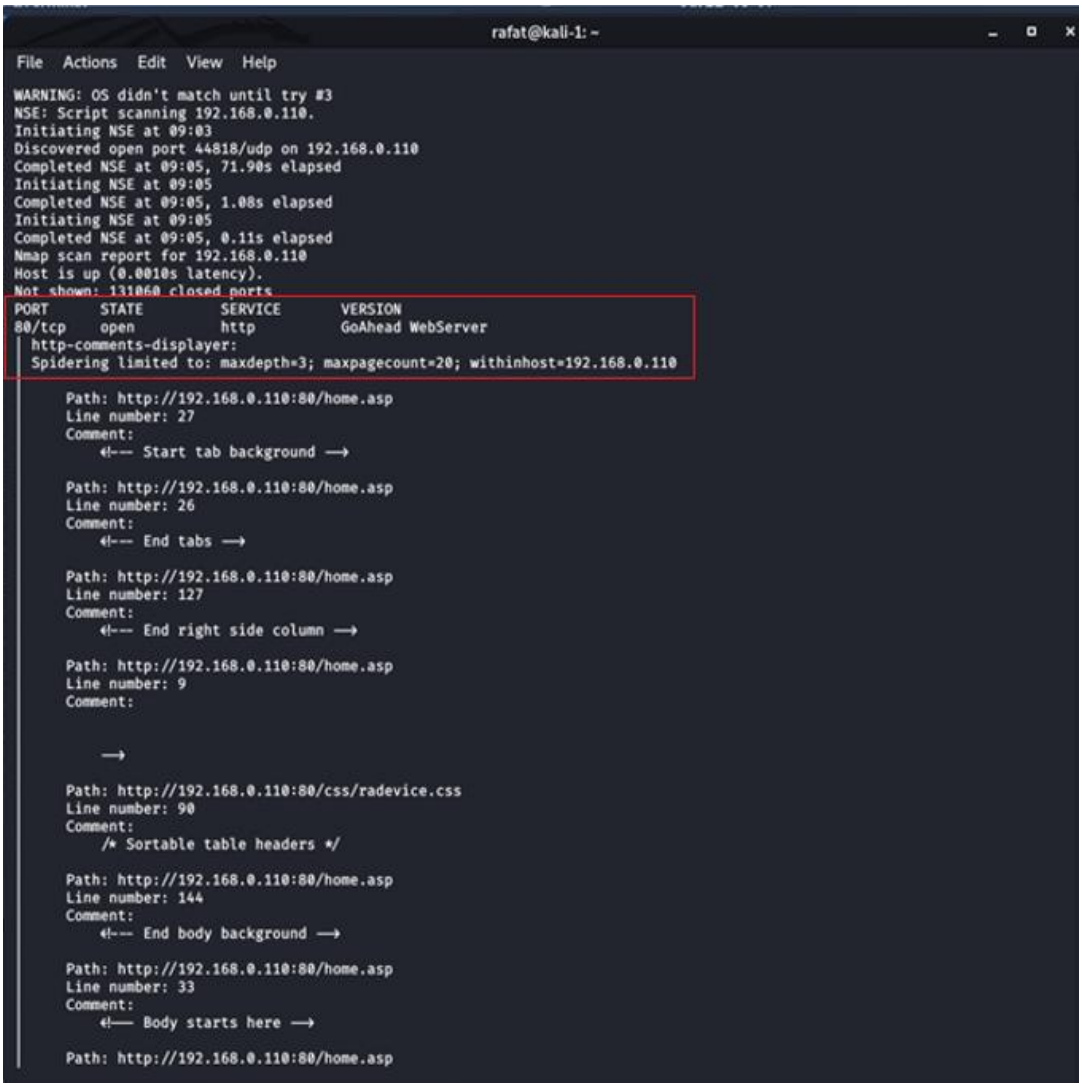
Shows the Nmap intense scan command.

a. The scan showed that by using Nmap and broadcast Internet Group Management Protocol (IGMP), we can detect neighbor ICS devices.

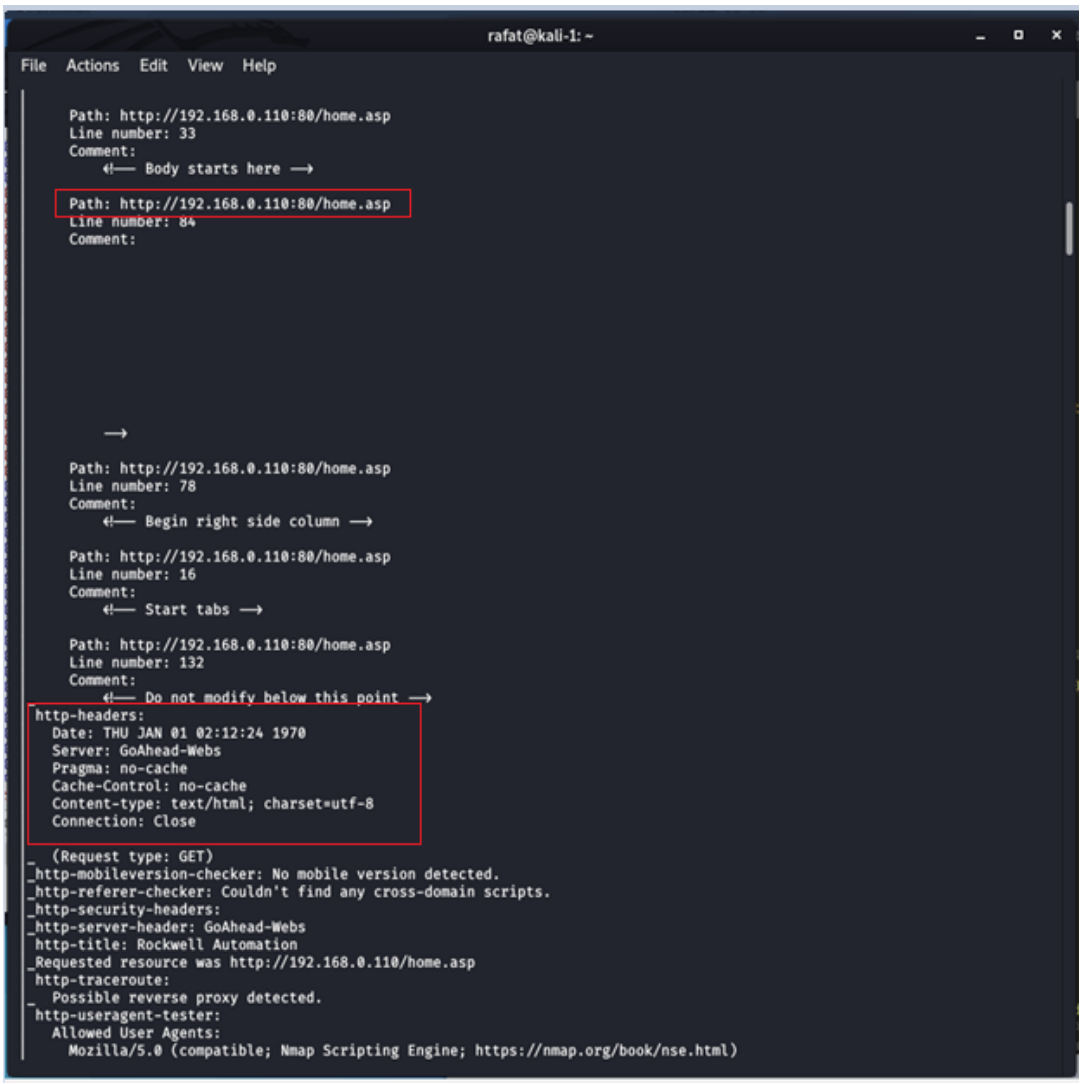
b. Port UDP 161/SNMPv1 – simple network management protocol (SNMP), version 1 and v2 is a nonsecure communication; SNMPv3 should be used.



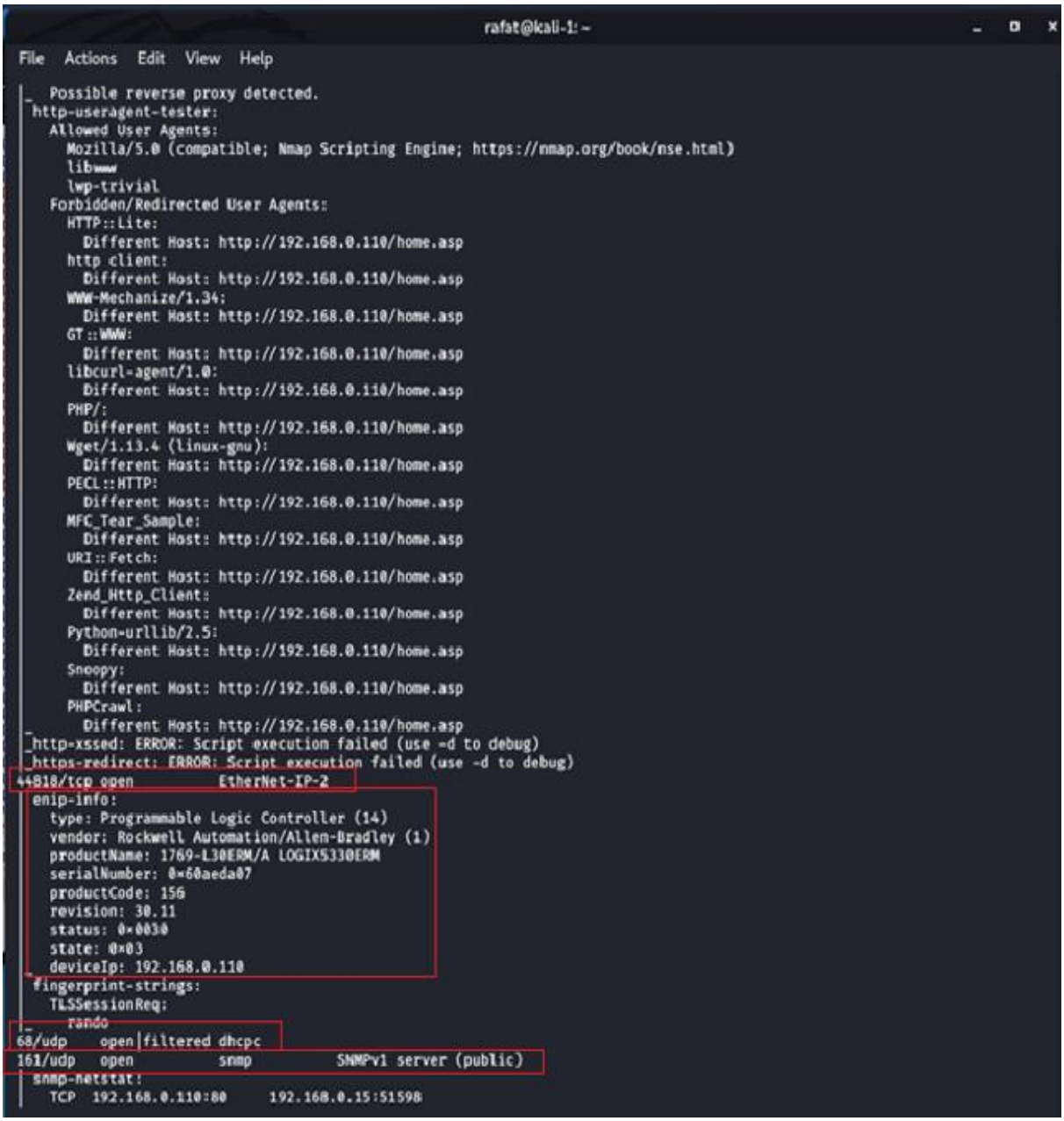
Slow comprehensive scan of PLC — Part 1



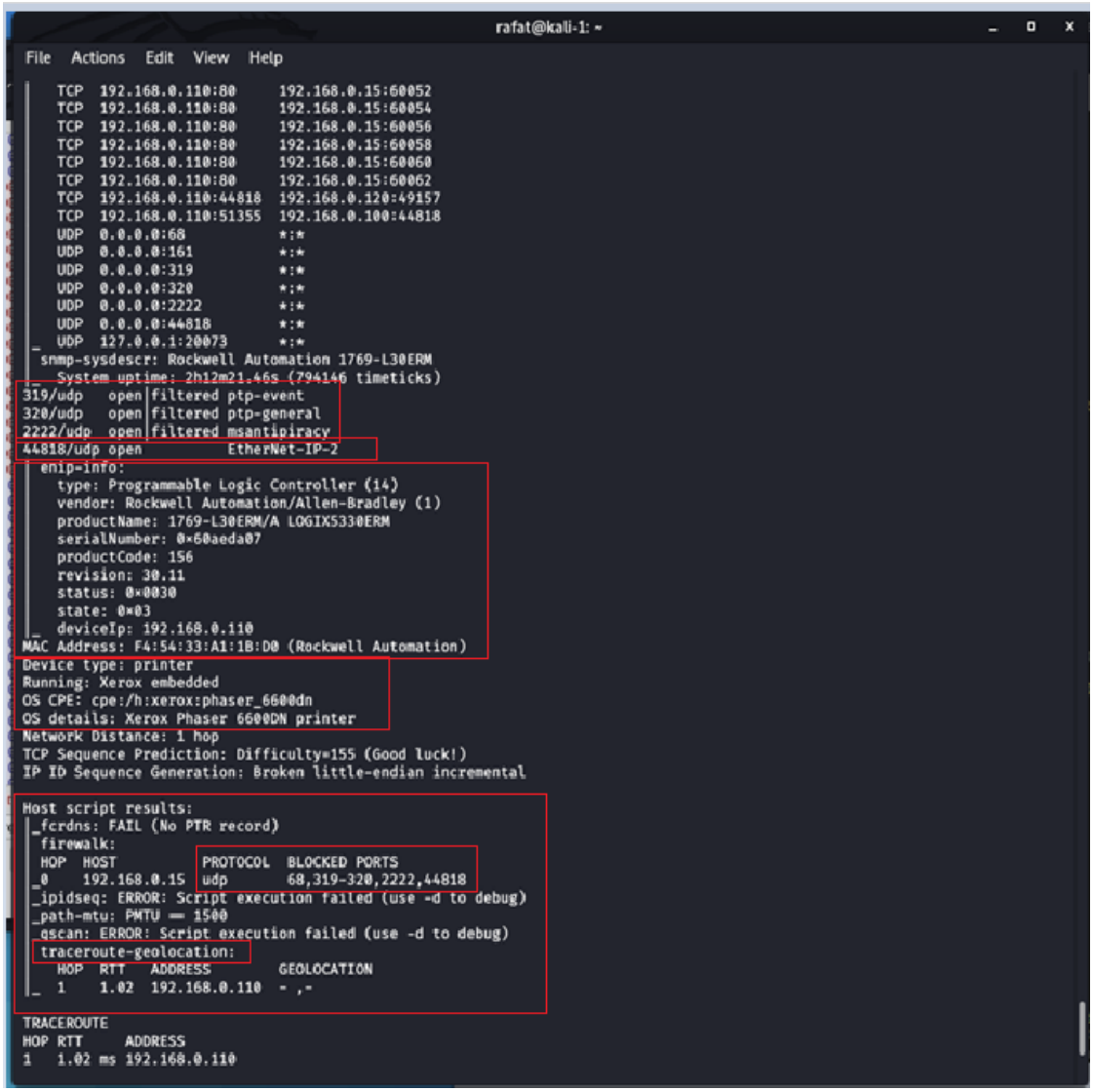
Slow comprehensive scan of PLC — Part 2



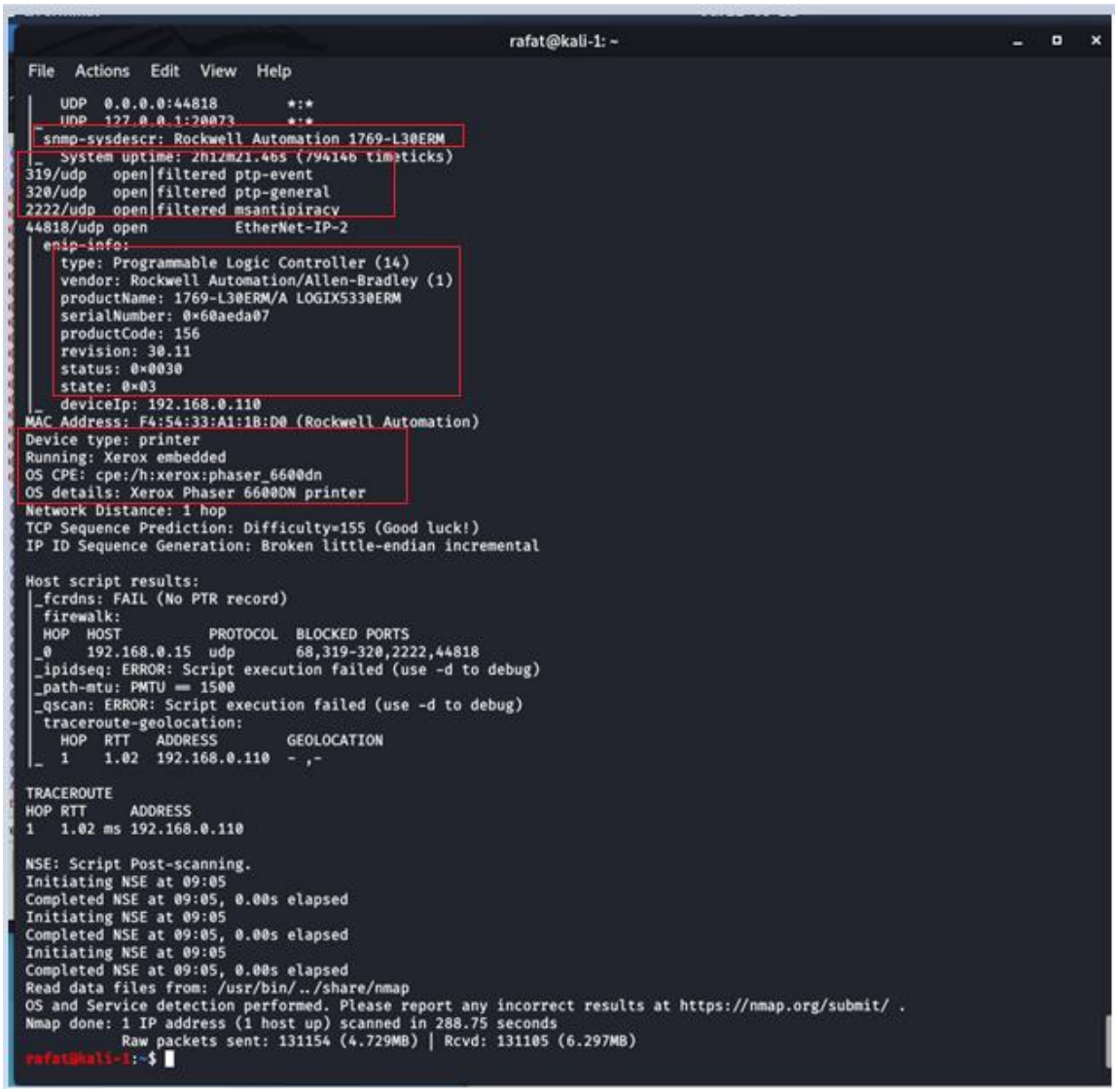
Slow comprehensive scan of PLC — Part 3



Slow comprehensive scan of PLC — Part 4



Slow comprehensive scan of PLC — Part 4



Slow comprehensive scan of PLC — Part 5

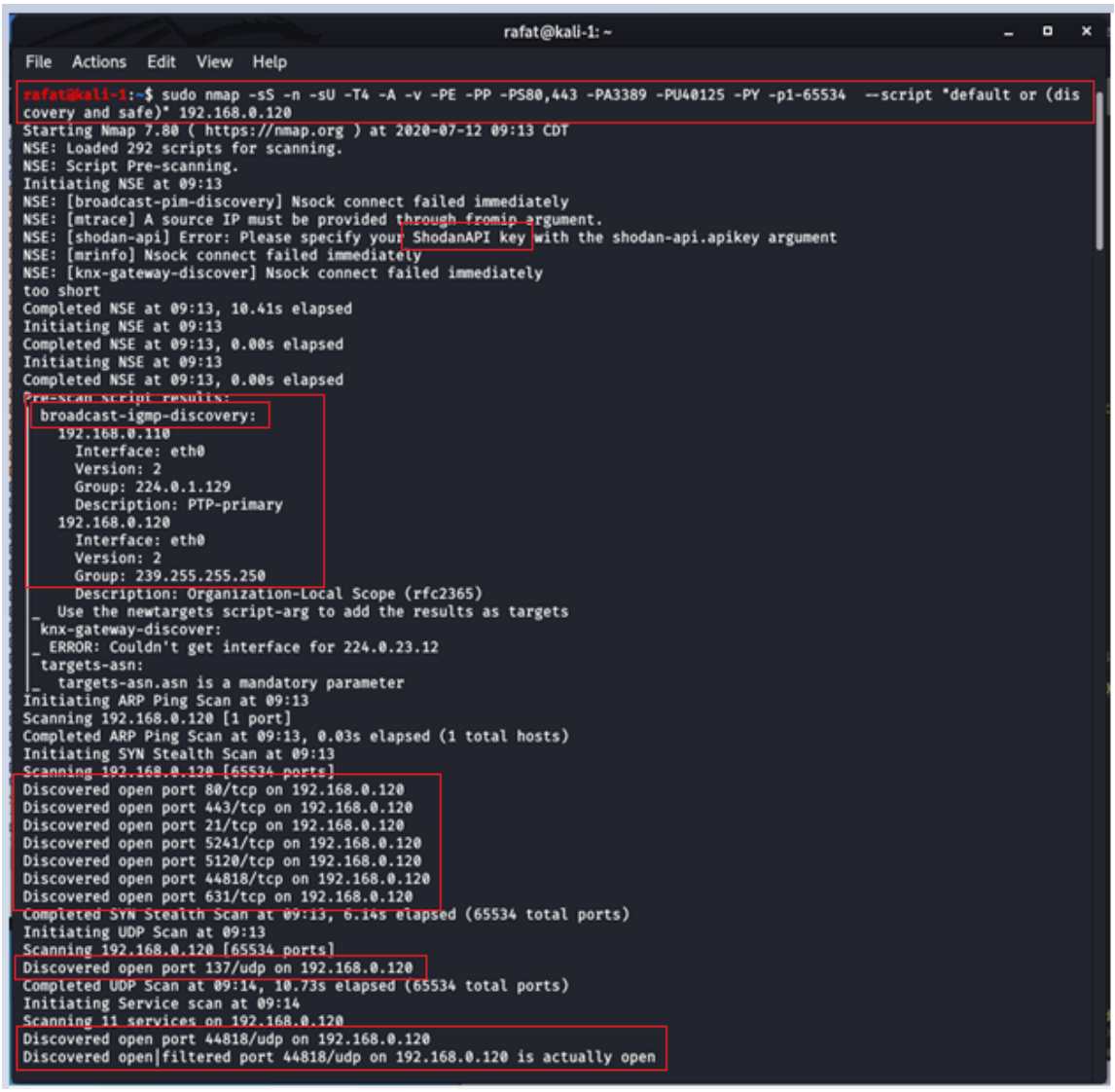
Results of slow comprehensive scan of the HMI:

a. Shows the Nmap intense scan command.

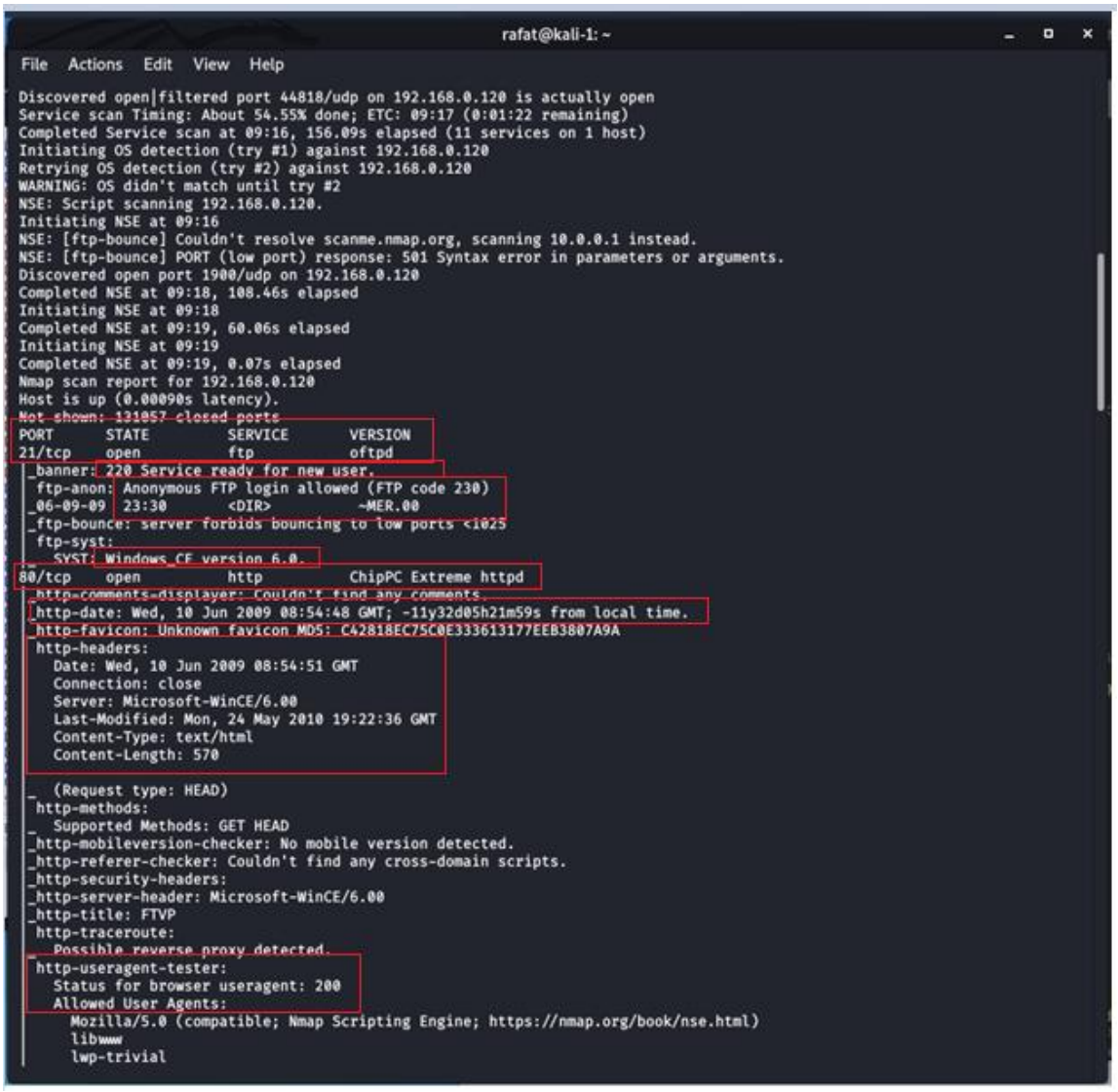
b. Scan discovered a Windows NetBIOS name: PVP61289.

c. The scan lasted for about 6 minutes.

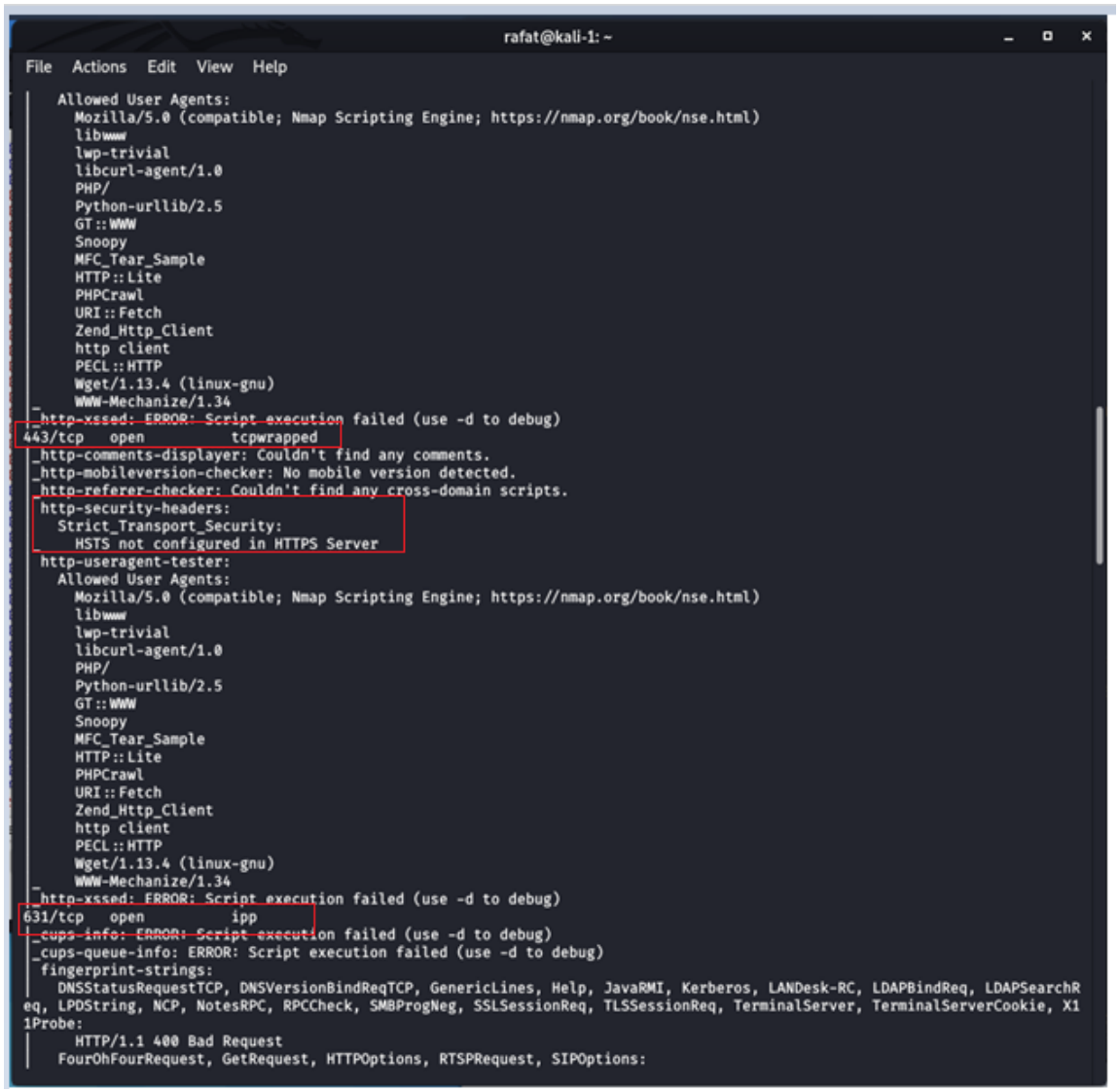
d. The rest of the scan output is the same as the previous ones.



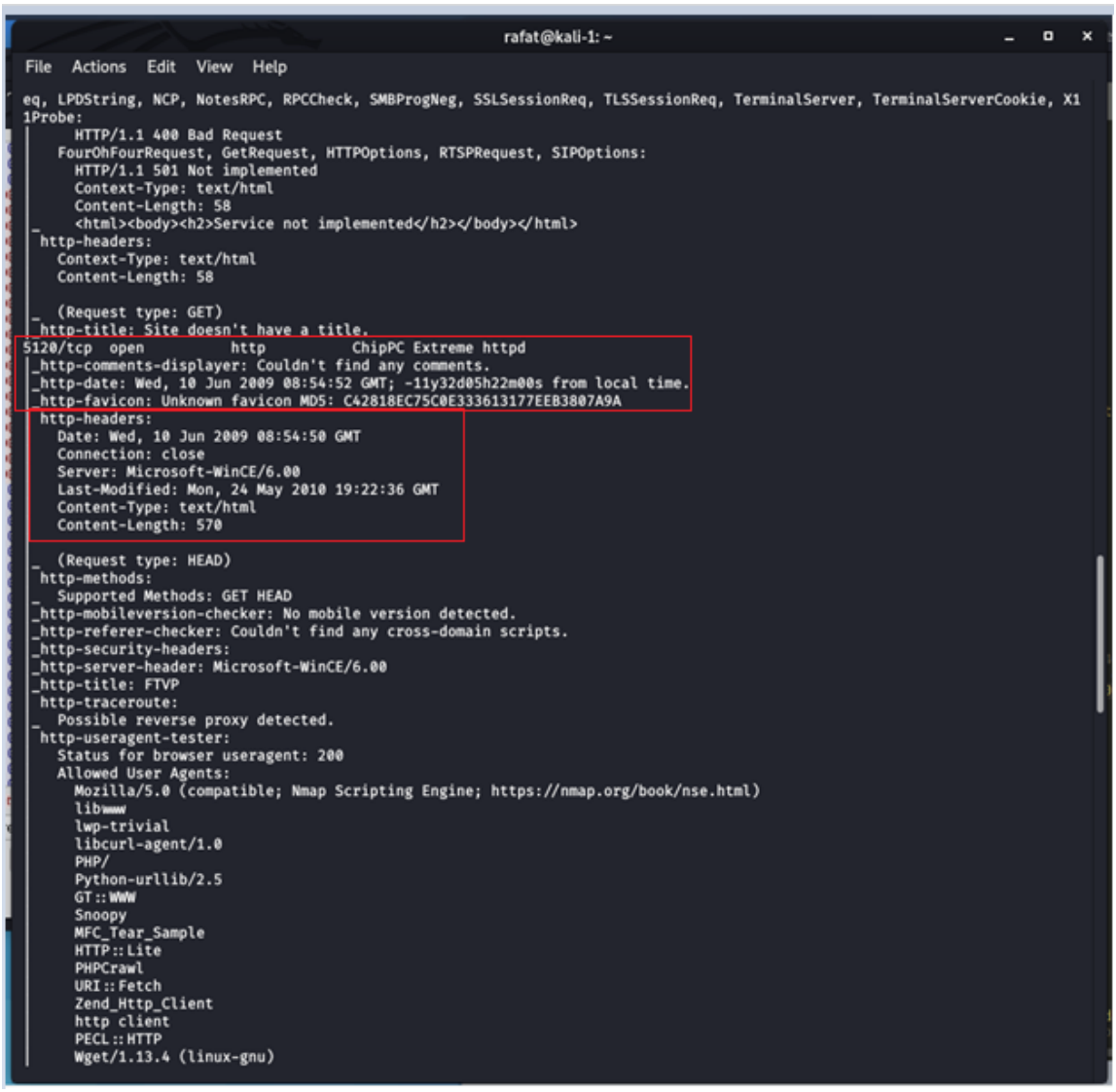
Slow comprehensive scan of HMI — Part 1



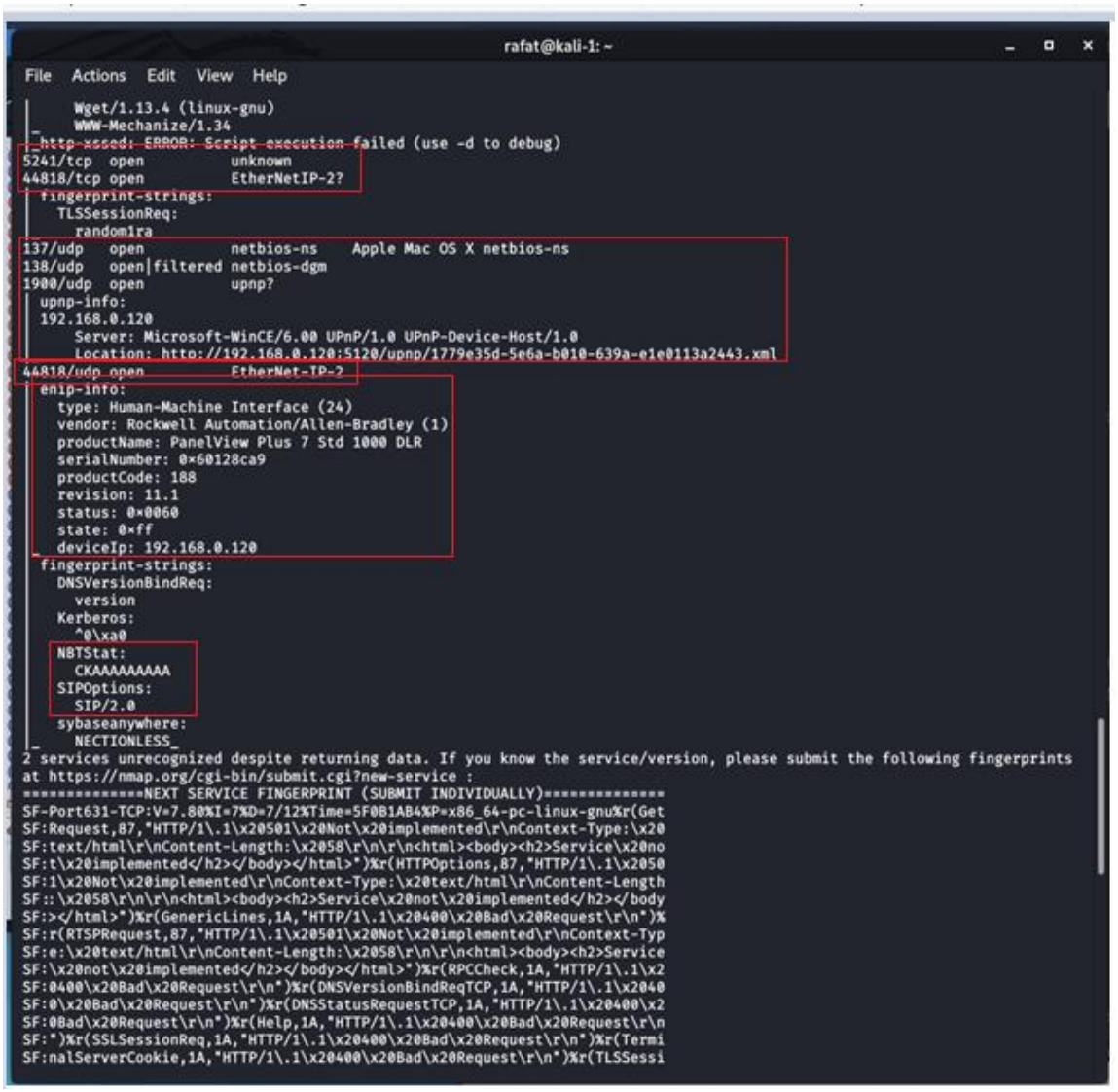
Slow comprehensive scan of HMI — Part 2



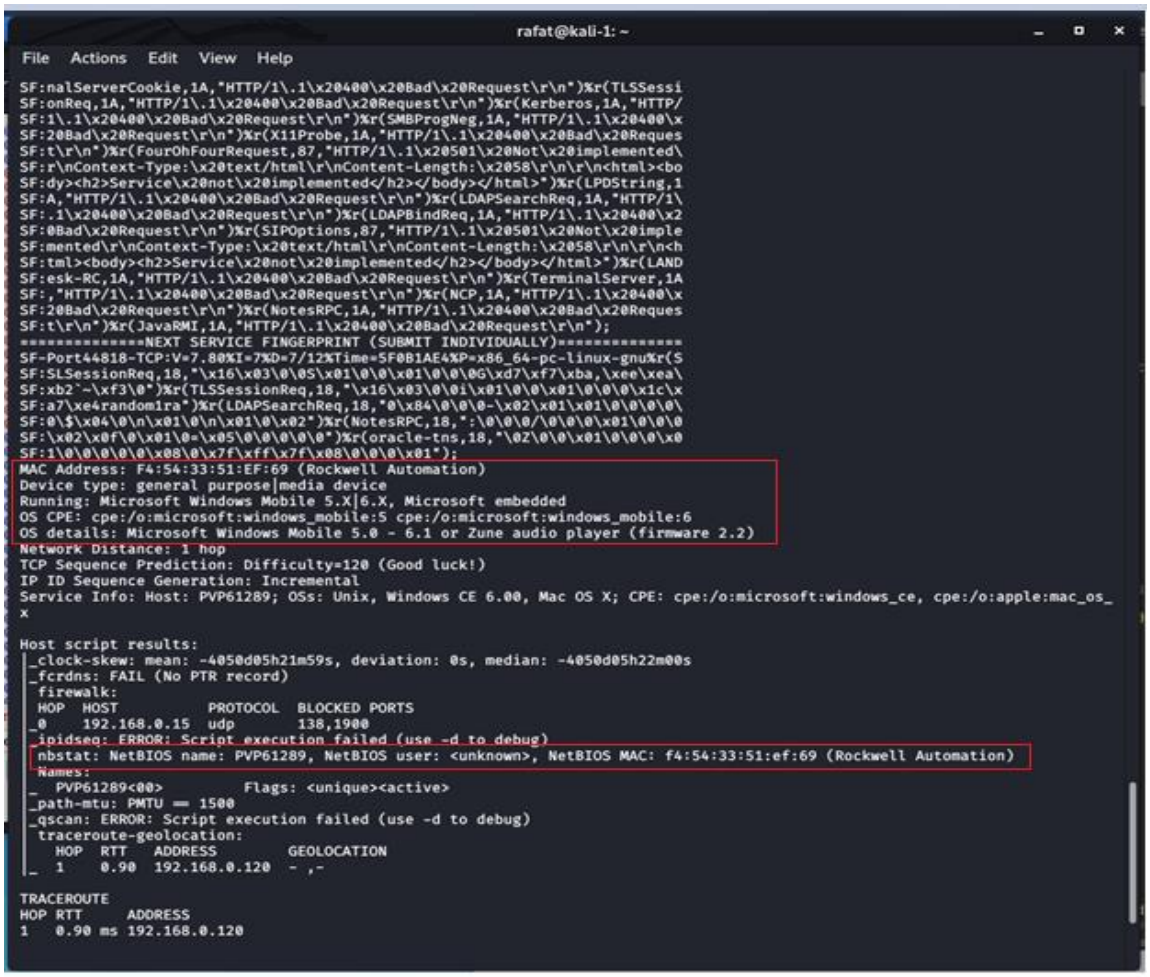
Slow comprehensive scan of HMI — Part 3



Slow comprehensive scan of HMI — Part 4



Slow comprehensive scan of HMI — Part 5



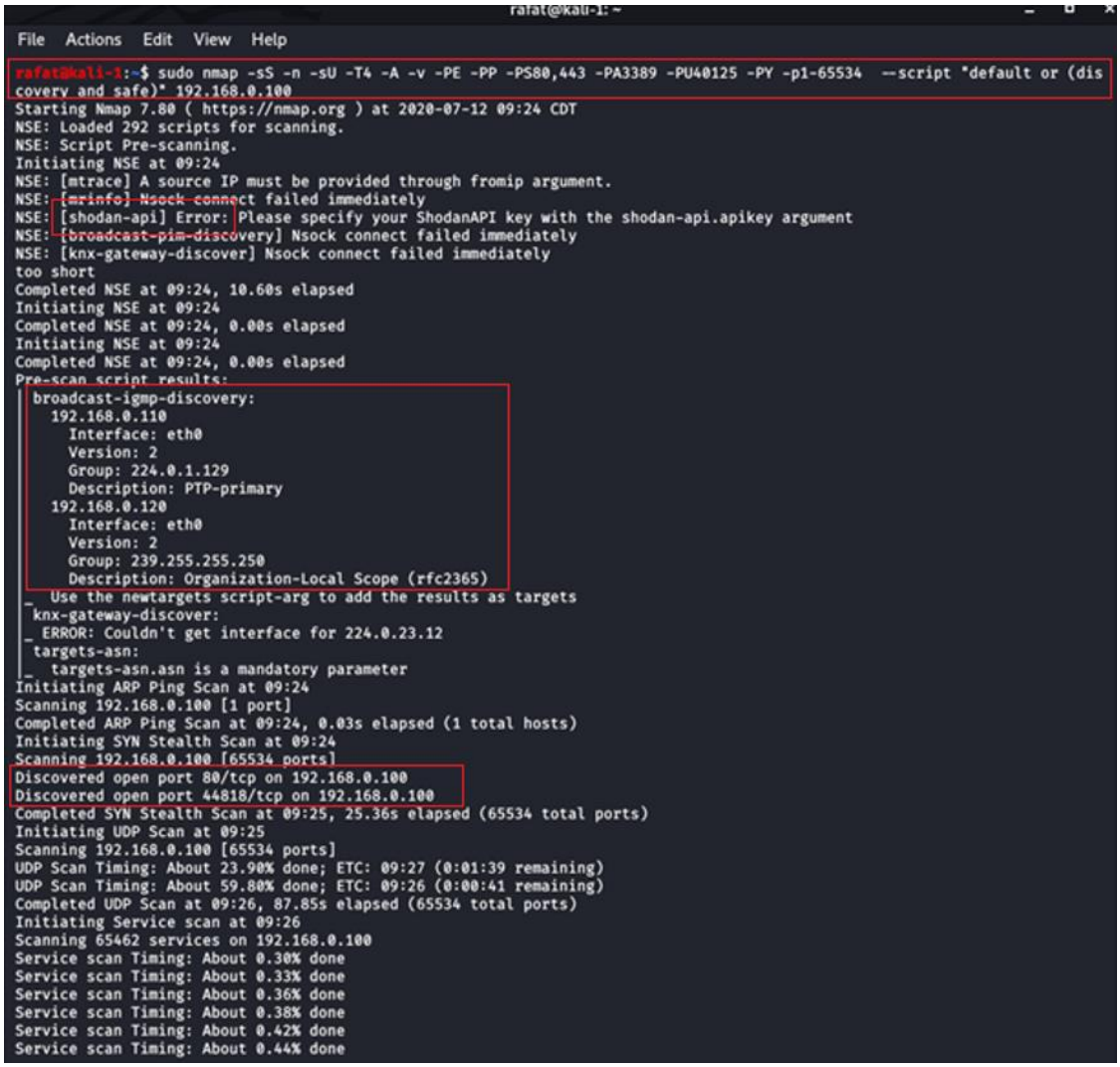
Slow comprehensive scan of HMI — Part 6

Slow comprehensive scan of HMI — Part 7

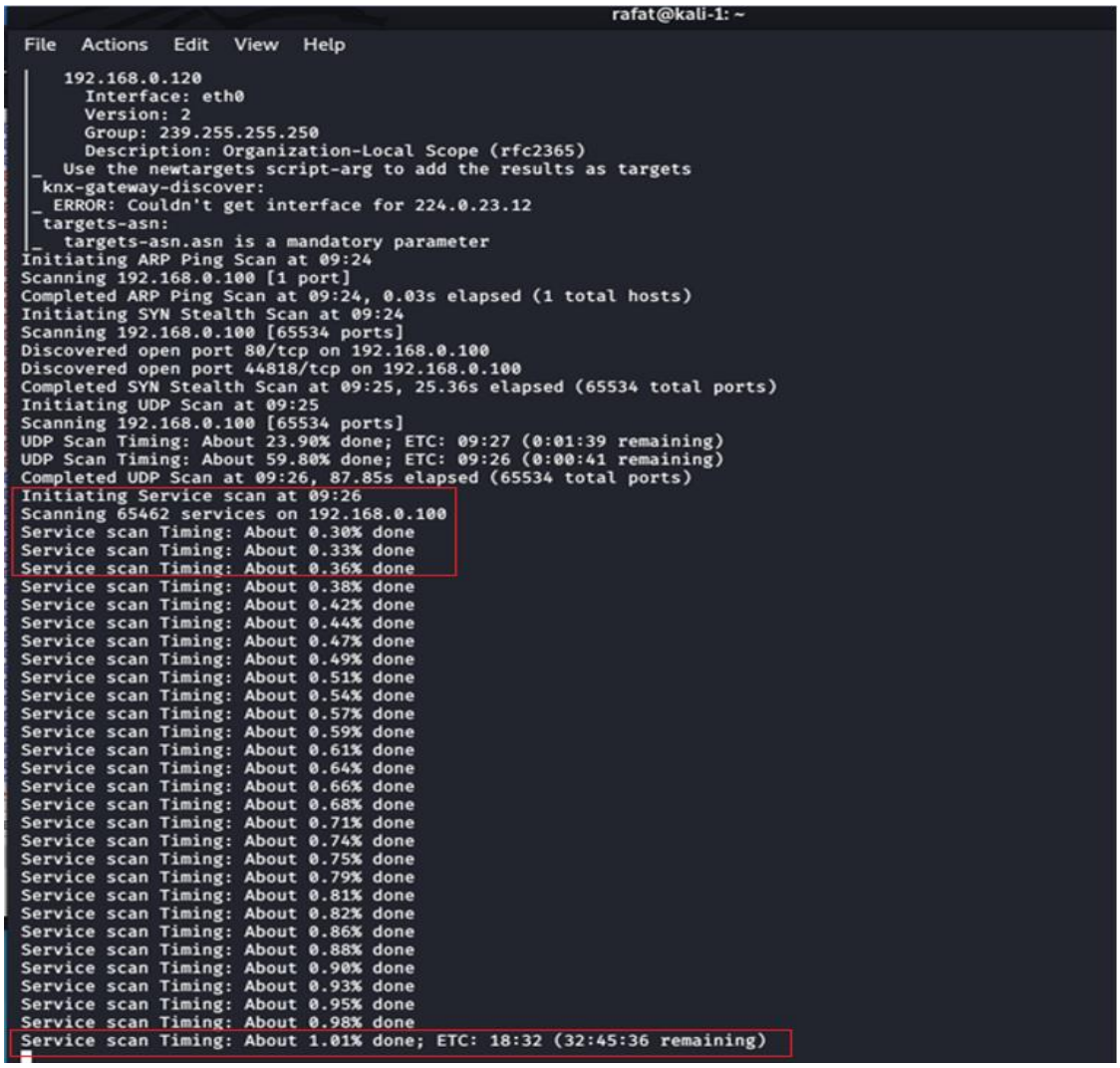
Results of slow comprehensive scan of the ABB drive:

Shows the Nmap intense scan command.

a. The ABB drive failed after about 9 seconds after starting the scan. We had to restart the motor manually using the HMI.



Slow comprehensive scan of ABB Drive — Part 1



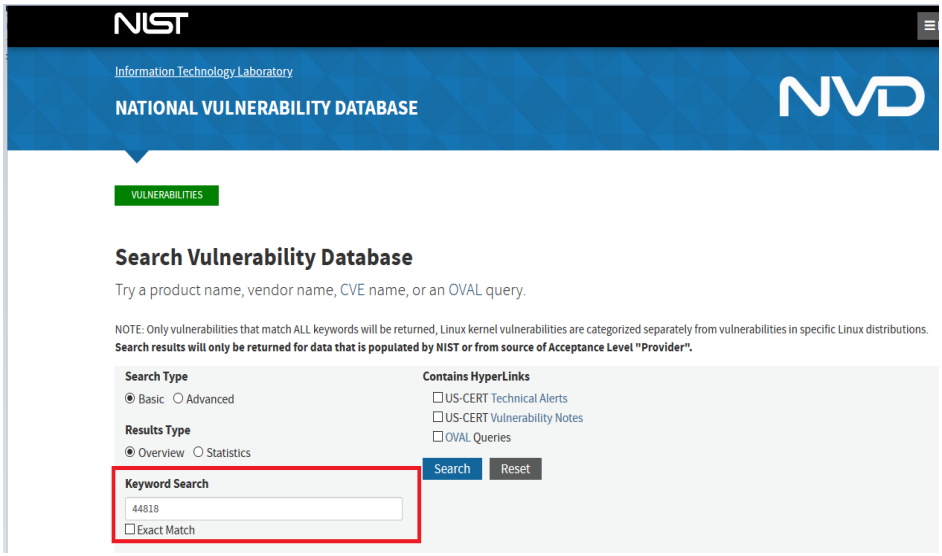
Slow comprehensive scan of ABB Drive — Part 2

Results of Searching for Vulnerability Using CVE Database

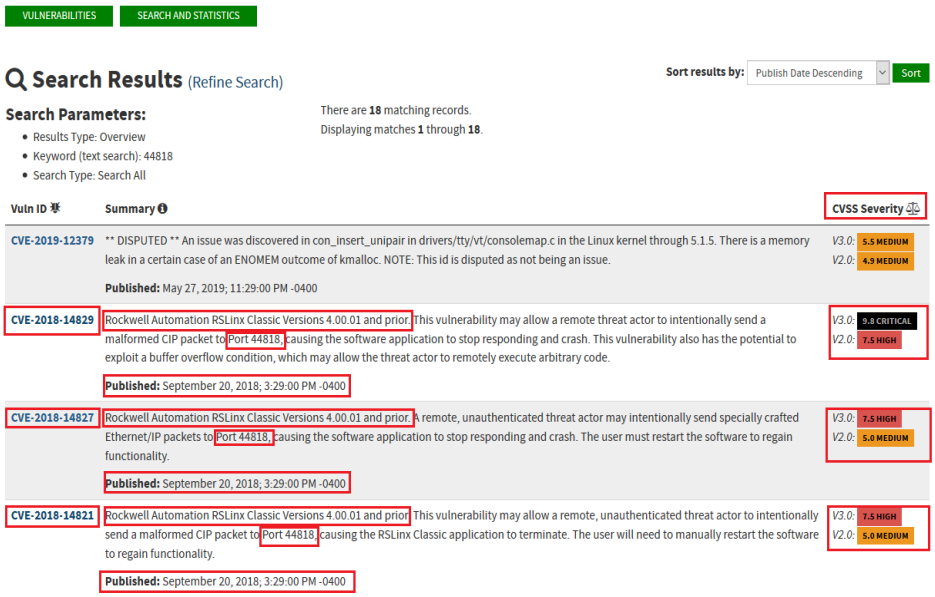
To search manually for vulnerability, we used the browser to connect to the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD)[41] and searched by port number, vendor, product, or any phrase.

As an example, we searched for port 44818, the port Ethernet/IP used to communicate with other ICS devices, as shown below. As a result of searching the database, we were able to retrieve the CVE ID, severity, date, the product and version of software, and the description and

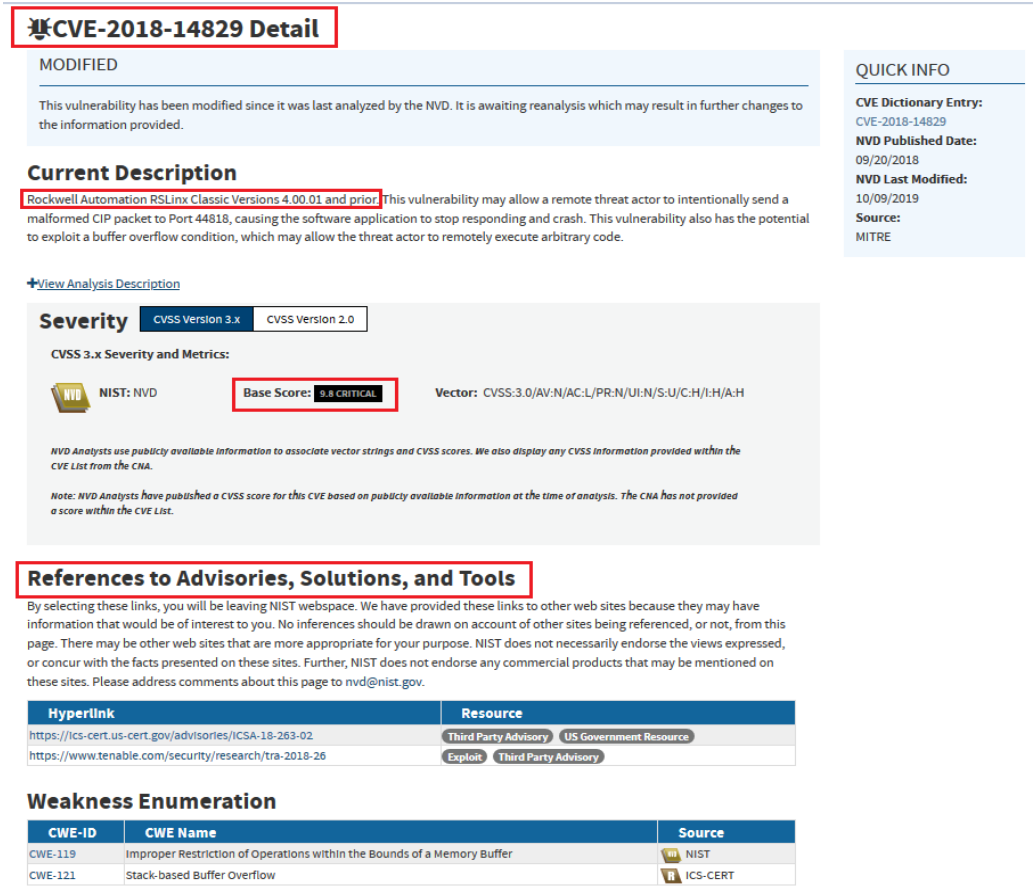
impact of the vulnerability. This is useful for companies so that they ensure that these vulnerabilities are secure; however, hackers can also use this as part of the reconnaissance phase to find out what weaknesses there are related to ICS.



NIST database to search for 44818 vulnerabilities — Part 1



NIST database to search for vulnerabilities — Part 2



CVE-2018-14829 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Rockwell Automation RSLinx Classic Versions 4.00.01 and prior This vulnerability may allow a remote threat actor to intentionally send a malformed CIP packet to Port 44818, causing the software application to stop responding and crash. This vulnerability also has the potential to exploit a buffer overflow condition, which may allow the threat actor to remotely execute arbitrary code.

+View Analysis Description

QUICK INFO

CVE Dictionary Entry: CVE-2018-14829
NVD Published Date: 09/20/2018
NVD Last Modified: 10/09/2019
Source: MITRE

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://ics-cert.us-cert.gov/advisories/ICSA-18-263-02	Third Party Advisory, US Government Resource
https://www.tenable.com/security/research/tra-2018-26	Exploit, Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	NIST
CWE-121	Stack-based Buffer Overflow	ICS-CERT

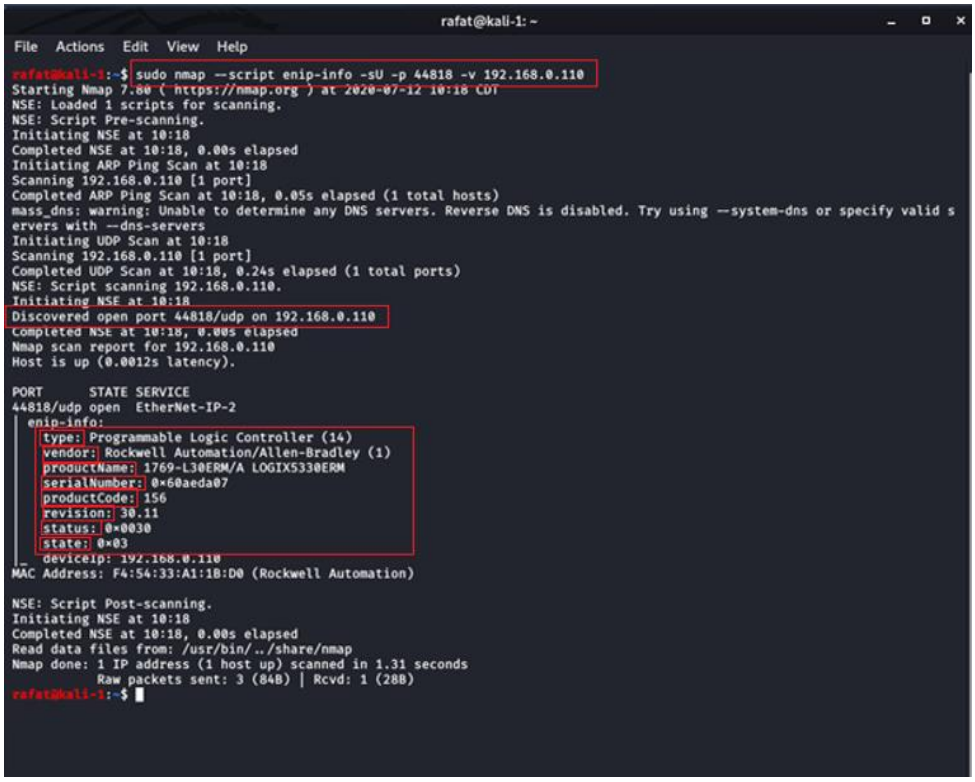
NIST database to search for vulnerabilities — Part 3

Results of Searching for Hardware Information

Results of hardware information scan of the PLC:

a. Shows the Nmap intense scan command.

b. Using port 44818 (Ethernet/IP) and Ethernet/IP script, the scan was able to identify hardware and software information regarding the PLC, such as the type of device, vendor, product name, serial number, product code, revision, status, and state. This is considered very valuable information in the penetration testing reconnaissance phase.

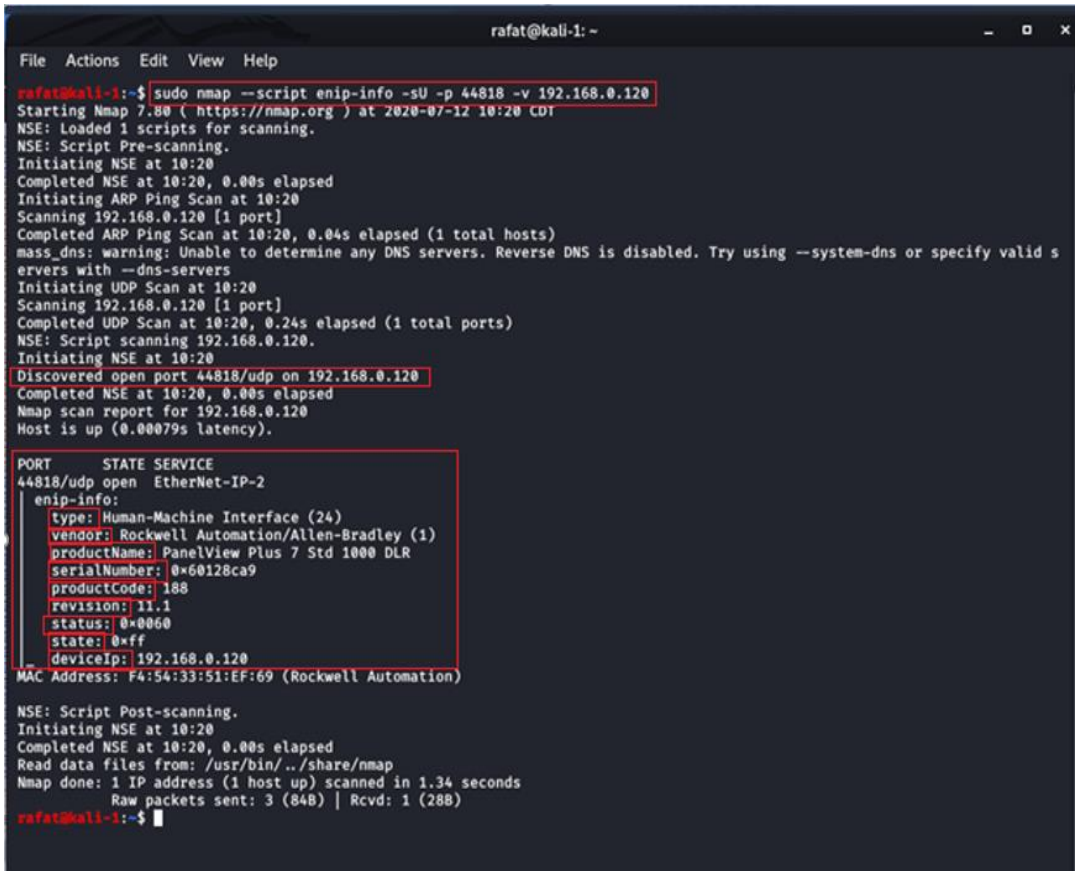


PLC hardware info

Results of hardware information scan of the HMI**:**

a. Shows the Nmap intense scan command.

b. Using port 44818 (Ethernet/IP) and Ethernet/IP script, the scan was able to identify hardware and software information regarding the HMI such as the type of device, vendor, product name, serial number, product code, revision, status, and state. This is considered very valuable information in the penetration testing reconnaissance phase.

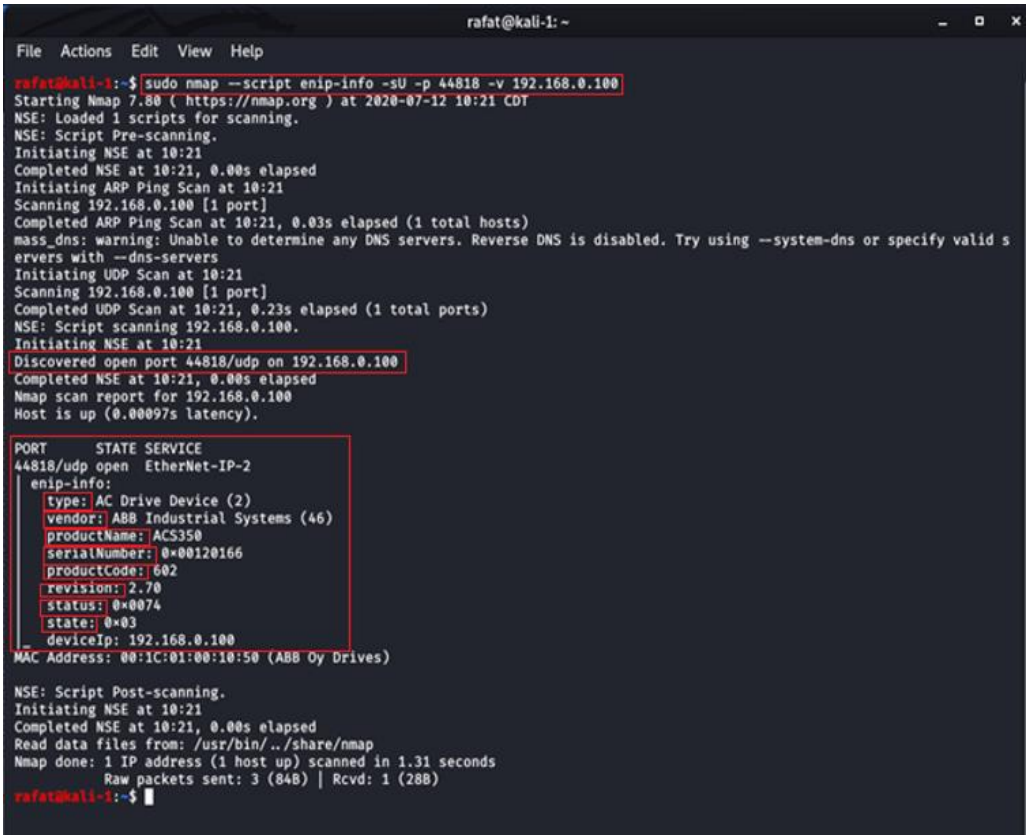


Hardware info for HMI

Results of hardware information scan of the ABB drive:

a. Shows the Nmap intense scan command.

b. Using port 44818 (Ethernet/IP) and Ethernet/IP script, the scan was able to identify hardware and software information regarding the ABB drive such as the type of device, vendor, product name, serial number, product code, revision, status, and state. This is considered very valuable information in the penetration testing reconnaissance phase.



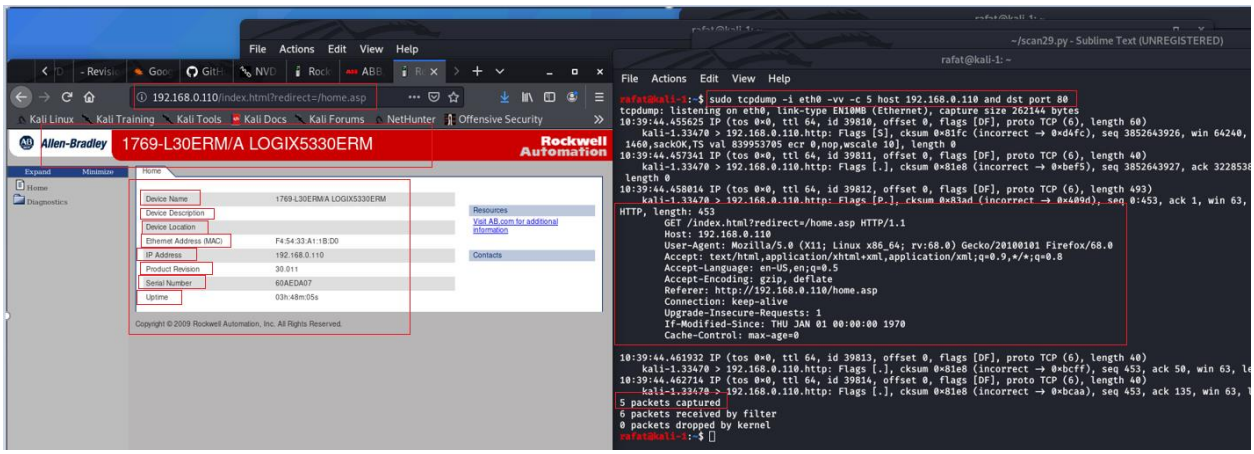
Hardware information for ABB drive

Results of Captured Traffic

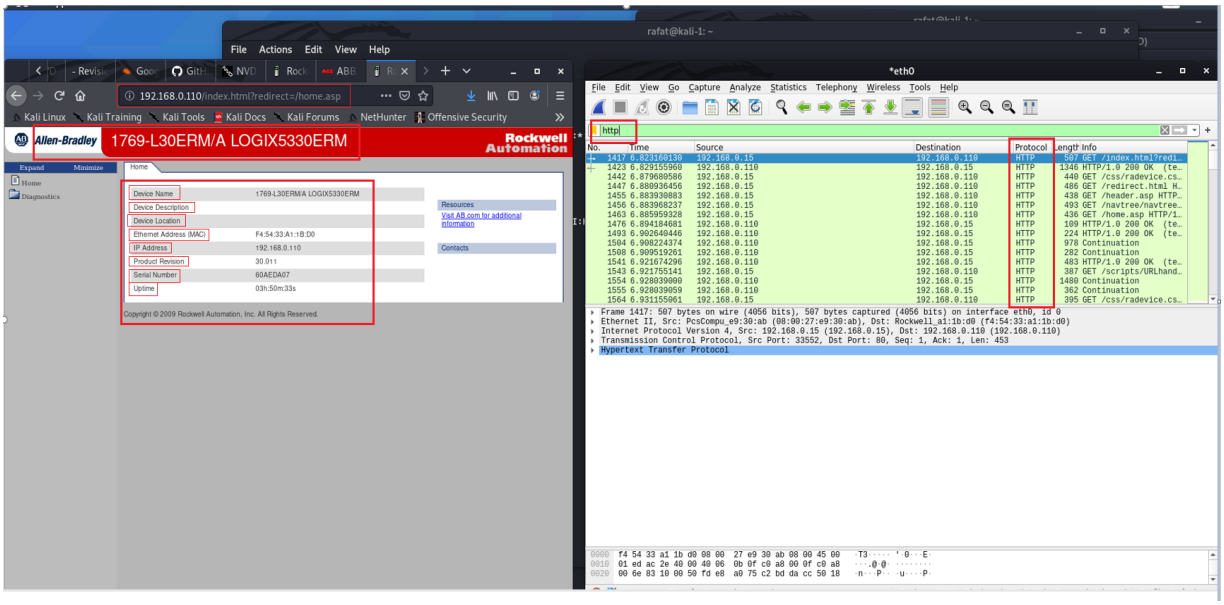
To capture traffic, we used Tcpdump, Tshark, and Wireshark.

Results of capturing traffic of the PLC:

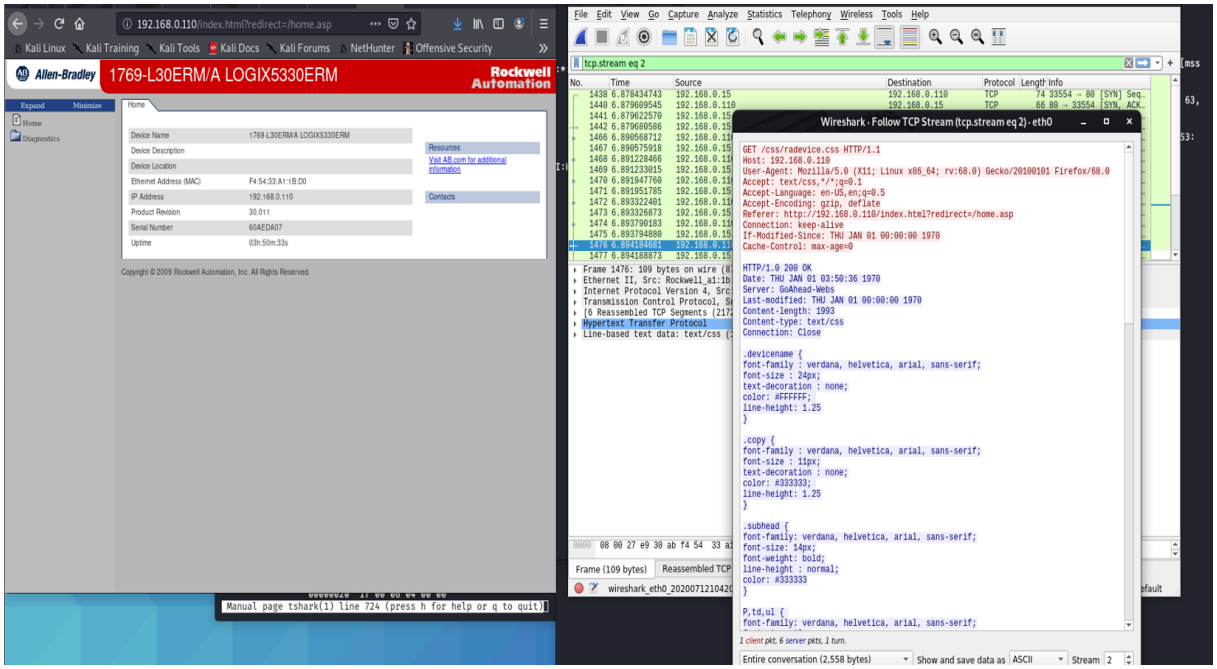
Since the traffic is completely in clear text, we were able to capture any information that was sent on the wire, from device name and serial number to CIP communications. This means capture and replay or man-in-the-middle attack can be done easily.



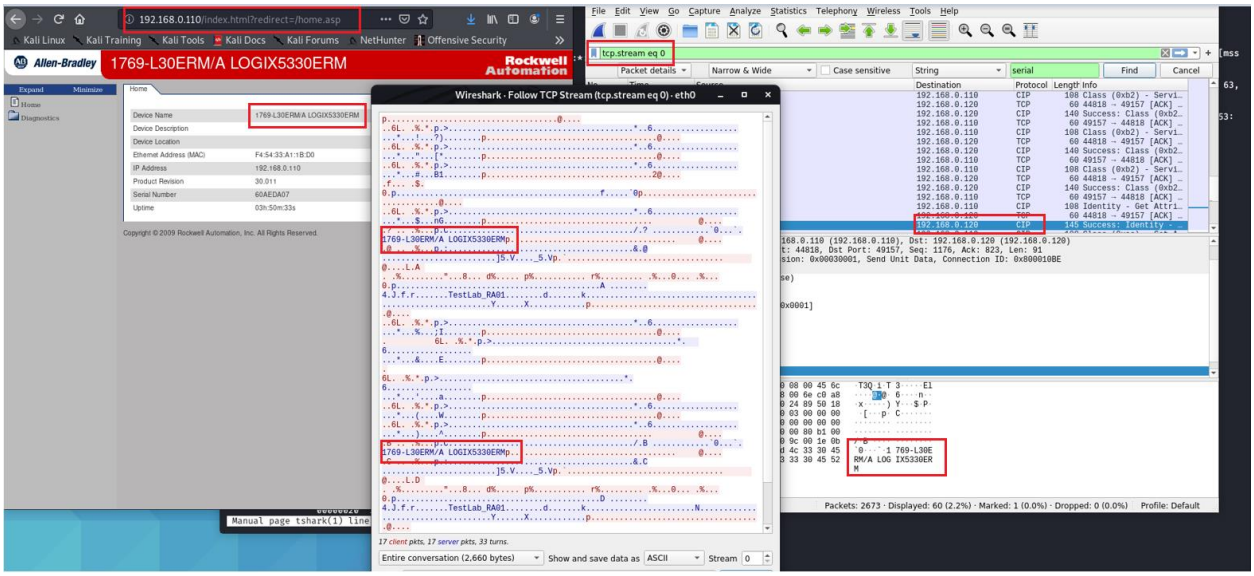
Capturing PLC home page using Tcpdump



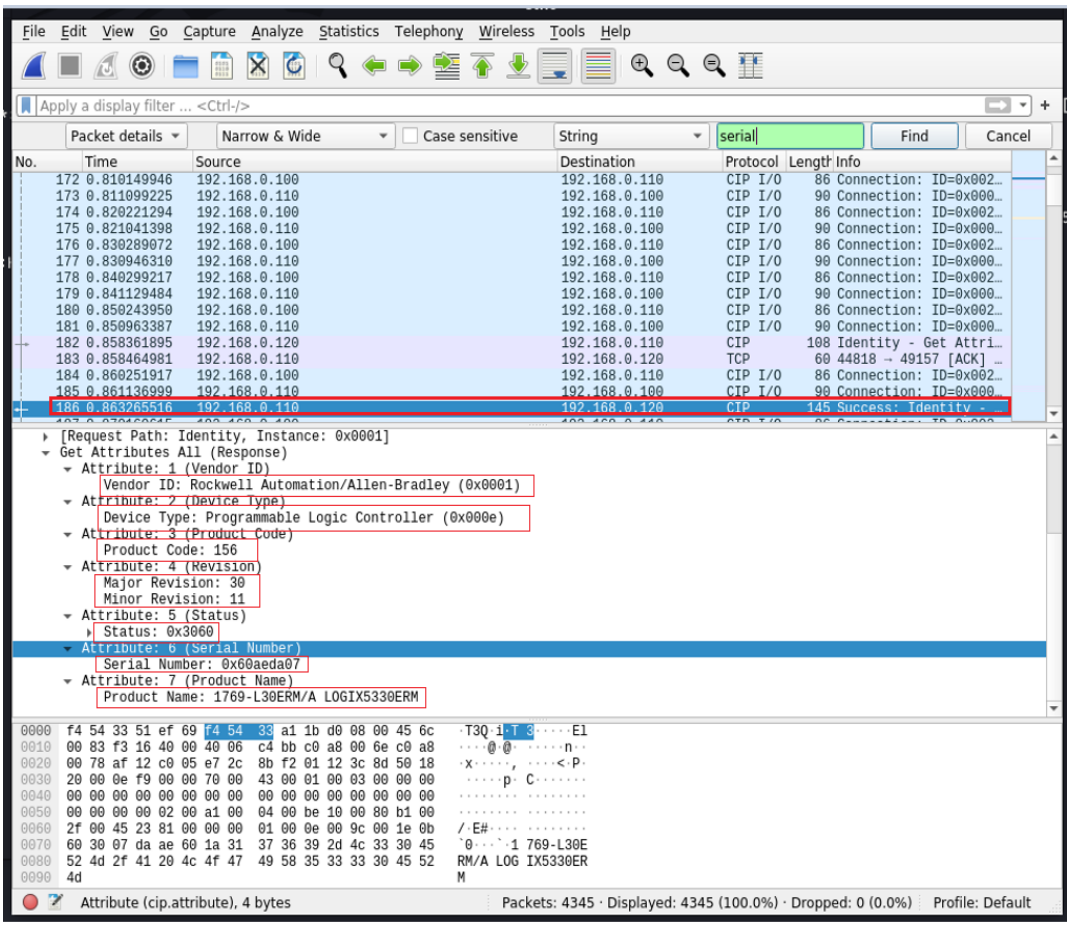
Capturing PLC home page using Wireshark with HTTP filter



Display unencrypted traffic using Wireshark



Capturing machine name in clear text using Wireshark



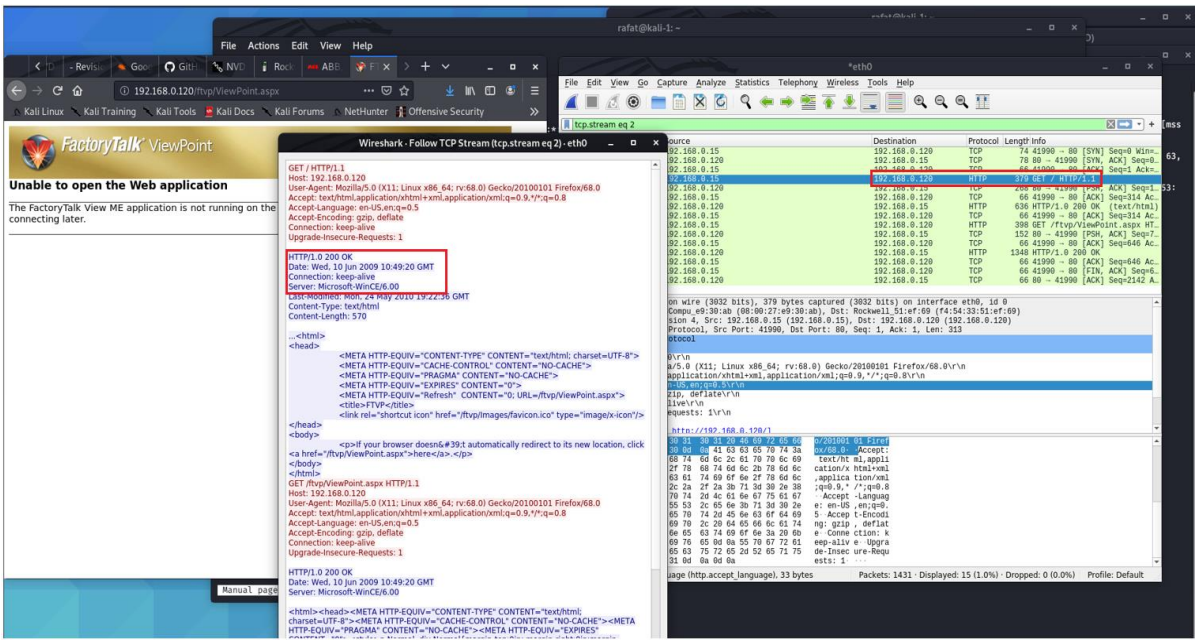
Capturing machine information using Wireshark in clear text

Results of capturing traffic of the HMI**:**

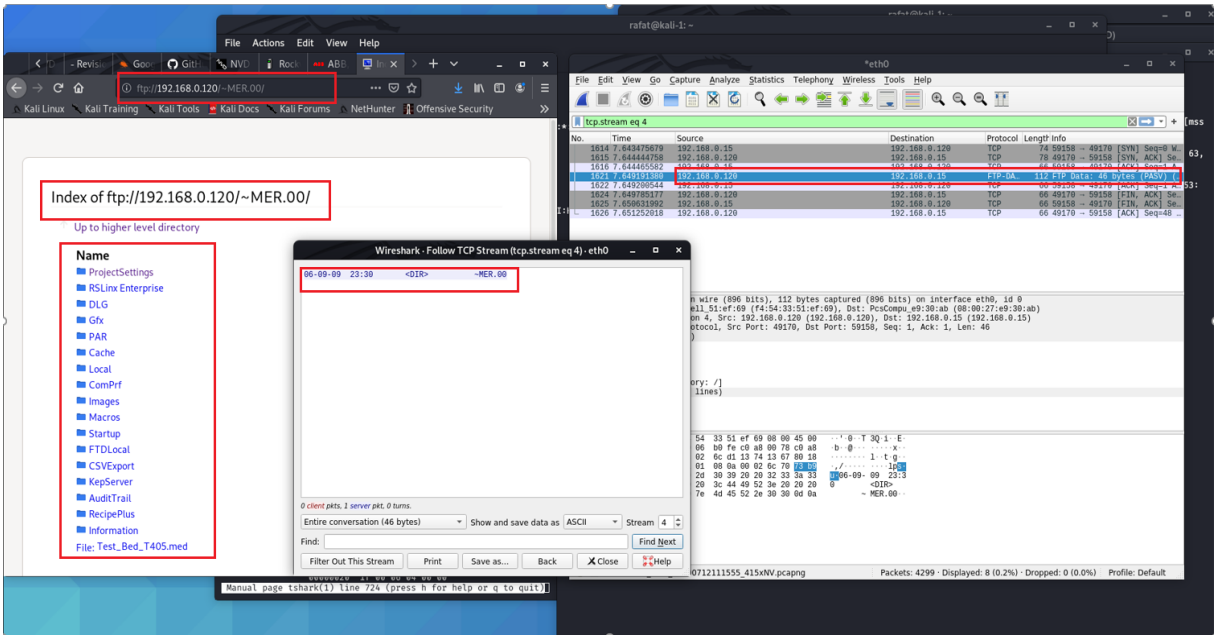
a. Capturing clear traffic from HTTP.

b. Capturing clear traffic form FTP.

c. Capturing hardware information in clear text using Wireshark.



Capturing http traffic in clear text for HMI



List of the files in the FTP directory MER.00 using anonymous log in

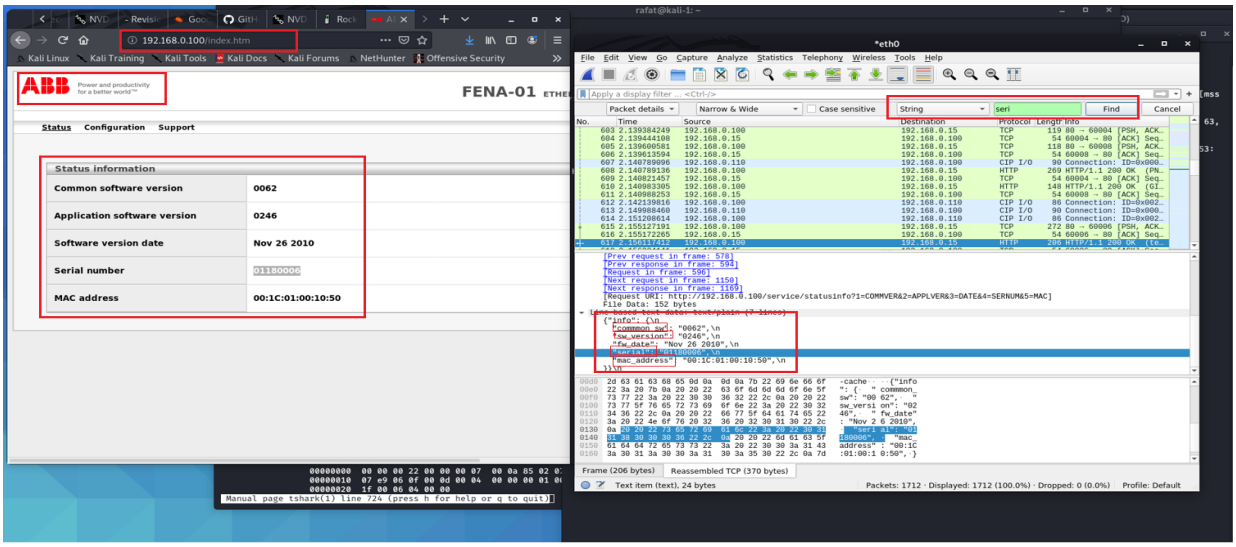
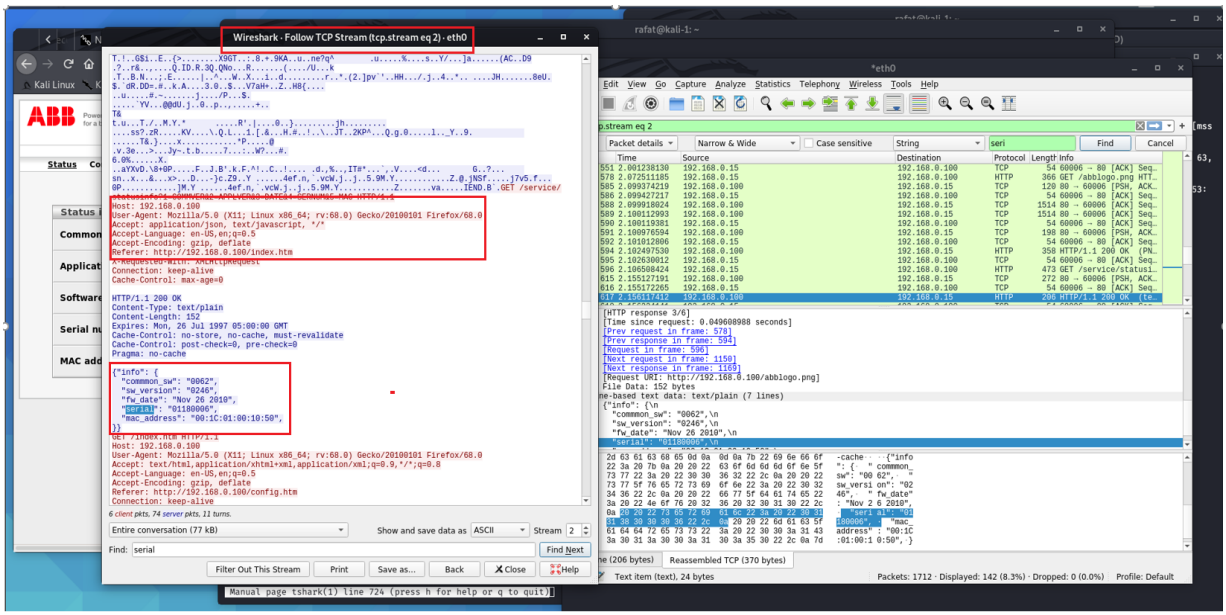


ABB drive clear text using http

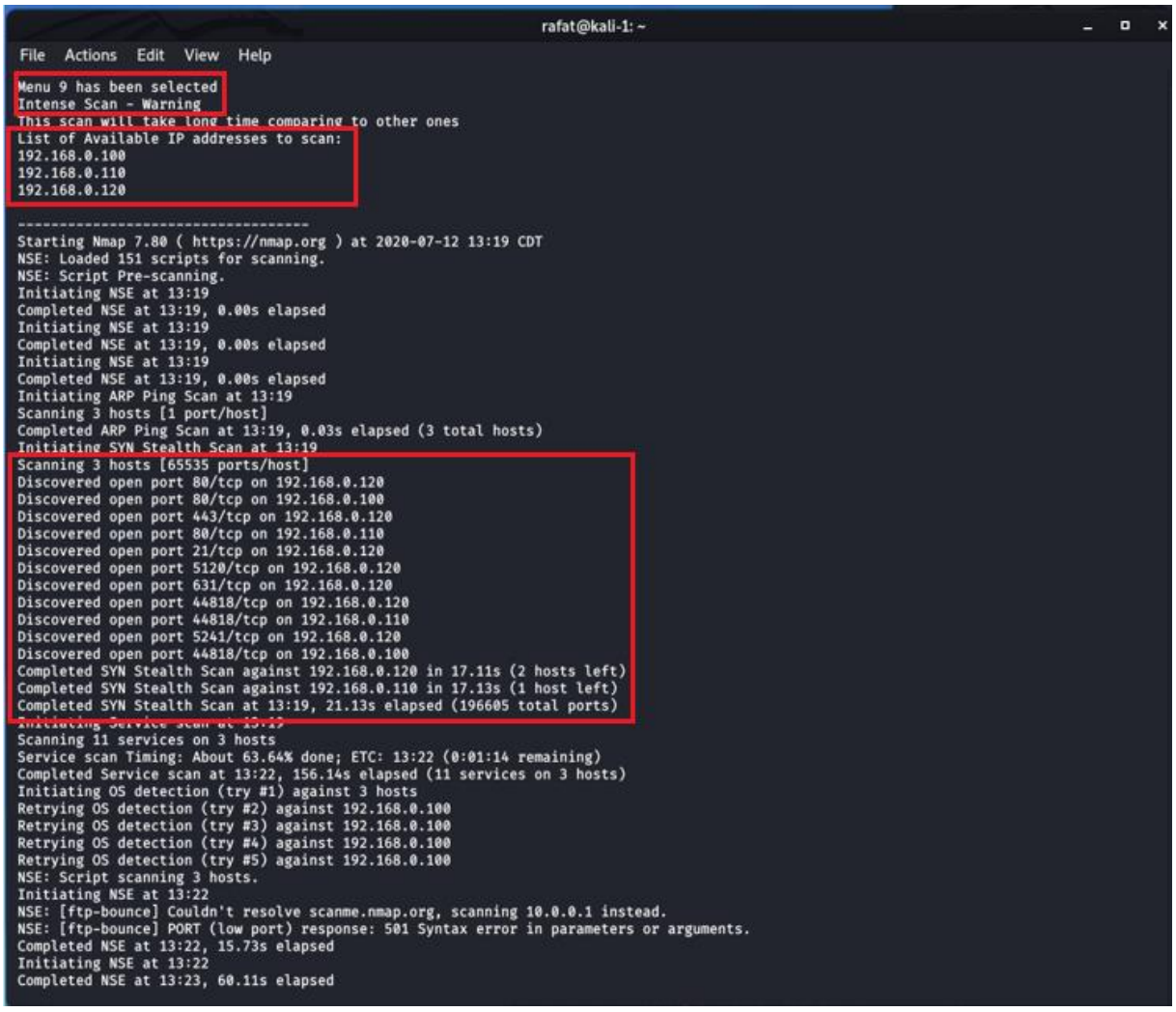


Clear text of device information using Wireshark TCP stream

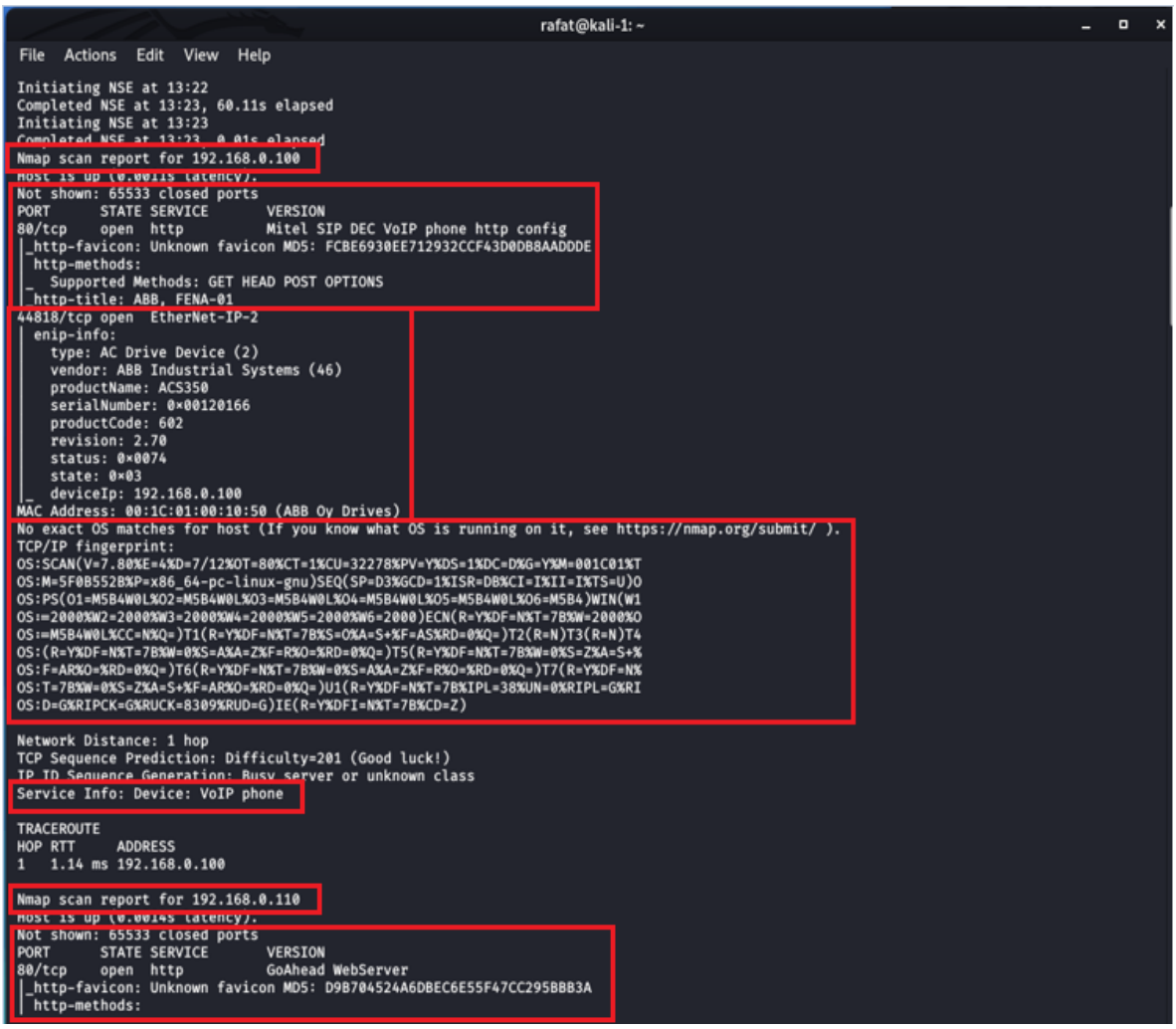
Appendix C: Output of Automated Penetration Testing

Option 9: Perform Intense Scan — Warning

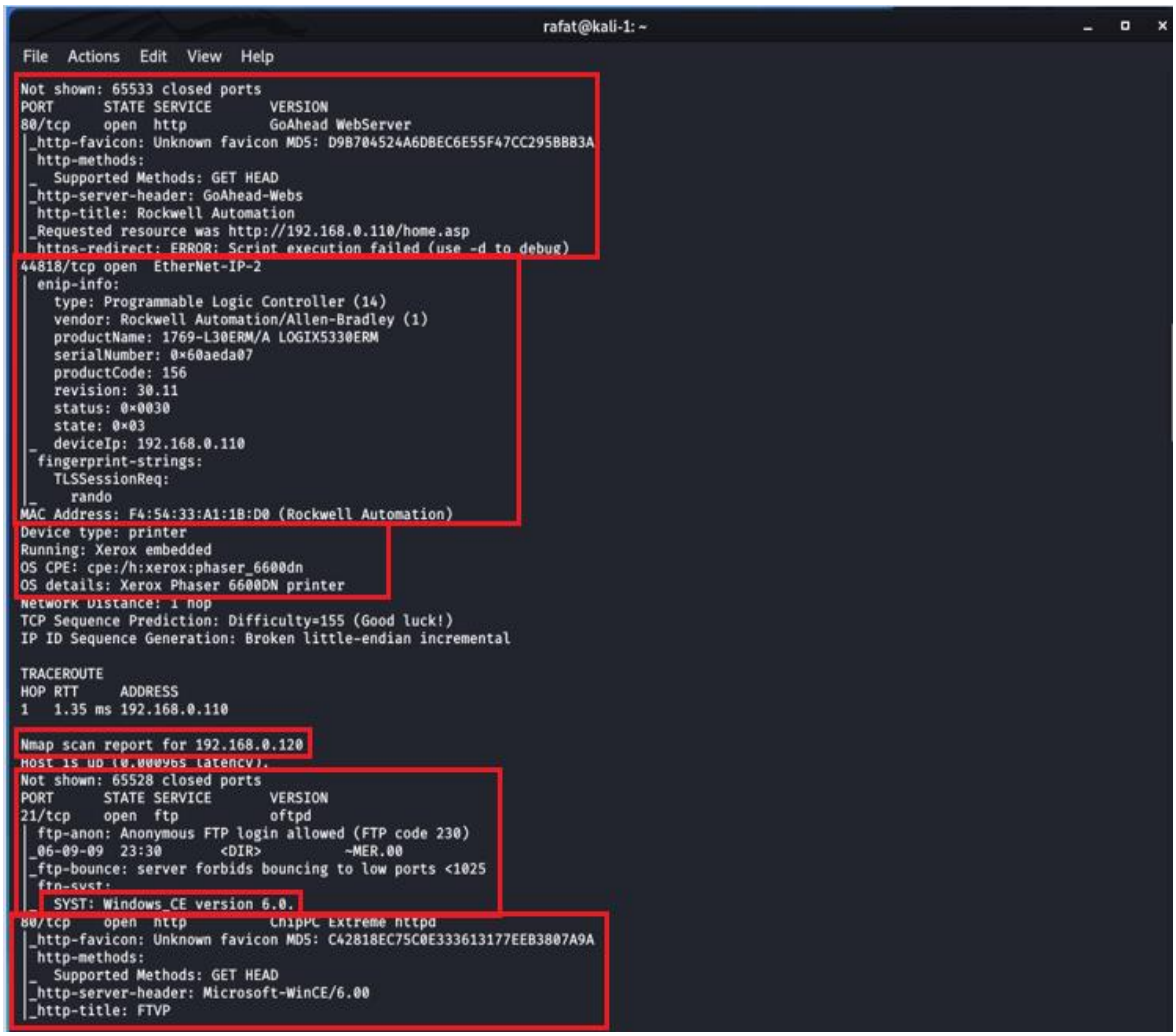
In selecting option 9 for the intense scan, the ABB drive stopped and gave an error fault 28. We had to reset the drive manually and restart using the HMI. After waiting for extra time, the scan went through, with the following results:



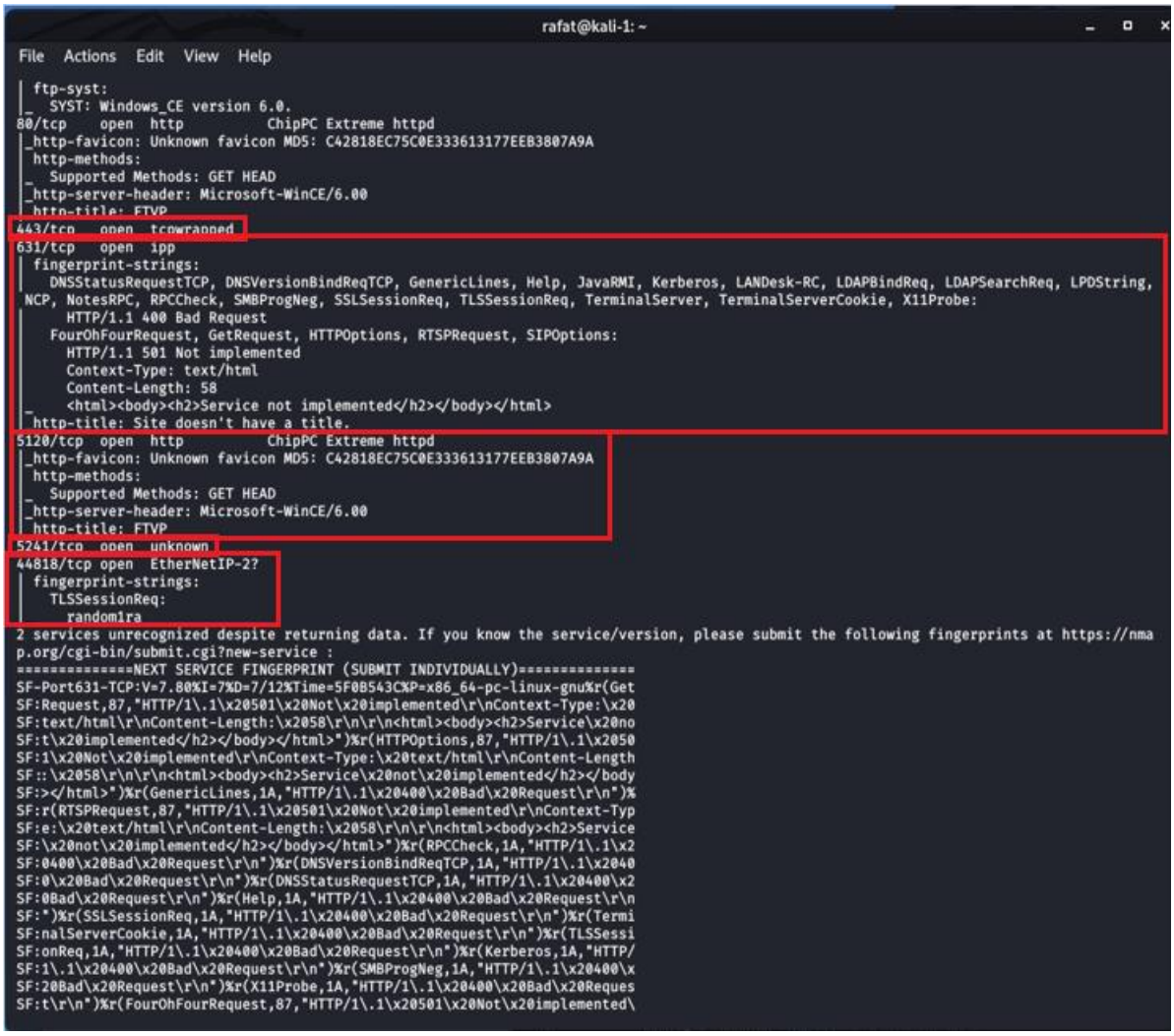
Option 9: Intense scan — Part 1



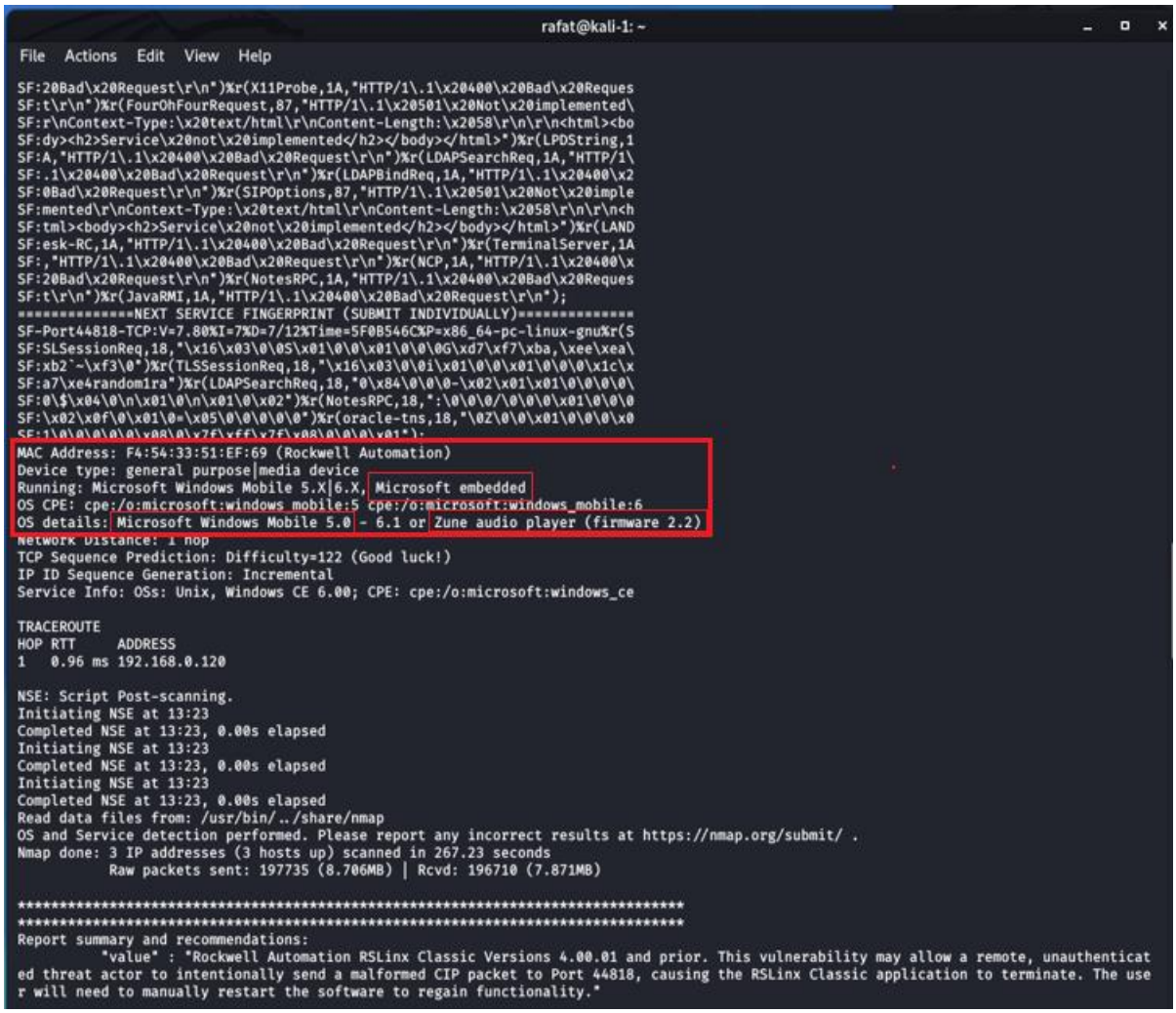
Option 9: Intense scan — Part 2



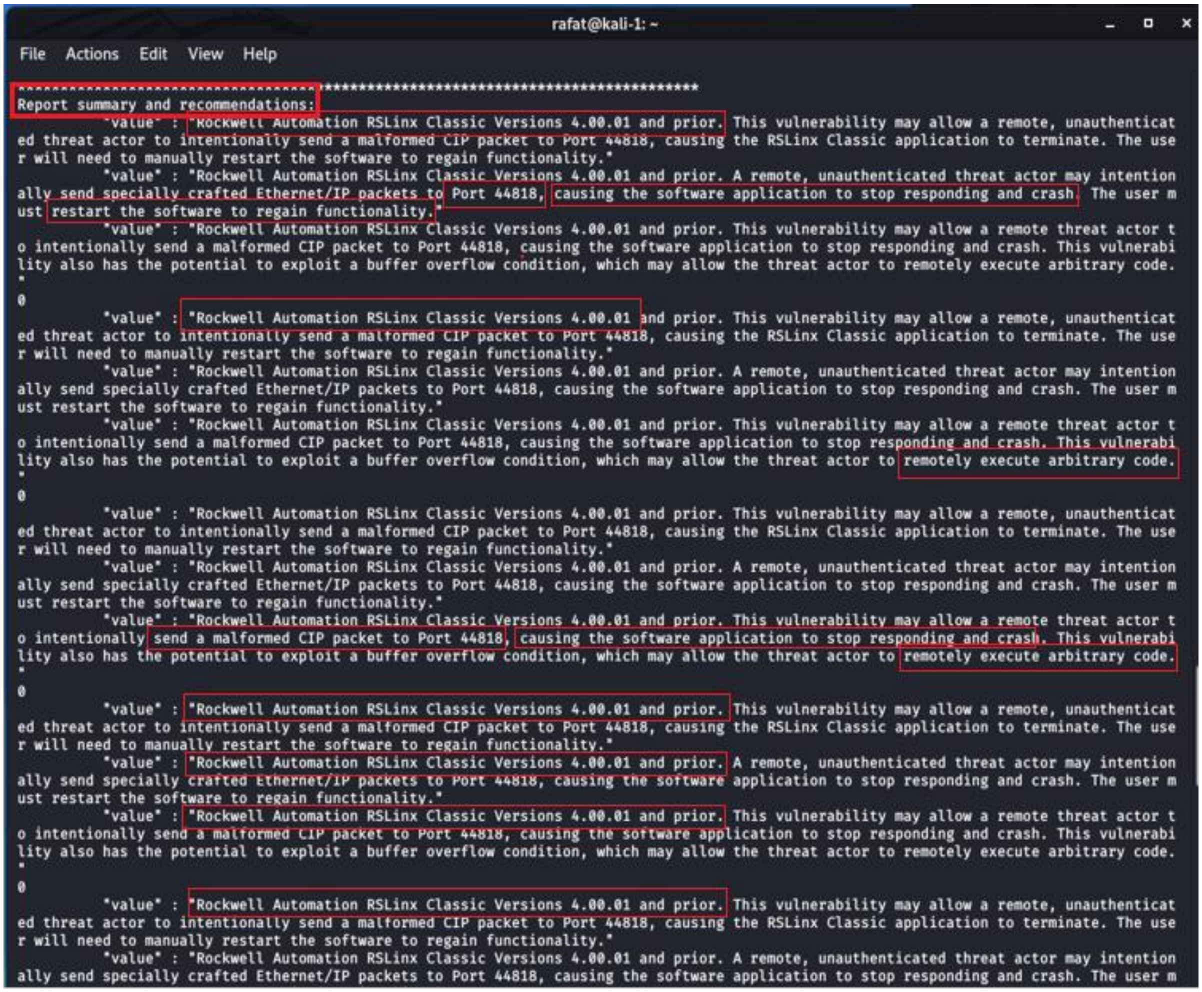
Option 9: Intense scan — Part 3



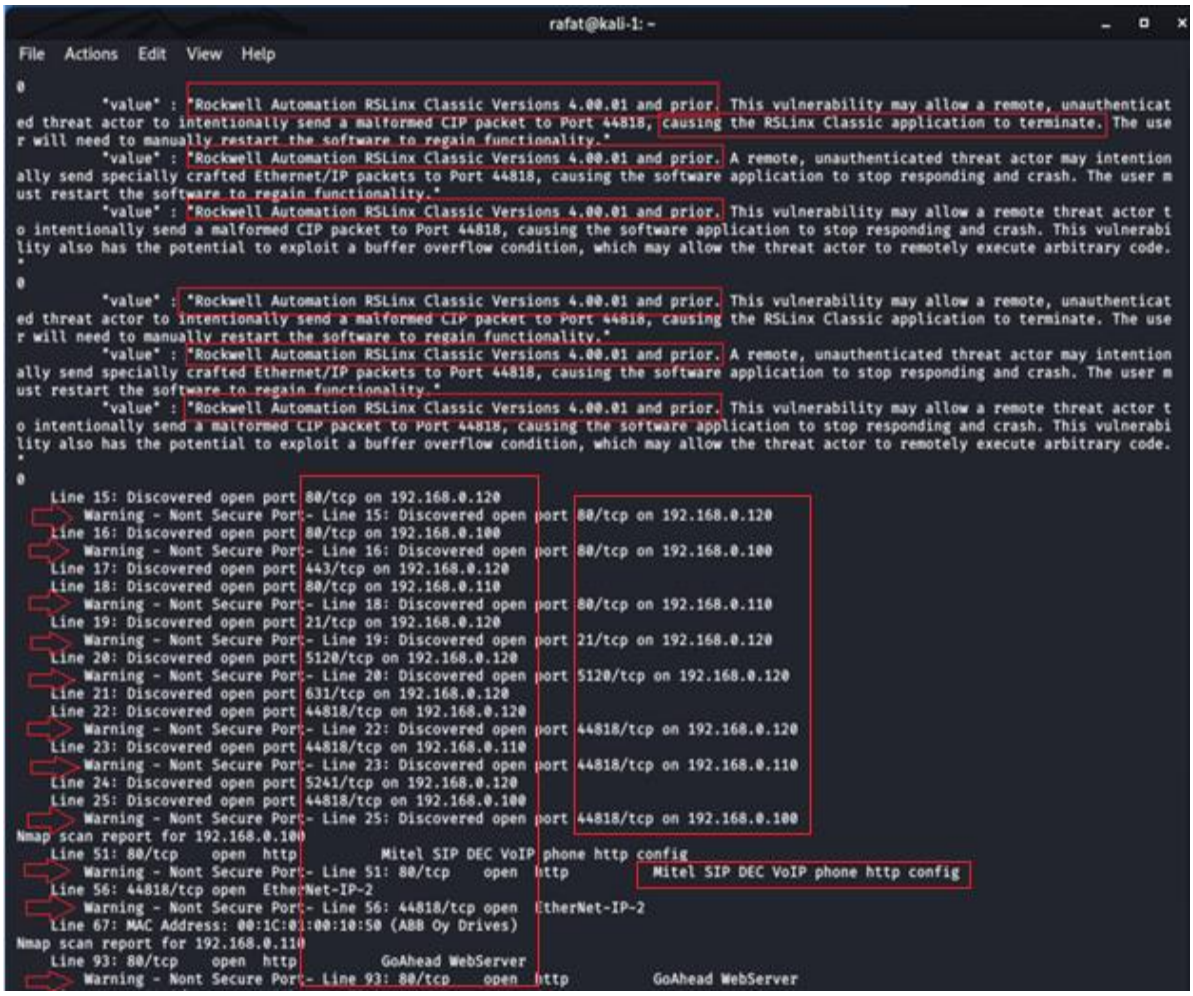
Option 9: Intense scan — Part4



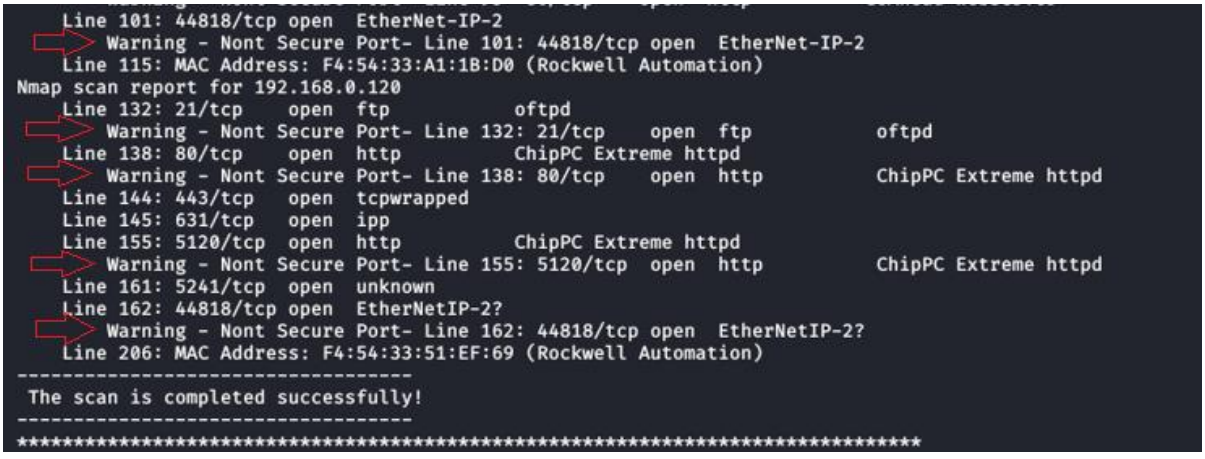
Option 9: Intense scan with a summary report and recommendation — Part 6



Option 9: Intense scan recommendation and CVE results — Part 7



Option 9: Intense scan recommendation and warning — Part 8

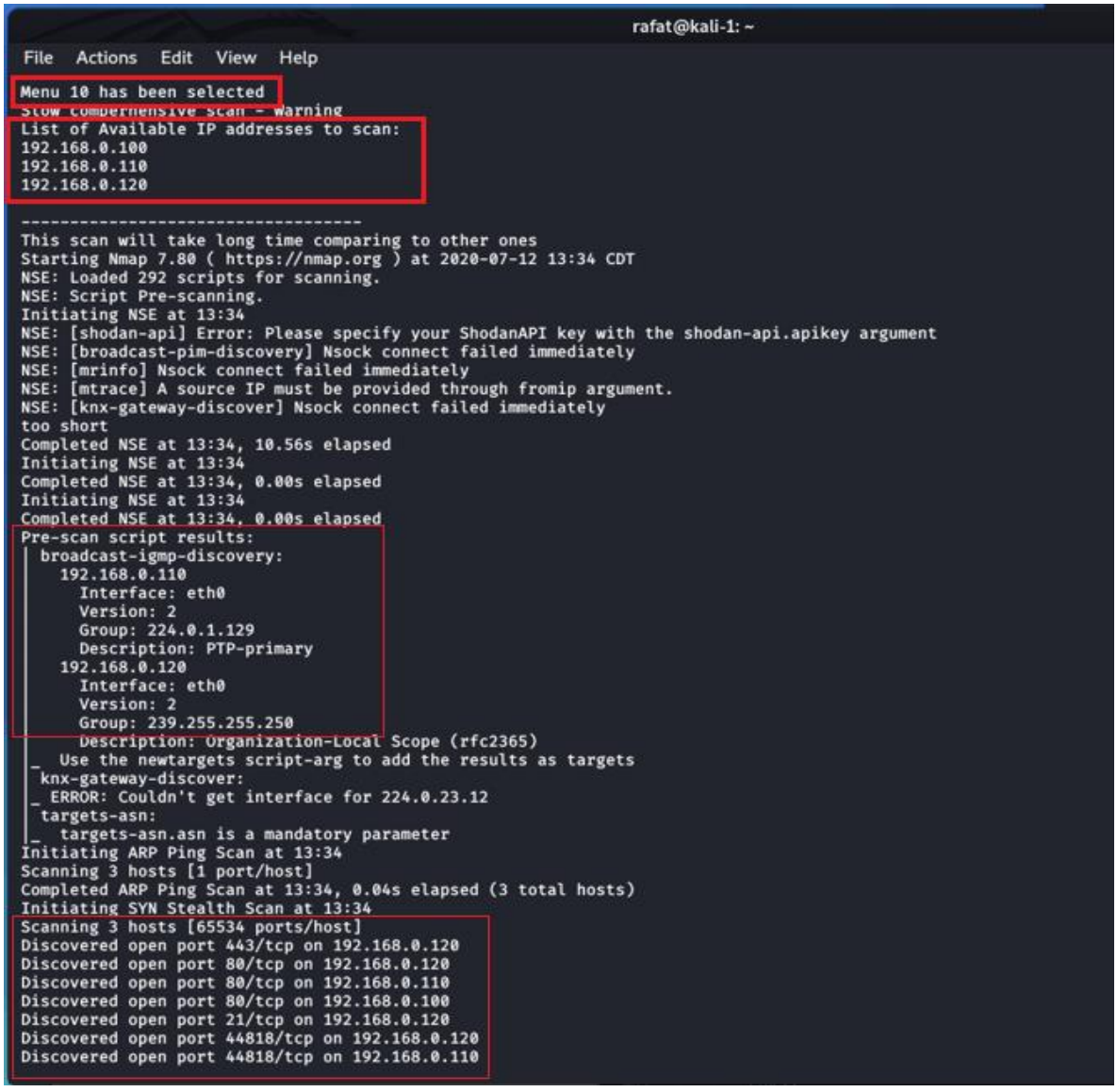


Option 9: Intense scan recommendation and warning — Part 9

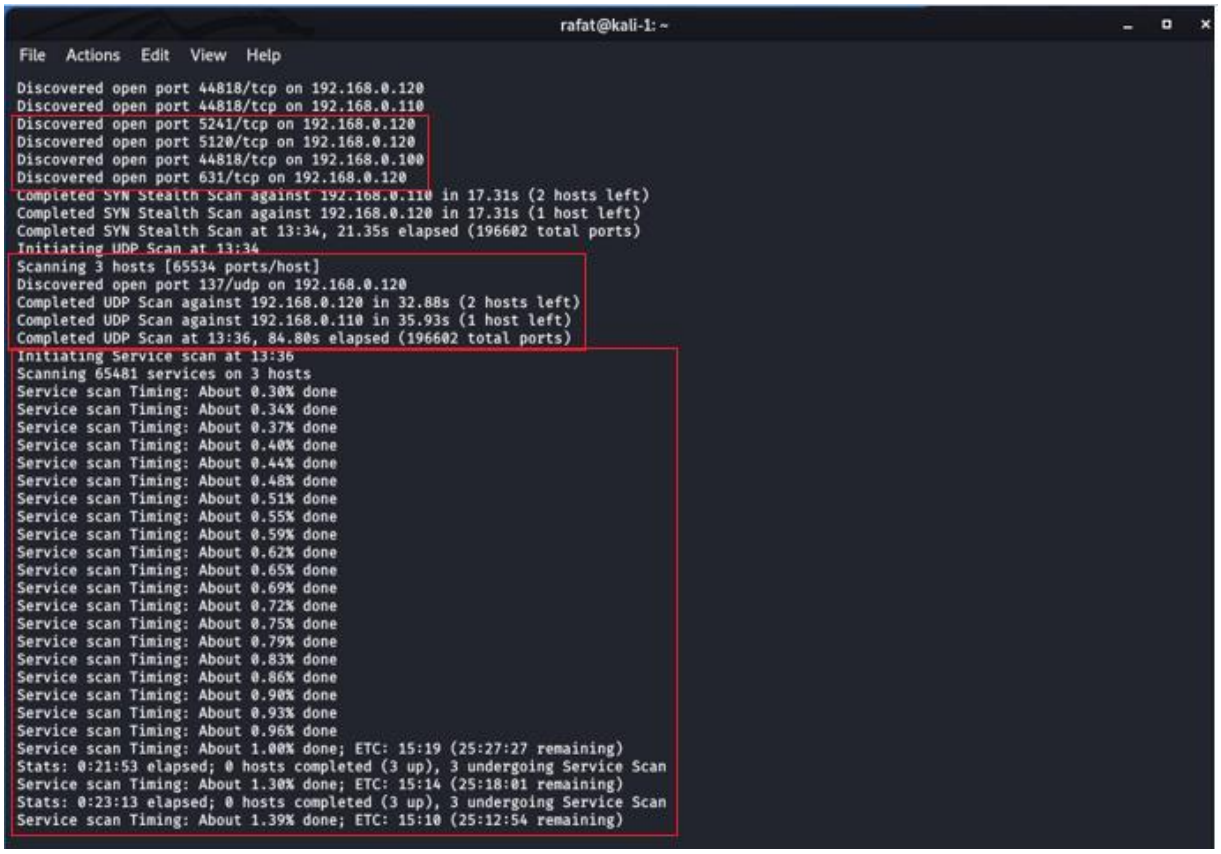
Output: Drive failed, fault 28, serial 1 error, the motor stopped, and the operation was interrupted.

Option 10: Perform Slow Comprehensive Scan — Warning

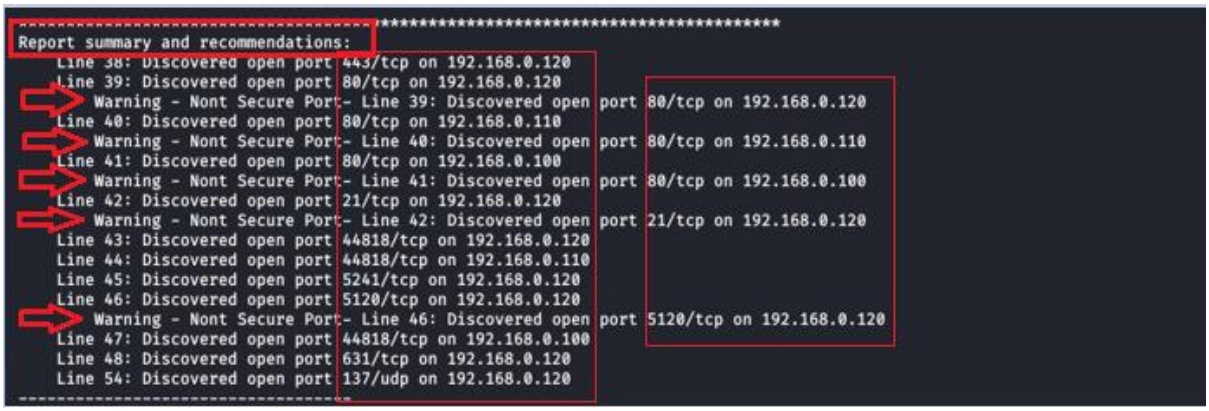
Results from this scan as shown below



Option 10: Slow comprehensive scan — Part 1



Option 10: Slow comprehensive scan — Part 2

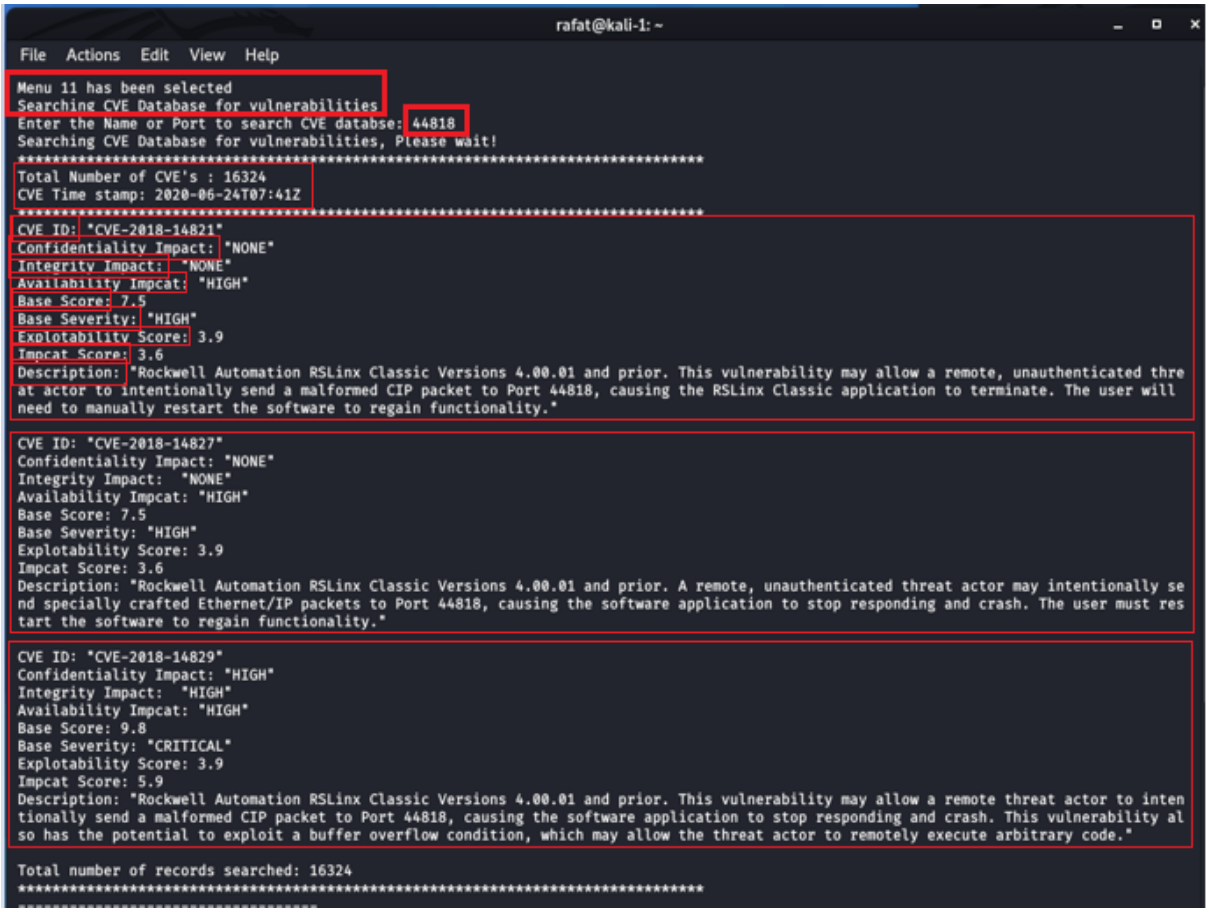


Option 10 slow comprehensive scan — Part 3

Option 11: Search CVE Database for Vulnerabilities

A local copy of the NIST database in JavaScript Object Notation (JSON) format was downloaded locally. The program is designed to search for any vulnerability in that database using any word, number, or string. The program is designed to search the database for any vulnerabilities related to our search selection and extract the eight fields listed below regarding the vulnerability and print the results for port 44818.

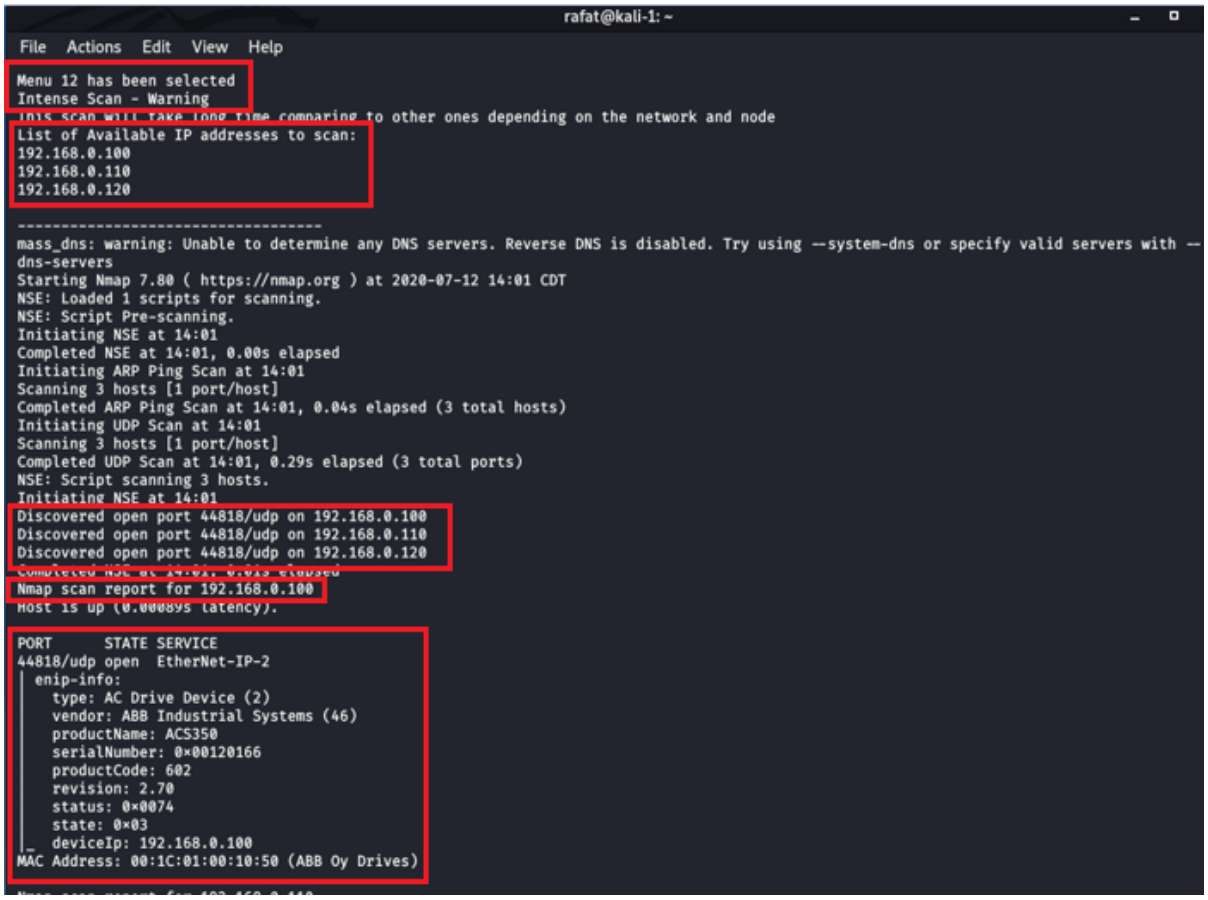
1. Confidentiality
2. Integrity
3. Availability
4. Base score
5. Base server
6. Impact score
7. Description



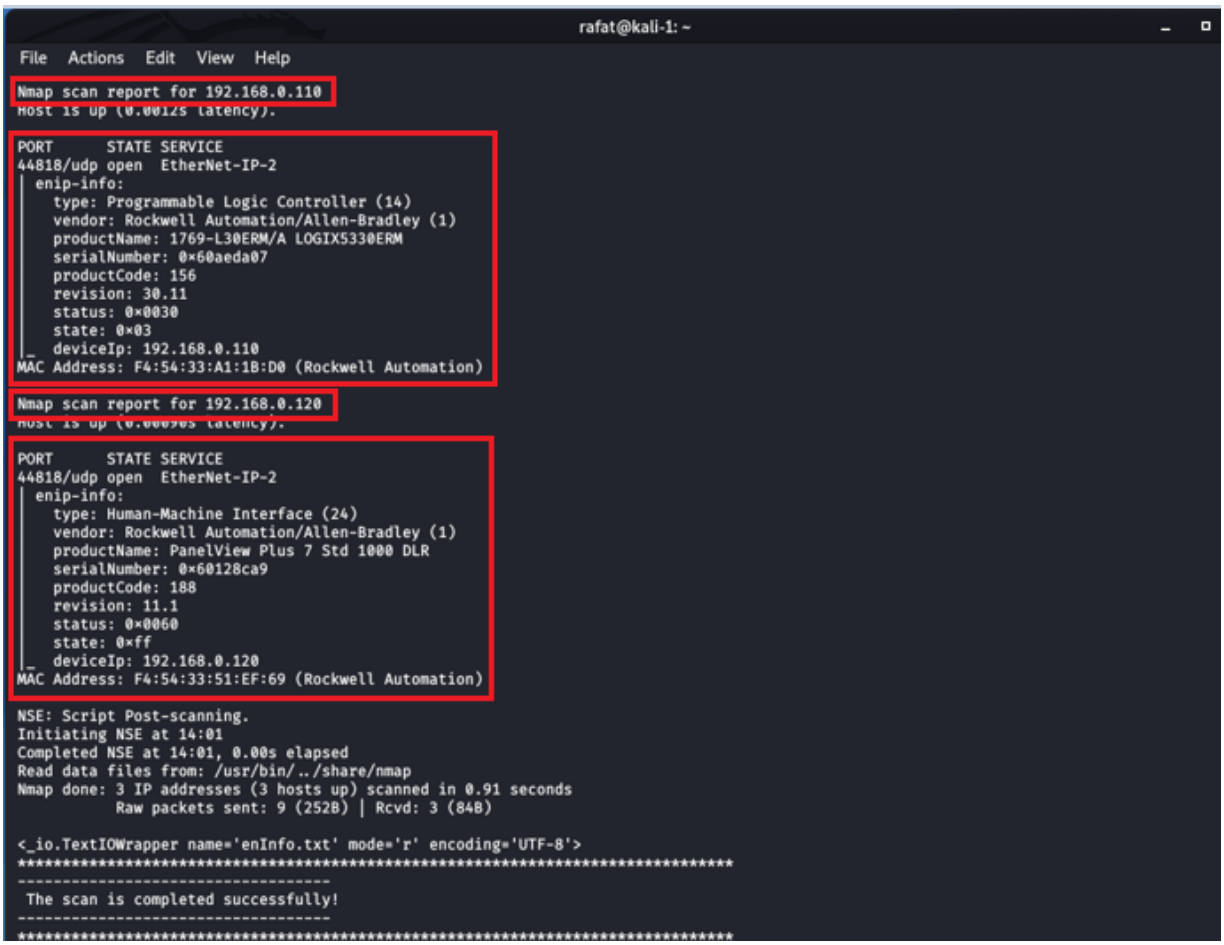
Option 11: CVE database search

Options 12 and 13: Hardware Information

Option 12 gives us the option of selecting a specific node, where option 13 gives search information for all connected ICS devices. The program uses Nmap, port 44818 (Ethernet/IP), and a Nmap script to scan ICS devices and retrieve hardware and software information. An example of this information is type of device, vendor, product name, serial number, product code, revision, status, and state. This is considered very valuable information in the penetration testing reconnaissance phase.



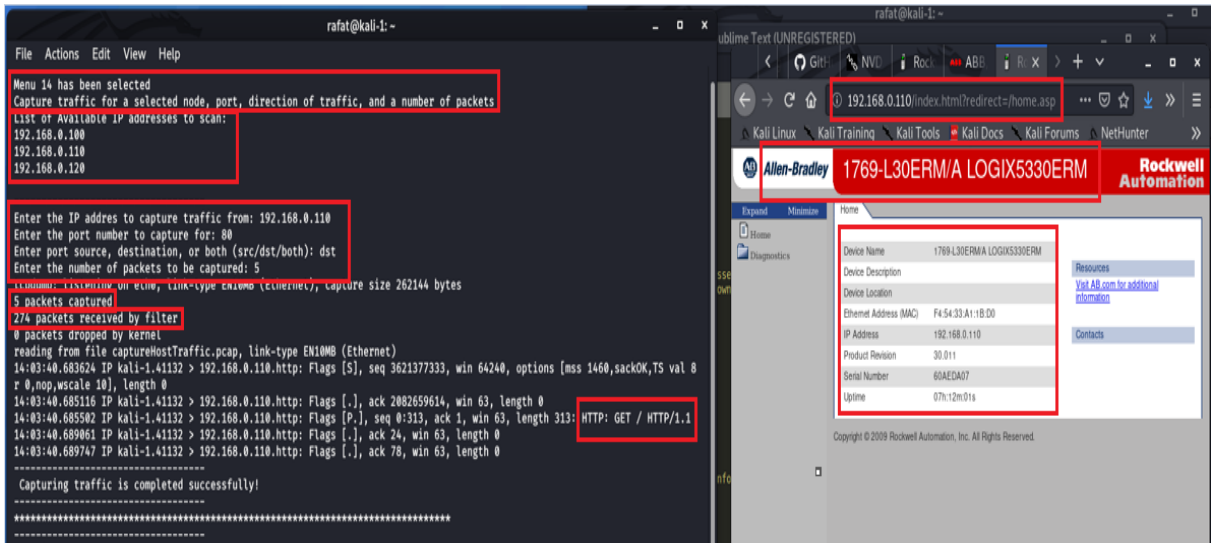
Option 12: Discover hardware information scan of nodes



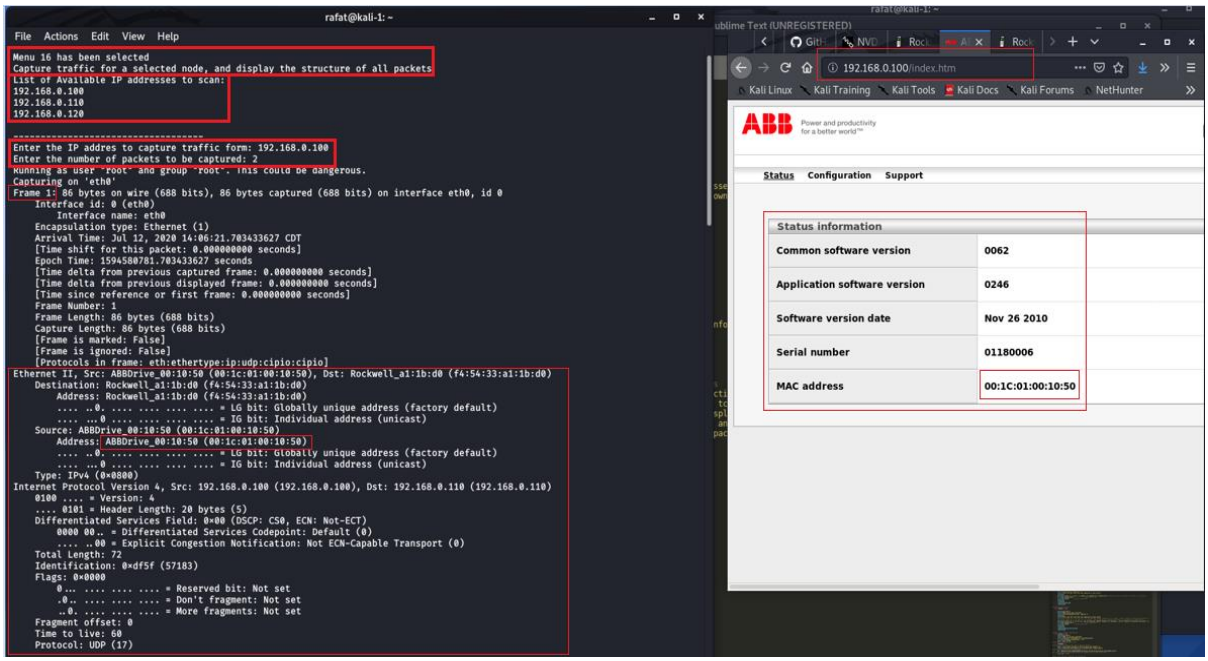
Option 13: Hardware information scan

Option 14 to 18: Traffic Analysis

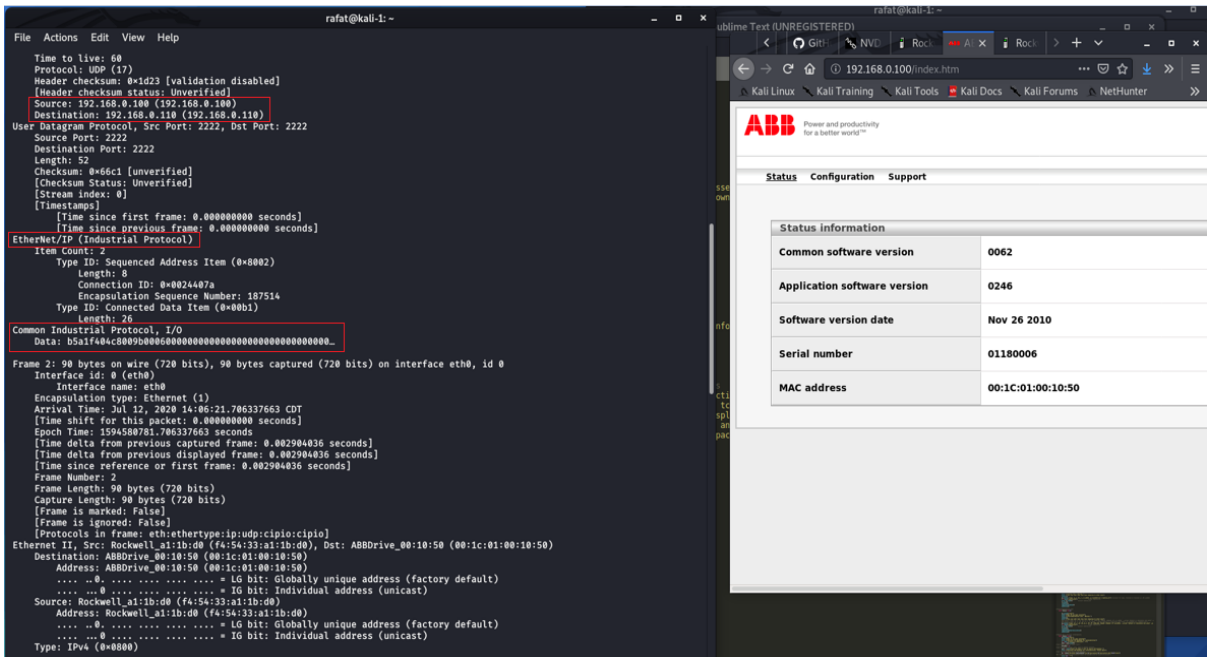
These options will give us a variety of ways to capture traffic, starting from more specific traffic for a specific node, port number, direction, and protocol to capturing all traffic on the ICS network.



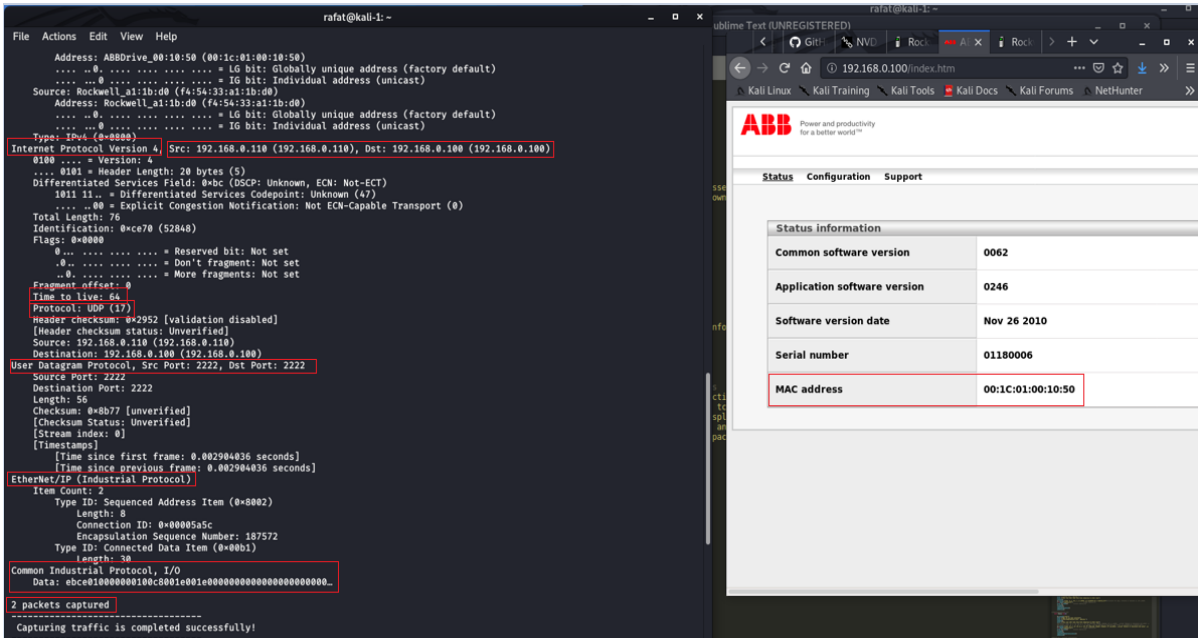
Option 14: Capture traffic for a selected number of packets for a specific node, port, and direction of traffic.



Option 15: Capture number of packet and display the structure of the packets



Option 17: Capture number of packet and display the structure of the packets



Option 18: Capture number of packet and display the structure of the packets

Curriculum Vitae

Rafat R. Elsharef

elsharer@matc.edu

EDUCATION

- **Bachelor of Science in Electrical Engineering, December 1987**
  - University of Wisconsin- Milwaukee
- **Master of Science, August 2002**
  - Cardinal Stritch University
- **PhD – Major: Industrial Engineering, December 2020**
  Minor: Computer Science
  - University of Wisconsin- Milwaukee
    Dissertation topic: Design of A Novel Manual and Automated Penetration Testing Frameworks for Connected Industrial Control Systems (ICS)

TEACHING EXPERIENCE

- **Faculty IT Networking and Security – Full time,** Milwaukee Area Technical College -MATC, 2001 – Present
- **Lecturer / TA,** UW-Milwaukee, 2005 - Present

TECHNICAL EXPERIENCE

- **Network Engineer / Security Engineer –** Full time – M&I Data Services / Metavante, (1999 – 2001)
- **Network Engineer –** Full time– WiscNet – Educational backbone for Wisconsin, (1996 – 1999)
- **Network Specialist –** Full time– UW-Madison, (1995 – 1996)
- **Network Specialist –** Full time– UW-Whitewater, (1993 – 1995)
- **Network Manager –** Full time- UW-Milwaukee, (1991 – 1993)