Testbed Reconnaissance and Vulnerability Analysis

Assignment 1 • Secure Infrastructures

Daniel Pereira
Department of Informatics Engineering
University of Coimbra
uc2021237092@student.uc.pt

Rodrigo Rodrigues
Department of Informatics Engineering
University of Coimbra
uc2022233032@student.uc.pt

***Abstract*—This report presents the process of vulnerability recognition and analysis carried out in a SCADA Testbed, as part of the Secure Infrastructures course. The objective was to map the network topology, identify devices, and characterize communication protocols, with a focus on Modbus/TCP. Passive scouting techniques (packet capture, ARP monitoring) and controlled scanning (arp-scan, nmap) were applied. The analyses revealed the absence of authentication and encryption in Modbus and the exposure of legacy services (Telnet, FTP, HTTP). No vulnerabilities were exploited (Testbed state preserved).**

***Index Terms*—SCADA systems, Modbus/TCP, network reconnaissance, vulnerability analysis, industrial cybersecurity, PLC, HMI**

I. Introduction

The growing digitalization of industrial infrastructures has brought significant benefits in efficiency, monitoring, and system integration but also exposed these environments to new cyber threats. Supervisory Control and Data Acquisition and Industrial Control Systems still rely heavily on legacy protocols and devices designed at a time when cybersecurity was not a fundamental principle. Understanding their architecture, behaviour, and weaknesses is therefore essential to ensure operational safety and continuity in critical infrastructures.

This work, developed as part of the Secure Infrastructures course, aimed to perform a reconnaissance and vulnerability analysis on a simulated SCADA Testbed.

The physical testbed emulates a small industrial cooling process using real cyber-physical components. It consists of two PLCs, a central HMI/SCADA workstation, a temperature sensor, a Variable Frequency Drive (VFD), and an electric motor. The temperature sensor continuously feeds measurements to the primary PLC, which processes the values and adjusts the VFD to control the motor's rotational speed, simulating the cooling response of an industrial system. As the sensed temperature increases, the VFD accelerates the motor to represent higher cooling demand; as the temperature decreases, the motor slows down accordingly. This setup provides a realistic environment for observing operational behaviour, analysing SCADA communication flows, and understanding the interaction between the HMI, PLCs, and field devices.

The study focused on network observation, device identification, and service mapping using non-intrusive and ethical approach. Techniques such as passive traffic analysis, ARP and port scanning, and controlled robustness test were applied using tools like tcpdump, arp-scan and nmap.

This methodology allowed the identification of potential weakness related to unauthenticated protocols, outdated services, and insufficient network segmentation. The work provides practical insights into common security issues affecting industrial systems and reinforces the importance of adopting layered defence strategies in SCADA environments

II. Task Plan

The task plan was designed to ensure a systematic, reproducible, and non-intrusive approach to reconnaissance and vulnerability analysis within the SCADA Testbed. The activities were structured in four main phases, complemented by OSINT research on the identified devices and continuous documentation of all actions.

A. Phase 1 – Device Discovery

1) Objective: Identify all devices present in the testbed and map their network interfaces.

2) Procedure: Passive traffic captures were performed using tcpdump and tshark to observe ARP activity and Modbus/TCP flows on the interface eth1. After initial observation, a controlled ARP sweep was executed to enumerate hosts at layer-2. This discovery was complemented by a low-impact ping sweep (using nmap in host-discovery mode) to confirm reachability at layer-3.

3) Justification: Starting with passive observation minimizes footprint and avoids disturbing the testbed. The subsequent low-rate ARP sweep (with spoofed source and timing delays) provides reliable layer 2 discovery while keeping network noise low; the ping sweep confirms IP level reachability without aggressive probing.

B. Phase 2 – Fingerprinting and Profiling

1) Objective: Determine the manufacturer, model, firmware or software version, and exposed services of each detected host.

2) Procedure: Controlled TCP SYN and service scans were executed using nmap, collecting services banners and identifying OUIs (Organizationally Unique Identifiers) from MAC addresses to infer device manufactures. Additional information was collected through HTTP banner and passive retrieval of configuration files using curl.

3) Justification: Detailed fingerprinting enables accurate classification of PLCs, HMIs, and supporting devices, allowing further OSINT-based vulnerability research without active exploitation.

C. Phase 3 – OSINT Vulnerability Research

1) Objective: Identify publicly known vulnerabilities associated with the discovered devices, firmware, or exposed services.

2) Procedure: Using the information obtained from fingerprinting, searches were conducted in public vulnerability databases to map Common Vulnerabilities and Exposures (CVEs) and known security issues.

3) Justification: Open-source intelligence research enables vulnerability assessment without interaction with devices, highlighting potential attacks vectors such as outdated Telnet or FTP services.

D. Phase 4 – Communication Flow Analysis

1) Objective: Identify existing communication flows, validate the inferred device roles (e.g., Master/Slave), and passively assess the risk of insecure protocols.

2) Procedure: A passive network capture was re-initiated on the interface eth2 using Wireshark. The capture was allowed to run for several minutes to collect a baseline of all network conversations. Analysis focused on the "Conversations" statistic (Statistics > Conversations) to map all TCP and UDP flows, identifying which hosts were communicating (Source/Destination IP) and over which ports. Display filters (e.g., modbus, ftp, telnet) were then applied to isolate these specific protocol streams for deeper inspection.

3) Justification: While active scans (Phase 2) identify potential services, this passive phase confirms actual, existing communication patterns without sending any packets, adhering to the non-intrusive constraint. This analysis is the only method to definitively map the Master/Slave relationships (e.g., which HMI is polling which PLC) and to passively observe if insecure protocols (like FTP or Telnet) are actively transmitting cleartext data on the network.

III. Toolset and techniques

The assessment of the SCADA testbed was performed using a combination of passive reconnaissance techniques, selected to provide comprehensive visibility while minimizing network impact. The primary tools included:

- tcpdump and Wireshark for passive traffic capture and protocol inspection, mainly focusing on ARP and Modbus/TCP communications.
- arp-scan for Layer-2 host discovery and MAC-to-IP mapping.
- nmap for Layer-3 host discovery, port scanning, service detection, and OS fingerprinting.
- curl for retrieving HTTP headers and validating the existence of management interfaces.
- OpenVAS for correlating discovered services with publicly known vulnerabilities (CVEs).

The methodology followed a progressive and ethical approach, starting with passive observation, continuing with low-intensity scanning, and concluding with protocol-specific verification. This toolset enabled accurate device enumeration, service identification, and vulnerability assessment without disrupting the operational behaviour of the testbed.

IV. Device Discovery

The first step of the reconnaissance process consisted of identifying all active hosts within the SCADA field network. A controlled ARP sweep was executed using arp-scan on the field interface (eth1), targeting the address range 172.27.224.1–172.27.224.253. The scan was configured with a forged ARP source address (–arpspa 172.27.224.80) and an inter-query delay of 250 ms (–interval=250), to minimize traffic impact on the testbed.

```
sudo arp-scan --interface=eth1
    --arpspa=172.27.224.80 --interval=250
    172.27.224.1-172.27.224.253
```

The results revealed five active hosts in the network segment. For each device, both IP and MAC addresses were recorded, and the vendor information was inferred from the MAC OUI (Organizationally Unique Identifier). The identified hosts are summarized in Table I.

TABLE I: Active hosts identified in the SCADA field network

IP Address	MAC Address	Device
172.27.224.10	00:0C:29:4D:DC:22	VMware
172.27.224.200	00:AD:24:C1:24:73	D-Link International
172.27.224.245	08:00:06:12:C0:DE	SIEMENS AG
172.27.224.250	00:80:F4:09:51:3B	Telemecanique Electrique
172.27.224.251	48:5B:39:64:40:79	ASUSTek Computer Inc.

This Layer-2 discovery stage provided an initial inventory of all reachable devices in the SCADA segment, serving as the foundation for subsequent fingerprinting and service analysis.

In addition to the Layer-2 ARP sweep, a Layer-3 discovery was conducted using nmap in ping-sweep verified which of the previously detected IPs responded to ICMP or TCP probes, confirming that the devices were reachable through the IP stack and not merely visible at the Ethernet level.

Both discovery stages provided a comprehensive view of the testbed's topology: the Layer-2 scan enumerated every device physically connected to the SCADA segment, while the Layer-3 verification confirmed their logical network availability. This dual-layer approach ensured that no active host was overlooked.

V. Fingerprinting and Profiling

Following the device discovery stage, a detailed fingerprinting procedure was performed to identify open TCP ports, active services, and running software versions for each host detected in the SCADA subnet. This process aimed to build an accurate profile of each system without interfering with its normal operation.

Controlled SYN scans were carried out using nmap with Ethernet-level packet injection through the field interface (eth1), covering the common service port range (1-1024). Host discovery was disabled (-Pn), as all the targets had already been confirmed during Layer-2 and Layer-3 reconnaissance. The scans were executed with conservative timing and ARP-ping disabled to minimize traffic footprint, using a command similar to:

```
nmap --send-eth -e eth1 -sS -n <target_IP>
    --scan-delay 1 -p 1-1024 -Pn --disable-arp-ping
```

For each host, open ports were manually verified, and service detection (-sV) was subsequently applied to identify the associated software or protocol. The results revealed that different classes of devices expose distinct services consistent with their industrial roles:

TABLE II: Open ports and identified services per host

Device	Open Ports and Services
VMware	HTTP (80/tcp) VNC (5900/tcp)
D-Link International	Telnet (23/tcp)
Siemens AG	HTTP (80/tcp) ISO-TSAP (102/tcp) Modbus/TCP (502/tcp)
Telemecanique Electrique	FTP (21/tcp) HTTP (80/tcp) Modbus/TCP (502/tcp)
ASUSTek Computer Inc.	Modbus/TCP (502/tcp)

The VMware host presented an open 80/tcp (HTTP) port, with other scanned ports showing as filtered. The presence of a single web service is not sufficient to determine its specific role in the testbed at this stage.

The D-Link International device exposed a single management service - Telnet (port 23/tcp) — suggesting that operates as a managed switch or network router running a minimal Linux-based system.

The Siemens AG host presented HTTP (80/tcp), ISO-TSAP (102/tcp) and Modbus/TCP (502/tcp) ports, which are characteristic of Siemens industrial controllers and communication modules (e.g., S7-200 or CP443). These protocols support engineering access, HMI connectivity, and data exchange within the SCADA network.

The Telemecanique Electrique device revealed FTP (21/tcp), HTTP (80/tcp) and Modbus/TCP (502/tcp) services, confirming it as a Schneider Electric PLC with a legacy configuration interface accessible through the web. The presence of an open FTP service suggests outdated or insecure management features that would be considered unsafe in production environments.

Finally, the ASUSTek Computer Inc. host responded only on Modbus/TCP (502/tcp), exposing no additional services within the scanned port range. At this stage, its specific role within the testbed could not yet be determined, but the presence of Modbus/TCP suggests potential participation in industrial communication flows.

After identifying the open ports for each host, a second phase of detailed fingerprinting was conducted using service and version detection scans. The command below was executed for each device.

```
nmap -sS -sV -sC -p <ports> -Pn -n <IP address>
```

This approach combined SYN-based port scanning (-sS) with service version enumeration (-sV) and Nmap's default script set (-sC), allowing the collection of additional details such as software versions, protocol banners, and device fingerprints. The objective was to validate the initial Layer-2 and Layer-3 discoveries, confirm manufacturer consistency, and uncover any new services or characteristics not visible in the initial scan.

A. VMware (172.27.224.10)

The scan on the open returned a service banner of Microsoft IIS httpd 7.5, with an http-title of IIS7. However, the most critical piece of information revealed by this scan was the service information: Service Info: OS: Windows. This finding indicates that the target was a Windows-based machine, likely running an older, unsupported version like Windows Server 2008 R2, given the IIS 7.5 banner. This discovery was the logical driver for the next step. A second, targeted scan was immediately initiated to enumerate common Windows remote management and administrative protocols that were missed in the initial port 1-1024 scan. The command below was used to probe for these services.

```
sudo nmap -sS -sV -sC -p 3389,5900,8080,445,135
    172.27.224.10
```

This second scan confirmed the hypothesis. It revealed that while the standard Windows file sharing ports (135/tcp and 445/tcp) were filtered (indicating an active firewall), two critical remote access ports were explicitly open: 3389/tcp (ms-wbt-server), the default port for Microsoft's Remote Desktop Protocol (RDP), and 5900/tcp (VNC), a second, distinct remote desktop protocol.

The synthesis of these findings strongly suggests that this device functions as the central HMI/SCADA server for the testbed, providing multiple avenues for remote management and process visualization.

Summary:

- Open ports: 80/tcp, 3389/tcp, 5900/tcp
- Services: HTTP, ms-wbt-server (RDP), VNC
- Identifiers: "Microsoft IIS httpd 7.5", "VNC (protocol 3.8)", "VMware"
- Function: HMI/SCADA Server

B. D-Link International (172.27.224.200)

The detailed scan confirmed a single open port: 23/tcp, running the Telnet service identified as Linux telnetd. The banner indicated that the device operates on a Linux-based embedded system, typical of managed switches or network routers. No additional services were detected beyond Telnet.

The presence of an unencrypted Telnet interface suggests that plaintext remote management is enabled. Although no

authentication attempt was made, this configuration would be considered insecure in production environments.

Summary:

- Open port: 23/tcp
- Service: Telnet
- Version: Linux telnetd
- OS detected: Linux (CPE: cpe:/o:linux:linux_kernel)

C. Siemens AG (172.27.224.245)

The Siemens device exposed three TCP services: HTTP (80/tcp), ISO-TSAP (102/tcp), and Modbus/TCP (502/tcp). The HTTP service returned Siemens-specific banners such as SIMATIC S7-200 and CP 443-1 EX40, confirming the host as a Siemens communication processor or PLC module.

The web service exhibited normal behaviour (302 redirects, 404 responses, and 200 OK on HTTP OPTIONS), indicating a minimal management interface. The combination of ISO-TSAP and Modbus/TCP confirms its role as a control-layer device, facilitating communication between engineering workstations and HMIs.

Summary:

- Open ports: 80/tcp, 102/tcp, 502/tcp
- Services: HTTP, ISO-TSAP, Modbus/TCP
- Identifiers: “Siemens SIMATIC S7-200 /CP 443-1 EX40”
- Function: PLC communication processor

D. Telemecanique Electrique (172.27.224.250)

The Telemecanique (Schneider Electric) host presented three open ports: FTP (21/tcp), HTTP (80/tcp), and Modbus/TCP (502/tcp). Version detection identified the web server as Schneider-WEB 2.1.3, part of the legacy web configuration interface used by Schneider Modicon PLCs.

The HTTP responses referenced resources such as /index.htm and configuration scripts (config.js, tools.js), both commonly present in PLC management interfaces. The FTP service was detected as either vsftpd (before 2.0.8) or WU-FTPD, both outdated and historically vulnerable daemons.

Additionally, the modbus-discover script was executed against port 502, successfully retrieving Modbus Device Identification fields. This confirmed the hardware identity of the device as:

Summary:

- Manufacturer: Schneider Electric
- Family: Modicon M340
- Model: BMX P34 20302
- Firmware: v2.4
- Version: Schneider-WEB 2.1.3 (HTTP); vsftpd/WU-FTPD (FTP)
- MAC: Telemecanique (Schneider industrial line)
- Open ports: 21/tcp, 80/tcp, 502/tcp
- Services: FTP, HTTP, Modbus/TCP
- Function: Schneider PLC with web configuration interface and Modbus support

E. ASUSTek Computer Inc. (172.27.224.251)

The ASUSTek device responded exclusively on 502/tcp (Modbus/TCP). However, version detection returned irregular responses containing non-Modbus strings such as MICROSOFT NETWORKS 1.03 and LANMAN 1.0, which are typically associated with SMB negotiation.

Despite the anomalous banner, the port remained open and stable throughout the scan. This inconsistent behaviour — a Modbus port returning SMB-like data — suggested the possibility that the host might be operating as a decoy or honeypot designed to mimic a Modbus endpoint.

Summary:

- Open port: 502/tcp
- Service: Modbus/TCP (anomalous response)
- Note: Returned SMB-related strings; further analysis required

1) Assessment of a Possible Honeypot: During the fingerprinting phase the host 172.27.224.251 produced ambiguous results when scanned using:

```
nmap -sS -sV -sC -p 502 -Pn -n 172.27.224.251
```

The output included unexpected ASCII strings such as "MICROSOFT NETWORKS 1.03", "Samba", and "LANMAN 1.0", which initially appeared to indicate SMB-related services. However, this responses are false positives caused by Nmap’s generic service probes, which send HTTP, SMB, and LDAP payloads to any open port in attempt to guess the service type. The device under analysis employs a WIZnet W5100 embedded TCP/IP chipset, which implements the network stack in hardware. When receiving unsupported or malformed packets, the firmware may return binary buffer fragments that Nmap takes the wrong meaning as text. When tested with Modbus-specific tools (modbus-discover.nse), the host correctly behaves as a Modbus/TCP slave, responding to standard function codes with valid register data. No other TCP or UDP ports are open, and the device does not expose any management interfaces (HTTP, SSH, SNMP), nor banners of any kind. Additional evidence supports its authenticity:

- Nmap fingerprint: "WIZnet embedded - W5100 TCP/IP chip";
- ICMP tests: TTL = 128 and sub-millisecond latency, consistent with embedded hardware;
- MAC address 48:5B:39 (ASUSTek) corresponds to the NIC manufacturer, not the device itself;
- Valid Modbus register responses and incremental Transaction IDs indicate a functioning Modbus firmware stack.

Known honeypots such as Conpot or Honeyd run on Linux, expose multiple simulated services, and produce predictable or textual banners. None of these characteristics are present here.

VI. OSINT Vulnerability Research

Open source intelligence (OSINT) research was conducted to contextualize the findings from the scanning phase, focusing

on known vulnerabilities associated with the identified protocols and software implementations. The subsequent analysis is divided into three classes of protocols found in the testbed: legacy management protocols (Telnet, FTP), web server protocols (HTTP), and industrial control protocols (Modbus, ISO-TSAP).

A. Legacy Management Protocols (Telnet and FTP)

The presence of Telnet (port 23) and FTP (port 21) protocols was identified. Both share a fundamental design vulnerability: the complete absence of encryption. All communications, including the exchange of authentication credentials, are transmitted in plain text. This flaw trivially exposes sessions to eavesdropping and Man-in-the-Middle (MITM) attacks, where an attacker positioned on the network can capture administrator credentials. In addition to the risk inherent in the FTP protocol, the implementation of specific software identified, ‘vsftpd‘ in versions prior to ‘2.0.8‘, presents a set of documented critical vulnerabilities. Such old versions are susceptible to Denial of Service (DoS) attacks due to memory leaks. ‘CVE-2008-2375‘ documents a flaw in versions prior to ‘2.0.5‘, where a large number of failed authentication attempts exhausts the device’s memory. Similarly, ‘CVE-2007-5962‘ describes an identical flaw in version ‘2.0.5‘, triggered by multiple ‘CWD‘ commands. In both scenarios, an attacker can exhaust the PLC’s resources, causing a crash and interrupting operations. The analysis also revealed risks in shared system libraries, such as ‘CVE-2009-5029‘. This describes an integer overflow in the ‘glibc‘ library that can be triggered by uploading a malicious timezone (TZ) file via FTP, resulting in a DoS or, potentially, Remote Code Execution (RCE). It is also noted that the Windows Telnet Service itself, found on Windows Server 2008, is vulnerable to buffer overflows (CVE-2015-0014) that allow remote code execution.

B. Web Server Protocols (HTTP)

The presence of web management interfaces on port 80 (HTTP) represents a significant attack surface. As a plain-text protocol, HTTP is a Security Misconfiguration, exposing session cookies to sniffing. The main risk, however, lies in specific software implementations. Research on the ‘Schneider-WEB 2.1.3‘ server (identified in the Telemecanique PLC) revealed ‘CVE-2014-0754‘, documented in advisory ‘ICSA-14-273-01‘. This is a Path Traversal vulnerability (CVSS 10.0) that allows an attacker to “bypass basic authentication” and gain “unauthenticated administrative access and control over the device” through a malformed URL. Further research on Modicon PLCs identified ‘CVE-2015-6461’, a critical stack-based buffer overflow in the GoAhead embedded web server used by these devices. An unauthenticated attacker can exploit this by sending an overly long password string via HTTP Basic Authentication, potentially leading to Remote Code Execution (RCE). Similarly, research into the ‘SIMATIC CP 443-1‘ module (identified in the Siemens PLC) revealed the official advisory ‘SSA-603476‘. This advisory groups two critical flaws: ‘CVE-2016-8673‘, a Cross-Site Request Forgery (CSRF) vulnerability that allows an attacker to perform actions (such as stopping the PLC) using an authenticated engineer’s session; and ‘CVE-2018-4843‘, a DoS flaw that crashes the PLC, requiring a manual restart of the equipment. Finally, the HMI/SCADA server (172.27.224.10) was found running Microsoft IIS httpd 7.5, which correlates to an obsolete Windows Server 2008 R2 OS. This specific implementation is notoriously vulnerable to CVE-2015-1635 (MS15-034), a critical flaw in the HTTP.sys kernel driver. This vulnerability allows an unauthenticated remote attacker to cause a Denial of Service (Blue Screen of Death) or achieve Remote Code Execution via a specially crafted HTTP request. This is part of a larger pattern of flaws in the Windows web stack, including CVE-2013-3195, an integer overflow in Comctl32.dll exploitable via ASP.NET, and CVE-2014-6321, a critical RCE flaw in the Microsoft Schannel component which handles SSL/TLS traffic.

C. Remote Desktop and OS Services

A third class of protocol was identified on the HMI/SCADA server (172.27.224.10): remote desktop and core OS services. The host exposed both RDP (port 3389) and VNC (port 5900), creating a significant and dual-pronged attack surface. The most critical vulnerability in this category is CVE-2019-0708 (BlueKeep), which directly affects the RDP implementation on the identified Windows Server 2008 R2 OS. This pre-authentication, "wormable" vulnerability allows a remote attacker to achieve kernel-level Remote Code Execution (RCE) without any credentials. This is compounded by other RDP-related flaws, such as CVE-2015-2473, where the RDP client itself can be exploited to gain privileges. The VNC service (protocol 3.8), in turn, uses ’VNC Authentication’, a weak mechanism susceptible to brute-force attacks.

The underlying Windows Server 2008 OS also introduces a class of systemic vulnerabilities. These include multiple RCE flaws in the handling of fonts, such as CVE-2015-6108, CVE-2015-2510, and CVE-2015-2426 (Adobe Type Manager), which can be exploited via specially crafted embedded fonts. Furthermore, core services like the Remote Procedure Call (RPC) subsystem are vulnerable to RCE via malformed requests (CVE-2013-3175).

D. Industrial Control Protocols (Modbus and ISO-TSAP)

Control protocols pose the most direct risk to the physical process. Modbus (port 502), found on both PLCs, lacks authentication and encryption by design. Schneider’s specific implementation, used in these PLCs, is documented as vulnerable to ‘CVE-2017-6034‘, a Replay Attack where an attacker can “record” and “resend” control commands (e.g., ‘STOP PLC‘). It is also vulnerable to ‘CVE-2018-7849‘, a DoS by malformed Modbus packets, and ‘CVE-2018-7846‘, which allows brute force attacks. Compounding this risk is ‘CVE-2017-6017’, another DoS vulnerability specific to Modicon PLCs, where a specially formatted packet (using function 0x5A) can freeze the device, requiring a physical reset by an operator.

The ISO-TSAP protocol (port 102), which encapsulates Siemens' S7comm protocol, shares these weaknesses. 'CVE-2016-9159' documents a flaw that allows an attacker with network access to extract credentials (passwords) from the PLC. Additionally, advisory 'SSA-969738' ('CVE-2024-43647'), although referring to a newer model ('S7-200 SMART'), demonstrates a pattern of fragility in the S7-200 family, which can be brought to a state of DoS by a single malformed TCP packet.

VII. Communication Flow Analysis

The final stage of the recognition process consisted of passive traffic monitoring, carried out using Wireshark directly on the testbed network. This method allowed us to meet the requirement of identifying existing communication flows without interfering with the operation of the infrastructure, enabling us to observe normal interactions between devices and confirm their operational roles.

The analysis of packet capture, mainly through TCP 'Conversations' statistics, provided a clear view of network activity. Two distinct Modbus flows (port 502) stood out, both originating from the HMI/SCADA (172.27.224.10) but directed to different devices. The first had a constant and high volume, corresponding to the actual operating cycle of the system, in which the HMI acted as a client, sending regular requests to the Telemecanique PLC (172.27.224.250). The second, less intense flow involved the ASUSTek device (172.27.224.251). Although it appeared in the list of TCP conversations, detailed Modbus packet inspection showed that it never issued Modbus requests. All Function Code requests were sent exclusively by the HMI (172.27.224.10). The ASUSTek device acted solely as a Modbus slave, responding only when queried. Its lower traffic volume reflects the fact that the HMI polls it less frequently than the primary PLC.

The capture also confirmed that the remaining devices were not participating in any relevant communications at that time. Neither the Siemens PLC (172.27.224.245) nor the D-Link network device (172.27.224.200) appeared in the list of active conversations. This absence suggests that the D-Link was functioning solely as support infrastructure and that the Siemens PLC was inactive or simply without an associated Modbus client during the observation period.

Finally, passive monitoring allowed us to assess the use of protocols considered insecure. Filters were applied to detect telnet and ftp traffic, but no corresponding packets appeared in the capture. This result is relevant: although the OSINT phase revealed serious vulnerabilities related to these services, passive analysis indicates that, during that time interval, such protocols were not being actively used, reducing the immediate threat, even though the potential risk remains.

VIII. Discussion of results

The consolidation of the results obtained in Sections V (Fingerprinting and Profiling), VI (OSINT Vulnerability Research) and VII (Communication Flow Analysis) allows for an integrated assessment of the overall security status of the testbed. The infrastructure demonstrates consistent operation as an industrial control system, but has severe weaknesses, mainly due to the existence of an unsegmented network, built on implicit trust, where an outdated HMI coordinates old and equally exposed PLCs.

The HMI/SCADA server (172.27.224.10) is the component whose exposure most influences the network risk. Its identification as a Windows machine (Section V-A), running Microsoft IIS httpd 7.5, confirms the use of an operating system that is no longer supported. The presence of remote management services, namely RDP (3389/tcp) and VNC (5900/tcp), significantly increases the likelihood of exploitation. The vulnerabilities associated with RDP and IIS show that the server can be compromised without authentication or through critical remote execution flaws. Traffic analysis (Section VII) demonstrates that this system is effectively the central point of Modbus operation, maintaining continuous and intensive communications with the PLC .250. As a result, any successful intrusion into the HMI implies virtually complete control of the network.

The Telemecanique PLC (172.27.224.250), identified as Schneider Modicon M340 (Section V-D), acts as the main subordinate unit and presents a notable attack surface. Traffic results confirm that all active Modbus flows converge on this device. The FTP service, based on an old version of vsftpd, has known flaws that can cause downtime. The web server (Schneider-WEB 2.1.3) contains documented vulnerabilities that allow everything from authentication bypass to remote code execution. Additionally, the Modbus service is associated with conditions that can lead to a physical restart of the equipment. Thus, there are multiple attack paths capable of compromising this PLC.

The Siemens PLC (172.27.224.245) behaves as a passive subordinate device. The absence of traffic directed to it (Section VII) indicates that the respective HMI was not operational during the capture. However, it remains vulnerable: the CP 443-1 network module has reported flaws related to insufficient defence against forged requests and denial-of-service situations that require manual intervention. The S7comm protocol, available through port 102, also allows the extraction of credentials as documented in OSINT sources (Section VI-B).

The analysis also highlights an interesting characteristic of the architecture: the presence of multiple Modbus-capable slave devices, but only a single Modbus controller. Packet inspection confirms that the HMI (.10) is the sole Modbus master, issuing all Function Code requests. The ASUSTek device (.251), although initially ambiguous due to anomalous Nmap banners, does not perform any polling activity. As clarified in Section V-E, it is not a honeypot but an embedded device based on the WIZnet W5100 chipset, operating strictly as a Modbus slave and responding only when queried by the HMI. The D-Link network device (.200), which exposes only a Telnet service, primarily represents a confidentiality risk (Section VI-A) and otherwise behaves as expected for a passive network component, generating no operational traffic.

Overall, the testbed shows an extremely fragile security posture, mainly due to the lack of segmentation, dependence on old equipment, and the use of exposed services and protocols that facilitate different forms of compromise.

IX. Conclusion

This study applied the proposed methodology, consisting of four stages, obtaining a clear and non-intrusive characterisation of the analysed SCADA testbed. The combination of network fingerprinting techniques (Section V) and detailed observation of communication flows (Section VII) enabled not only the identification of the topology and active services, but also an understanding of the centralised control structure used in the environment. The main conclusion is that the overall security of the testbed depends heavily on a single component: the HMI/SCADA server (172.27.224.10). The traffic analysis presented in Section VII demonstrated that this equipment acts as the sole Modbus Master, holding operational authority over the Slave devices (.250 and .251). As described in Section V-A, the HMI uses a discontinued Windows system (Windows Server 2008 R2, inferred from the use of IIS 7.5) and keeps remote services such as RDP and VNC accessible. The OSINT results (Section VI) reinforce that this Master is the most vulnerable point in the infrastructure, being associated with several serious flaws that allow remote code execution without prior authentication, including widely known vulnerabilities such as BlueKeep (CVE-2019-0708) and flaws in the HTTP module. sys module (CVE-2015-1635). Compromising this server gives an attacker complete control over the industrial process. The risk is amplified by the fragile state of the slave devices. The Telemecanique PLC (.250) has critical vulnerabilities, including authentication bypass (CVE-2014-0754) and remote execution (CVE-2015-6461). The Siemens PLC (.245) has flaws susceptible to denial-of-service attacks that require manual restart (CVE-2018-4843) and mechanisms that allow credential extraction (CVE-2016-9159). Thus, the testbed operates on a flat network, without segmentation, in which an obsolete Master manages devices with severe flaws, resulting in a significantly increased attack surface.

References

[1] Nmap Project, "Nmap Reference Guide," 2024. [Online]. Available: https://nmap.org/book/man.html

[2] Schneider Electric, "PLC, PAC e Controladores Dedicados – Catálogo Portugal," Schneider Electric Portugal, 2024. [Online]. Available: https://www.se.com/pt/pt/product-category/3900-plc-portugal-pac-e-controladores-dedicados/

[3] WIZnet Co., Ltd., "W5100 Hardwired TCP/IP Embedded Ethernet Controller – Datasheet," 2015. [Online]. Available: https://docs.wiznet.io/Product/iEthernet/W5100/datasheet

[4] National Institute of Standards and Technology, "CVE-2008-2375: vsftpd Memory Leak Vulnerability," National Vulnerability Database, 2008. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2008-2375

[5] NIST, "CVE-2007-5962: vsftpd CWD Command Denial of Service," National Vulnerability Database, 2007. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2007-5962

[6] NIST, "CVE-2009-5029: glibc Timezone File Integer Overflow," National Vulnerability Database, 2009. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2009-5029

[7] MITRE Corporation, "CVE-2015-0014: Windows Telnet Service Remote Code Execution Vulnerability," CVE.org, 2015. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0014

[8] CISA ICS-CERT, "ICSA-14-273-01: Schneider Electric Modicon Path Traversal Vulnerability (CVE-2014-0754)," 2014. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-14-273-01

[9] CISA ICS-CERT, "ICSA-15-202-01: Schneider Electric Modicon Buffer Overflow Vulnerability (CVE-2015-6461)," 2015. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-15-202-01

[10] CISA ICS-CERT, "ICSA-16-287-02: Siemens SIMATIC CP 443-1 Vulnerabilities (including CVE-2016-8673)," 2016. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-16-287-02

[11] CISA ICS-CERT, "ICSA-18-094-01: Siemens SIMATIC Multiple Vulnerabilities (CVE-2018-4843)," 2018. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-18-094-01

[12] Microsoft, "Microsoft Security Bulletin MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (CVE-2015-1635)," 2015. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2015-1635

[13] Microsoft, "MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (CVE-2014-6321)," 2014. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2014-6321

[14] NIST, "CVE-2013-3195: Comctl32.dll Integer Overflow," National Vulnerability Database, 2013. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2013-3195

[15] NIST, "CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability (BlueKeep)," National Vulnerability Database, 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

[16] NIST, "CVE-2015-2473: RDP Client Privilege Escalation Vulnerability," National Vulnerability Database, 2015. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2015-2473

[17] NIST, "CVE-2015-6108: Adobe Type Manager Font Parsing Remote Code Execution Vulnerability," NVD, 2015. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2015-6108

[18] NIST, "CVE-2015-2510: Windows Font Handling Remote Code Execution Vulnerability," NVD, 2015. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2015-2510

[19] NIST, "CVE-2015-2426: Adobe Type Manager Font Driver Remote Code Execution," NVD, 2015. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2015-2426

[20] NIST, "CVE-2013-3175: Remote Procedure Call (RPC) Remote Code Execution Vulnerability," NVD, 2013. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2013-3175

[21] CISA ICS-CERT, "ICSA-17-040-01: Schneider Electric Modicon M340/M580 Replay Attack Vulnerability (CVE-2017-6034)," 2017. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-17-040-01

[22] CISA ICS-CERT, "ICSA-19-013-02: Schneider Electric Modicon DoS Vulnerability (CVE-2018-7849)," 2019. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-19-013-02

[23] CISA ICS-CERT, "ICSA-18-107-01: Schneider Modicon Modbus Weak Authentication Vulnerability (CVE-2018-7846)," 2018. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-18-107-01

[24] CISA ICS-CERT, "ICSA-17-094-01: Schneider Electric Modicon Denial of Service Vulnerability (CVE-2017-6017)," 2017. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-17-094-01

[25] Siemens ProductCERT, "SSA-969738: SIMATIC S7-200 SMART DoS Vulnerability (CVE-2024-43647)," Siemens, 2024. [Online]. Available: https://cert-portal.siemens.com/productcert/html/ssa-969738.html

[26] UK Cyber Security. "What Makes Telnet Vulnerable." [Online]. Available: https://www.ukcybersecurity.co.uk/blog/news-advice/what-makes-telnet-vulnerable/

[27] PureVPN. "What is HTTP vulnerability?" [Online]. Available: https://www.purevpn.com/ddos/http-vulnerability

[28] Veridify. "Modbus Security Issues and How to Mitigate Cyber Risks" [Online]. Available: https://www.veridify.com/modbus-security-issues-and-how-to-mitigate-cyber-risks/