Exploring ICS/SCADA Network Vulnerabilities

Hala Strohmier(✉), Aaryan R. Londhe, Chris A. Clark, Ronit Pawar, and Brian Kram

University of South Carolina Aiken, Aiken, SC, USA
hala.strohmier@usca.edu

Abstract. This paper investigates vulnerabilities in the University of South Carolina Aiken (USCA) Centre's IP infrastructure, focusing on ICS/SCADA network security. The study follows a systematic approach, incorporating the CIS (Center for Internet Security) security controls methodology throughout the project phases, including asset identification, vulnerability assessment, risk assessment, and flexibility study. The asset identification phase utilized tools such as Nmap, Maltego and Lansweeper to comprehensively identify and catalog assets within the network. Subsequently, the vulnerability assessment phase employed tools like OpenVAS, Nexpose, Nessus and manual penetration testing to uncover potential weaknesses. The research team then conducted a risk assessment using the FAIR (Factor Analysis of Information Risk) Methodology to quantitatively analyze and prioritize identified risks. In parallel, a flexibility study was undertaken to assess the system's adaptability to potential threats. Collaborating with the technology service department(TSD), the research team addressed the identified vulnerabilities. This research paper provides a thorough exploration of ICS/SCADA network vulnerabilities, offering insights into the effectiveness of the CIS security controls methodology in enhancing cybersecurity measures.

Keywords: ICS/SCADA · Cybersecurity · Vulnerablity Assessment · Operations Center · CIS Security Controls · Factor Analysis of Information Risk (FAIR) · Network Security · Risk Assessment

1 Introduction

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks constitute the backbone of critical infrastructures, playing a pivotal role in the seamless operation of essential services. As these systems become increasingly interconnected and reliant on digital technologies, they also become susceptible to a growing array of cyber threats. The security of ICS/SCADA networks is paramount to safeguarding industries such as energy, water supply, and manufacturing [1].

A. Moallem (Ed.): HCII 2024, LNCS 14729, pp. 215–233, 2024.
https://doi.org/10.1007/978-3-031-61382-1_14

This research delves into the intricate landscape of ICS/SCADA network vulnerabilities, with a specific focus on the operation center's IP infrastructure at the University of South Carolina Aiken (USCA). The escalating complexity of these networks, coupled with the ever-evolving threat landscape, necessitates a comprehensive exploration of potential weaknesses. Addressing these vulnerabilities is crucial not only for protecting critical assets but also for maintaining the reliability and resilience of the interconnected systems that underpin modern society.

2 Literature Review

The security of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks has garnered significant attention in the realm of cybersecurity due to their pivotal role in critical infrastructure. The literature on ICS/SCADA security underscores the growing complexity of these systems and the corresponding increase in vulnerabilities.

Numerous studies have highlighted the evolving threat landscape surrounding ICS/SCADA networks. Researchers have demonstrated the feasibility of cyber-attacks targeting critical infrastructure, emphasizing the need for robust security measures. Incidents such as Stuxnet have underscored the potential real-world impact of cyber threats on industrial processes, amplifying the urgency for proactive security strategies [2,3].

The adoption of comprehensive security frameworks has become imperative in addressing the multifaceted challenges of ICS/SCADA security. The Center for Internet Security (CIS) security controls framework has emerged as a prominent guideline for enhancing cybersecurity defenses in critical infrastructure settings. Studies evaluating the effectiveness of the CIS controls have shown promising results in fortifying ICS/SCADA networks against a spectrum of cyber threats.

Risk assessment methodologies play a crucial role in identifying and prioritizing vulnerabilities in ICS/SCADA environments. The Factor Analysis of Information Risk (FAIR) methodology has gained recognition for its ability to provide a quantitative analysis of risks associated with identified vulnerabilities. Research has demonstrated the applicability of FAIR in diverse contexts, contributing to the understanding of risk in ICS/SCADA systems [4,5].

Asset identification and vulnerability assessment tools are integral components of a robust cybersecurity strategy. Studies have utilized tools like Nmap, Nessus, and OpenVAS for identifying assets and assessing vulnerabilities in ICS/SCADA networks. These tools contribute to a comprehensive understanding of the network landscape and potential points of weakness.

Collaboration between cybersecurity researchers and industry practitioners is crucial for addressing identified vulnerabilities. Literature has highlighted successful cases where collaboration with technology departments and industry experts has led to the effective mitigation of cybersecurity risks in ICS/SCADA environments [6].

In summary, the literature review reveals a growing awareness of the challenges posed by cyber threats to ICS/SCADA networks. The adoption of frameworks like CIS security controls, methodologies such as FAIR, and the use of advanced tools for asset identification and vulnerability assessment collectively contribute to the evolving landscape of cybersecurity in critical infrastructure settings.

3 Methodology

This research integrates a comprehensive methodology, incorporating the Center for Internet Security (CIS) Critical Security Controls (CIS Controls) for asset identification, vulnerability assessment, and risk analysis. The research methodology integrates the Center for Internet Security (CIS) security controls, a recognized framework designed to fortify cybersecurity defenses. The study follows a structured approach, encompassing the following:

- Asset identification
- Vulnerability assessment
- Risk analysis
- Feasibility Study and Effectiveness Evaluation
- Factor Analysis of Information Risk (FAIR)
- Quantifiable risks associated with these vulnerabilities.
  - Identify Assets
  - Identify Threat Scenarios
  - Identify Vulnerability Severity
  - Determine Threat Capability
  - Calculate Risk
  - Prioritize Risks
  - Implement Mitigation Measures

3.1 CIS Critical Security Controls (CIS Controls)

Phase 1: Asset Identification: We used sophisticated tools such as Maltego, Nmap, and Lansweeper to systematically enumerate and categorize assets within the USCA network. Maltego played a pivotal role in visually representing and linking information, while Nmap and Lansweeper were instrumental in conducting comprehensive network discovery, security auditing, and detailed asset profiling. This approach is necessary to gain a clear understanding of the devices being scanned, providing valuable insights for subsequent phases of the process.

Phase 2: Vulnerability Assessment: A thorough examination of identified assets using tools such as Nexpose, Nessus, and OpenVAS was conducted to proactively identify and address vulnerabilities within the system. This proactive approach aimed to enhance the overall security posture of the system by uncovering potential weaknesses and ensuring that appropriate measures could

be taken to mitigate any security risks. Manual penetration testing was employed to validate and supplement automated assessments, providing a more comprehensive understanding of the system's security landscape and ensuring robust protection against potential threat.

Phase 3: Risk Assessment: Leveraging findings from the vulnerability assessment, we systematically assessed the risks associated with each vulnerability. To further enhance the depth of our risk assessment, we employed the Factor Analysis of Information Risk (FAIR) methodology. This comprehensive approach not only facilitates a detailed understanding of potential risks but also enables effective risk prioritization. By prioritizing risks, organizations can focus resources on addressing the most critical vulnerabilities, thereby enhancing overall security posture and mitigating potential threats more efficiently.

Phase 4: Feasibility Study and Effectiveness Evaluation: Conducting a feasibility study to evaluate the practicality of implementing proposed security measures, encompassing a thorough assessment of viability and effectiveness, was the initial step. In collaboration with the Technology Services Department (TSD), we ensured alignment with organizational goals and addressed technical feasibility considerations. Once the security suggestions were implemented, a meticulous testing phase was initiated to reevaluate vulnerabilities, ensuring their proper resolution and assessing the overall effectiveness of the measures. This comprehensive approach, from feasibility study to post-implementation testing, is necessary for informed decision-making, optimal security enhancement, and ongoing risk management.

3.2 Factor Analysis of Information Risk (FAIR)

Phase 1: Identify Assets: Enumerating and identifying assets affected by vulnerabilities involved a comprehensive assessment that encompassed servers, printers, applications, and critical systems within the USCA network. This process aimed to provide a thorough understanding of the diverse assets scanned and yielded valuable insights into their information. In addition, we meticulously sorted the IP addresses, concentrating specifically on USCA's Operations Centre. This focused approach has contributed to a thorough understanding of connected devices, ensuring a comprehensive grasp of the network's infrastructure.

Phase 2: Identify Threat Scenarios: Identifying potential threat scenarios for each vulnerability, delving into various methods attackers might employ to exploit vulnerabilities and compromise the identified assets. Developing 3 to 4 instances for each vulnerability, outlining specific threat scenarios. This comprehensive exploration is essential to understanding the diverse ways in which vulnerabilities can be exploited, providing insights that aid in crafting robust security measures. By anticipating potential threats, organizations can proactively strengthen their defenses and mitigate risks effectively.

Phase 3: Identify Vulnerability Severity: Evaluating the severity of each vulnerability by leveraging findings from Nexpose, Nessus, and OpenVAS. This assessment considered factors such as Ease of Exploitation, Scope of Impact, Ease of Detection, Availability Impact, Mitigation Difficulty, and Existence of Public Exploits. Employing a scoring scale from 1 to 10 for each factor, we calculated averages to derive a final rating. This systematic approach is necessary to quantitatively measure the potential risk posed by vulnerabilities, providing a comprehensive and objective basis for prioritizing remediation efforts. It ensures that resources are allocated effectively, addressing the most critical vulnerabilities that pose significant threats to the security of the system or network [7,8].

Phase 4: Determine Threat Capability: Assessing the capabilities of potential threat actors who could exploit vulnerabilities, taking into account factors such as skill level, resources, and motivations. Assigned a score out of 10 to gauge their proficiency and intent. This evaluation is crucial to understanding the potential threat landscape and tailoring security measures accordingly. By comprehensively assessing threat actors' capabilities, organizations can better anticipate and prepare for potential attacks, ensuring that defense strategies are aligned with the likely tactics, techniques, and procedures of adversaries [8].

Phase 5: Calculate Risk: Applying the formula: Risk = (Vulnerability Severity $\times$ Threat Capability) to quantify the risk associated with each vulnerability, utilizing the values obtained in the previous phase. This calculation is essential for prioritizing vulnerabilities based on their potential impact and the capabilities of potential threat actors. By assigning a numerical value to the risk, organizations can systematically prioritize remediation efforts, focusing on addressing vulnerabilities that pose the highest risk to the security of the system or network. This approach ensures a strategic and efficient allocation of resources to enhance the overall cybersecurity posture [7].

Phase 6: Prioritize Risks: Ranking the calculated risks to prioritize mitigation efforts, giving precedence to vulnerabilities with higher calculated risks.

Phase 7: Implement Mitigation Measures: Developing and implementing mitigation measures based on prioritized risks, which involved actions such as patching vulnerabilities, implementing security controls, or modifying system architecture. Collaborating closely with the Technology Services Department (TSD) to comprehensively explain the vulnerabilities and conduct a thorough study, facilitating the implementation of the most effective security measures. This collaborative approach is necessary to ensure that mitigation efforts align with organizational goals, technical feasibility, and the severity of identified risks.

This dual-methodology approach, coupled with collaboration with the Technology Services Department (TSD), ensures a holistic and effective strategy for addressing vulnerabilities and enhancing the cybersecurity posture of the USCA network.

4 Conducting the Research

Our research for the ICS/SCADA network vulnerabilities at USCA's Operation Centre followed a meticulous process, incorporating a series of well-defined steps to ensure accuracy and depth in our findings.

4.1 Asset Identification and Vulnerability Assessment

In our initial phase, termed the asset identification phase, the project owner provided us with specific subnets to focus on, including xxx.xxx.178.0/24, xxx.xxx.179.0/24, xxx.xxx.182.0/24, xxx.xxx.185.0/24, xxx.xxx.186.0/24, xxx.xxx.188.0/24, xxx.xxx.190.0/24, xxx.xxx.198.0/24, and xxx.xxx.199.0/24. Our task was to gather as much information as possible about the devices within these subnets, including details such as the operating system, device names, and other relevant information.

To accomplish this, we researched and identified three powerful tools for asset identification: Nmap, Maltego, and Lansweeper. These tools are known for their effectiveness in providing comprehensive insights into the characteristics of networked devices. Subsequently, we initiated scans on the specified subnets using the most aggressive and powerful scanning capabilities offered by these tools.

The gathered information encompassed critical details such as the operating systems employed, device names, MAC addresses, and running services on each device. Once the data was documented, we meticulously sorted and filtered the IPs to focus exclusively on those related to the USCA Operation Centre, following the specific instructions provided by our project owner. This refined inventory ensured that our subsequent phases would be targeted and aligned with the assets directly relevant to the operations center, facilitating a more focused and efficient security assessment.

In the vulnerability assessment phase, following the finalization of the IP list associated with the USCA Operation Centre, we conducted research to identify the most effective vulnerability scanning tools. Opting for a comprehensive approach, we selected three tools: OpenVAS, Nexpose, and Nexus. It's noteworthy that we utilized the professional version of Nexus, provided by our university specifically for this research.

Proceeding with the chosen tools, we initiated the vulnerability scanning process by inputting the identified IPs. The scanning approach adopted was the most aggressive setting available in these tools to ensure a thorough examination. Upon completion of the scans, our next step involved meticulously documenting the vulnerabilities detected by these tools. This documentation served as a foundational step in understanding and addressing the identified vulnerabilities in the USCA Operation Centre's network. Also using our expertise, we did manual testing to uncover vulnerabilities that were not discovered by the vulnerability scanner.

4.2 Risk Assessment

After concluding the vulnerability assessment, the subsequent phase involved a comprehensive risk assessment utilizing the Factor Analysis of Information Risk (FAIR) methodology. The FAIR process unfolds in the following step.

Assets Identification and Threat Scenarios: We listed and identified assets affected by vulnerabilities, such as servers, databases, applications, or critical systems. For each vulnerability, determine potential threat scenarios by exploring various ways attackers could exploit vulnerabilities and compromise identified assets.

Vulnerability Severity: We assessed the severity of each vulnerability based on findings from Nexpose, Nessus, and OpenVAS. Consider factors like Ease of Exploitation, Scope of Impact, Ease of Detection, Availability Impact, Mitigation Difficulty, and Existence of Public Exploits. Assign a score out of 10 for each factor and calculate an overall score.

Examples of Factors

- Ease of Exploitation: Refers to how straightforward it is for an attacker to exploit a vulnerability.
- Scope of Impact: Assesses the potential reach or extent of consequences resulting from vulnerability exploitation.
- Ease of Detection: Evaluates how easily security professionals can identify vulnerability exploitation.
- Availability Impact: Assesses potential harm to system or service availability if a vulnerability is exploited.
- Mitigation Difficulty: Evaluate how challenging it is to apply effective countermeasures to address vulnerability.
- Existence of Public Exploits: Considers whether attackers can readily access tools or techniques to exploit the vulnerability.

Threat Capability and Calculating Risk: Again assigning a score out of 10, we evaluated the capabilities of potential threat actors who might exploit vulnerabilities, considering skill level, resources, and motivations. Utilize the formula Risk=(Vulnerability Severity×Threat Capability) to calculate the risk score for each vulnerability. This quantitative measure provides insights into the potential impact and likelihood of exploitation.

Prioritize Risks: We rank the calculated risks from the previous phase to prioritize mitigation efforts. Focus on addressing vulnerabilities with higher calculated risks first, ensuring a strategic allocation of resources to address the most critical security concerns.

This systematic FAIR methodology allows for a comprehensive understanding of the risk landscape associated with vulnerabilities. By factoring in asset

identification, potential threat scenarios, vulnerability severity, and threat capability, organizations gain actionable insights to prioritize and implement effective risk mitigation strategies.

4.3 Feasibility Study and Effectiveness Evaluation

In the Feasibility Study and Effectiveness Evaluation phase, collaboration with the Technology Services Department (TSD) was paramount. We engaged in a detailed explanation of identified vulnerabilities, providing insights into the best mitigation strategies. Once a consensus was reached and we were confident in the chosen mitigation strategy, TSD took charge of the implementation. After the security measures were successfully implemented, we conducted thorough testing to ascertain their effectiveness. This involved a comprehensive vulnerability assessment utilizing both automated tools and manual testing methodologies used earlier. The objective was to ensure that the identified issues were not only addressed but also effectively resolved, validating the robustness of the implemented security measures. This collaborative and iterative approach aimed to enhance the overall cybersecurity posture of the USCA network.

5 Findings and Results

5.1 Asset Identification

Upon scanning with Nmap, Lansweeper, and Maltego, we obtained details of the assets. We then sorted out the IPs related to the operation centre as specified by the Project Owner. The IPs related to the operation center are: xxx.xxx.185.10, xxx.xxx.188.11, xxx.xxx.186.9, xxx.xxx.185.3, xxx.xxx.185.26, xxx.xxx.186.109, xxx.xxx.198.4, xxx.xxx.186.205, xxx.xxx.178.126, xxx.xxx.179.252, xxx.xxx.185.7, xxx.xxx.185.157, xxx.xxx.185.160, xxx.xxx.185.163, xxx.xxx.185.17, xxx.xxx.185.179, xxx.xxx.185.18, xxx.xxx.185.182, xxx.xxx.185.198, xxx.xxx.185.5, xxx.xxx.185.78, xxx.xxx.185.82, xxx.xxx.185.87, and xxx.xxx.185.9. These IPs are associated with the operation centre, and we gathered details such as device names, MAC addresses, device types, and running OS for each. This targeted approach enhances our understanding of the assets within the operation centre, ensuring a more effective vulnerability assessment and mitigation strategy (Table 1 and Fig. 1).

5.2 Vulnerability Assessment

Commencing the vulnerability assessment, we utilized tools like Nexpose, Nessus, and OpenVAS, complemented by manual penetration testing to uncover vulnerabilities potentially missed by automated scans. Post-assessment, the focus shifted to vulnerabilities of high and medium severity. The identified vulnerabilities and their impacted assets include:

Table 1. USCA's Operation Centre IPs

IP Address	Vendor	OS	Open Ports
xxx.xxx.185.10	Linux	Linux 3.2–4.9	22, 80, 443, 4444
xxx.xxx.188.11	Linux	Linux 3.2–4.9	22, 80, 443, 4444
xxx.xxx.186.9	Linux	Linux 3.2–4.9	80, 1935, 5959
xxx.xxx.185.3	–	Brother DCP-8065D printer	80
xxx.xxx.185.26	–	–	NA
xxx.xxx.186.109	Linux	Linux 3.2–4.9	22, 80, 443, 4444
xxx.xxx.198.4	Linux	Linux 3.2–4.9	22, 80, 443, 4444
xxx.xxx.186.205	Linux	Linux 3.2–4.9	22, 80, 443, 4444
xxx.xxx.178.126	-	Brother MFC-8460N	80
xxx.xxx.179.252	–	–	NA
xxx.xxx.185.7	–	Brother HL-2270DW	80
xxx.xxx.185.157	Linux	Linux 3.10–4.11	443
xxx.xxx.185.160	Microsoft	Microsoft Windows Server 2019	135, 139, 445, 3389
xxx.xxx.185.163	Linux	Linux 3.10–4.11	443
xxx.xxx.185.17	Linux	Linux 2.6 13–2.6 32	80, 443
xxx.xxx.185.179	Microsoft	Microsoft Windows Server 2019	135, 139, 445, 3389
xxx.xxx.185.18	Linux	Linux 2.6 13–2.6 32	80, 443
xxx.xxx.185.182	Microsoft	Microsoft Windows 10 1909	135, 139, 445, 3389
xxx.xxx.185.198	Microsoft	Microsoft Windows Server 2019	135, 139, 445, 3389
xxx.xxx.185.5	–	Apple AirPort Extreme WAP	80, 3011
xxx.xxx.185.78	Linux	Linux 2.6.32	22, 80, 443, 10001
xxx.xxx.185.82	Linux	Linux 2.6.32	22, 80, 443, 10001
xxx.xxx.185.87	Microsoft	Microsoft Windows 10 1909	135, 139, 445, 3389
xxx.xxx.185.9	Linux	Linux 2.6 13–2.6 32	80, 443

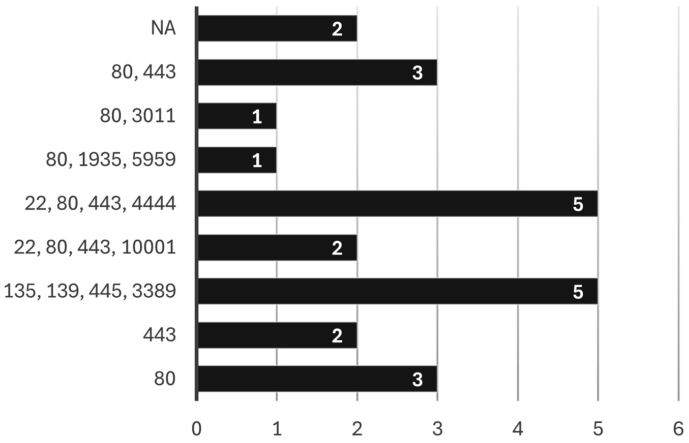

Fig. 1. Count of IP Addresses by Open Ports

1. HTTP Brute Force Logins with Default Credentials. This vulnerability involves attackers attempting to gain unauthorized access to the system by repeatedly trying different usernames and passwords.

- **Impacted Assets:** xxx.xxx.178.126, xxx.xxx.185.17, xxx.xxx.185.18, xxx.xxx.185.9

2. Lack of HTTPS Implementation. The absence of HTTPS implementation poses a security risk as it leaves communications between users and the website unencrypted.

- **Impacted Assets:** xxx.xxx.185.10, xxx.xxx.188.11, xxx.xxx.186.9, xxx.xxx.186.109, xxx.xxx.198.4, xxx.xxx.186.205, xxx.xxx.178.126, xxx.xxx.185.17, xxx.xxx.185.18, xxx.xxx.185.5, xxx.xxx.185.9

3. SSL/TLS: Renegotiation Dos Vulnerability/deprecated TLS V1.0 and TLS V1.1 Protocol Detection. This vulnerability pertains to weaknesses in SSL/TLS protocols, potentially leading to Denial of Service (DoS) attacks.

- **Impacted Assets:** xxx.xxx.185.10, xxx.xxx.188.11, xxx.xxx.186.9, xxx.xxx.186.109, xxx.xxx.198.4, xxx.xxx.186.205, xxx.xxx.185.160, xxx.xxx.185.179, xxx.xxx.185.182, xxx.xxx.185.198, xxx.xxx.185.78, xxx.xxx.185.82, xxx.xxx.185.87

4. Default or Guessable SNMP Community Names: Public (SNMP-read-0001). This vulnerability involves using default or easily guessable SNMP community names, potentially exposing sensitive information.

- **Impacted Assets:** xxx.xxx.185.26, xxx.xxx.178.126, xxx.xxx.179.252, xxx.xxx.185.3, xxx.xxx.185.7

5. SNMP Credentials Transmitted in Clear Text (SNMP-Clear Text-Credential). This vulnerability highlights the risk of transmitting SNMP credentials in plaintext, making it susceptible to interception.

- **Impacted Assets*:*** xxx.xxx.185.26, xxx.xxx.178.126, xxx.xxx.179.252

6. SSH Terrapin Prefix Truncation Weakness. This vulnerability involves a weakness in SSH (Secure Shell) related to Terrapin prefix truncation.

- **Impacted Assets*:*** xxx.xxx.185.10, xxx.xxx.186.205, xxx.xxx.188.11, xxx.xxx.198.4

This meticulous approach to addressing vulnerabilities enhances the precision of mitigation strategies, fortifying the USCA network's overall security.

5.3 Risk Assessment

Our risk assessment relies on the FAIR methodology, a structured approach comprising multiple phases to assign a risk score. This score plays a crucial role in prioritizing vulnerabilities, giving heightened attention to those with higher risk scores. Additionally, we must conduct thorough research on each vulnerability, exploring its description, potential impact, and the associated consequences. This comprehensive analysis ensures that we gain a deep understanding of vulnerabilities, facilitating effective prioritization. By grasping the risks thoroughly, we can plan and implement more effective strategies to safeguard against potential threats and vulnerabilities.

1. SSL/TLS: Renegotiation DoS Vulnerability/Deprecated TLS V1.0 and TLS V1.1 Protocol Detection

- **Threat Scenarios**: During Service Disruption, an attacker exploits the Renegotiation DoS Vulnerability, causing downtime. Coordinated Resource Exhaustion attacks lead to degraded server performance. In Man-in-the-Middle Attacks, outdated TLS/SSL protocols risk unauthorized access. SSL Stripping involves forcing a downgrade, and exposing data in plaintext.

- **Vulnerability Severity:**

- *Ease of Exploitation:* 8/10
- *Scope of Impact:* 7/10
- *Ease of Detection:* 5/10
- *Availability Impact:* 8/10
- *Mitigation Difficulty:* 6/10
- *Existence of Public Exploits:* 3/10
- *Overall Severity Rating:* 6/10

- **Threat Capability:**

- *Score:* 6/10

- **Risk Score:**
  - *Risk = Vulnerability Severity × Threat Capability*
  - *Score:* 36

2, Lack of HTTPS

- **Threat Scenarios:** In Man-in-the-Middle Attacks, intercepting unencrypted communication risks unauthorized access to sensitive data. Data Tampering involves maliciously modifying unencrypted data, risking misinformation. Session Hijacking captures unencrypted session tokens, allowing unauthorized access. Eavesdropping on Confidential Information exposes sensitive data. Phishing Attacks use deceptive websites to capture user information, leading to potential identity theft or credential compromise.

– **Vulnerability Severity:**

– *Ease of Exploitation:* 5/10
– *Scope of Impact:* 8/10
– *Ease of Detection:* 6/10
– *Availability Impact:* 4/10
– *Mitigation Difficulty:* 3/10
– *Existence of Public Exploits:* 5/10
– *Overall Severity Rating:* 5/10

– **Threat Capability:**

– *Score:* 3/10

– **Risk Score:**

– *Risk = Vulnerability Severity × Threat Capability*
– *Score:* 15

Default or Guessable SNMP Community Names: Public

– **Threat Scenarios:** In Unauthorized Access to SNMP Devices, attackers use default or commonly guessed SNMP community names, resulting in unrestricted access, potential retrieval of sensitive information, and device configuration modification. Device Configuration Tampering involves exploiting default community strings to alter SNMP-enabled device configurations, leading to service disruptions, unauthorized access, or compromised device integrity. Information Disclosure occurs when attackers leverage default SNMP community names to extract sensitive information, leading to the unauthorized disclosure of device details or network topology.

– **Vulnerability Severity:**
  - *Ease of Exploitation:* 8/10
  - *Scope of Impact:* 9/10
  - *Ease of Detection:* 5/10
  - *Availability Impact:* 7/10
  - *Mitigation Difficulty:* 6/10
  - *Existence of Public Exploits:* 8/10
  - *Overall Severity Rating:* 7.2/10

– **Threat Capability:**

– *Score:* 6/10

– **Risk Score:**

– *Risk = Vulnerability Severity × Threat Capability*
– *Score:* 43.2

SNMP Credentials Transmitted in Cleartext

- **Threat Scenarios:** During Network Sniffing, attackers eavesdrop on network traffic to capture SNMP credentials transmitted in cleartext, resulting in unauthorized access to SNMP-enabled devices and potential unauthorized configuration changes or information disclosure. Credential Interception involves malicious actors intercepting SNMP traffic containing cleartext credentials, compromising network security. In Man-in-the-Middle Attacks, attackers position themselves between the SNMP manager and agent to intercept cleartext credentials, leading to unauthorized access, device manipulation, or unauthorized information retrieval from SNMP-enabled devices. The use of Credential Sniffing Tools by attackers allows them to capture SNMP credentials transmitted in cleartext, potentially leading to unauthorized access, service disruptions, unauthorized configuration changes, or information disclosure.

Vulnerability Severity:

- *Ease of Exploitation:* 6/10
- *Scope of Impact:* 8/10
- *Ease of Detection:* 4/10
- *Availability Impact:* 5/10
- *Mitigation Difficulty:* 7/10
- *Existence of Public Exploits:* 6/10
- *Overall Severity Rating:* 6/10

- **Threat Capability:**
  - *Score:* 5/10

- **Risk Score:**

- *Risk = Vulnerability Severity × Threat Capability*
- *Score:* 30

HTTP Brute Force Logins with Default Credentials

- **Threat Scenarios:**In Unauthorized Actions by Attackers, successful brute force login allows attackers to perform unauthorized actions within the web application, compromising data integrity and introducing malicious content. Credential Guessing Attacks involve attackers launching brute force attacks against HTTP login pages using default credentials, leading to unauthorized access to web applications or services and potentially resulting in data breaches or unauthorized action.

- **Vulnerability Severity:**

- *Ease of Exploitation:* 7/10

- *Scope of Impact:* 8/10
- *Ease of Detection:* 5/10
- *Availability Impact:* 3/10
- *Mitigation Difficulty:* 6/10
- *Existence of Public Exploits:* 8/10
- *Overall Severity Rating:* 6/10

- **Threat Capability:**

- *Score:* 8/10

- **Risk Score:**

- *Risk = Vulnerability Severity × Threat Capability*
- *Score:* 48

SSH Terrapin Prefix Truncation Weakness

- **Threat Scenarios:** In a Man-in-the-Middle Attack, the attacker exploits the Terrapin Prefix Truncation Weakness to manipulate SSH connections, leading to the interception and potential alteration of transmitted data between the client and server. Unauthorized Access occurs when an adversary takes advantage of the vulnerability to truncate prefixes in SSH traffic, attempting unauthorized access to a system by exploiting weakened cryptographic protections. Additionally, Data Manipulation ensues as the vulnerability is exploited to modify the content of SSH traffic, allowing attackers to manipulate commands or data transmitted between the client and server.

- **Vulnerability Severity:**

- *Ease of Exploitation:* 7/10
- *Scope of Impact:* 8/10
- *Ease of Detection:* 5/10
- *Availability Impact:* 7/10
- *Mitigation Difficulty:* 6/10
- *Existence of Public Exploits:* 6/10
- *Overall Severity Rating:* 6.5/10

Threat Capability:

- *Score:* 7/10

- **Risk Score:**

- *Risk = Vulnerability Severity × Threat Capability*
- *Score:* 45.5

5.4 Mitigation Measures

SSL/TLS: Renegotiation Dos Vulnerability/Deprecated TLS V1.0 and TLS V1.1 Protocol

- Firstly, we prioritize updating our software regularly, focusing on the SSL/TLS library and server software to address any known vulnerabilities, such as the renegotiation DoS vulnerability. Additionally, we optimize our SSL/TLS configuration settings to minimize the impact of renegotiation. This involves considering options to limit its frequency or even disabling renegotiation based on the specific server software in use. In cases where uncertainty or assistance is needed, we recommend reaching out to the vendor or support community associated with the server software for guidance on configurations and updates.

Lack of HTTPS

- We've installed a valid SSL/TLS certificate for robust HTTPS encryption, ensuring the confidentiality and integrity of transmitted data. All resource references, both internal and external, have been updated to exclusively use HTTPS. Additionally, we've configured automatic redirection of HTTP traffic to the secure HTTPS version, activated HSTS for enhanced security, and established a well-protected environment for secure user-system communication.

Default or Guessable SNMP Community Names: Public

- Firstly, we've strengthened security by changing the SNMP community string from the default "public" to a resilient, non-guessable value, heightening protection against unauthorized access. Additionally, to fortify security, we've embraced strong authentication mechanisms, particularly SNMPv3, which supports secure authentication and encryption, providing an advanced layer of protection for SNMP communications. To exercise greater control, we've configured access control lists (ACLs) to restrict SNMP access solely to authorized IP addresses or specific network ranges. As a proactive step, we conduct regular audits of SNMP configurations, enabling the detection and rectification of any instances of default or weak community strings.

HTTP Brute Force Logins with Default Credentials

- Firstly, we've proactively replaced default credentials for all systems and applications with strong, unique passwords. This foundational step significantly reduces the risk associated with default login information, fortifying our security stance. Additionally, to mitigate the impact of brute force attacks, we've enforced account lockout policies, limiting the number of failed login attempts and enhancing security by temporarily locking out accounts

displaying suspicious activity. Furthermore, we've introduced Multi-Factor Authentication (MFA) to add an extra layer of security, requiring users to provide multiple forms of verification for authentication.

SNMP Credentials Transmitted in Cleartext

– To enhance the security of our SNMP (Simple Network Management Protocol) implementation, we've adopted SNMPv3, which offers secure transmission through encryption and authentication mechanisms. Specifically, we've configured SNMPv3 with robust authentication protocols to ensure the confidentiality and integrity of transmitted credentials. In addition, access control lists (ACLs) have been employed to restrict SNMP access solely to authorized devices, minimizing the risk of unauthorized interception.

SSH Terrapin Prefix Truncation Weakness

– To enhance SSH server security, we've upgraded our software to patch against the Terrapin vulnerability. Additionally, we've temporarily disabled vulnerable key exchange algorithms, like ChaCha20-Poly1305, and reached out to the vendor for guidance on specific configurations and updates. These proactive steps ensure a more secure SSH server environment. Additionally, to address any uncertainties or seek assistance in this process, we've proactively reached out to the vendor or support community associated with our server software (Fig. 2).

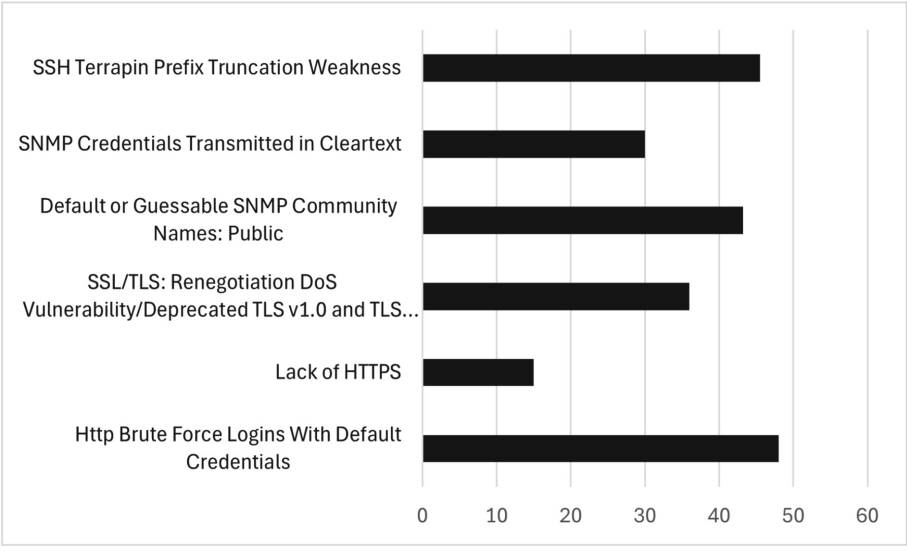

Fig. 2. Risk Score of Vulnerabilities

6 Conclusion

6.1 Summary of Findings

This research has meticulously identified and examined significant security vulnerabilities within various network protocols, providing insights into the potential threats and risks associated with these weaknesses. Notably, the SSL/TLS renegotiation vulnerability presents a substantial risk of service disruption and resource exhaustion, while the absence of HTTPS implementation exposes users to diverse attacks like man-in-the-middle and session hijacking. Additionally, vulnerabilities stemming from default or easily guessed SNMP community names and the cleartext transmission of SNMP credentials may result in unauthorized access and information disclosure. The study also delves into the risks linked to HTTP brute force logins and the SSH Terrapin Prefix Truncation Weakness, emphasizing the possibilities of unauthorized actions and data manipulation.

It is crucial to highlight the significance of manual penetration testing, as demonstrated in the discovery of the default password vulnerability, which was identified through manual testing rather than automated vulnerability scanners. This underscores the importance of human intervention in uncovering nuanced vulnerabilities that automated tools might overlook. This emphasizes the significance of having a responsible disclosure program because penetration testers worldwide, each possessing diverse expertise and perspectives, can identify vulnerabilities within the system.

Furthermore, regular assessments using scanners such as Nexpose, Nessus, and OpenVAS are imperative. This approach ensures continuous monitoring and vulnerability identification, especially in educational institutions like USCA, where maintaining a secure environment is of utmost importance.

Also the incorporation of both CIS (Center for Internet Security) and FAIR (Factor Analysis of Information Risk) methodologies greatly benefited this project's risk assessment. CIS provided a structured approach for implementing security controls, ensuring comprehensive vulnerability management. Meanwhile, FAIR's systematic risk scoring process offered a quantitative way to assess and prioritize risks, leading to a nuanced understanding of potential impacts. The synergy between these methodologies resulted in a robust risk assessment framework, identifying critical vulnerabilities and facilitating the development of effective mitigation strategies. This integrated approach enhanced the overall resilience and security of the network environment.

6.2 Limitations

1. **Scope of Manual Human Pen-testing:** Another limitation stems from the reliance on manual human penetration testing. The effectiveness of manual testing is subject to the expertise of the researcher conducting the assessments. The research acknowledges the variability in the skill levels of different researchers, with some being advanced penetration testers and others having

varying levels of expertise. This introduces a potential limitation in the thoroughness and accuracy of manually identified vulnerabilities. The diversity in skill levels among researchers may impact the comprehensiveness of the vulnerability assessment [9,10].

2. **Limited Vulnerability Scanners:** One notable limitation of this research lies in the use of only three automated vulnerability scanners-Nexpose, Nessus, and OpenVAS. While these scanners are reputable and widely used, there are several other prominent tools in the market, such as Qualys and Acunetix, which were not included in this study. The exclusion of these alternative scanners may result in a potential oversight of vulnerabilities that they might have been more adept at identifying. The findings may not represent the full spectrum of vulnerabilities present in the systems under investigation [9,10].
3. **Dynamic Nature of Cybersecurity:** The rapidly evolving landscape of cybersecurity poses an inherent limitation to any research in this domain. The vulnerabilities identified and discussed in this study are based on the state of technology up to the knowledge cutoff date. New vulnerabilities may emerge after this date, rendering the research susceptible to being outdated. The dynamic nature of cyber threats emphasizes the need for continuous monitoring and updates to stay abreast of the latest vulnerabilities [11,12],

References

1. Samtani, S., Yu, S., Zhu, H., Patton, M., Chen, H.: Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. In: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pp. 25–30. IEEE (2016)
2. Nankya, M., Chataut, R., Akl, R.: Securing industrial control systems: components, cyber threats, and machine learning-driven defense strategies. Sensors **23**(21), 8840 (2023)
3. Kaura, C., Sindhwani, N., Chaudhary, A.: Analysing the impact of cyber-threat to ICS and SCADA systems. In: 2022 International Mobile and Embedded Technology Conference (MECON), pp. 466–470. IEEE (2022)
4. Francia III, G. A., Thornton, D., Dawson, J.: Security best practices and risk assessment of SCADA and industrial control systems. In: Proceedings of the international conference on security and management (SAM), p. 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) (2012)
5. Shypovskyi, V.: Enhancing the factor analysis of information risk methodology for assessing cyberresilience in critical infrastructure information systems. Polit. Sci. Secur. Stud. J. **4**(1), 25–33 (2023)
6. Christensen, K.K., Petersen, K.L.: Public-private partnerships on cyber security: a practice of loyalty. Int. Aff. **93**(6), 1435–1452 (2017)
7. Tunggal, A.T.: How to Perform a Cybersecurity Risk Assessment. UpGuard (2018). Accessed 19 Oct 2023. https://www.upguard.com/blog/how-to-perform-a-cybersecurity-risk-assessment
8. Cybersecurity risk assessments. SailPoint (2023). Accessed 19 Oct 2023. https://www.sailpoint.com/identity-library/cybersecurity-risk-assessments/

9. Stefinko, Y., Piskozub, A., Banakh, R.: Manual and automated penetration testing. Benefits and drawbacks: modern tendency. In: 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), pp. 488–491. IEEE (2016)
10. Alavi, S., Bessler, N., Massoth, M.: A comparative evaluation of automated vulnerability scans versus manual penetration tests on false-negative errors. In: Proceedings of the Third International Conference on Cyber-Technologies and Cyber-Systems, IARIA, Athens, Greece, pp. 18–22 (2018)
11. Cremer, F., et al.: Cyber risk and cybersecurity: a systematic review of data availability. Geneva Papers Risk Insur.-Issues Pract. **47**(3), 698–736 (2022)
12. Johnston, A.C.: A closer look at organizational cybersecurity research trending topics and limitations. Organ. Cybersecur. J. Pract. Process People **2**(2), 124–133 (2022)