**Industrial Cybershield Project Proposal**

**Submitted by:**

Negin Sorati, Bita Kiyani, Brahmjot

**Submitted to:**

Victor Mendez

James ....

BCIT Industrial Networking Cybersecurity Program

**Submission Date:**

May 22, 2024

**Project Duration:**

April 22nd - May 23rd, 2024

**Executive Summary**

The "Industrial Cybershield" is the final project for our course “INCS” that aims to showcase the impact of cyberattacks against networks and industrial control systems. The primary objectives are to build an industrial network environment virtually, find security loopholes and vulnerabilities in un-patched systems.

To achieve our objectives, we will use VMware to create a virtual environment that accurately replicates various components of an industrial network. This virtual setup will include servers, workstations, networking devices, and other critical infrastructure elements typically found in such environments.

Once the virtual environment is established, we will proceed to conduct thorough vulnerability assessments. These assessments will be designed to identify any potential weaknesses, misconfigurations, or security gaps within the systems. By doing so, we aim to uncover vulnerabilities that cybercriminals might exploit. We will utilize a Kali machine to systematically exploit the identified vulnerabilities within the network. By doing so, we aim to gain unauthorized access to the network infrastructure. Once access is achieved, we will proceed to take control of the actual industrial controllers. This process will help illustrate the potential impact of such security breaches on a real-world industrial plant.

Then, we will work on securing the network by applying cybersecurity standards such as ISA/IEC 62443. We will enhance security by segmenting the network into different zones, configuring Access Control Lists (ACLs) on the firewalls, and blocking unused ports. These measures will help to create a more robust and secure network infrastructure, mitigating the risk of cyberattacks and ensuring the integrity and reliability of the industrial control systems.

The project's successful conclusion will demonstrate the team's capacity to plan, carry out, and manage a safe industrial control system environment. Organizations seeking to improve the cybersecurity of their industrial networks can benefit greatly from the knowledge gained and the security solutions created.

**Introduction**

In this report, we will showcase what we accomplished for our culminating project over the past five weeks. We created a virtual industrial network using VMware, conducted vulnerability assessments and penetration testing with Kali Linux, and applied cybersecurity standards to secure the network. Our efforts included network segmentation, firewall configuration, and blocking unused ports to enhance overall security.

**Project Description**

**Project Scope**

The scope of this project involves the creation and security enhancement of a virtual industrial network environment over a period of five weeks. The key components of the project scope include:

1. **Virtual Environment Creation**:
   * Utilize VMware to construct a comprehensive virtual environment that accurately replicates various components of an industrial network, including servers, workstations, and critical infrastructure elements.
2. **Vulnerability Assessment and Penetration Testing**:
   * Employ Kali Linux OS to conduct thorough vulnerability assessments and penetration testing.
   * Identify and exploit vulnerabilities within the virtual network to demonstrate potential security breaches.
3. **Security Enhancement:**
   * Apply cybersecurity standards, specifically ISA/IEC 62443, to improve network security.
   * Implement network segmentation to create isolated zones within the network.
   * Configure Access Control Lists (ACLs) on firewalls to regulate traffic and enhance security.
   * Block unused ports to reduce potential entry points for cyberattacks.
4. **Impact Demonstration:**
   * Illustrate the potential impact of identified vulnerabilities by controlling industrial controllers within the virtual environment.
   * Demonstrate the effectiveness of implemented security measures in mitigating risks and protecting the network.

**Team Coordination & Task Allocation**

During the whole project work we would be using WhatsApp for sharing content & Communication with each other along with Google docs if needed. Mostly everyone will participate in designing, configuring, creating the vulnerable network and an exploit for the vulnerable network.

Bita will oversee both the vulnerable and secure networks' OT (Operational Technology) components. This will involve installing and configuring the PLC and Factory IO. Recognizing the inherent vulnerabilities of OT systems, Bita will also focus on implementing robust security measures to safeguard these critical elements.

Negin is going to oversee the project's IT components. Installing and setting up the PfSense firewall, Windows Server for DNS and Active Directory services, and IT workstation running Windows 10 are all included in this. To ensure a thorough defense-in-depth approach, Negin will be responsible for configuring the firewall rules for both the initial and secure network segments.

Brahmjot will take on the responsibility of creating and executing the attack plan for the vulnerable network. He will research and identify the most suitable attack vectors, potentially bypassing security measures like Windows Defender, to gain unauthorized access and extract critical information from the system. Brahmjot's expertise in offensive security techniques will be instrumental in exposing the network's weaknesses.

The team members will cooperate and communicate freely to resolve any problems that may occur in the network or during the execution of the attack throughout the project. By working together, the team will be able to promptly recognize and address any issues, preserving the integrity of the virtual ICS environment.

The team will also collaborate to create the PowerPoint presentation and put together the final report. A complete and well-rounded deliverable that highlights the team's accomplishments and lessons learned will be the product of this collaborative effort.

**Resource Limitation:**

We had to utilize our personal laptops instead of lab computers to accommodate the necessity of working on separate project components and for the sake of our comfort. However, this decision led to slower processing speeds and performance in the demo.

Furthermore, we encountered a limitation in not having access to a public domain for hosting an accurate phishing website.

Additionally, we faced challenges with port forwarding due to a lack of available means, compounded by the absence of access to a public IP address for translating it to our private IPs.

**Project Milestones:**

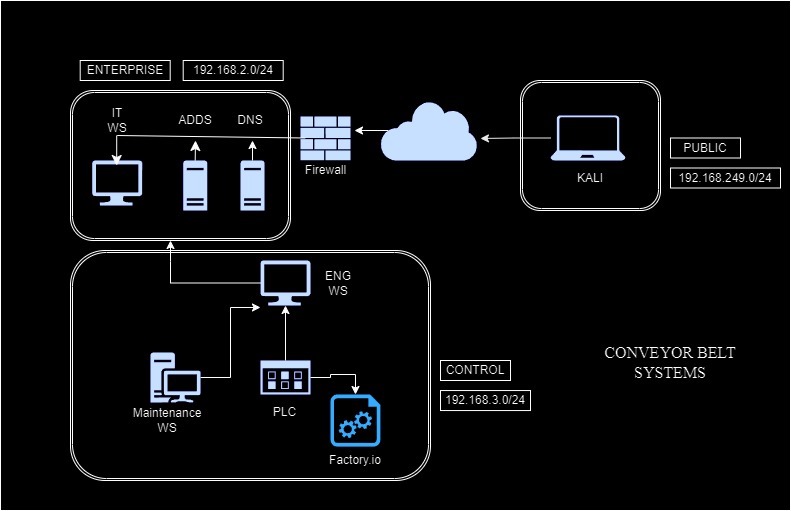
The conclusion of the final design phase will be the first and most important milestone of our project. We will have a detailed blueprint after this phase that outlines the architecture and elements of our virtual Industrial Control System (ICS) network. This plan will act as the foundation for the next stages of implementation and execution. By reaching this milestone, we will lay the groundwork for the project. We will have a clear plan to follow as we proceed with the construction and testing of our virtual ICS environment after the network design is complete and approved. This benchmark will provide us the assurance and guidance we need to complete the project effectively and on schedule. After reaching this milestone, we will be well-positioned to proceed with the project's next phases, which will involve installing security measures, assessing vulnerabilities, and delivering the project's final deliverables.

**Project Details:**

**Virtualization Software**

We will use VMware Workstation Pro, as it makes it easier for us to set up a shared network and virtual machines that everyone in the group may use. Also, we can configure and install all components of both vulnerable and secure networks in VMware.

**Initial Network Topology**



Public Network:

This network is divided into three main areas: Public (External), Enterprise (IT), and Control (OT). In the External area, a Kali Linux machine represents the simulated threat actor, connected to the internet, and positioned to exploit any vulnerabilities in the network. The pfSense firewall serves as the primary defense mechanism, positioned between the internet and the internal IT network segment.

Enterprise Network:

Within the Enterprise area, the network includes an IT Workstation running Windows 10 and an IT Domain Controller running Windows Server 2022. These IT components provide the essential services and infrastructure for the overall enterprise operations.

The IT Workstation is a typical end-user device that workers in the company would use to get access to different IT tools and programs. It functions as a client system, enabling users to engage with the enterprise network and carry out their regular tasks.

Active Directory Domain Services (AD DS) and the Domain Name System (DNS), which are essential to the IT infrastructure, are provided by the IT Domain Controller, which is powered by Windows Server 2022. Within the enterprise network domain, user accounts, group memberships, and machine accounts are managed by the Active Directory Domain Services, which are also hosted by the Domain Controller. When a person or device tries to access resources, AD DS oversees verifying their identity and granting them access according to their roles and group memberships. The IT infrastructure's access controls, password regulations, and other security-related settings may be enforced thanks to this centralized user and device management.

Control Network and OT Network Configuration

**System Components**

1. OT Workstation

The OT workstation is a Windows 10 machine that serves as a connection between the IT and OT parts of the network.

2. PLC Workstation

The PLC workstation is a dedicated Windows 10 machine that hosts both the OpenPLC Editor and the OpenPLC Runtime.

* OpenPLC Editor: This software is used to create and edit our program written in ladder logic, that is a graphical programming language used for designing control schemes in industrial automation.
* OpenPLC Runtime: After developing the ladder logic in the OpenPLC Editor, the program is uploaded to the OpenPLC Runtime on the same workstation. The runtime environment executes the control logic, managing inputs and outputs according to the defined program.
* Cygwin64: A Unix-like environment and command-line interface for Windows, used to facilitate the connection and interaction with the OpenPLC Runtime. Cygwin64 provides a range of Unix tools and utilities that make managing and monitoring the runtime environment more efficient.

3. Factory IO

Factory IO is another Windows 10 system used for visualizing industrial processes in a 3D simulation environment. It connects to the PLC workstation via IP addresses and the Modbus protocol (server) to display real-time graphical results of the control logic executed by the OpenPLC Runtime.

**Network Configuration**

Modbus is a widely used communication protocol in industrial environments, facilitating data exchange between devices. In this OT network, Modbus TCP/IP is utilized to connect the PLC workstation and Factory IO.

**Modbus Server Configuration**

The PLC workstation runs a Modbus server through the OpenPLC Runtime. This server listens for connections from Factory IO.

Appropriate IP addresses and port numbers are configured to establish reliable communication. We used the default Modbus TCP port, that is 502.

**Ladder Logic Programming and Execution**

All ladder logic programming and execution occur on the PLC workstation, which simplifies the development and deployment process.

Programming:

The OpenPLC Editor on the PLC workstation is used to create ladder logic diagrams. These diagrams consist of various logic elements like contacts, coils, timers, and counters, arranged to represent the desired control sequences and conditions.

Deployment and Execution:

Once the ladder logic program is developed, it is uploaded directly from the OpenPLC Editor to the OpenPLC Runtime on the same PLC workstation, The OpenPLC Runtime then interprets and executes the ladder logic. It reads input signals, processes the control logic, and updates output signals in real time.

Connection with Cygwin64: To facilitate this process, Cygwin64 is used to provide a Unix-like environment on the Windows-based PLC workstation. This setup allows for more efficient management and monitoring of the OpenPLC Runtime through familiar Unix tools and commands.

**Visualization with Factory IO**

Factory IO provides a 3D simulation environment to visualize the results of the ladder logic executed by the OpenPLC Runtime written in OpenPLC Editor.

Connection Setup:

Factory IO is configured to connect to the Modbus server running on the PLC workstation. The IP address and port number of the PLC workstation are specified in the Factory IO settings.

This connection allows Factory IO to access the state of the inputs and outputs managed by the OpenPLC Runtime.

**Draft Potential Vulnerabilities:**

The network suffers from a critical weakness due to the absence of network segmentation and access controls between the IT and OT zones. This vulnerability is worsened by a single permissive rule on the pfSense firewall, allowing unrestricted traffic between these domains. The rule's default action of "Pass" permits any packet that meets the criteria to flow through without limitations. Moreover, applying this rule to the "LAN" interface blurs the distinction between the OT (192.168.3.0/24) and IT (192.168.2.0/24) network segments, leaving them vulnerable to external threats. Additionally, the rule allows unfettered communication within the network by designating "LAN subnets" as the source and "Any" as the destination, further exposing it to potential risks.

In addition to the firewall vulnerabilities, the PLC and Factory IO components in the network setup are not properly secured. Since these devices are part of the OT network, there's a chance that flaws in their operating system, installed apps, or firmware might allow hackers to take over industrial operations and cause systemic disruptions.

Starting with the Attack

**Gathering Information:**

In this initial phase, we collected vital information about the plant, including the names of operators, their managers, the software they used, and the controller's company.

**A screenshot of a computer screen

Description automatically generatedCreating the Payload:** For this crucial step, we utilized a Hoaxshell tool to generate a PowerShell reverse shell.

*NGROK Public IP for kali Machine, listening to port 8080*

**Obfuscating The Payload:**

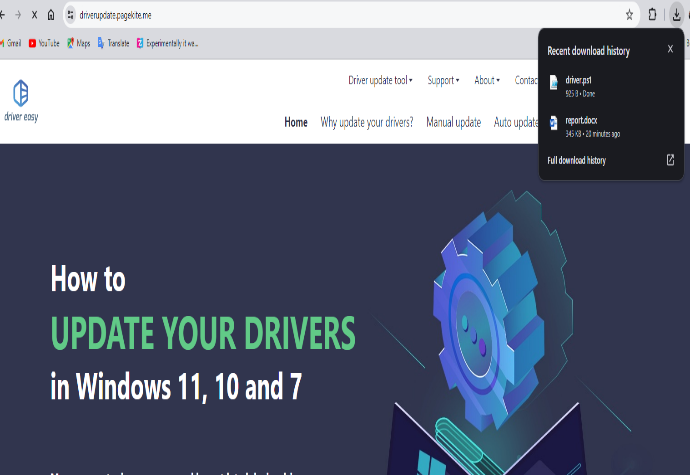
A screen shot of a computer screen

Description automatically generatedInitially, we manually obfuscated the payload to evade detection by Windows Defender, But then created OBf.py to do the obfuscation by concealing client names and substituting them with other terms and adding random apostrophes (‘)s. To enable the reverse shell over the internet, we then translated our Kali machine's IP to Ngok's public IP.

*This will make the PowerShell windows hidden!*

**Delivery:**

To execute the attack, we crafted a convincing phishing email to deceive the admin, urging them to update/install a new driver from a designated website. Leveraging the information gathered, we fabricated a fake website (driverupdate.pagekite.me), which we hosted on a PageKite web server to make it publicly accessible.

A computer screen shot of a program

Description automatically generated

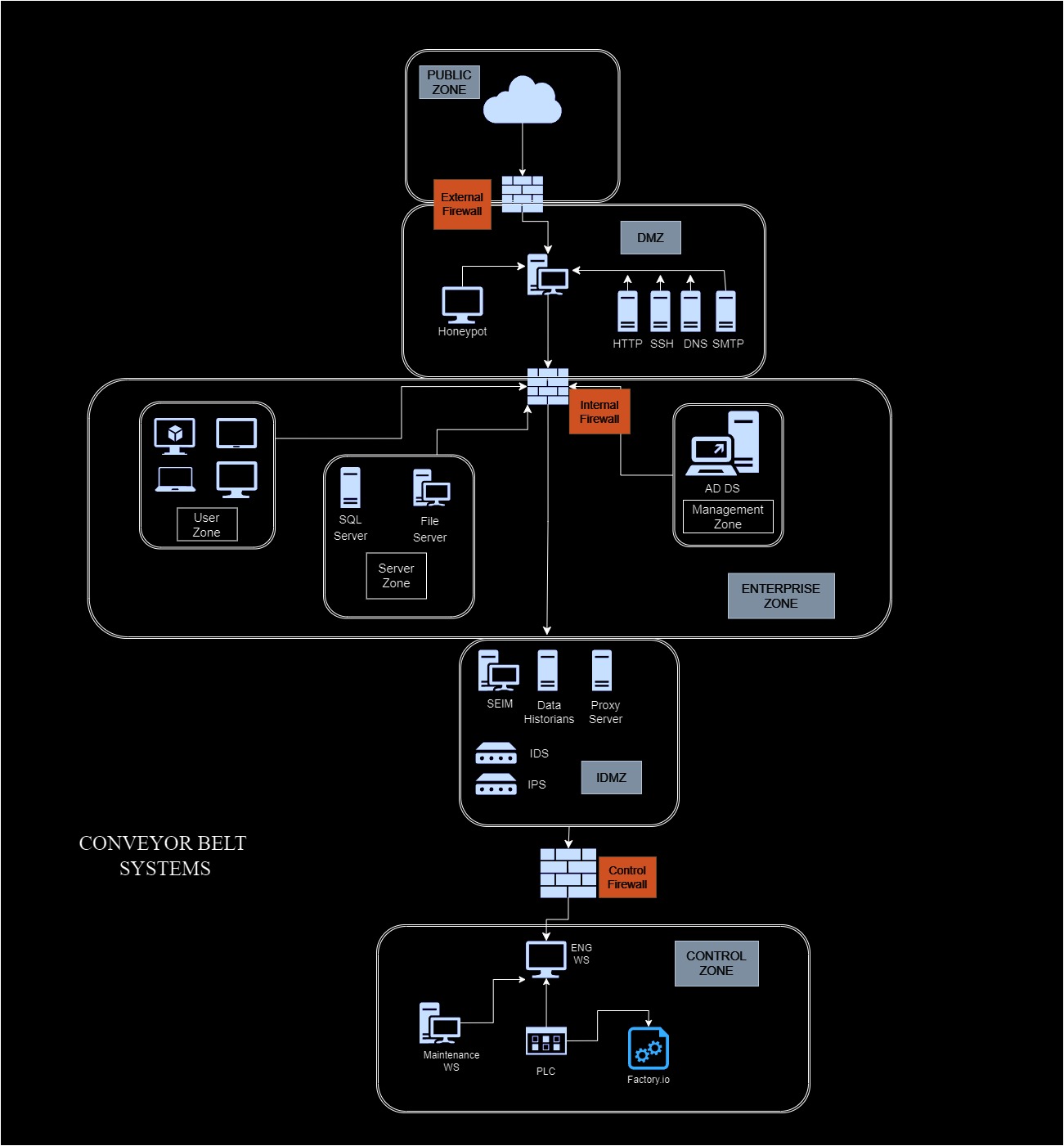
A white background with text

Description automatically generatedUpon visiting the website, the payload would automatically install on the victim's machine, remaining concealed.

**Exploiting and Pivoting:**

With the initial shell, we extracted crucial system information such as hardware details, IP addresses, and usernames. Subsequently, we changed the passwords of all users to gain further control. To establish a persistent backdoor, we created a second shell using simple python file within the initial shell using the echo command. This shell was scheduled as a task triggered by workstation restarts, ensuring a shell connection whenever the system reboots. Leveraging the obtained IP, username, and password, we remotely accessed the OT workstation via RDP to gain GUI control. Finally, we manipulated the PLC software to upload a disruptive program, interfering with plant operations.

**Proposed Security Implementation:**



To address the identified vulnerabilities and strengthen the security of the virtual test network, the Industrial Cybershield project will implement a comprehensive set of security measures and configurations.

Network Segmentation and Conduits

The first step will be to establish clear security zones and configure the necessary conduits to control the flow of information between the external, DMZ, and internal network segments. This network segmentation will help isolate critical assets and limit the potential impact of a successful attack.

Firewall Configuration

The Indistrial Cybershield project team has implemented a comprehensive, multi-tiered firewall approach using three distinct pfSense firewalls to secure the network.

The first firewall is positioned at the boundary between the Public Zone and the DMZ. This firewall is carefully configured with strict security policies to rigorously control and filter all incoming traffic from the internet. The team has allowed only the necessary and authorized protocols and ports, such as HTTPS, to reach the DMZ, while blocking all other potentially malicious traffic.

The second firewall is placed between the DMZ and the Enterprise Zone. This firewall is responsible for controlling the communication between these two network segments. The team has permitted only the required protocols and ports needed for the services hosted in the DMZ to access the internal resources.

The third firewall is positioned between the IDMZ and the Control Zone. This firewall ensures that the communication between these critical zones is strictly controlled. The group has blocked all other unwanted traffic and only permitted the appropriate protocols and ports to get through.

The team has meticulously set up the intrusion prevention, access control lists, and firewall rules on each of the three firewalls to impose stringent security regulations and stop illegal access to the industrial control system components inside the Control Zone.

To further improve security and stop illegal access to the firewall control interfaces, the project team has also modified the default login credentials for the pfSense firewall.

Industrial Demilitarized Zone (IDMZ)

An IDMZ will be implemented to establish a safe buffer between the OT network and the corporate IT network. The services and programs needed for remote monitoring and control will be hosted in this IDMZ, keeping the two network domains clearly divided and reducing the risk of cross-contamination.

Security Monitoring and Incident Response

To increase network visibility and monitoring capabilities, a Security Information and Event Management (SIEM) system will be incorporated. The team will be able to identify, look into, and address possible security problems thanks to this SIEM system, which will centrally collect, analyze, and correlate security-related logs and events from many network devices.

Securing OT Components

The OT network in the Industrial Cybershield project consists of the Maintenance Workstation, PLC (Programmable Logic Controller), and Factory I/O. To secure these critical OT components, the project team will implement the following measures:

The team will make sure that robust access controls and authentication procedures are in place for the Maintenance Workstation, and that the most recent secure operating system version is installed. As the main interface for monitoring and managing the industrial operations, the Maintenance Workstation is vulnerable to illegal access and exploitation. As such, multi-factor authentication must be put in place.

The PLC, as the central component that automates the industrial operations, will also be a focus of the security efforts. The team will verify that the PLC is running the latest secure firmware version and will configure robust access controls to restrict unauthorized modifications or tampering with the control logic.

Lastly, the Factory I/O, which represents the physical industrial equipment and sensors, will be secured by integrating it with the PLC in a way that maintains the integrity of the communication and control mechanisms. The team will implement secure communication protocols and access restrictions to prevent any unauthorized access or disruption to the simulated industrial processes

Honeypot Integration

A honeypot system will be set up to monitor and identify any potential intrusion attempts to improve the security posture of the network. This decoy system will attract and monitor the actions of hostile actors, offering important insights to reinforce the overall security measures. It is meant to replicate the vulnerabilities of the OT network.

The Industrial Cybershield project will establish a strong and resilient virtual test network by putting these security measures into place. This will show that the team can protect industrial control systems from cyber threats and effectively mitigate the vulnerabilities that have been found.

**Result**

**........**

**Initial Challenges**

The Industrial Cybershield project faces several unique challenges that the team will need to navigate and overcome throughout the development and implementation process.

First and foremost, there is a big obstacle because of the short timeline—just over a month, from April 22 to May 23. To guarantee that all project milestones are reached within this shortened timeline, the team will need to practice careful planning, effective resource allocation, and faultless execution.

The integration and configuration of the virtual pfSense firewall is one of the technological challenges. We expect a challenging learning curve in comprehending the intricate rule-based setup, access control lists, and intrusion prevention features of the firewall, since none of the team members have any experience configuring and maintaining pfSense firewalls. It will be vital, but technically challenging, to make sure the firewall is set up correctly to impose stringent security regulations and separate the OT network from the corporate IT network.

Additionally, the team must find a way to expose vulnerabilities in the pfSense firewall itself. Our initial plan to leverage the DHCPv6 vulnerability by leaving it enabled on an inexperienced system administrator's configuration had to be abandoned due to difficulties in configuring IPv6 on the VMware environment. This setback has forced the team to explore alternative approaches to identify and exploit vulnerabilities within the pfSense firewall, which will require extensive research and technical expertise.

Furthermore, the team faces the challenge of creating an attack that can bypass the Windows Defender security measures on the Windows 10 virtual machines. As we are unable to disable Windows Defender, the team will need to research and develop a sophisticated attack strategy that can effectively circumvent this security mechanism without triggering alerts or being detected. This will require a deep understanding of Windows security features and advanced exploitation techniques.

**Projected Solutions:**

To address the initial challenges, we have developed a comprehensive set of strategies and solutions:

Tight Timeline

To meet the project's short timeline—just over a month—the team will carefully plan and carry out every step of the process. To guarantee that all activities are finished on schedule, this will entail developing a thorough project plan with distinct milestones, assigning resources effectively, and regularly monitoring progress. Along with keeping lines of communication open, the team will work closely to locate and fix any potential delays or bottlenecks.

Pfsense firewall configuration

The team will invest a lot of time in study and practical learning because they understand how little experience, they have with configuring and maintaining pfSense firewalls. To obtain a complete grasp of the firewall's capabilities and best practices for implementation, the team will go over the pfSense documentation in detail, investigate online tutorials and forums, and maybe consult the instructor. They will be able to properly set up the pfSense firewall and guarantee that the OT network is successfully isolated from the corporate IT network thanks to this.

Disclosing vulnerabilities in pfSense

The team has chosen to use the "Any Ports" rule in the pfSense firewall to reveal possible vulnerabilities after the initial setback with the DHCPv6 issue. This approach will allow them to create a permissive firewall rule that permits all traffic to flow between the network zones, simulating a scenario where the firewall is misconfigured or left in its default state. By taking this technical approach, the team can still demonstrate the risks associated with inadequate firewall configurations and explore alternative methods for exploiting the pfSense firewall.

Bypassing Windows Defender

To create an attack that can bypass the Windows Defender security measures on the Windows 10 virtual machines, the team will conduct extensive research on Windows security features and advanced exploitation techniques. This may involve exploring techniques like code obfuscation, process injection, or leveraging vulnerabilities in Windows Defender itself to circumvent the security controls without triggering alerts or being detected. By developing a sophisticated attack strategy, the team will demonstrate their technical expertise and the importance of implementing robust security measures to protect against such threats.

By proactively addressing these challenges through thorough research, hands-on learning, and the implementation of well-designed technical solutions, the Industrial Cybershield project team will be better equipped to navigate the complexities of the project and deliver a comprehensive and secure industrial control system network.

**Schedule/Tasks for Completing the Industrial Cybershield Project:**

The Industrial Cybershield project has a one-month deadline from April 22 to May 23 to be completed and presented. Then, it is important that we break the job up into five different phases and give each group member a task based on their abilities and areas of interest.

**Phase 1: Initiation phase (April 22nd - May 1st)**

* Task 1: Get together as a group to discuss project ideas and evaluate viability considering the deadline.
* Task 2: By May 1st, complete and submit the project proposal.

**Phase 2: Planning phase (May 2nd – May 7th)**

* Task 3: Define the project scope, course of action, and assign responsibilities to group members.
* Task 4: Develop a Gantt chart, work breakdown framework, and project completion requirements.
* Task 5: Design vulnerable network topology.
* Task 6: Plan the secure network strategies, by adding another firewall, zones, conduit, and IDMZ to improve the security posture.
* Task 7: Complete the topology diagrams of the networks, both hardened and vulnerable.

**Phase 3: Execution phase (May 8th – May 13th)**

* Task 8: Put the attack into the vulnerable network.
* Task 9: Set up the intended security measures on the pfSense firewall.
* Task 10: put created attack into our vulnerable network from Kali.

**Phase 4: Monitoring and Controlling phase (May 14th - May 16th)**

* Task 11: always Keep an eye out for any security issues or plan deviations on the network.
* Task 12: Maintaining network integrity by debugging and resolving any problems discovered.

**Phase 5: Closing phase (May 17th - May 23rd)**

* Task 13: To ensure accuracy and quality, make last-minute changes to the project deliverables.
* Task 14: Put together an exhaustive project report that covers every stage of the process.
* Task 15: Prepare and practice the project's final presentation, emphasizing its successes, weaknesses, and solutions.
* Task 16: By May 23rd, provide a compelling presentation and turn in the project report.

**ISA/IEC 62443 Standard Alignment**

We have meticulously matched the essential specifications given in the ISA/IEC 62443 standard with our Industrial Cybershield project's security implementation. An extensive set of principles for creating a strong cybersecurity management system for industrial automation and control systems (IACS) is provided by this industry-recognized framework.

FR1 - Identification and Authentication Control (IAC) and FR2 – Use Control To address the IAC requirement, we have implemented a Windows Server 2022 domain controller as the central authentication server for our network. This ensures that all users, processes, software, and devices are properly identified and authenticated before accessing necessary resources. Furthermore, we have configured the domain controller to enforce the principle of least privilege, granting users and entities only the minimum permissions required to perform their designated tasks, in alignment with the use control requirement.

FR3 - System Integrity

Maintaining the integrity of our system has been a top priority. We have established a secure network environment protected by multiple pfSense firewalls, which are meticulously configured to allow only the necessary traffic flow. Additionally, our SIEM (Security Information and Event Management) solution, leveraging the SELK (Suricata, Elasticsearch, Logstash, and Kibana) stack, actively monitors the network for any suspicious activities. This comprehensive approach ensures that processes and data within our IACS network remain authentic and operational, minimizing the risk of system disruptions.

FR4 - Data Confidentiality

One of the most important components of our security approach is guaranteeing data confidentiality. Every piece of data that is sent across our network is passed via the SIEM system, which keeps a watchful eye out for any suspicious activity involving data handling or illegal access. In keeping with the least privileged concept, we have also put strong access controls in place, allowing people access to the data that is necessary for their job tasks.

FR5 - Restricted Data Flow

We have set up a multi-tiered firewall configuration with an Industrial Demilitarized Zone (IDMZ) between the corporate and industrial network segments to satisfy the requirement of restricted data traffic. By ensuring that data only moves across the required zones, this strategy guards against potential security breaches and unauthorized access. Through meticulous configuration of firewall rules and user rights, we have successfully isolated the company and industrial networks, maintained data security, and reduced the possibility of illegal data transfer.

FR6 - Timely Response to Events

We understand how critical it is to react to security occurrences as soon as possible. To do this, we have set up our SIEM system with both active and passive monitoring procedures to find any possible security events. We adhere to a set response protocol based on the incident's severity when it happens. We may reduce possible threats and their impact on our network and systems by closely monitoring the SIEM system and promptly addressing security issues.

FR7 - Resource Availability

It is essential to guarantee our IACS network's availability and uptime. We have included several safeguards, such as our multi-tiered firewall design, to ensure the availability of resources. Through the implementation of security measures on industrial components, like Modbus servers, we have reduced the possibility of possible interruptions, maintained system continuity, and avoided large-scale financial losses due to system failures.

By aligning our security implementation with the key foundational requirements of the ISA/IEC 62443 standard, we have strengthened the overall security posture of our virtual IACS network.

Conclusions and Recommendations

Conclusion

A secure virtual industrial control system (ICS) network may be designed, implemented, and maintained by the team, as shown by the Industrial Cybershield project's successful completion. Utilizing the pfSense firewall's capabilities and coordinating the security implementation with the ISA/IEC 62443 standard, the group has produced a robust and all-encompassing network architecture.   
  
Critical network segments have been successfully segregated, and illegal access to the industrial control components has been limited, thanks to the multi-tiered firewall configuration with stringent access control lists and traffic inspection. Establishing an Industrial Demilitarized Zone (IDMZ) has improved security even more by creating a haven between corporate IT networks and operational technology (OT).

The team's attempts to secure the factory I/O and Programmable Logic Controller (PLC) among other OT components have shown that they are aware of the difficulties and weaknesses that come with industrial control systems. The total protection of these vital assets has been reinforced by the addition of strong access restrictions, authentication procedures, and secure communication protocols.   
  
Important new information about the possible effects of cyber threats on industrial operations has been made possible by the successful exploitation of the weak network and the subsequent deployment of security countermeasures. The team now has the expertise and abilities needed to recognize, lessen, and effectively address such dangers because of this practical experience.

Recommendation

The following suggestions are put forth considering the Industrial Cybershield project's lessons gained and results:

1. Constant Monitoring and Incident Handling: Keep up with the SIEM system and keep an eye out for any unusual activity on the network. Create a clear incident response strategy to guarantee prompt and efficient action in the case of a security breach.

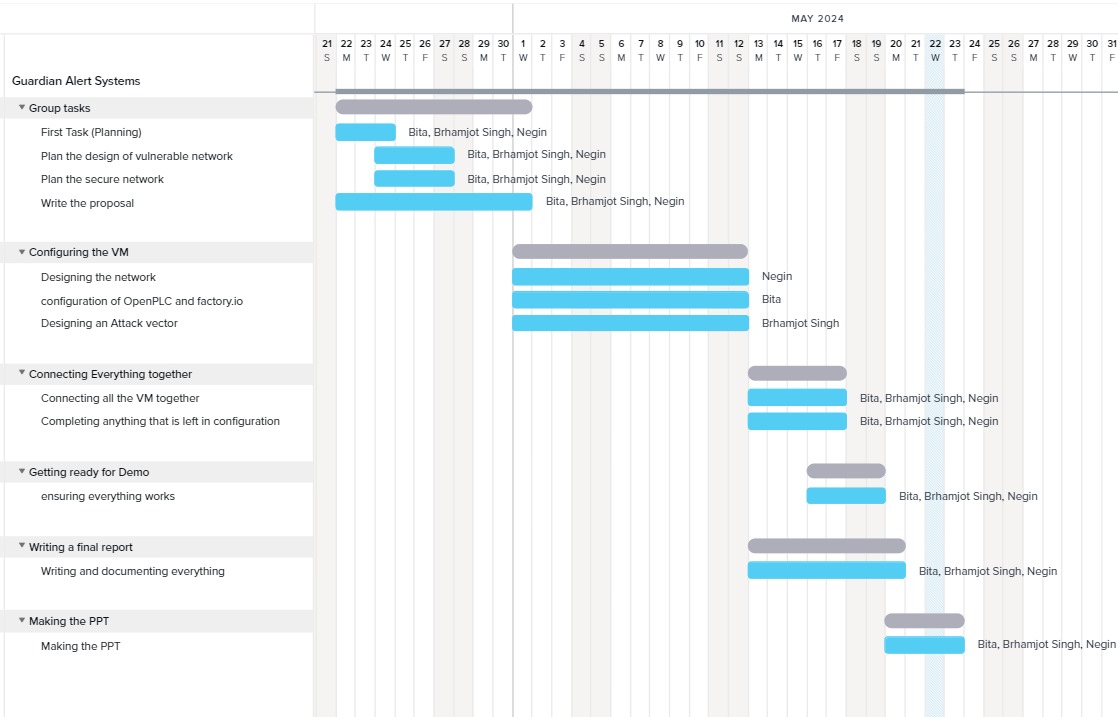
2. Continuous Vulnerability Assessments: To detect and counter new threats, perform vulnerability assessments on an ongoing basis on the ICS network. Apply the most recent security patches and updates to preserve the system's integrity.

3. Employee Cybersecurity Awareness: To improve staff members' comprehension of security best practices and their part in safeguarding the industrial control system, comprehensive cybersecurity training programs should be put in place for all staff members, including engineers and operators.

4. Cooperation and Knowledge Sharing: To stay up to date on the newest trends, risks, and best practices in industrial cybersecurity, connect with colleagues in the industry, security specialists, and regulatory agencies. Make a proactive effort to increase the industrial control systems' overall security posture by participating in the knowledge-sharing community.   
  
5. Continuous Improvement: To keep up with the changing threat landscape, regularly examine and update security configurations and strategies. Assimilate input, insights gained, and new technologies to improve security protocols and preserve the ICS network's robustness.

Appendices which may include  
 Schematics  
 Screenshots (project design, simulations)  
 Data sheets (links to websites)

Gantt Chart



**………**

**pfsense firewall**

The pfSense firewall was selected by the team to serve as the primary security measure for the Industrial Cybershield project. They chose pfSense because it was free and open-source software with a wealth of networking and security features.

The stateful inspection features of the pfSense firewall are one of its main advantages. Because pfSense monitors network connection statuses, it can make more informed decisions about what traffic to accept or deny than standard stateless firewalls. This allows the team to design precise firewall rules to control the flow of traffic between different network zones.

In the vulnerable network design, the team configured a single, permissive pfSense firewall rule between the external and internal IT networks. This rule allowed all traffic to pass freely, effectively removing the logical division between the zones and leaving them exposed to potential threats.

To create a robust security architecture for the secure network, the team implemented a multi-tiered pfSense firewall configuration with three distinct firewalls:

1. The first firewall, situated between the public zone and the DMZ, enforced strict security policies to tightly regulate and filter traffic between these segments.

2. The second firewall, between the DMZ and the enterprise zone, allowed only the necessary protocols and ports for communication between these zones.

3. The third firewall, separating the IDMZ and the control zone, permitted only the required and approved traffic while blocking all other unauthorized access.

This comprehensive, defense-in-depth firewall configuration provided enhanced access control, traffic inspection, and network segmentation capabilities, which are essential for maintaining the overall security and resilience of the virtual ICS environment.

**Firewall Rules of the Secure Network:**

Firewall 1 (External Firewall - Between Public Zone and DMZ

1. WAN (External) Interface Rules

* Allow Inbound HTTPS (TCP port 443) traffic from the Public Zone to the DMZ
* Block all other inbound traffic.
* Allow necessary outbound traffic from the DMZ to the internet with security measures.

2. LAN (IT) Interface Rules

* Allow Required IT protocols and ports for the services hosted in the DMZ.
* Deny all other traffic between the Public Zone and the DMZ
* Implement strict access control lists (ACLs) to restrict unauthorized access to the DMZ.

Firewall 2 (DMZ Firewall - Between DMZ and Enterprise Zone)

1. LAN (IT) Interface Rules

* Allow the necessary communication protocols and ports between the DMZ and the Enterprise Zone
* Deny all other trafifc between the DMZ and the Enterprise Zone

2. WAN (IT Zone) Interface Rules

* Allow the required communication from the Enterprise Zone to the DMZ
* Deny all other traffic from the Enterprise Zone to the DMZ
* Implement strict access control lists (ACLs) to restrict unauthorized access between the DMZ and the Enterprise Zone

Firewall 3 (IDMZ Firewall - Between IDMZ and Control Zone)

1. LAN (IT) Interface Rules

* Allow the necessary communication protocols and ports between the IDMZ and the Control Zone
* Deny all other traffic from the IDMZ to the Control Zone

2. OPT1 (Control Zone) Interface Rules

* Allow the required communication from the Control Zone to the IDMZ
* Deny all other traffic from the Control Zone to the IDMZ
* Implement strict access control lists (ACLs) to restrict unauthorized access between the IDMZ and the Control Zone

Resources

<https://www.pfsense.org/>

<https://www.cygwin.com/>

<https://autonomylogic.com/>

<https://factoryio.com/>