A1 Cybersecurity Solutions Ltd

INCS 4810 Culminating Project

Project Proposal

Jason Dhaliwal – Jevin Heer – Gursher Singh

Table of Contents

Project Proposal: Simulating a Cyberattack on an ICS Network

I. Introduction

This project aims to design and build a virtual test network with vulnerabilities to simulate a cyberattack on an Industrial Control System (ICS) network. The attack will involve a Kali Linux machine hacking into a Windows 10 machine using a phishing email, gaining enterprise-level access to the Active Directory (AD), and then accessing the Operational Technology (OT) side engineering workstation. The attacker will gain control over a level tank process, change values, and cause damage to the process itself.

The purpose of this project is to demonstrate the potential consequences of a successful cyberattack on an ICS network, as well as highlight the importance of implementing robust cybersecurity measures to protect critical infrastructure. By creating a virtual test network with intentional vulnerabilities, we can showcase how an attacker can exploit these weaknesses. Once the attacker has gained unauthorized access to the system, they can cause significant damage or disruption.

Furthermore, this project will provide hands-on experience in designing and implementing a secure ICS network architecture. By following the ISA-62443 standard for assessing and mitigating vulnerabilities, the team will gain valuable insights into the best practices for securing industrial control systems. The project will also involve implementing countermeasures such as network segmentation, firewalls, and intrusion detection systems to enhance the security of the virtual test network. Through this process, the team will develop a deeper understanding of the challenges and solutions involved in protecting critical infrastructure from cyber threats.

II. Project Overview

Problem Statement:

Industrial Control Systems (ICS) are vulnerable to cyberattacks due to outdated software, lack of security controls, and insufficient cybersecurity awareness and initiatives. This project aims to demonstrate the impact of a successful cyberattack on an ICS network and emphasize the need for stronger cybersecurity measures. The project scope includes designing a virtual test network with intentional vulnerabilities that mimic real-world applications, following the ISA-62443 standard for assessment and countermeasures, conducting a simulated attack on the test network and remediating any vulnerabilities that are found. Limitations include a simplified network architecture and focus on a specific attack scenario.

Proposed Solution:

The proposed solution involves designing a virtual test network using VMware, consisting of a separated business and ICS network, with an engineering workstation. The network will be intentionally designed with vulnerabilities such as lack of secure segmentation, unpatched operating systems, and weak security controls. The attack scenario will involve using phishing emails to gain access to the network, lateral movement to the ICS network, and manipulation of the simulated industrial process. Countermeasures will be implemented following the ISA-62443 standard, including secure network segmentation with zones and conduits, system updates, and deploying security monitoring tools with a possible honeypot if time allows. The project aims to demonstrate the vulnerabilities in ICS networks and showcase the effectiveness of cybersecurity measures in mitigating risks.

III. Schedule for Completing the Project

Week 1: Research and planning

Identify the required hardware and software components for the virtual test network. Design the network architecture, including the business network, ICS network, and internet-facing components. Plan the cyberattack scenario and the steps involved in exploiting the vulnerabilities. Assign specific research tasks to each team member based on their expertise and interests.

Week 2: Setting up the virtual test network

Install and configure the virtualization software VMware on the host machine. Create virtual machines for the business network components, such as the workstations, servers, and firewall. Set up the virtual machines/simulation applications for the ICS network, including the PLC, HMI, and maintenance workstation. Configure the network settings and establish connectivity between the virtual machines. Test the basic functionality of the virtual test network and troubleshoot any issues.

Week 3-4: Simulating the cyberattack and implementing countermeasures

Conduct a vulnerability assessment of the virtual test network using the ISA-62443 standard as a guideline. Simulate the cyberattack by exploiting the vulnerabilities by using a phishing email. Gain unauthorized access to the business network and pivot to the ICS network through the Domain Controller. Gain command and control of the engineering workstation, and manipulate the industrial process parameters to demonstrate the potential impact of the cyberattack. Implement countermeasures to mitigate the risks and enhance the network security based on the ISA-62443 standards.

Week 1-5: Documentation and Final Deliverables

Prepare a comprehensive technical report and presentation documenting the project objectives, methodology, findings, and recommendations. Include detailed descriptions of the virtual test network architecture, vulnerability assessment results, and implemented countermeasures. Create network diagrams, configuration files, and screenshots to support the technical explanations. Organize the project files for easy reference and future use.

IV. Team Coordination

Gursher: Gursher has always been interested in the virtualization and network setup section of our course material, and so he will be responsible for setting up the virtual test network. Using his previous work experience and what he has learned from attending seminars, Gursher will be able to achieve the goals promptly and efficiently that we set out for in regard to his role.

Jason: Jason has shown an interest in the penetration testing and exploitation aspect of our program and will use his experience in cybersecurity and penetration testing to be in charge of planning and executing the simulated cyberattack. Once he is able to access the network Jason will use his expertise controlling ICS processes using simulators such as DeltaV to take control of the engineering workstation and hijack the process control. He has volunteered to be the lead communicator for this project.

Jevin: Jevin is knowledgeable in ICS and OT systems and will be responsible for setting up the simulated process and implementing countermeasures. Jevin will be able to draw upon his experience in setting up a level tank process in the BCIT lab and translate that to a virtual environment. With his attention to detail and adaptability he will be able to refine his virtualization and security implementation skills while being a great fit for his role.

Regular team meetings will be held to discuss progress, challenges, and next steps. These meetings will take place both in-person and through WhatsApp, allowing for flexibility and convenience in communication. A shared Google Drive folder and GitHub will be set up to facilitate collaboration on documents, code, and other project files. This centralized repository will ensure that all team members have access to the latest versions of the project materials and can easily contribute their work.

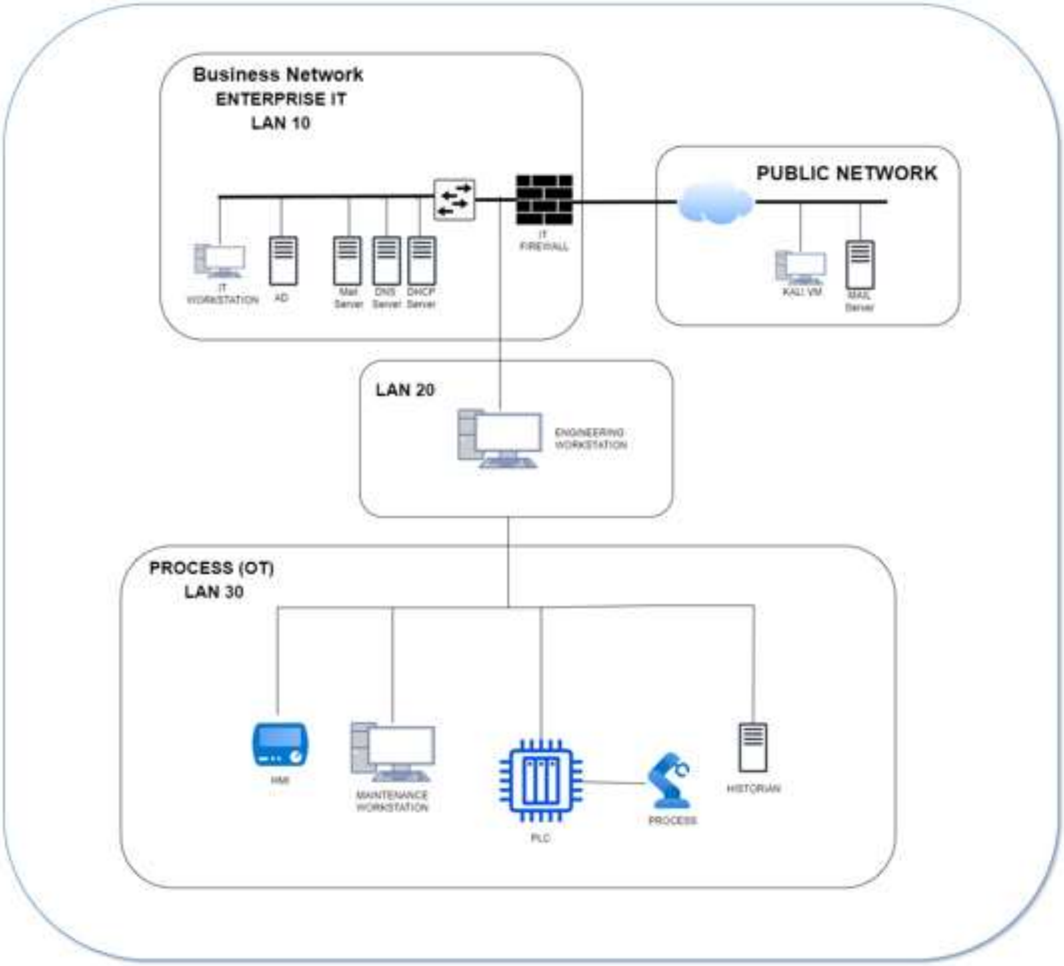
V. Detailed Design

Virtual Test Network:

Business Network: Windows 10 machine with enterprise-level AD access, DNS server, and IT workstation (business side).

ICS Network: Engineering workstation, PLC, HMI, maintenance workstation, historian, and simulated level tank process.

Internet: Kali Linux machine and mail server as the attacker and firewall.

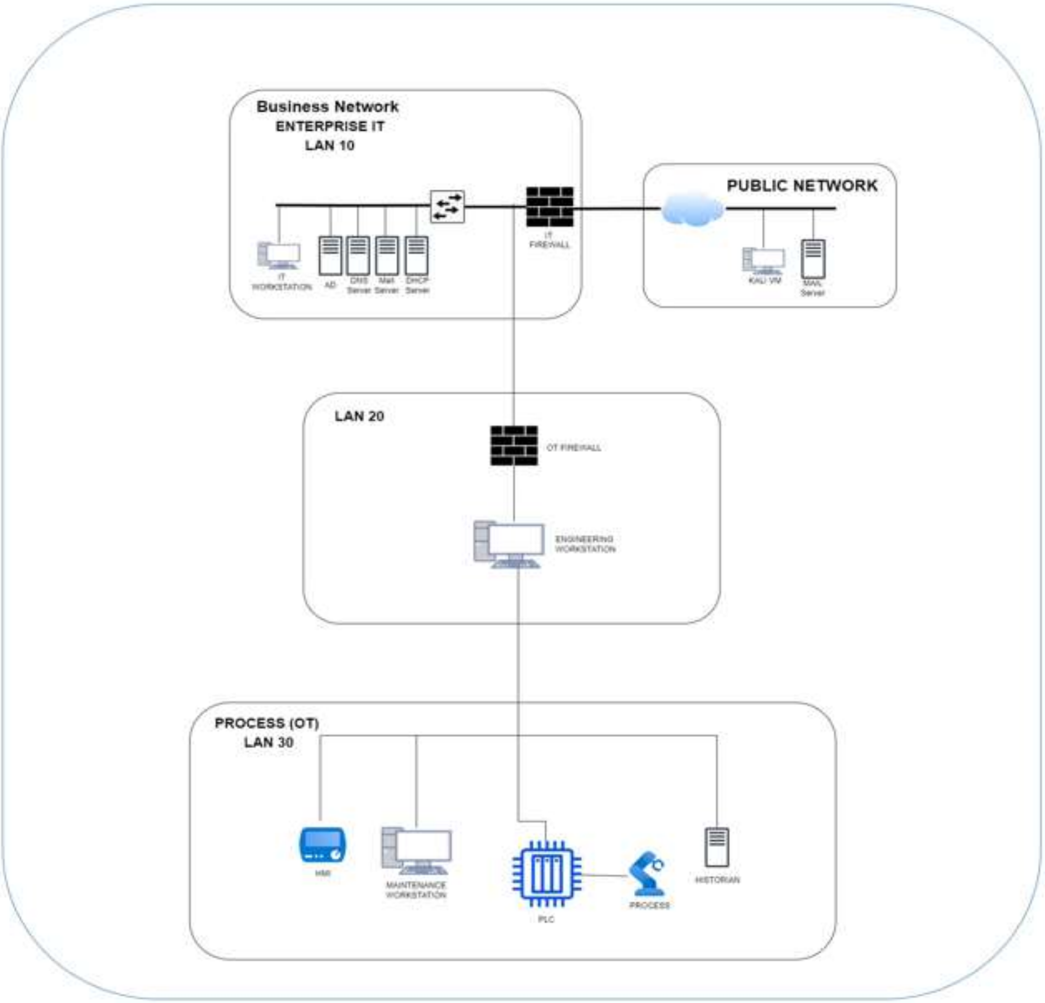


Vulnerabilities:

Weak passwords on the Windows 10 machine and engineering workstation. Lack of secure network segmentation between the business and ICS networks. Absence of intrusion detection and prevention systems (IDS/IPS). Unpatched or outdated software on the ICS components.

Security Implementation:

Implement network segmentation using VLANs and firewall rules to isolate the business and ICS networks. Configure strong, unique passwords for all devices and accounts. Set up an Intrusion Detection and Prevention System (IDS/IPS) to monitor network traffic. Regularly patch and update software on all devices.



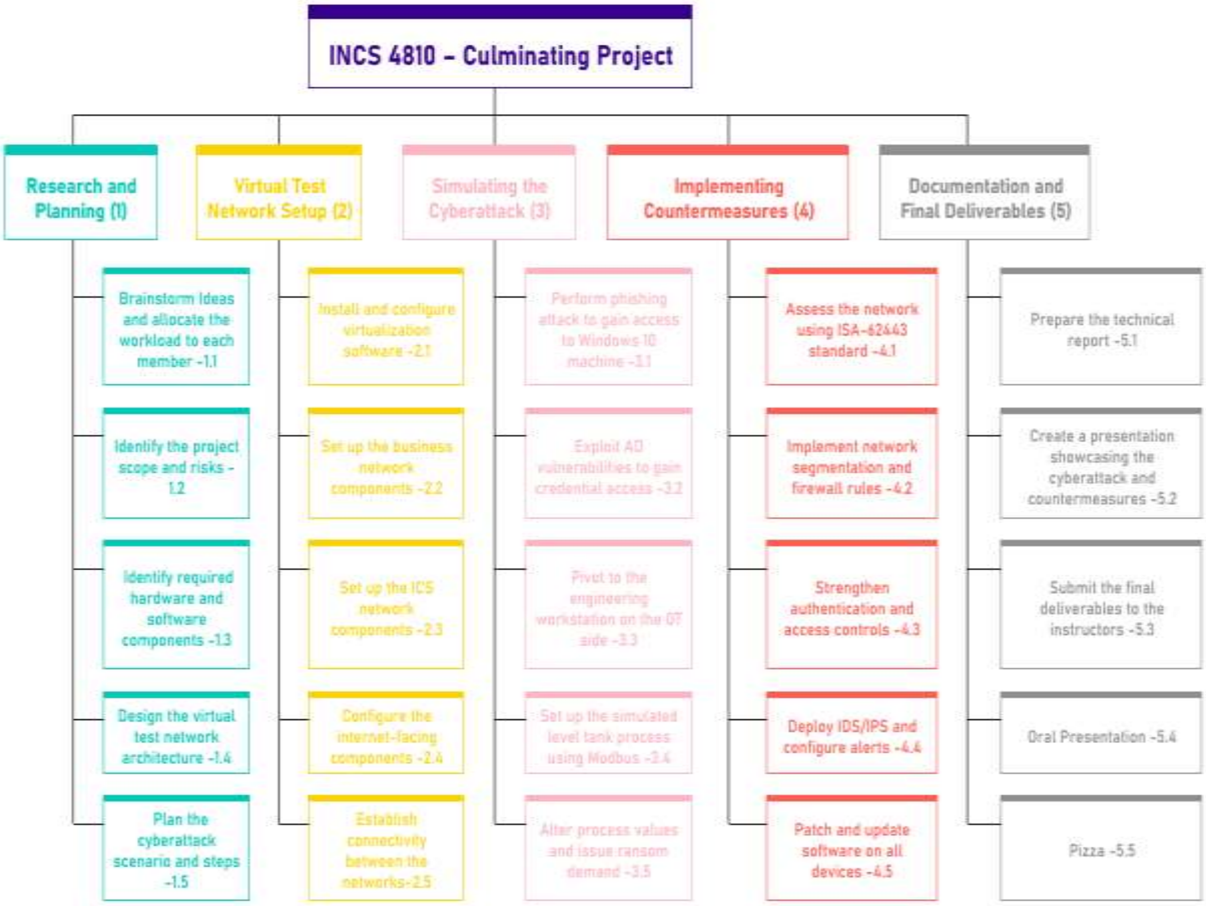
Challenges:

Difficulty setting up the virtual test network using virtualization software. Challenges in establishing the client/server connection for the simulated process. Time constraints impacting the final deliverables.

Mitigation:

Allocate extra time for troubleshooting, consult documentation and online resources, and seek guidance from instructors if needed. Research industrial communication protocols/applications thoroughly, plan extra time for configuring the connection, and have backup options like using a different software. Create a detailed schedule with milestones, regularly track progress, and be prepared to prioritize tasks.

VI. Work Breakdown Structure (WBS)


INCS 4810 – Culminating Project
Research and Planning (1)
Virtual Test Network Setup (2)
Simulating the Cyberattack (3)
Implementing Countermeasures (4)
Documentation and Final Deliverables (5)
Brainstorm Ideas and allocate the workload to each member -1.1
Identify the project scope and risks - 1.2
Identify required hardware and software components -1.3
Design the virtual test network architecture -1.4
Plan the cyberattack scenario and steps -1.5
Install and configure virtualization software -2.1
Set up the business network components -2.2
Set up the ICS network components -2.3
Configure the internet-facing components -2.4
Establish connectivity between the networks-2.5
Perform phishing attack to gain access to Windows 10 machine -3.1
Exploit AD vulnerabilities to gain credential access -3.2
Pivot to the engineering workstation on the OT side -3.3
Set up the simulated level tank process using Modbus -3.4
Alter process values and issue ransom demand -3.5
Assess the network using ISA-62443 standard -4.1
Implement network segmentation and firewall rules -4.2
Strengthen authentication and access controls -4.3
Deploy IDS/IPS and configure alerts -4.4
Patch and update software on all devices -4.5
Prepare the technical report -5.1
Create a presentation showcasing the cyberattack and countermeasures -5.2
Submit the final deliverables to the instructors -5.3
Oral Presentation -5.4
Pizza -5.5

Task delegation

Level	WBS Task #	Task	Gursher	Jason	Jevin
1	1.0	Research and Planning	-	-	-
2	1.1	Brainstorm Ideas and allocate the workload to each member	X	X	X
2	1.2	Identify the project scope and risks	X	X	X
2	1.3	Identify required hardware and software components	X	X	X
2	1.4	Design the virtual test network architecture	X	X	X
2	1.5	Plan the cyberattack scenario and steps	X	X	X
1	2.0	Virtual Test Network Setup	-	-	-
2	2.1	Install and configure virtualization software	X		
2	2.2	Set up the business network components	X		
2	2.3	Set up the ICS network components	X		X
2	2.4	Configure the internet-facing components	X		
2	2.5	Establish connectivity between the networks	X	X	
1	3.0	Simulating the Cyberattack	-	-	-
2	3.1	Perform phishing attack to gain access to Windows 10 machine		X	
2	3.2	Exploit AD vulnerabilities to		X	

		gain credential access			
2	3.3	Pivot to the engineering workstation on the OT side		X	
2	3.4	Set up the simulated level tank process using Modbus			X
2	3.5	Alter process values and issue ransom demand		X	
1	4.0	Implementing Countermeasures	-	-	-
2	4.1	Assess the network using ISA-62443 standard		X	X
2	4.2	Implement network segmentation and firewall rules	X		
2	4.3	Strengthen authentication and access controls		X	X
2	4.4	Deploy IDS/IPS and configure alerts	X	X	
2	4.5	Patch and update software on all devices			X
1	5.0	Documentation and Final Deliverables	-	-	-
2	5.1	Prepare the technical report			
2	5.2	Create a presentation showcasing the cyberattack and countermeasures	X	X	X
2	5.3	Submit the final deliverables to the instructors	X	X	X
2	5.4	Oral Presentation	X	X	X
2	5.5	Pizza	X	X	X

VII. Project Milestone

Our project milestone will be having the complete IT and OT networks set up and configured correctly to have connectivity. We are anticipating having this completed by May 7. Once the networks are operational we will proceed with thorough testing to ensure seamless communication between all devices and systems. Achieving this milestone will lay the foundation for the subsequent phases of the project, allowing us to move forward.

VIII. Budget

As students at BCIT we have the unique advantage of accessing the institution's resources for our project at no cost. Our team consists entirely of students who are contributing their time and skills voluntarily, eliminating the need for a labor budget. By using the support provided by BCIT and the commitment of our student team, we are able to pursue this project without the requirement of a traditional financial budget.

IX. Risk Assessment and Mitigation

Risk	Likelihood	Impact	Risk Score	Mitigation
Difficulty setting up virtual test network using virtualization software	3	4	12	Allocate extra time for troubleshooting, consult documentation and online resources, seek guidance from instructors if needed
Challenges establishing Modbus client/server or application based client/server connection for simulated process	4	5	20	Research Modbus and industrial communication applications thoroughly, plan extra time for configuring the connection, have backup options like using different software
Time constraints impacting final deliverables	4	4	16	Create detailed schedule with milestones, regularly track progress, identify and address blockers early, be prepared to prioritize tasks
Data loss or corruption during the simulation process	2	5	10	Implement regular data backups, use version control for code and configurations, document all changes, and have a disaster recovery plan

X. Final Deliverables

A fully functional virtual test network with vulnerabilities and then with countermeasures implemented. A detailed technical report documenting the project, including the attack scenario, vulnerabilities, countermeasures, and lessons learned. A presentation demonstrating the simulated cyberattack and its impact on the ICS process. All project files, including network diagrams, configuration files, and code.

XI. Conclusion

This project proposal outlines the plan to design and build a virtual test network with vulnerabilities to simulate a cyberattack on an ICS network. By following the ISA-62443 standard and implementing appropriate countermeasures, the project aims to demonstrate the potential consequences of a successful cyberattack and the importance of robust cybersecurity measures in protecting critical infrastructure.

The project will be completed over a period of 5 weeks, with tasks distributed among team members based on their strengths and expertise. Regular communication and collaboration will be maintained throughout the project to ensure timely completion and high-quality deliverables.

Potential challenges and risks have been identified, along with mitigation strategies to minimize their impact on the project's progress and success. A comprehensive testing and validation plan will be followed to ensure the virtual test network and the simulated cyberattack meet the project's objectives and requirements.

Upon completion, the project will provide valuable insights into the vulnerabilities of ICS networks and the effectiveness of various cybersecurity measures in preventing or mitigating cyberattacks. The final deliverables, including the technical report and presentation, will serve as a valuable resource for educating stakeholders on the importance of cybersecurity in the context of industrial control systems.

References

- "pfSense 2.7.0 Daily on VMware Workstation 17 Pro - Linux Fedora 37," DimensionQuest, Apr. 5, 2023. [Online]. Available: https://www.youtube.com/watch?ab_channel=DimensionQuest&t=694s&v=bZYR-ifkx90
- BiZken, "GitHub - BiZken/PhishMailer: Generate Professional Phishing Emails Fast And Easy," Apr. 25, 2024. [Online]. Available: https://github.com/BiZken/PhishMailer
- P. Ackerman, *Industrial Cybersecurity*. Packt Publishing Ltd, 2017.
- P. Ackerman, *Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment*. Packt Publishing Ltd, 2021.
- plcgoods, "How to create function & function blocks in CODESYS - CODESYS function blocks," *YouTube*. Jul. 06, 2023. [Online]. Available: https://www.youtube.com/watch?v=kCk0wMtyS1g
- ChunzPS, "Factory I/O Tutorial linked with Codesys," *YouTube*. Sep. 11, 2018. [Online]. Available: https://www.youtube.com/watch?v=lnadq56anXs
- Rajvir Singh, "Learn about FACTORY I/O- Automation Sandbox- The best PLC Simulator," *YouTube*. Feb. 04, 2018. [Online]. Available: https://www.youtube.com/watch?v=ba-os-jH-OA
- Pete Vree, "Siemens TIA Portal & Factory IO (Tank Project_Various Fill Levels using the same PB Input)," *YouTube*. Jun. 19, 2018. [Online]. Available: https://www.youtube.com/watch?v=Ss-dZv9GXik

- plcgoods, “Tutorial on linking CODESYS with Factory IO | CODESYS tutorial on Sensors, Counters, RS & SR,” *YouTube*. Nov. 14, 2021. [Online]. Available: https://www.youtube.com/watch?v=aIDMe4A4qww