Cyber Range SCADA Scenario

by

Feras Alghalayini, Nate Barton, Chase Lindquist

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

Nate Barton	04/15/2019
Feras Alghalayini	04/15/2019
Chase Lindquist	04/15/2019

Technical Advisor	
Bogdan Vykhovanyuk	04/15/2019

University of Cincinnati
College of
Education, Criminal Justice, and Human Services
April 2019

Table of Contents

List of Illustrations

Tables

Figures

Abstract

Critical infrastructure are the systems deemed necessary to live with our current modern standards. These systems require a combination of support systems and SCADA systems that control the machinery to provide us our essentials we take for granted such as power and water. Qualified cybersecurity professionals are becoming increasingly more difficult to find to defend these networks. We created a learning tool to help facilitate college student's knowledge of defending critical infrastructure, and as we know, the best way to defend is to learn how the attacker will think. This tool consists of a series of virtual machines within two sub scenarios, a water treatment plant and a power plant. Students will be able to conduct penetration tests of these in a simulated environment in order to learn more about critical infrastructure and how to defend it.

INTRODUCTION

1.1 Problem

Supervisory control and Data Acquisition (SCADA) systems are used to control or monitor plant or industrial equipment in real time. Organizations that use SCADA systems include the electrical, water, nuclear and communication industries. If SCADA systems get compromised, the damage can be costly, time-consuming, and resource excessive. Students today are entering the workforce with few practical skills when it comes to defending critical infrastructure (Carlisle 2018), understanding how SCADA systems work, showing the damage that is caused by a SCADA system, and having adequate experience and training can help mitigate SCADA system breaches and damage caused if there is a breach.

1.2 Solution

To create a scenario showing the impact of a SCADA system breach in various critical infrastructure industries, while displaying the defender's point of view to help students learn what an attack looks like. Future security professionals need to be aware of the types of risks that infrastructure can encounter when it comes to the safety and integrity of the company employees and who live nearby (Reuters, 2013). We have several example scenarios, including networks reflexive of the Water, Energy, Manufacturing, and ISP industries. We will show the impact that manipulating critical infrastructure networks and the systems that generate their revenue can cause. These networks will feed into a logging machine so that the user can see their attacks from the

defender's point of view in real time. The user will have the opportunity to gain control of SCADA systems, which will help the user learn how to secure. Finally, we will create several challenge machines in the networks, so that the users may test their penetration skills against hardened and difficult puzzle like vulnerable boxes

1.3 Project Goals

- Enhance and expand awareness of Supervisory Control and Data Acquisition (SCADA) that are used in critical infrastructure.
- Build Lab based experimental for a learning environment
- Provide a live demonstration of Infiltrating a SCADA system.
    - The training program can be tailored for infrastructure environments based on the company requirements.
- Demonstrate the possible outcome of sabotaging industrial control system which results in power outages, cut water supply and shutting down data centers.
- Educate UC students in how to attack and defend critical infrastructure networks.
- Demonstrate ways to mitigate damage from SCADA breach.

1.4 Overview

The remainder of this report outlines how the project was completed. The report includes the sections: Project concepts and plans, user information, technical approach, use cases, and other diagrams, problems encountered, and a conclusion.

2.0 Project Concept

We want students to be able to enhance their skills not only in penetration testing, but also in detecting attacks and learning how to defend our critical infrastructure. We were inspired to shift our project to this by Bogdan Vykhovanyuk our senior design mentor, who mentioned SCADA systems when our original idea to create a cyber range for UC, frankly, had already happened. We believe that this will be an invaluable learning tool for UC students, and will help bridge the widening gap in skills needed. (John 2018.)

2.1 Design Objectives

We created 2 critical infrastructure scenarios for the users to interact with. We created a simulated Water Treatment Plant and simulated Power Plant. In addition to this, we also will provide the user with a Kali machine to work off. We fleshed out the virtual machines with red herring programs and other programs that make them appear more realistic, as well as working documents so that the scenarios mimics a real life environment. If time allows it, we will add more machines to the networks in order for them to feel more like a true business, and to increase

2.2 Methodology/Technical Approach

The design requirements allowed us to set concrete goals for us to reach. Setting ourselves a goal of two scenarios forced us to work diligently to accomplish our goals. The primary technical tool we utilized was Virtualbox, this allowed us to host and network our virtual machines. We also utilized RapidSCADA in order to create and host

the visualizations for the SCADA systems. The primary operating systems used were Windows XP-10, Ubuntu, and CENTOS. Focusing on critical infrastructure and the SCADA systems that power it allowed us to expand our knowledge on these subjects due to the research taken to ensure that the scenario was reflexive of a live, critical infrastructure network. Our procedures have set us up for success by fostering a cooperative and team-based environment within our team. By working on the virtual machines one at a time, we were able to ensure quality and functionality by creating and then testing before taking on a new challenge. All of our methodologies have allowed us to further our progress, despite some recent setbacks.

2.3 User Profile

2.3.1 Project Title

Cyber Range SCADA Scenario

2.3.2 Potential Users

-Students

-Professors

-IT Personnel

2.4 Software, Interface, and Related Experience

The intended users will have a baseline knowledge of cybersecurity principals and penetration testing. Knowledge of penetration testing methodology would be beneficial, but detailed tutorials should help the users bridge this gap.

Non-technically focused users will likely not be interested in the critical infrastructure scenario unless they desire to learn more about penetration testing and in enhancing their technical skills. This project is designed to facilitate the learning and development of future cybersecurity professionals.

2.4.1 Experience with Similar Applications

Cybersecurity students may have experience with penetration testing through classes on campus, as well as possible personal experience with vulnerable machines found online or through labs such as in OSCP. While the methodology would be similar, the resources for critical infrastructure and SCADA focused penetration testing scenario are few and far in between. Students without a cybersecurity focus will most likely have little to no experience with penetration testing, which can be learned through practice.

2.4.2 Task Experience

Cybersecurity students may have experience with tasks such as

- scanning networks
- researching vulnerabilities
- reading and fixing exploit code
- creating custom shells

- escalating privileges
- extracting information from compromised machines.

2.4.3 Key Project Design Requirements That the Profile Suggests

- Varied penetration testing scenario
- Tutorials on each machine to help stuck users
- The scenario is reflexive of a real-world critical infrastructure environment

2.4.4 Team Rules

- There will be no plagiarism. We do not want a zero.
- If a team member is struggling, they will bring it up to the rest of the team.
- If a team member is absent, they will let the other team members know and the team member will relay information.
- Every Friday by 5 pm, team members will give a report on what was accomplished this week via GroupMe, email, text, or in person.
- Each team member will proofread the final paper.
- Team members will share the knowledge learned to other group members.
- Each team member will do their work to the best of their ability.

2.4.5 Budget

The original budget was offset by the hosting on UC's sandbox. Due to the events of losing our VMs on the University of Cincinnati platform, we had to use a local Client system implement this Critical infrastructure and network. Which in this case didn't cost us anything to complete the project. We utilized free and open source software to complete the project.

2.5 Gantt Chart

Table A: Gantt Chart presents our project timeline for when we need to have certain aspects done for the project. Each section is done by a different team member but is double checked by everyone.

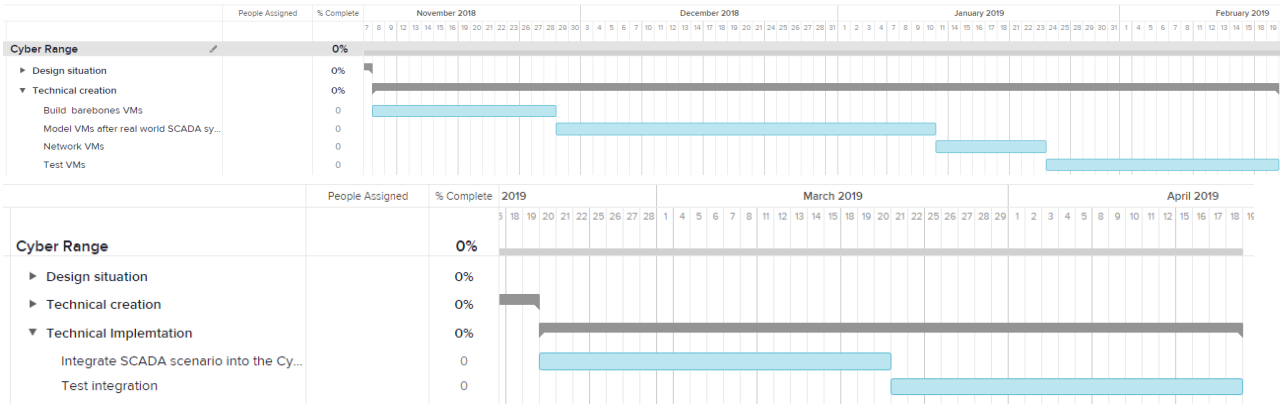


Table A: Gantt Chart

2.6 Scenario Use Case Diagram

Figure 1: Use Case Diagram presents information on what the users can do and what the administrators can do to the virtual machines. The administrators will be able to have full control over the virtual machines while the users will have most of the controls that the administrators have with the addition of a few features.

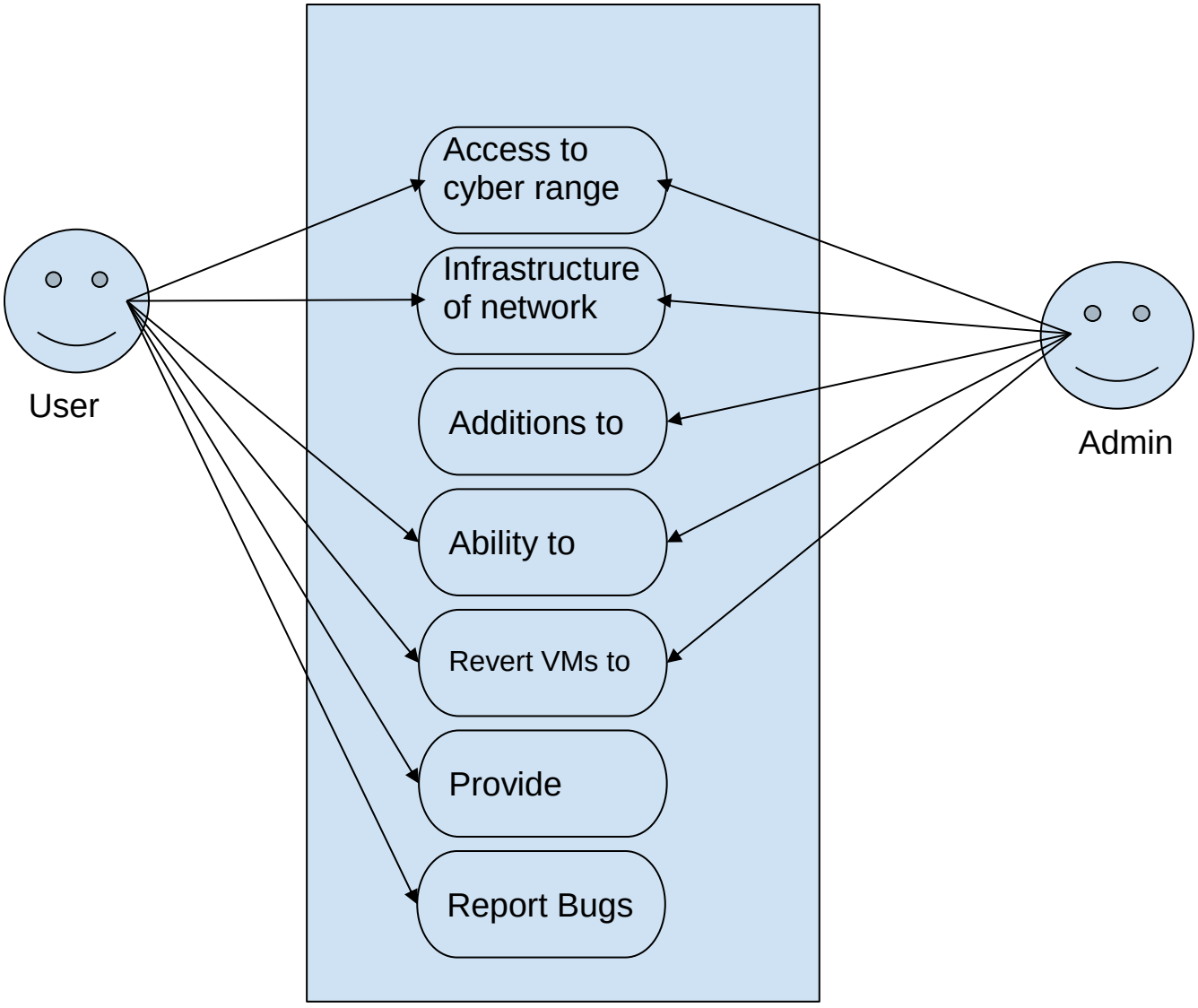


Figure 1 Use Case Diagram

2.7 Technical Architecture

Figure 2: Network Diagram presents information about each scenario that is created. Each scenario has the number of virtual machines in it with the operating system, exploits and pivot points are in each machine. Included in each scenario shows the direction the user should go to gain access to the SCADA machine.

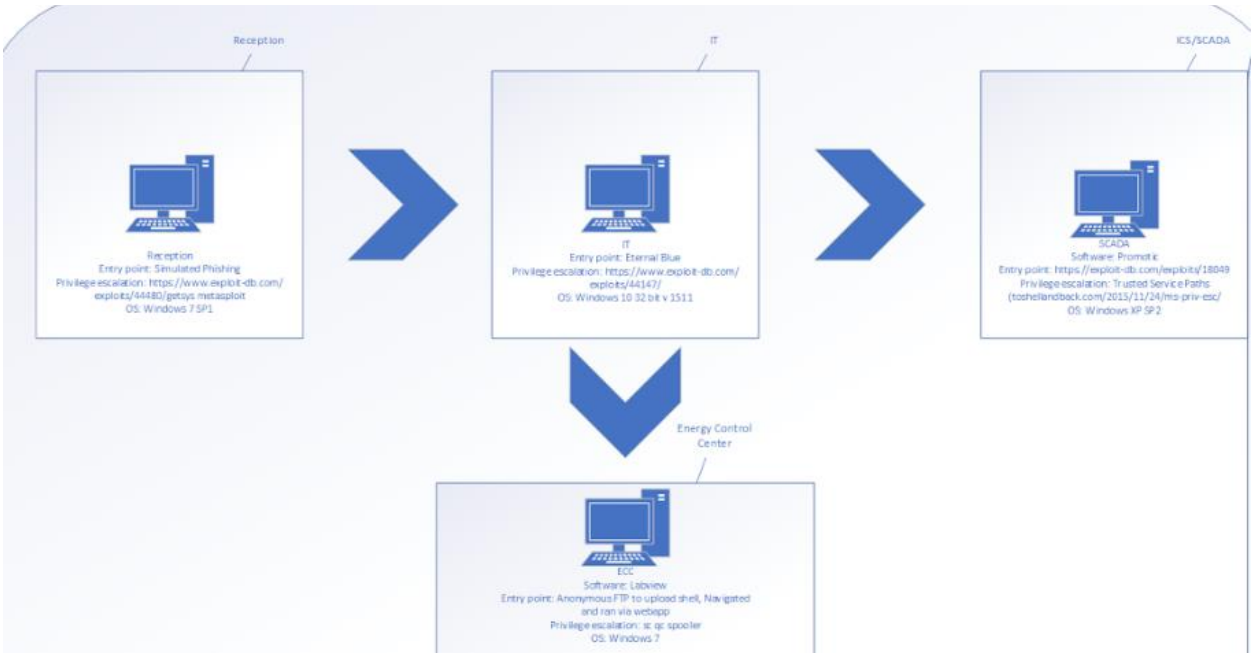


Figure 2 Network Diagram 1

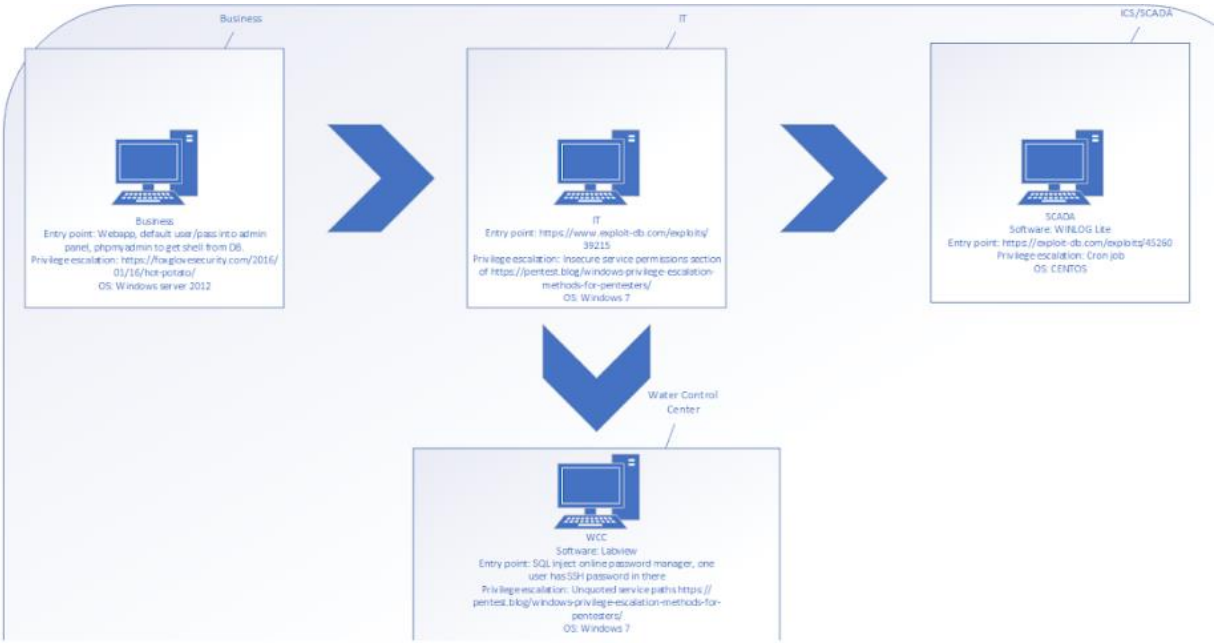


Figure 3 Network Diagram 2

2.8 Technical Discussion

We created 8 virtual machines that are reflexive of a real network. The machines were meant to summarize a business, as creating a 1:1 replica would be near impossible with the amount of resources we had available. The first virtual machine we created had several vulnerabilities. This one was meant to show a soft target, a reception computer, and was vulnerable to an exploit with a mail application. The second was an IT machine vulnerable to an SMB Eternal Blue exploit and then a kernel exploit privilege escalation. The third was a SCADA system for power generation and was vulnerable to two windows XP exploits. The Energy Control Center featured a web application that allowed the user to issue commands via SQL and file creation.

The next VM was to resemble a business made publicly facing commercial web site with a hidden log in page and default credentials. This web site allowed for module uploads that would allow remote code execution. This was vulnerable to a windows

privilege escalation exploit. The next was an IT machine vulnerable to an FTP exploit and then escalated via insecure service permissions. The third machine in this scenario was vulnerable to Apache Struts (the RAPID SCADA web application was hosted via this Apache version). The escalation was via an abusable CRON job. The fourth machine in the second scenario had a password manager that was vulnerable, this allowed users to access it and see a hashed version of one of the user account passwords. The machine was escalated via a windows vulnerability with unquoted service paths.

The energy control center, water control center, and the two SCADA machines were running an open source program called RapidSCADA. This program allowed for the creation and customization of visuals and dynamic data. Custom made visuals were created for this program and were based off of publicly available information.

2.9 Testing

The testing was conducted during the creation of the virtual machines. Before we marked a machine as “done” we ensured that the exploits worked and that the system was stable throughout the process. Testing was fairly simple and binary for our project. We did not have to be concerned about UI or custom built code as this was mainly about configuring existing programs. Creating the visualizations in RapidSCADA required a bit more testing, just to ensure the link between the database and the visualizations was intact. The testing was done by working through the machines like how a user would.

Machine	Initial Exploit	Privilege Escalation	SCADA System	Overall
Energy - Reception	Working	Working	Working	Done
Energy - IT	Working	Working	Working	Done
Energy - SCADA	Working	Working	Working	Done
Energy - ECC	Working	Working	Working	Done
Water - Business	Working	Working	Working	Done
Water - IT	Working	Working	Working	Done
Water - SCADA	Working	Working	Working	Done
Water - WCC	Working	Working	Working	Done

Table B.

2.9-A Problem Encountered

We have encountered several problems on our road thus far. The largest problem has occurred as a result of UC sandbox. We ran into some slight issues in regard to the operating systems available to us. In order to provide users with a fleshed out and varied network, we required more than just the standard windows images default to the sandbox. There have also been issues in creating virtual machines, as we have to go through a point of contact on UC staff in order to create new VMs. There have also been hardware concerns, as running the number of machines that we intend can be taxing on the University's servers. At one point, all of our VMs were deleted and were unable to be recovered. We have worked around these issues by creating the machines and networks on our personal computers, which we will pack up in modules and hand off to the UC Cyber Range team to use how they choose.

2.9-B Future Recommendations

The project was a small percentage of what exploiting a Critical infrastructure network would be like. Manipulating infrastructure as a video game, make prettier graphical user interface with the ability to move freely within the Cyber Range box. However, this type of implementation could take more than a year to complete. Also, will require consistent patching and maintenance. Therefore, Cyber Range demonstrates the ability to get into Industrial systems and how easy it can be to manipulate. If this project were to have more time, it would have more potential to grow and invest in other areas in Industrial control system. The initial plan was to expand the project to include

other infrastructure, such as public transportation control systems, Internet Service providers, city traffic lights and other similar systems that cities rely on. The suggestions we were given to us were to set up an educational module that assisted students to learn to prevent these types of attacks and many other. The plan for the project is to follow up with the team in a few months to re-evaluate we the team stands and what can be done to improve the project as a whole.

3.0 Conclusion

Throughout the year, we learned a lot about what it takes to create a working SCADA scenarios. We focused our scope on having a two scenarios then having four scenarios. We wanted to spend more time creating high quality virtual machines for only the two scenarios then having four scenarios with mild quality virtual machines. In the end, we created two quality scenarios of water and electric plants that people are allowed to test their penetration testing skills on various virtual machines that lead to the SCADA machine. Once in the SCADA machine, the attacker is able to manipulate data and see repercussions from the manipulated data. We are also going to give our project to the Cyber Range and the University of Cincinnati and the government will be able to use our project with future trainings.

Appendix A. References

"NSA Chief Says U.S. Infrastructure Highly Vulnerable to Cyber Attack." *Reuters*, Thomson Reuters, 12 June 2013, www.reuters.com/article/us-usa-cybersecurity/nsa-chief-says-u-s-infrastructure-highly-vulnerable-to-cyber-attack-idUSBRE95B10220130612.

Carlisle, Peter. "Nurturing Talent to Close the UK Cyber Security Skills Gap." *IT Pro Portal*, ITProPortal, 28 Nov. 2018, www.itproportal.com/features/nurturing-talent-to-close-the-uk-cyber-security-skills-gap/.

John, Michael. "Forget the Skills Gap, in Energy Cyber Security, It's a Chasm." *Euractiv.com*, 16 Apr. 2018, www.euractiv.com/section/energy/opinion/forget-the-skills-gap-in-energy-cyber-security-its-a-chasm/.

Appendix B. Equipment

1x Kali VM

2x Windows 10 VM

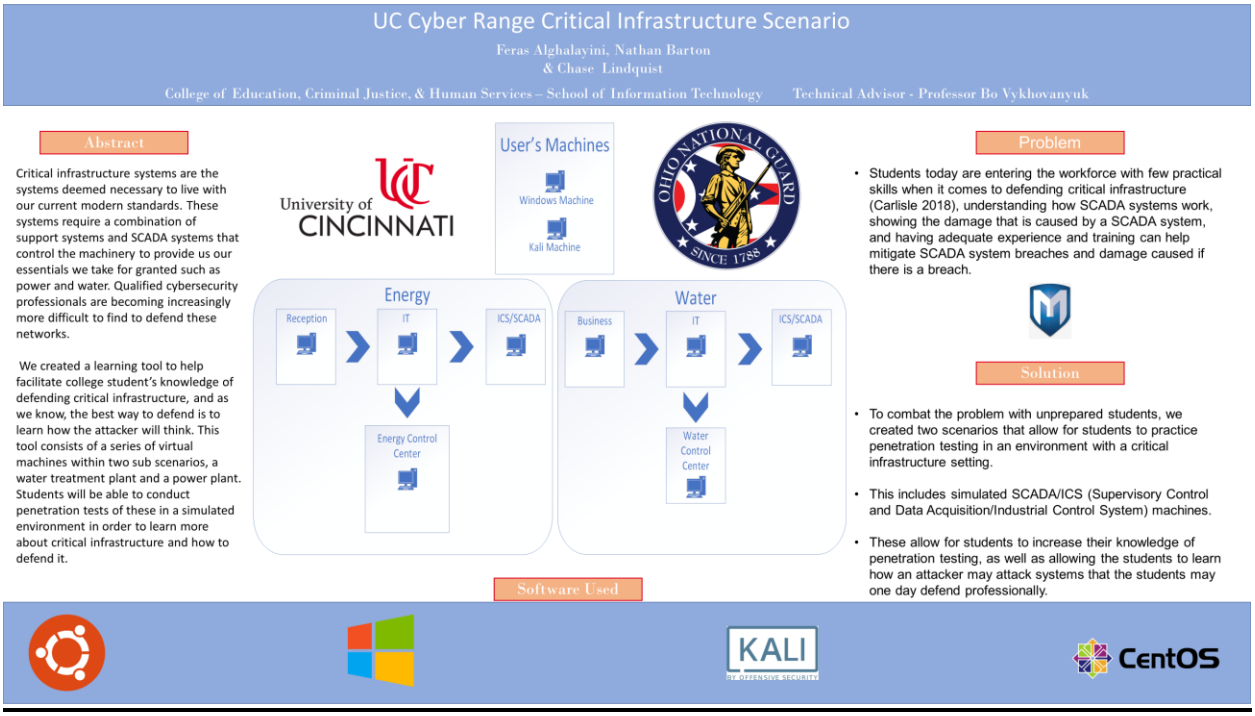
2x Windows 7 VM

1x Windows XP VM

2x Ubuntu VM

1x CENTOS VM

Poster


UC Cyber Range Critical Infrastructure Scenario
Feras Alghalayini, Nathan Barton
& Chase Lindquist
College of Education, Criminal Justice, & Human Services – School of Information Technology
Technical Advisor - Professor Bo Vykhovanyuk
Abstract
Critical infrastructure systems are the systems deemed necessary to live with our current modern standards. These systems require a combination of support systems and SCADA systems that control the machinery to provide us our essentials we take for granted such as power and water. Qualified cybersecurity professionals are becoming increasingly more difficult to find to defend these networks.
We created a learning tool to help facilitate college student's knowledge of defending critical infrastructure, and as we know, the best way to defend is to learn how the attacker will think. This tool consists of a series of virtual machines within two sub scenarios, a water treatment plant and a power plant. Students will be able to conduct penetration tests of these in a simulated environment in order to learn more about critical infrastructure and how to defend it.
University of CINCINNATI
User's Machines
Windows Machine
Kali Machine
OHIO NATIONAL GUARD
SINCE 1788
Energy
Reception
IT
ICS/SCADA
Energy Control Center
Water
Business
IT
ICS/SCADA
Water Control Center
Software Used
KALI
CentOS
Problem
Students today are entering the workforce with few practical skills when it comes to defending critical infrastructure (Carlisle 2018), understanding how SCADA systems work, showing the damage that is caused by a SCADA system, and having adequate experience and training can help mitigate SCADA system breaches and damage caused if there is a breach.
Solution
To combat the problem with unprepared students, we created two scenarios that allow for students to practice penetration testing in an environment with a critical infrastructure setting.
This includes simulated SCADA/ICS (Supervisory Control and Data Acquisition/Industrial Control System) machines.
These allow for students to increase their knowledge of penetration testing, as well as allowing the students to learn how an attacker may attack systems that the students may one day defend professionally.