Nathan Satterfield

Prof. Julie Henderson

May 2022

Proposal

**Problem Statement**

The Charleston Southern cyber competition team currently lacks an environment to practice many of the skills and techniques that they are learning. For many students it is very difficult to truly learn and understand without hands on practice. This leads to students having the knowledge of what to do but without the experience to be able to implement that knowledge.

The simplest way to fix this issue is to setup an environment where they can practice what they have learned leading to a better understanding of the topic. This would also increase the team’s performance in many of the competitions that they compete in as it could be used to simulate the competition environment.

**Project Description**

The goal of this project is to provide Charleston Southern computer science and cyber security students somewhere to practice the skills they are learning. This will be accomplished by providing a server that will host several virtual machines to emulate the format of many of the competitions the students participate in. These virtual machines will be purposefully misconfigured to be insecure so the students can practice hardening systems. There will be several different operating systems included consisting of at least a few windows and linux based systems. Also included will be a list of items that will be scored vulnerabilities and a guide on how to find and fix them along with information on why it is a vulnerability when possible. Along with the list of vulnerabilities when possible there will be an automatic scoring engine so the students know how many of the scored issues, they have found without having to cheek the list. There will also be a check list of items to complete for each operating system type which will allow the students to follow along which will help them know what steps are most important and what they have completed along with what steps they have remaining.

**Proposed Implementation Language(s)**

There will be some scripts written using windows power shell, bat files, bash, and sed to automate many of the tasks for hardening the systems.

**Additional Software/Equipment Needed**

For hardware there will need to be a server to host the virtual machines and networking equipment to be able to access the server. For software Windows and linux operating systems will be needed as well as esxi as a hypervisor to host the virtual machines. The CyberPatriot Scoring Engine will be needed to automate scoring on the machines from <https://www.uscyberpatriot.org/competition/training-materials/practice-images>

**Personal Motivation**

By completing this project, I will gain a better understanding of many cybersecurity policies and networking. This is because in order to create a competition environment a better understanding of the issue rather than just how to fix them is required. Creating a purposely insecure system will give a better understanding as to what make it insecure and how to make it secure. This will also expand on my knowledge of networking as I have previously focused primarily on strictly hardening systems.

**Outline of Future Research Efforts**

Future research will into what systems already exist for this purpose as there is a cyber range currently in place although it was never completed fully. Deliverables that should be expected is a fully functional cyber range for Charleston Southern student to practice for competitions and deepen their understanding of hardening systems. As well as cheek lists, solutions to all the virtual machines and some tools for automation.

Schedule

Functional requirements 2/25/2021

Finish first draft of requirements 3/18/2021

Final draft due 4/20/2021

**August 23 fall 2021 starts**

3 weeks to configure network 9/13/2021

3 weeks to setup virtual machines 10/4/2021

2 weeks to write checklists/walkthroughs for virtual machines 10/18/2021

2 weeks to write automation tools 11/8/2021

**December 6-10** **Finals**

Requirement Specification

Req #1 Enumerate network

Functional

Create a network map of the network that the cyber range will run on.

The goal of this project is to create a cyber range that can be accessed over the network which requires knowing how the network is currently setup so the cyber range can be added to the network.

After this requirement is completed there should be a finished network map available that describes the network.

Priority #1

Dependencies none

Req #2 Configure network

Functional

Ensure the network is configured properly to let students access the cyber range over the proper network.

If the network is misconfigured students will not be able to access the cyber range and thus will not be able to use it.

After this requirement is completed students should be able to connect to the network that the range will run on

Priority #2

Dependencies #1

Req #3 Setup the host server.

Functional

Configure the server that will host the virtual machines.

This server is the base for the cyber range without it the virtual machines that make up the range will not be accessible by the students.

After this requirement is completed the host server for the cyber range should be ready to host virtual machines to students over the network.

Priority #3

Dependencies #1 and #2

Req #4 Create virtual machines.

Functional

Create the virtual machines that will make up the environment.

The virtual machines are what the students are going to use to practice on they are the main part of the project that the students will interact with.

After this requirement is completed there should be standalone virtual machines that students can use to practice on.

Priority #4

Dependencies none

Req #5 Host the virtual machines on the server.

Functional

Take the virtual machines that have been created and move them onto the sever to be hosted.

Once the virtual machines have been created and the host server configured the last step to create a functional cyber range is to combine the two so that students can access the virtual machines via the server.

After this requirement is completed there should a functional cyber range with virtual machines accessed over the network.

Priority #5

Dependencies #1-4

Req #6 Accessibility

Security/Access

The cyber range should be configured in such that it can only be accessed via the correct local area network.

This is important as unauthorized users should not be able to access the range so the server should only allow host to connect from the CSU computer lab network.

After this task is done the server should only be accessible from the CSU computer lab network.

Priority #6

Dependencies #1-5

Req #7 User capacity

Performance/ Capacity

The cyber range should be able to support up to 6 people concurrently.

This is important as most competitions are team competitions generally allowing up to six team members so this would allow the whole team to practice at the same time.

After this task is done the server should be able to support a minimum of six users connecting at the same time.

Priority #7

Dependencies #1-5

Req #8 expandability

Performance/ Scalability

The cyber range should be configured in such that new virtual machines can be added at any time.

This is important as what the students want to practice may change as new operating systems and updates to existing ones happen.

After this task is done the server should be configured such that adding new virtual machines or making changes to existing ones can be done.

Priority #8

Dependencies #1-5