Blue Team Defense

by

Johnny David, Mitchell Rolfes, Lukas Schumaker

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/Cybersecurity

Johnny David — Date: 4/19/2022

Mitchell Rolfes — Date: 4/19/2022

Lukas Schumaker — Date: 4/21/2022

Tyler Hopperton, Advisor — Date: 4/21/2022

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

April 2022

Table of Contents

List of Illustrations

TABLES

PICTURES

Abstract

Exploiting systems using known vulnerabilities has become a concern for companies. To protect their systems, penetration testers are being offered lucrative contracts to find vulnerabilities and exploits on a company's system. Our team noticed there are many training programs for penetration testers and red teamers to hone their skills. When looking for blue-team training programs, there are much fewer, making it difficult for IT professionals to train on how to defend against such attacks. Our team set out to create labs in which an attack has already occurred, and it is up to the user to diagnose the attack, research the incident, and return the system to a working state. Our goal was to create an environment that simulates real world attacks and give the user tools to take out the attack.

Introduction

Project Summary

We have created a series of virtual environments set up to simulate cyber-attacks. Users must be able to detect, respond, and recover from these scenarios. This lab environment will help defensive cybersecurity personnel, known as ‘blue team’, develop their skills in responding to attacks from both offensive cybersecurity personnel, known as ‘red team’, and outside attackers.

Problem Statement

A cyberattack can have devastating consequences on a corporation's network. While most companies have a cybersecurity team, many of these team members do not have much experience in responding and mitigating a cyber-attack. While there are resources for blue team professionals on the market, DeCusatis et al. (2021) suggests that “there is a lack of activities specifically addressing threat[s]”. Security personnel need interactive training to improve their skills and with little to no affordable training labs for blue team personnel, there is a lack of trained individuals in the field. According to HelpNetSecurity (2020), “research shows that 62 percent of blue teams have difficulty stopping red teams during adversary simulation exercises.” This lack of training leads to a great threat to the security posture of companies globally, leading to potential attacks that can have serious consequences.

Solution

Blue Team Defense creates virtual labs that simulate real world cyber-attacks, where blue team security personnel can hone their skills in preventing and responding to these incidents. Users are tasked with investigating incidents, documenting their results using various tools provided in the lab, and restoring systems to a working state. Each lab has a different attack and difficulty level, allowing our users to be prepared for any scenario, both simulated and actual.

Project Source

With each of our team members being security majors, we wanted to create a project where we applied what we have learned in the classroom and in our jobs. Lukas brought up how there are not many engaging and interactive labs available for defensive security personnel, unlike the abundance of material for offensive security personnel. That is how we came up with our idea, where we would create virtual environments where defensive security teams can work on their skills in investigation and response.

Project Discussion

Project Objectives/Goals

- Create a lab environment that simulates devices that have been attacked by malicious actors.
- Users can go through the lab and accomplish objectives such as detecting the attack, understand the material given to them, and taking the steps to clean the system back to its original state.
- Help train any individual, with labs ranging from easy to hard. The user will be able to understand concepts of blue team security after completion of each lab.
- We want users to put their knowledge to the test. This means we want to give users the situation and environment and let them work through the lab on their own.

Project Scope

Our team will develop a lab environment that simulates various attacks and their perceived difficulty. This will give users the opportunity to increase their knowledge from realistic challenges that would occur during an attack. Users will have a brief understanding of each lab before they begin, so they can select a lab that can help them improve their skills or because the lab interests them. Labs will vary depending on difficulty and will focus on a range of topics. The most important features will be the simulated environment and the tools to help the users complete the required tasks. These will likely be the biggest constraints throughout the project, as the virtual environments may require extended amounts of memory and processing capabilities. We will provide an inclusive lab environment, where once an account has been created, our users will be able to begin the lab without having to download extra software, as the files and software needed for the lab are already on the system. During the labs, the user will go through a quiz to make sure they are understanding the core concepts of each lab. If the user decides to leave the lab, their progress will be saved and will be able to come back to where they left off. Once the user has completed the lab, they can submit their quiz to gain immediate feedback.

Quick Project Timeline

Table 1 Project Timeline

Task #	Task Name	Duration	Start Date	End Date
1	Plan of what attacks will be used	28 days	9/13/21	10/11/21
2	Plan of using hardware/VM finalized	28 days	9/13/21	10/11/21
3	Implement/Testing initial environment(s)/lab(s)	20 days	10/11/21	10/31/21
4	Completing/Presenting of Proof of Concept	Month	11/1/21	12/3/21
5	Implement/testing additional labs/environments	2 Months	1/10/21	3/7/22
6	Create website for end user access	1 Month	3/8/22	3/31/22

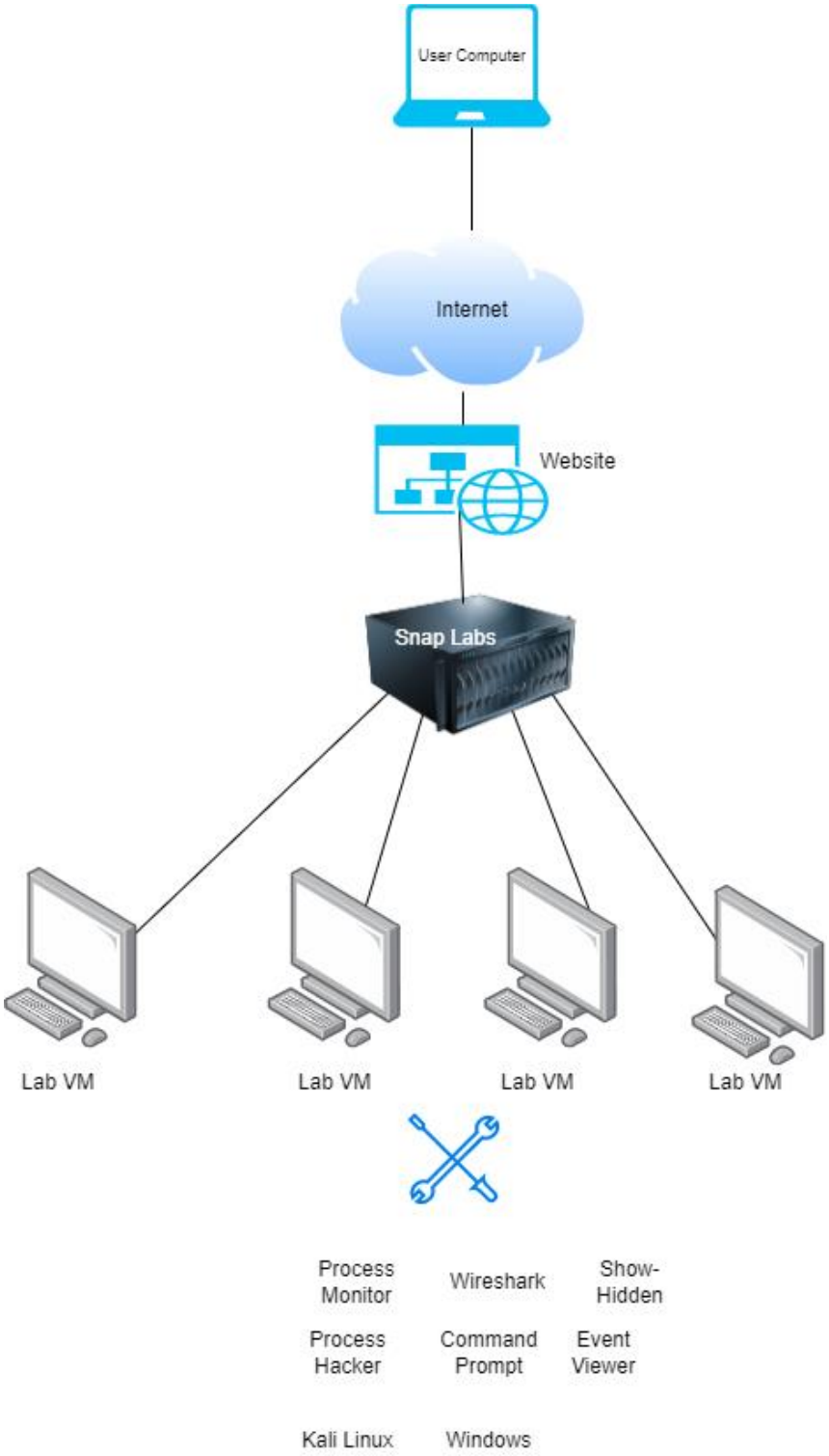
7	Create final presentation	1 Month	3/8/22	3/31/22
Final Task	IT Expo	1 Day	4/12/22	4/12/22

Technologies Used

We used a wide range of technologies to help simulate realistic environments in our challenges. We set up virtual machines in VMware to test our scenarios and make sure our lab concepts worked. We then ran tests and exploited vulnerabilities on the targets, which tested the security of the tools installed on the virtual machines. Considering these machines are already vulnerable, these environments were realistic examples of what a system might look like after a cyber-attack. We used a wide range of tools such as Windows, Linux, Wireshark, Show-Hidden, Event Viewer, Process Hacker, and Process Monitor to give the user hands-on experience of using blue-team software. For the hosting of our labs, we are using Snap Labs, which uses Amazon Web Services to host labs and allows Snap Labs to create templates of the labs to share with other Snap Labs users. Our website was created using HTML and CSS and is hosted locally on a Raspberry Pi that runs Apache Web Server.

Technical Architecture Diagram

Picture 1 Technical Diagram



User Personas

Table 2 User Persona 1

User Persona: 1	
Picture: 	Title: Cyber Security Student Name: Hayden Age: 22 Gender: Male
Behavior	Hayden is an ambitious college student ready to graduate and get a job in cyber security. He is hard working and wants to build his resume.
Pain	Hayden is a cyber security student that wants to work on a blue team, but he can't get hired because he has no real-world experience.
Needs & Goals	● As a college student, Hayden is struggling financially and wants an affordable way to practice realistic blue-team exercises. ● He does not have much experience

	with blue-team concepts, so he wants something that will start him out with low difficulty. ● Hayden wants to gain real-world skills that will help build his resume and land him a job in the cyber security field.

Table 3 User Persona 2

User Persona: 2	
Picture: 	Title: User transitioning to a new field in IT Name: Max Age: 27 Gender: Male
Behavior	Max is a highly motivated family man working in a networking position but wants to transition into a security role that recently opened at his company. He is bored with his current role and wants a change of scenery.

Pain	Max wants to transition into a blue team role but doesn't believe he has the skills due to lack of exposure in his current role. He has talked to his supervisor, and the company is not willing to pay for any classes or certifications. He is left to build his skills on his own.
Needs & Goals	● As a family man, bills are tight, and Max needs an affordable option to learn about blue-team concepts. ● Max has an IT background and some understanding of security, so he needs some practice that isn't too hard, but isn't for beginners either. ● Max's goal is to transition into a new security role, where his work more closely aligns with his interests.

Table 4 User Persona 3

User Persona: 3	
Picture:	Title: Experienced User sharpening skills Name: Chris

	Age: 52 Gender: Male
Behavior	Chris is the head of a blue team at a Fortune 500 company. He is extremely hard-working but spends a lot of his time doing management related tasks. He wants to make sure his blue team skills stay sharp and his knowledge of current practices stay up to date.
Pain	Chris is always stuck in meetings and dealing with upper management, so he does not have a lot of time to keep his blue-team skills sharp. He feels like he is slowly falling behind.
Needs & Goals	● Chris is an experienced blue-team professional who requires expert-level practice to test his skills. ● Chris wants to test that his skills are still sharp, so he can lead his team

	effectively.

Use Cases

Table 5 Use Case BTD_001

Use Case ID	BTD_001
Use Case Name	Selecting a lab
End Objective	The user selects a lab that they feel comfortable with beginning.
User/Actor	Blue Team Defense member.
Trigger	The user selects a course to begin.
Frequency of Use	Every user will need to go through this process to use one of our labs.
Preconditions	The lab is online and available for the user to select.

Basic Flow	1. User selects a lab based on the description and difficulty of the lab. 2. The user will be prompted to login into their Snap Labs account. 3. User confirms their selection on Snap Labs. 4. Snap Labs builds the lab environment. 5. The user will be automatically logged into the lab they have selected.
Alternate Flow	AF1. User is already logged in Snap Labs. 1. Skip to Basic Flow 3 AF2. User quits the lab. 1. Return to Basic Flow 1. AF3. User returns to the lab.

	1. Skip to Basic Flow 2. 2. User skips Basic Flow 3 and 4. AF3. User does not have an account 1. User is prompted to create a Snap Labs account. 2. User is prompted to connect an Amazon Web Services account. 3. Snap Labs confirms account creation. 4. Return to Basic Flow 4.
Postconditions	User begins BTD_002.

Table 6 Use Case BTD_002

Use Case ID	BTD_002
Use Case Name	User reads information/backstory of the attack scenario.

End Objective	The user will have sufficient information to begin the lab.
User/Actor	Blue Team Defense Member
Trigger	The user selects the lab. See BTD_001 Use Case.
Frequency of Use	This will be determined by how often users choose to read the lab information.
Preconditions	The user opened the lab.
Basic Flow	1. User interacts with the lab. (see AF1) 2. User selects the folder ‘Lab Information’. 3. User reads information on the lab, getting enough backstory as to how the attack happened and what to look for.

	4. User begins the lab
Alternate Flow	AF1. User exits the lab while in progress. 1. User goes back to lab selection.
Postconditions	The user will have information needed to begin the lab.

Table 7 Use Case BTD_003

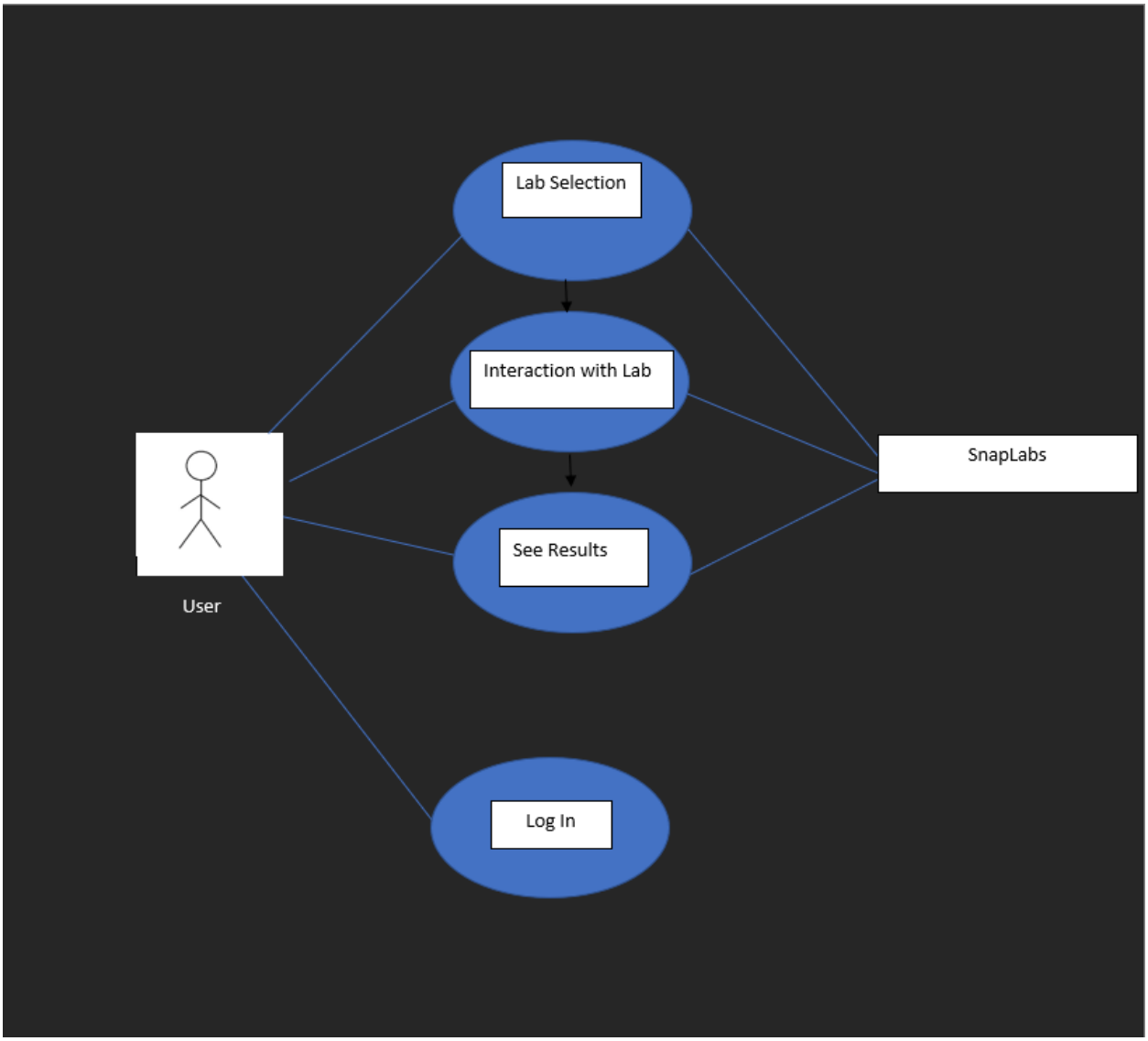
Use Case ID	BTD_003
Use Case Name	User is presented with their results and what they were supposed to find after the lab is completed.
End Objective	We want to show the user how well they did and what they missed.
User/Actor	Blue Team Defense member.

Trigger	The lab is completed and the user sees their results.
Frequency of Use	After every lab is completed.
Preconditions	The user has completed the lab and has submitted their results.
Basic Flow	1. Once the lab is finished and the user's answers are submitted, an option to see results appears. 2. The user clicks on the button to see results. 3. The results of the lab appear, and the user can see their score/grade. 4. User has option to exit the lab after seeing score
Alternate Flow	AF1. User exits the lab without seeing score 1. Users can see scores later if they are still logged in.

Postconditions	User can see how well they performed in the lab.

Use Case Diagram

Picture 2 Use Case Diagram



Testing Plan

Overview

Our testing plan will use integration testing and user acceptance to ensure that our project meets our core goal. Our scope will include the use cases that are shown in our report. We will be describing what our goals are through testing, what we will be doing to ensure our project works well with each of our components, what users will be testing when going through our labs, the results of our testing and what we have learned from testing.

Methodology

We will be using two types of testing. The first is integration testing. Since we all have different responsibilities in our project, it is important to test integration to make sure each of our components work with one another. Each member will ensure that their component works on its own, and then we can bring together each aspect and make sure they flow cohesively with one another. We will also be using User Acceptance Testing. Our project is centered around teaching others about being on the blue team. By having users test our project, we will ensure that we are reaching our core goal.

Scope

The use cases we will be using are BTD_001 (Selecting a Lab) and BTD_003 (Results). BTD_001 will be tested because it is vital that a user is able to select one of our labs. If they cannot use one of our labs, then we have failed to reach one of our core goals. The BTD_003 will be tested to make sure that the results the user sees are correct. The features that we will be testing is the lab environment. We will need to test each lab to make sure it works as intended.

Objectives

All use cases will be accounted for when testing to ensure they are completed as expected. Bugs will be reported immediately and will be worked on as a team to resolve the issue. The project will be in a stable condition by the time we reach the IT Expo.

Test Logs and Procedures

Test Case #: BTD_Test_1
Date of Test: January 18th, 2022
User Type: User Persona 2, medium level IT professional
Test Summary: This is the first instance of user acceptance testing that we have completed for our project. We invited a close friend, who currently works full time as a technical support analyst, to try completing the three labs that we have currently designed. We explained the labs

briefly, without revealing any specifics the user should be looking for. Essentially, we wanted the user to begin the test without any help from us.
Expected Output: We expected our user to complete the easy lab environment without much difficulty. As for the medium level environment, we knew it would be a bit more of a challenge. Our group believed the user would be able to complete the lab, although it would be significantly more difficult and take more time. In regard to the expert-level lab, we were not optimistic about the user's success, although we believed the user might be able to piece a few things together.
Actual Output: Our user was able to defeat the first challenge, without much difficulty. It was helpful that the user had prior experience with Wireshark, as well as understanding of keyloggers. For the medium-level lab, our user struggled significantly more than the first lab, as they were unfamiliar with some of the technology used. Once, we nudged the user to start looking around the file system, and research .HTA files, everything went much smoother. As for the expert-level challenge, our user had a tough time and could not identify the vulnerability in the cron job. The user also had to do more research regarding the software he was observing, considering he was unfamiliar with pspy, and not entirely confident maneuvering in the Linux CLI. Ultimately, we had to nudge the user several times in the right direction to complete the challenge.
Pass/Fail: Pass
Reason for Pass/Fail: We were pleased with the results of this testing. We believed that the skill levels for each lab were just right for this user. Considering the user does not work directly in security, it made sense that the medium and hard level labs would be a bit difficult to complete. We were also pleased that no technical difficulties were experienced during the testing.
Notes: Our user suggested that we make the labs environments more realistic, by adding more fake files to the directories. This is something we planned on doing beforehand, and we were glad to hear similar feedback. The user also commented that we needed a way to ensure future users that the changes they make to the lab environment is the correct response behavior. We discussed the idea of comparing hash values for files, which we will implement moving forward.

Test Case #: BTD_Test_2
Date of Test: January 22nd, 2022
User Type: User Persona 1, beginner level IT student
Test Summary: This is the second instance of user acceptance testing that we completed. We invited another close friend, who transferred out of Information Technology after a year in the major. Once again, we had this user attempt each of our labs. Like our prior testing, we made sure the user understood the concept of the labs but did not reveal any specifics.
Expected Output: Our group believed the user could complete the easy lab, but it would require a significant amount of research and time. We did not believe the user would be able to complete the medium or expert lab. This expectation was due to the lack of familiarity with technologies used in the labs, especially with Linux, as well as other security concepts.
Actual Output: Our user had more difficulty with the easy lab then expected, specifically with the usage of Process Monitor, since it was a piece of software that he had never used before. We had to provide significant guidance and explanation to get the user completely through the lab. As for the medium and hard lab, our user had high levels of difficulty, and could not progress through the lab on his own. The user was more comfortable with the medium lab due to the Windows OS, although a similar amount of struggle was shown in each environment.
Pass/Fail: Pass

Reason for Pass/Fail: Like the first test case, we believe this session proved the skill levels required for the labs are accurate. Considering our user had only one year of IT classes as experience, his difficulties with each lab seemed fitting, especially the medium and hard level lab. We were once again pleased with the lack of technical difficulties.
Notes: Our user proposed that we put some links to articles/websites that may be helpful during the lab. We explained that we did not want to do guided labs, but this seemed like an interesting middle ground we could think about implementing.

Test Case #: BTD_Test_3
Date of Test: February 3rd, 2022
User Type: Any user
Test Summary: Once we put our labs on Snap Labs, we wanted to see what the process was of creating an account on Snap Labs to be able to use our labs. This test was done with a friend who had no prior knowledge of Snap Labs, so we could make notes of what instructions a user may need in order to create an account and then the process to build our lab.
Expected Output: We expected the user to understand the sign-up process up until needing an AWS account. We provided details as to how signing up for AWS works and why it is needed. We expected the process to take about 15 minutes.
Actual Output: The user was able to create an account without further instruction and was able to build our lab with the template easily as well. Overall, the process took about 20 minutes from start to finish.
Pass/Fail: Pass
Reason for Pass/Fail: We are happy that the user was able to complete the objectives without any additional information. The process took a little bit more time than expected, but once they have their account, they will only need to build the template, which took about 5 minutes.

Testing Review

Overall, we are quite happy with how our testing has gone. Specifically, it was good to see that the projected skill level of each lab is accurate. We are glad our second use case persona was able to complete the first lab rather easily but showed signs of difficulty in the remaining two labs. We did expect the first user persona to have more difficulties, however it was clear that if the user does not have some basic understanding of the tools, then they will have a harder time with the labs. We are happy with the account creation process and the time it takes to build the lab from our templates. We also appreciated the feedback the users gave us, as it will help us continue to improve upon our labs.

Change Management Plan

Who can make a change and in what circumstances?

Any of our team members and advisors can request a change be made. The request guidelines are that it must be reasonable, able to be implemented in an adequate amount of time and improve the project.

How are we going to triage it?

We will identify the pros and cons of our current plan compared to the requested change. If we decide to go with the change, the original process will be backed up/saved. If the change meets our three guidelines, then it will be approved.

How are you going to communicate this with the stakeholders?

Depending on the impact of the change will determine how it is communicated. Small changes can be brought up in our bi-weekly standups with our advisor. Otherwise, changes should be mentioned in Teams prior to our meeting, and it should be determined if we need to meet before our scheduled stand up.

Budget

Picture 3 Budget

				Ongoing Annual		
	Rate Per/Hr	**Work Effort (Hours)**	**1 X Costs**	**Rate Per/Hr**	**Work Effort (Hours)**	**1 X Support Cost**
Labor - IT	20	400	$ 8,000.00	20	100	$ 2,000.00
Labor - External	0	0	$ -	0	0	$ -
Software - External						$ 500.00
Hardware - External						$ 500.00
Misc.						
TOTAL			$ 8,000.00			$ 3,000.00

When looking at our budget for this project, the two biggest things for us to consider are hosting and service licenses. Our labs need to be hosted by a provider such as AWS or Azure, simply because we do not have the hardware to host it ourselves and our laptops can certainly not handle it once users are doing the labs. Cloud providers give us an opportunity to scale up and down as needed, and all the group members will be able to access it to work on it. Other costs to consider are OS licenses on the VM's for our labs, such as Windows. Because of this, we included both the license fee and hosting service fee in the annual cost column of the table above. In terms of labor, we are the only ones currently working on it, and we do not have outside help to include. So, we kept the cost at 0. Annual work hours for our internal IT team are at 100.

Problems Encountered and Analysis of Problems Solved**:**

- One of our attack scenarios was not able to be replicated on Snap Labs where we host our environments. This is because of the way Amazon Web Server's network is set up, so we had to run the attack locally and complete it there. We had to put this lab aside, as we were not able to port it over to Snap Labs at this time.

- We had a difficult time figuring out where we wanted to host our labs, and sometimes disagreed on it, but at this point we have a good idea of what we will be using. We believed that using either Snap Labs or CTFd would be a good resource for hosting. We ultimately decided on Snap Labs for hosting because of the ability to share templates of our labs.

- Finding simulated attacks that include multiple steps and many things for the user to do was a difficult process. A lot of the attack scenarios we brought up only include a few steps to solve, so we need to think of some more challenging labs. We decided a keylogger, rogue task being created, and Linux file directory labs were the best labs to create.

- Creating a way to ask questions for the user to respond and how that can be tracked. Right now, we are using Google Forms quizzes which the user will open once they have connected to the lab. We want to be able to test the user while they are using our lab as well as show the progress they have made.

- We wanted to make labs that people could use without too much guidance. However, this creates a problem where if a user has no idea what to do with a lab, they must essentially give up. Adding reading material so the user can learn about the scenario and software used will at the very least educate the user and allow them to potentially come back to the lab later.

Conclusion

We made the decision to create a blue team defense training project because we believe there are not enough resources to help those who want to pursue an opportunity in defense security. We wanted to create an environment that gives security enthusiasts of all skill levels the opportunity to learn different techniques and procedures that may be useful post-attack. The skills that we have learned include researching different attacks like ARP poisoning and keyloggers, implementing these attacks on virtual machines, using various tools to detect and cleanup the attacks, and creating environments for users to learn the tools and skills that we have implemented. Overall, we are very pleased with the project as we finish the course. We believe we have completed each of our goals that we had at the beginning of the year, where we created labs that help current and future blue team members grow their skills.

References

Casimer, D., Davaro, T., Cannistraci, B., Jenkins, J., & Ronan, M. (2021). Red-blue team exercises for cybersecurity training during a pandemic. *Marist College,* 1055.

Help Net Security August 20, Help Net Security, & 20, A. (2020, August 19). *62% of blue teams have difficulty stopping red teams during adversary simulation exercises*. Help Net Security. Retrieved March 21, 2022, from https://www.helpnetsecurity.com/2020/08/20/blue-teams-red-teams-challenges/