2018-12-11

Evaluating an Educational Cybersecurity Playable Case Study

Tanner West Johnson
Brigham Young University

Evaluating an Educational Cybersecurity Playable Case Study

Tanner West Johnson

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Derek L. Hansen, Chair
Justin S. Giboney
Dale C. Rowe

School of Technology

Brigham Young University

ABSTRACT

Evaluating an Educational Cybersecurity
Playable Case Study

Tanner West Johnson
School of Technology, BYU
Master of Science

The realities of cyberattacks have become more and more prevalent in the world today. Due to the growing number of these attacks, the need for highly trained individuals has also increased. Because of a shortage of qualified candidates for these positions, there is an increasing need for cybersecurity education within high schools and universities. In this thesis, I discuss the development and evaluation of Cybermatics, an educational simulation, or playable case study, designed to help students learn and develop skills within the cybersecurity discipline.

This playable case study was designed to allow students to gain an understanding of the field of cybersecurity and give them a taste of what a day in the life of a cybersecurity professional might be. It focuses on being an authentic experience so that students feel immersed within the simulation while completing their tasks, instead of regarding it as merely another assignment. We ran a pilot test of this playable case study in a university-level, introductory Information Technology class of 51 students. We found that Cybermatics increased the self-reported likelihood of over 70% of participants to pursue a career in a cybersecurity field. It also helped students understand the importance of leadership and ethics to a cybersecurity professional. We also found that the simulation helped students feel more confident about their ability to complete cybersecurity-related tasks.

Keywords: playable case study, cybersecurity, simulation, educational

ACKNOWLEDGEMENTS

I will always be grateful to Dr. Hansen for his continuous help throughout the development and analysis of this project. I would also like to thank Dr. Giboney and Dr. Rowe, the other members of my graduate committee, who offered their advice and feedback. Special thanks to the team that I worked with to create Cybermatics (Dan, Lexie, Anna, and Cara) for all their help. Most of all, I would like to thank my family, especially my mother, for their support and encouragement during this whole experience.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Nature of the Problem

Recent global events have awakened the world to the realities of cyber threats. There are stories of breaches, data loss, and downtime of services in the news every few days. Because of the growing number of these attacks, both the public and private sectors have increased their defenses and have grown their cybersecurity teams. There are more jobs available in this field than there are qualified people to fill those jobs. The Bureau of Labor Statistics stated that the job outlook for Information Security Analysts will increase by 28% (much faster than average) between 2016-2026 (U.S. Bureau of Labor Statistics, 2018). These jobs require highly trained individuals with training in a wide variety of skills.

Because of the shortage of qualified candidates for these positions, there is an increasing need for cybersecurity education within high schools and universities (Rowe, Lunt, & Ekstrom, 2011). Many students are not aware that these types of jobs exist, and those who are aware often do not know where to start or have the confidence they need in order to succeed. Some cybersecurity competitions exist that perform a function of cybersecurity education. These are helpful to students who already have a foundation in cybersecurity and enjoy competitive settings, but they are not as helpful to students who are new to the cybersecurity field or dislike competitions.

To provide a possible solution to this situation, this research developed and evaluated the effectiveness of Cybermatics. Cybermatics is a cybersecurity playable case study, a type of immersive simulation designed to introduce players to an authentic cybersecurity workplace environment (Balzotti, Hansen, Ebeling, & Fine, 2017). Cybermatics can easily be run in a formal classroom setting. It includes an authentic context where students work in a team and complete a realistic (though simplified) penetration test, and it lends itself to novices who otherwise might not be interested in learning about cybersecurity.

1.2 Objectives/Goals

My goal was to create a novel playable case study, named Cybermatics, aimed at teaching novices the nuances of cybersecurity in the form of a penetration test. It revolves around a plot that we created including a fictional pentesting company called Cybermatics, individuals within that company, the company that is being pentested called RipTech, as well as a bad actor.

This simulation is a replayable series of events that occurs over a five-day period and mimics events that could occur in a real scenario. Students interact with fictional characters that advance the plot through videos, emails, chat, and a real website. It is designed to be carried out within a classroom environment where a teacher who has knowledge of the entire situation will be available for questions, as well as help guide the participants in the event of frustration or loss of direction. It also allows for meta-reflection where participants can meet with their instructor to reflect about the simulation after each session.

The overall goal of the simulation is that participants come away from the simulation intrigued to learn more about cybersecurity and have a basic understanding of the structure of penetration tests as well as introductory-level penetration testing dispositions, knowledge, and skills. For knowledge, it teaches SQL injection, basic password cracking, as well as the Linux

terminal. For skills, it allows students to perform SQL injection, crack passwords, and navigate through a Linux environment, as well as gives students experience in technical writing. Finally, for dispositions it teaches students to behave ethically, think like a hacker (e.g., try and break things), and think outside the box. It enables students to put themselves in the shoes of the bad actors, which in turn teaches students how to defend against them.

1.3 Research Objective/Questions

Research Objective 1 (RO1): Develop an authentic cybersecurity simulation for novices where students will learn about introductory-level penetration testing dispositions, knowledge, and skills.

Research Question 1 (RQ1): How does a playable case study affect students' a) likelihood of going into a cybersecurity career, b) intention to continue learning about cybersecurity, and c) confidence in their ability to succeed in a cybersecurity job? How do these correlate with each other?

Research Question 2 (RQ2): Did the simulation change students' understanding of the cybersecurity profession? How did their understanding change?

Research Question 3 (RQ3): Did the simulation change students' confidence in specific cybersecurity-related skills change? How did their confidence change?

Research Question 4 (RQ4): How do different design features of a playable case study relate to a feeling of realism? What improvements could be made to the simulation?

1.4 Definitions

- Access Control - ensures that resources are only granted to users who need them.
- Authentication - the process of confirming the validity of a claimed identity.

- Backdoor - a tool installed after a system is compromised to give the attacker easier access to the compromised system around security mechanisms.
- Brute Force – an attack method that uses an exhaustive procedure that tries every possible combination in a given problem space.
- Defense In-Depth - the approach of using multiple layers of security to guard against attackers as opposed generally to perimeter defense.
- Dictionary Attack - an attack that tries all the phrases or words in a given dictionary, attempting to crack a password or key.
- Hardening - the process of identifying and fixing vulnerabilities on a system.
- Hash - a one-way mathematical function used to safely store passwords
- Password Cracking - the process of attempting to guess passwords, given the password file information, generally in a hashed format.
- Penetration Test - the practice of performing an authorized attack on a system to evaluate the security of the system.
- Phishing - the use of emails that appear to originate from a trusted source attempting to trick a user, generally into giving up credentials.
- Reconnaissance - the phase of an attack where attackers find new systems, map out networks, and probe for exploitable vulnerabilities.
- Risk - the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.
- Scope Document - a document that enumerates the systems and techniques in scope for a penetration test

- SQL Injection - a code injection attack where modified SQL statements are inserted into a form field to be executed as part of the original SQL query.

1.5 Summary of Chapters

The remainder of the thesis is organized into the following chapters: Chapter 2 discusses relevant literature related to educational simulations, cybersecurity education, and playable case studies. Chapter 3 describes the development process, what data was collected, and how the data was evaluated and analyzed. Chapter 4 outlines the Cybermatics playable case study itself, the characters, the storyline, and the key simulation features. Chapter 5 goes over the findings as related to the research questions. Finally, Chapter 6 discusses the results from Cybermatics, feedback received from students, the impact Cybermatics had on students, the limitations we experienced, as well as future research ideas.

2 LITERATURE REVIEW

2.1 The Need for More Cybersecurity Professionals

There is a growing need for cybersecurity professionals. An estimated 1.8 million positions in cybersecurity jobs will be empty by 2022 (Sullivan, 2017). Furthermore, other technical jobs require at least some level of cybersecurity knowledge to be able to fulfill job responsibilities (Kay, Pudas, & Young, 2012). It is important to reach out to future professionals early in their education, so they are aware of the opportunities in cybersecurity. Despite significant efforts to advance cybersecurity education, there is room for improvement. When choosing a major/career, millennials continue to have a lack of awareness for cybersecurity education as well as job opportunities within cybersecurity despite the high salaries and amount of opportunities (Baker, 2016; Vogel, 2016). In particular, women are underrepresented in cybersecurity professions, with only 14% female representation in North America (Sullivan, 2017). New techniques for recruiting women and other potential professionals into the field are desperately needed.

2.2 Existing Cybersecurity Education Techniques are Not Sufficient

Cybersecurity competitions have been used prevalently in cybersecurity education. Competitions provide both hands-on experience and entertainment through a game-based learning approach (Katsantonis, Fouliras, & Mavridis, 2017). Cybersecurity competitions are highly engaging in nature and seem to attract the type of student that is already interested in

cybersecurity (Cheung, Cohen, Lo, Elia, & Carrillo-Marquez, 2012). They are also useful in reinforcing the interests and skills of participants who already have high proficiency for their level (Mirkovic, Tabor, Woo, & Pusey, 2015). Many cybersecurity competitions exist today. Here are two notable examples:

Capture the Flag (CTF) is a type of competition that is used prevalently in the field. CTFs generally have questions or puzzles separated into multiple categories found in the cybersecurity field ranging from web vulnerabilities, reverse engineering, to cryptography and digital forensics. Individuals or teams try to solve these puzzles and earn points that are shown on a leaderboard. picoCTF is one such competition that has been held yearly and is targeted at middle and high school students (https://picoctf.com/).

Another program is the Collegiate Cyber Defense Competition (CCDC). CCDC provides institutions with cybersecurity curriculum and allows for competitive simulations to assess students' understanding and operational competency in managing networks and systems (https://www.nationalccdc.org/). CCDC events allow for student teams to assume the administrative and protective duties of an existing network. Students travel to the event generally having trained in the specific role they will be performing. CCDC is a one-time event that is played out live that incorporates a basic narrative for a storyline. A team of trained individuals form a red team to provide a tangible external threat and perform cyberattacks on student-controlled networks and computers. This competition allows for students to gain real world experience within a controlled system.

These and other cybersecurity competitions can be useful educational experiences for the right student. Unfortunately, they are not as useful in teaching new concepts or recruiting prospective students into the cybersecurity profession. Competitions can be demoralizing to

some participants who are not as competitive (especially female participants); additionally, they can lower self-efficacy for those are not as proficient in the skills used (Cheung et al., 2012; Mirkovic et al., 2015). Cybersecurity competitions can also be less authentic as simulations because of the competitive nature involved, and they are difficult to use in a classroom setting. Alternatives to competitions are needed that are appealing to a wider audience, fit well in a classroom setting, and are more authentic to workplace contexts.

2.3 Education Simulations are a Promising Solution

Simulations have been proven to be a powerful tool for learning, gaining experience, and building problem solving skills (White & Ingalls, 2016). Simulations allow participants to perform experiments based on models. These models mimic some form of system and allow for the behavior of the participants to be observed without incurring real-world consequences. These types of simulations can model important aspects in the chosen topic while also including the context that might otherwise be difficult to include (Gredler, 1996). Within cybersecurity, simulations can include the full context in which cybersecurity scenarios exist instead of an abstract puzzle that participants must figure out with little foundation to base their decisions on.

Educational simulations place participants into authentic scenarios where they can learn knowledge, skills, and dispositions within a workplace context (Gredler, 2004). Because students feel that they are in an authentic and realistic scenario when they participate in simulations, they can better make connections between those skills, knowledge, and dispositions. Simulations can also help students make a connection between "knowing and doing" (Shaffer, 2005; Bonsignore, Moulder, Neustaedter, Hansen, Kraus, & Druin, 2014). Metacognitive and soft skills are best taught through "experiential learning" where learning occurs through the process of applying knowledge and conceptual understanding to real-world problems (Kolb, 2014). Through

simulations, participants are able to learn through discovery from their own actions and gain experiences that would be difficult to obtain through other mediums of education.

Epistemic games, which are simulated game experiences on computers, have been shown to help students deal more effectively with situations outside of their learning environment (Shaffer, 2005). Within simulated game experiences, students have a safe environment to try things out and learn from their mistakes. Students can also be observed and taught during and after the simulation. One example of an epistemic game is virtual internships. A virtual internship is a method for students to have an authentic experience within a simulated but realistic workplace. Virtual internships allow educators to mentor students within a collaborative environment as well as provide an introductory-level experience. This has been shown to increase students' interest within STEM majors (Chesler, Ruis, Collier, Swiecki, Arastoopour, & Shaffer, 2014). One example of a virtual internship is named Nephrotex. In Nephrotex, students intern at a fictional company that designs and manufactures "ultrafiltration membranes for the hemodialysis machinery used to treat end-stage renal failure" (Chesler et al., 2014). Although examples of virtual internships exist, there are opportunities to further develop and test new types of epistemic games.

2.4 Playable Case Studies are Ideal for Cybersecurity Education

A playable case study (PCS) is a new form of epistemic game and experiential simulation. It incorporates an immersive storyline with aspects of alternate reality games to increase realism and student learning (Balzotti, Hansen, Ebeling, & Fine., 2017). A PCS can help students learn the skills, knowledge, and dispositions pertinent to a particular profession. So far, only one has been created and it focused on technical writing (Balzotti et al., 2017). However, the approach is

general and can be applied to many domains, such as cybersecurity – the focus of the Cybermatics PCS discussed in this thesis.

Playable case studies allow students to perform the role of a professional without having the necessary expertise in a similar way to virtual internships (Chesler et al., 2014). Specific skills, knowledge, and dispositions relative to a desired learning outcome can be applied in a PCS ensuring that the PCS is justifiable from an educational perspective. Playable case studies use a philosophy used in traditional alternate reality games called This is Not a Game (TINAG) (Flushman, Gondree, & Peterson, 2015). The TINAG philosophy dictates that all aspects of the simulation are included as part of the game world itself, ensuring a realistic and authentic player experience. Because of these key features, a PCS is a good fit for the educational field of cybersecurity.

2.5 What Influences a Prospective Cybersecurity Professional

Several factors may influence the careers that students choose to pursue. A student's perceived efficacy (i.e., how well they think they can do at a job) is a key determinant in their preferred career (Bandura, Barbaranelli, Caprara, & Pastorelli, 2001). So, creating interventions that can improve students' cybersecurity self-efficacy should increase their likelihood of going into a cybersecurity career.

Motivation is an important factor in student engagement. Studies have shown that interventions that help build this motivation as well as confidence (i.e., self-efficacy), and help students professionally identify themselves within a STEM field, are needed to increase persistence in STEM majors (Graham, Frederick, Byars-Winston, Hunter, & Handelsman 2013). Unfortunately, the majority of high school students never hear about cybersecurity as a career option from teachers, mentors, or career counselors (Raytheon, 2016). More cybersecurity

education options such as the ones described in this chapter will help a greater number of students understand that cybersecurity could be a career option for them.

3 METHODOLOGY

3.1 Development Process

To create this playable case study, we employed robust design methodology to ensure that it was (a) authentic, (b) engaging/fun, and (c) immersive. To ensure authenticity, we interviewed cybersecurity experts, completed a literature review of the subject, and made sure the interface and narrative match the most important aspects of the job. To ensure that it was engaging/fun, we created characters and organizations that gave a real-life feel to the simulation and used best-practices from creative writing to introduce a plot that players influence through their contributions. To ensure that it was immersive, we created a portal that acts as the entry way for the participants to interact with the simulation. It includes features such as chat, documentation, videos from the characters, a Linux terminal emulator, and other ways to interact with the simulation. We also worked as an interdisciplinary team to bring perspectives from the Creative Writing and Information Technology departments. We ran the simulation with a class of undergraduate students in IT 101 in Fall 2017. This was our first full test of the completed simulation. The plan is to improve Cybermatics based on the findings from this study. The Cybermatics playable case is described in detail in Chapter 4.

3.2 Evaluation Data Collection

To address the research questions, we conducted a formal evaluation of the simulation with the students in IT 101. We worked with the Institutional Review Board (IRB) to create an ethical protocol that was followed, including collection of consent forms from students willing to participate in the study. A mixed-method approach was used in order to gain both quantitative and qualitative insights. Data was collected using multiple sources including pre- and post-surveys, classroom observations, interviews with selected students, log files, and in-game assignment submissions.

3.2.1 Survey Design

Students completed the pre-survey approximately a week before they began the simulation itself. The pre-survey asked participants about their prior experience with cybersecurity, interest in cybersecurity and related careers, understanding of the profession, demographic information, and questions that assessed their confidence in their ability to perform certain cybersecurity-related activities. It included both closed- and open-ended questions. The complete pre-survey is available in Appendix A.

After the simulation, we conducted a post-survey with all participants to measure changes in their knowledge, skills, and dispositions based on the pre-survey they took. The post-survey was available immediately after completing the simulation, and participants had up to a week to complete it. It asked some of the same questions as the pre-survey, including interest in cybersecurity and related careers, understanding of the profession, and confidence in their ability to perform certain cybersecurity-related activities. It also included questions about what they liked and disliked about Cybermatics, as well as how their perceptions about cybersecurity had changed

after completing the simulation. The pre- and post-surveys also measured changes in self-efficacy, understanding of cybersecurity careers, and interest in pursuing a career in cybersecurity.

3.2.2 Classroom Observations and Interviews

Two undergraduate researchers and I observed the classroom instruction and discussed our observations, which were similar. I interviewed three participants after they completed the simulation. These students were sampled based on their survey responses as I wanted to obtain qualitative perspectives on those students who were most impacted by the PCS and those students who were least affected. I took detailed notes during the interviews. Interviews included questions about which parts of the simulation were their favorite, which parts could be improved, which day of the simulation did they learn the most, which principles in the simulation did they like the most, which principles could have been explained better, as well as questions on simulation features and if the simulation felt real.

3.2.3 Log Files and In-Game Assignment Submissions

The portal to the simulation also collected analytics on how they interacted with the simulation. This data was analyzed after the simulation to better understand gameplay. Every chat message that students sent in the chat was saved and we analyzed the number as well as the quality of the messages. At the end of each simulation day, students completed a written submission of what was accomplished during the day. In order to progress within the simulation, students were required to complete daily tasks. Finally, the students completed a summative penetration test report on the last day of the simulation. This report detailed the penetration test findings, vulnerabilities, as well as the information found on the client's server.

3.3 Evaluation Data Analysis

We evaluated the data collected using both qualitative and quantitative analysis as described below.

3.3.1 Statistical Analysis of Pre- and Post-Survey

Paired t-tests were used to compare closed-ended questions from the pre- and post-surveys. We corrected for covariates (gender, year of college, day 5 report completion, number of reports, and number of chats) in our analysis of covariance model. However, none of the covariate variables showed significant results, so a standard paired t-test was used. Results and p-values are presented in Chapter 5.

3.3.2 Coding of Qualitative Data

Qualitative data from open-ended survey questions was coded into themes that emerged from the data. A grounded-theory approach was used, wherein a team of three researchers independently coded and discussed emergent themes. A codebook was developed and iteratively improved based on preliminary coding agreement and discussion with all three coders. Once agreement seemed high enough, two people independently coded each comment into non-mutually exclusive themes. Inter-rater reliability was calculated using Cohen's Kappa. One theme ("Interactive" post-survey) was 0.72, two were 0.81 ("Knowledgeable" post-survey) and 0.87 ("Knowledgeable" pre-survey), and the rest were above 0.9. Scores above 0.8 are typically considered excellent. Since all but one of our scores were above that point, they were determined to be sufficiently high. In Chapter 5 when we report total numbers in each category, we include any message coded by either coder that included the theme. This is more inclusive, and it helps ensure that we did not miss comments that included relevant information for the theme.

4 CYBERMATICS

This chapter describes the playable case study itself: its characters, its storyline, as well as the portal used to access the simulation. The main features used within the portal are also laid out in this chapter.

4.1 Educational Goals

Our primary goal was to help novices gain a better understanding of the job and skills needed to be a professional penetration tester. We accomplished this by defining the learning outcomes for each simulated day as listed below.

Learning Outcomes:

Day 1:

Knowledge

a) Understand what a scope document is and why it's important to ethical hacking
b) Understand the purpose of a penetration test

Skills

a) Use the group chat functionality as part of a team

Disposition

a) Have an ethical mindset

Day 2:

Knowledge

a) Understand what a database and SQL
b) Understand what SQL injections is and how to perform it

Skills

a) Perform a SQL injection to progressively uncover information

Disposition

a) Think like a hacker (e.g., break, test, persistence)

Day 3:

Knowledge

a) Understand password security

b) Understand how passwords are hashed and stored

Skills

a) Perform password cracking

Disposition

a) Have a defensive mindset

Day 4:

Knowledge

a) Understand the Linux file structure and how to navigate through it

b) Understand how hidden files work and how to find them

Skills

a) Perform tasks using Linux terminal including navigation

Disposition

a) Learn to keep digging

Day 5:

Knowledge

a) Understand role of law enforcement

b) Understand what a penetration testing summary report is

Skills

a) Draft sections of a penetration testing summary report

Disposition

a) Document everything

4.2 Simulation Properties

The simulation has a number of properties that allow it to be a useful educational experience for the participants. It is based in part on some real-world events and incorporates real-world vulnerabilities as well as resolutions. The simulation revolves around a penetration testing company and the organization that is being pentested. The organization allows its networks to be available for the participants to use. The network and the computers on the network are set up in a way that mimics what an organization would use, but they are simplified to help novices better understand. Students are able to access this network in the same way that it would be accessed by the organization. The simulation is set up in a way that will make it easy to duplicate and reset for multiple simulations.

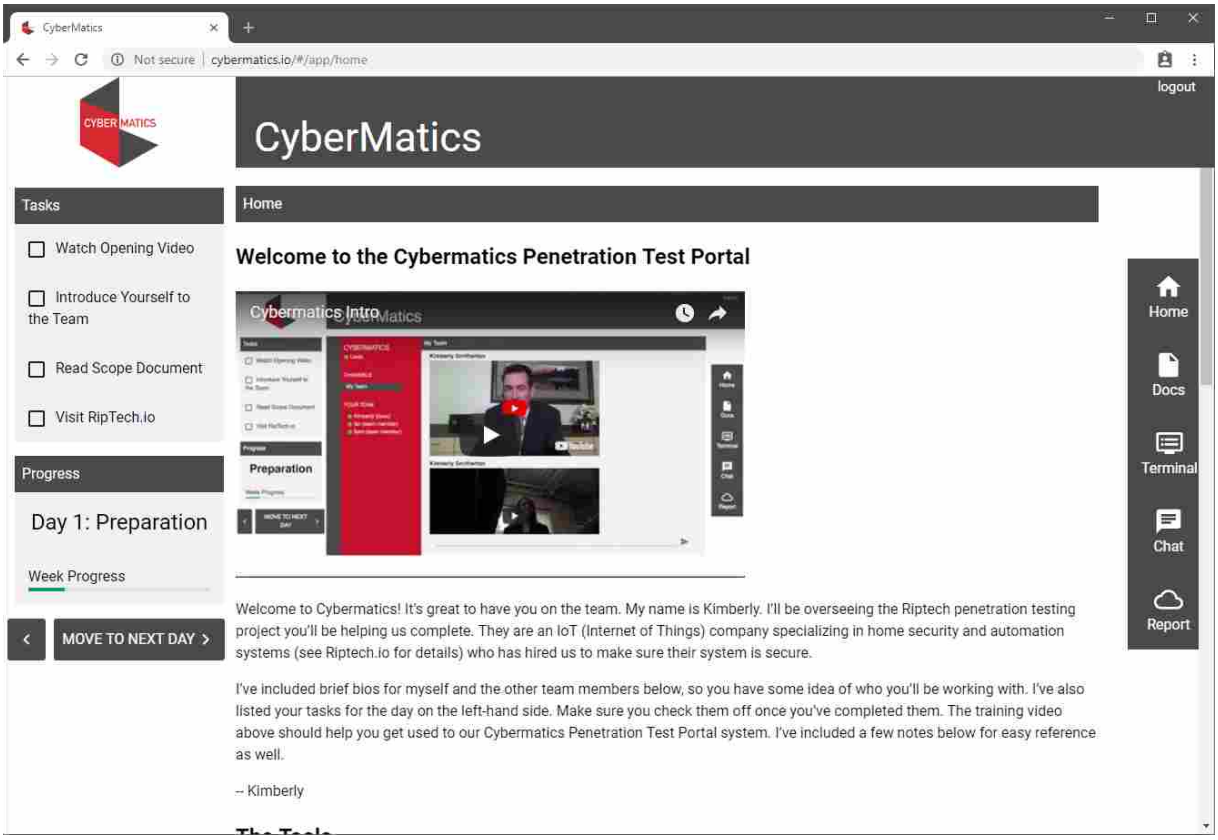

Figure 4.2.1: Simulation Portal

4.2.1 Real-World Features

We filmed several videos with actors playing the parts of the participant's teammates, boss, and the bad actor. These videos help progress the storyline as well as give tips to the participants on various leads to pursue. The videos are coupled with a chat functionality that mimics real-time chatting with team members. It does this using pre-written messages that are triggered based on specific progress within the simulation as well as on trigger words that the participant is instructed to use. There is also a Linux terminal emulator that allows participants to perform tasks in the same manner that they would using real systems. These features are available to the participants to give a sense of realism to the simulation and they are described in more detail below.

4.2.2 Technical Documentation

Documentation is available to participants to teach them how to use various tools and methodologies, and to advance them within the simulation. There are also hints from third parties, such as their boss, given to participants at specific times during the simulation to help them if they are struggling. Also, participants are given concrete tasks to accomplish during the simulation - from finding suspicious accounts or behaviors to writing reports about their daily progress. At the end of the simulation, participants complete a technical report on their findings.

4.3 Simulation Portal

In order to accomplish the educational goals listed in Section 4.1, we designed and implemented a portal to be used by participants while completing the simulation. It was introduced to the students by their simulated team leader named Kimberly. This is her introduction:

Welcome to Cybermatics! It's great to have you on the team. My name is Kimberly. I'll be overseeing the RipTech penetration testing project you'll be helping us complete. They are an IoT (Internet of Things) company specializing in home security and automation systems (see RipTech.io for details) who has hired us to make sure their system is secure.

I've included brief bios for myself and the other team members below, so you have some idea of who you'll be working with. I've also listed your tasks for the day on the left-hand side. Make sure you check them off once you've completed them. The training video above should help you get used to our Cybermatics Penetration Test Portal system. I've included a few notes below for easy reference as well. - Kimberly

The portal was designed with simplicity in mind as well as ease of use. The portal is shown in Figure 4.2.1. On the left-hand sidebar, the daily tasks are listed. The tasks help students understand what needs to be done in order to progress throughout the simulation and can be checked off when completed. Once all the daily tasks for a certain day are completed, the simulation can be advanced by pressing the 'Move to next day' button. On the right-hand sidebar, a menu is presented that gives access to the simulation features. These features include the home page, the documentation, the Linux terminal, the chat, and the report page. These pages can be accessed regardless of which day it is in the simulation, but certain tasks are completed on certain pages. A video is provided on the home page to help participants understand how to use the simulation portal. The dialog is written in the voice of a Human Relations employee. Also included on the home page is the welcome message by Kimberly shown above, as well as a description of the other characters that students encounter within the simulation. All the simulated characters that students interact with are described in Section 4.4.

4.4 Characters

Students interact with four main characters within the simulation. Three of them are on their penetration test team with them (the Cybermatics team), with the other being the CEO of the company (RipTech) that they are penetration testing. The Cybermatics team interacts with the students in the chat based on which simulation day they are on as well as responds to messages that the students type. All four characters also appear in videos portrayed by actors that are placed in the participants' chat as they progress within the simulation. The following are the character bios that students are given on the first day.

4.4.1 The Cybermatics Team

The following fictional character bios are found on the site. These were designed to make sure the characters have a personality and seem real. Some attempt at humor is also included.

Kimberly

The team lead. From South Carolina. Spent five years at Microsoft and ten years in cybersecurity, both as a freelancer and working for Cybermatics. Proud member of the women's chapter of Association of Computing Machinery (ACM) for the past twenty years. Married to a wonderful man. Mother of three teenage boys. Hobbies include reading, playing soccer, and taking naps when her children give her the chance. Her motto? "If you don't have time to do it right, then you don't have time to do it over."

Ian

A native of Bangor, Maine, Ian has been with Cybermatics for four years. Ian has always been interested in computers; to family and friends he is known as the "Ian the Incredible" for fixing broken phones and cracking old Facebook passwords. He attended MIT, where he

managed a 3.9 GPA while maintaining no social life whatsoever. In his spare time, Ian likes winning hacking competitions and trying to complete Zelda: Breath of the Wild.

Sam

Raised by feral wolves, Samuel McCarthy has taken to heart a simple truth he learned in his youth: “If the squirrel is still moving, don’t eat it yet.” Sam attained a full ride to UC Berkeley for his bachelor’s and Stanford for his master’s degree. He is responsible for saving at least 200 orphans from 12 burning buildings within the past four years. Sam likes fishing, hiking, and watching Netflix for twelve hours without stopping. At night, he likes to dress up in tights and pretend he’s Spiderman, working through vigilante justice through his determination to keep his city safe. Sam’s greatest goal in life is to personally ride in a helicopter with Chris Pratt, holding a crystal ball in one hand and a live armadillo in the other. He already has the armadillo.

4.4.1 RipTech

Jomel Panoga

Jomel heads RipTech as President and CEO. He recently finished an MBA after returning to school at the age of 47. His work at RipTech is informed by a long career with Microsoft, which he left six months ago in order to work closer to where his three children go to school and fulfill his dream of owning his own business.

4.5 Storyline

The simulation is divided into five simulated days. Each day has specific tasks that need to be completed before the student can progress to the next day. The daily tasks build upon each other throughout the simulation. The characters are programmed to help the participants with

their daily tasks through chats and videos. They act as if the student is part of their team and they start the penetration test with the student as a new team member.

The student's actions help influence the outcomes and the characters play off what the student finds when they type in the chat. For example, the student is asked to break into a website using SQL injection. The student's teammates guide the student through the encounter and give progressively harder tasks as the student finds more and more information in the database. The student types what they find into the chat and the characters react to it.

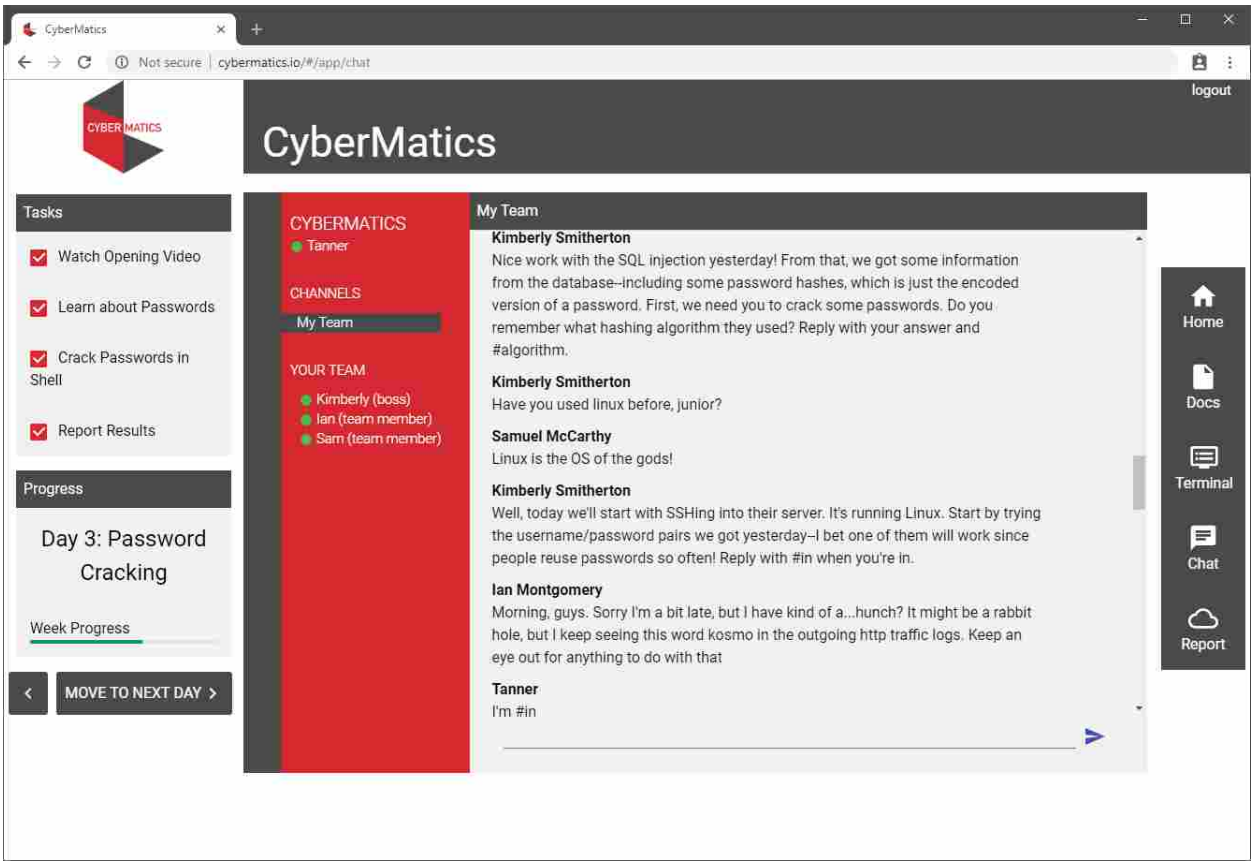

Figure 4.5.1: Day Three Chat

The general storyline starts with the student being introduced to RipTech. They are introduced to the various characters and learn a little of what they will be doing within the simulation. The following day they are given the assignment to investigate the RipTech site and eventually break into it. They do so by performing SQL injection on the login form. They eventually obtain the usernames and hashed passwords of the RipTech users.

The next day students are tasked with cracking the passwords they gathered on day two. They do this using the emulated Linux terminal in the simulation portal. After cracking the passwords, they find that a few of the credentials give them access to the backend RipTech server using SSH. On the fourth day, they learn how to use the Linux terminal and search through the server for any evidence they can find. They eventually find a hidden file that is a backdoor to the server placed by the bad actor, Kosmo. They then work with their team to use their gathered clues to determine the identity of Kosmo. On the last day of the simulation, the Cybermatics team finds the real Kosmo and she is arrested. The students finish the simulation by writing a final report of their findings and recommendations.

4.6 Features

4.6.1 Real-Time Chat

The chat feature is one of the key aspects of the simulation. It is the driver behind the simulation narrative. It helps students know what needs to be done to complete their daily tasks and guides students when they were lost. There are pre-programmed chats for each of the characters that students interact with throughout the simulation. These chats are triggered by events such as progressing to the next day. There are also chats that are programmed to wait for a specific message from the participant. These specific messages are marked with a '#' by the

student. For example, on Day 3 Kimberly introduces the day's objectives and asks the student to reply with '#in' when they are ready to begin. The student can then reply with a message that includes '#in' and an appropriate message will be triggered. This is demonstrated in Figure 4.5.1. Another example with the trigger '#greetings' which is the first message the student types is shown in Figure 4.6.1.

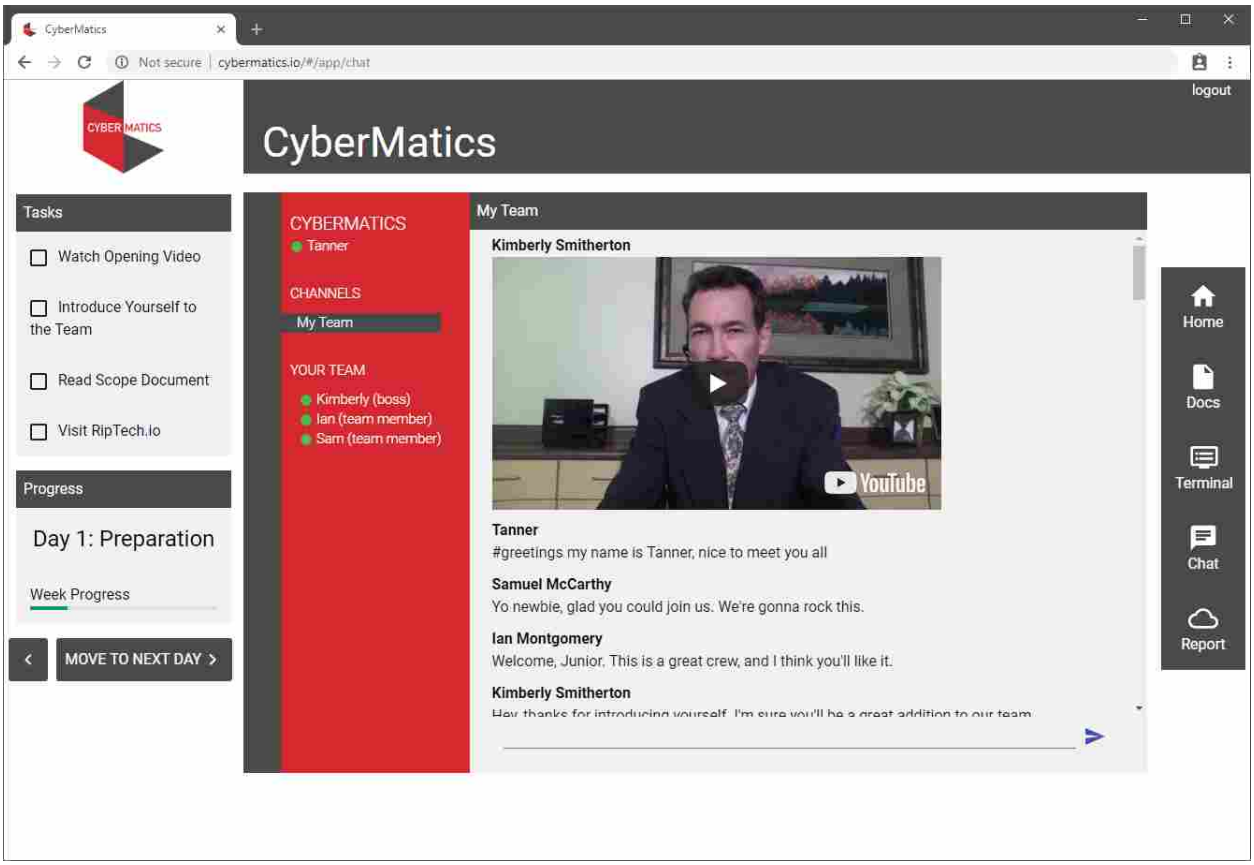

Figure 4.6.1: Screenshot of Chat

The chat functionality is introduced to the participants with this paragraph: Communication with your team is extremely important during a penetration test. Make sure to check the chat regularly. We tend to share our progress via chat and expect you to do the same.

You can start things off by introducing yourself using #greetings in your message. BTW, we've been having some technical difficulties with the chat lately. If nothing is showing up, please just refresh the page and it should appear.

4.6.2 Linux Terminal

A Linux terminal emulator is included in the simulation portal and is a key tool for participants to complete their daily tasks. It emulates many terminal commands and has a full file structure for students to familiarize themselves with. Some of these commands are shown in Figure 4.6.2.

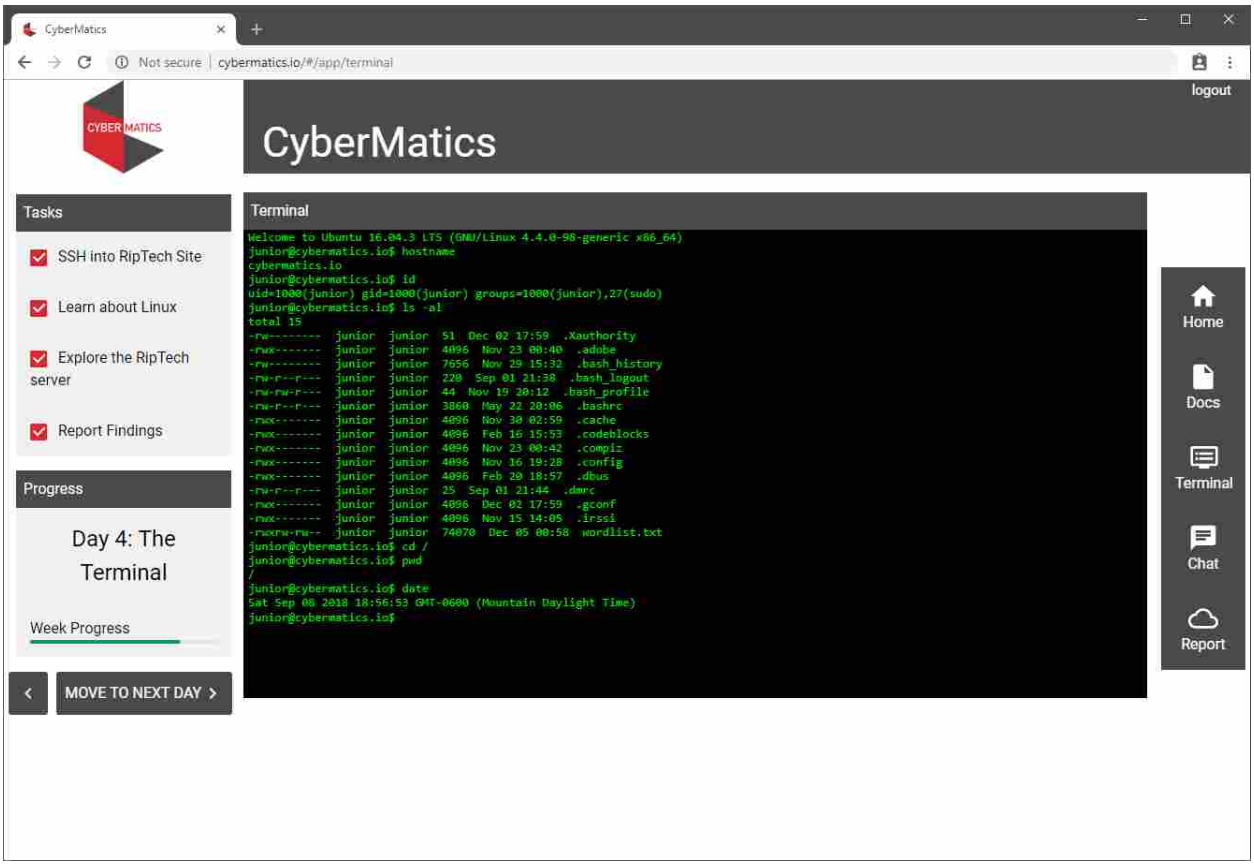

Figure 4.6.2: Linux Terminal Emulator

The terminal includes a password-cracking program that students need to learn and use to complete their password-cracking task on day three of the simulation. Students also employ the terminal when they login via SSH to the RipTech backend server with the credentials they gathered from the RipTech website via SQL injection.

The Linux terminal is introduced to the students with this paragraph: The terminal is your entryway to the computer you will use to perform some important tasks such as cracking passwords or remoting into another computer (e.g., RipTech's server). It does not have a graphical interface like you may be used to but learning to use the Linux command line will be invaluable during your cybersecurity career.

4.6.3 Documentation

We designed the documentation to be the first place students look for information when they are lost or want to know more. It includes information pertinent to every task that students encounter throughout the simulation. We also wanted to familiarize students with how documentation is generally structured in the technical world, so we designed our documentation in a similar fashion. A screenshot of the documentation is shown at Figure 4.6.3.

The documentation is introduced to the students with this paragraph: Our internal documentation includes tips on how to perform various penetration testing tasks, as well as overview information on the Scope Document, etc. If you're ever stuck, make sure you check the docs. BTW, opening them in another tab (see link at the top) makes for much easier reading.

The first section of the documentation starts with these paragraphs:

Welcome to the Cybermatics documentation page. In the real world, companies use the practice of documentation to ensure that when new people come aboard they can jump right in and figure out how the company chooses to program their structure. This page should be a

resource you turn to as you figure out the techniques you need to learn to accomplish your daily tasks. Happy hacking! Make sure to read this documentation as thoroughly as possible, as the difficult challenges you encounter will be discussed within these pages.

This documentation is organized into activities, with specific terminology and instructions associated with each activity. If you're having trouble during a specific task, reference this documentation by visiting the activity's section and reviewing it.

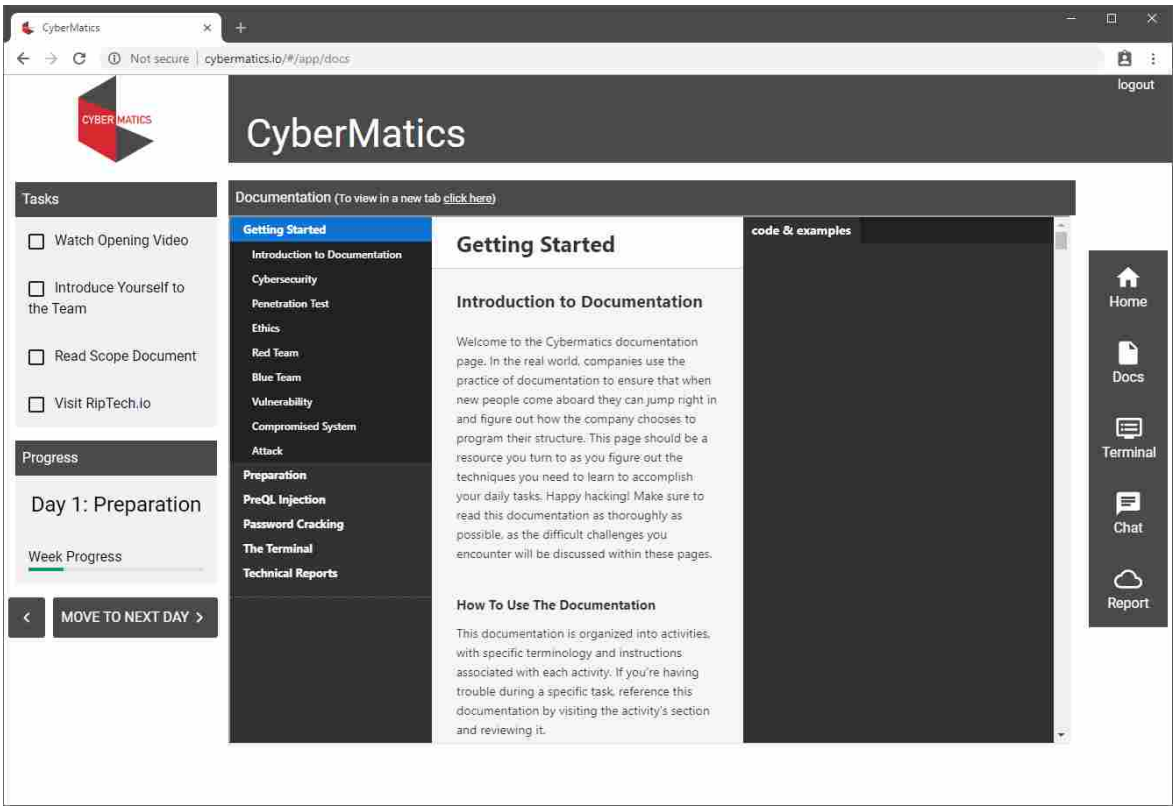

Figure 4.6.3: The Documentation

The documentation is organized to coincide with simulation tasks. It begins with an introduction to cybersecurity and covers general topics that might be of interest to someone beginning to learn about cybersecurity. This includes subjects such as the definition of a

penetration test, what red and blue teams are, as well as the scope document. Following that, there is information about SQL databases, structured query language, and how SQL injection works. This coincides with the tasks that participants complete on day two of the simulation. After that section is the password-cracking section. This is helpful to students on day three of the simulation and includes information on password security and how password hashing works. The next section deals with the Linux terminal. It shows various important files as well as useful commands to know. The last section in the documentation gives a description of technical reports and has links to real penetration test reports.

4.6.1 Reporting

At the end of most days, the last task students complete is to report what they did during that simulated day. This is shown in Figure 4.6.4. On the last day of the simulation, the students complete a Penetration Test Final Report. Some of the final report is already 'completed' by the simulated teammates, but the students are required to fill in sections such as what they did during the SQL injection and what they found on the RipTech server. The final report is shown in Figure 4.6.5. The reporting is introduced to the students with this paragraph: A penetration test is useless without good reporting. Every day you will need to go to the report page and describe what you did during that day. On the last day, you will add sections about what you did to our Penetration Testing Report for RipTech. I'll write the introduction and conclusion sections, but we'll expect you to professionally summarize your activities and findings in the appropriate sections of the document.

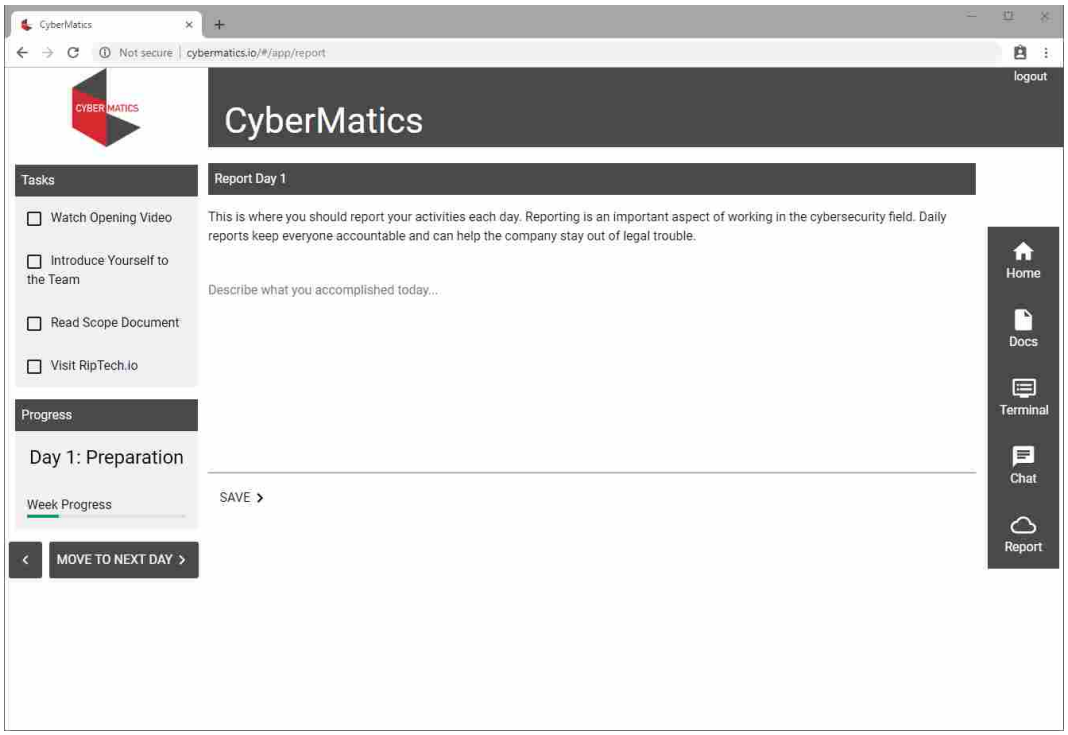

Figure 4.6.4: Daily Report

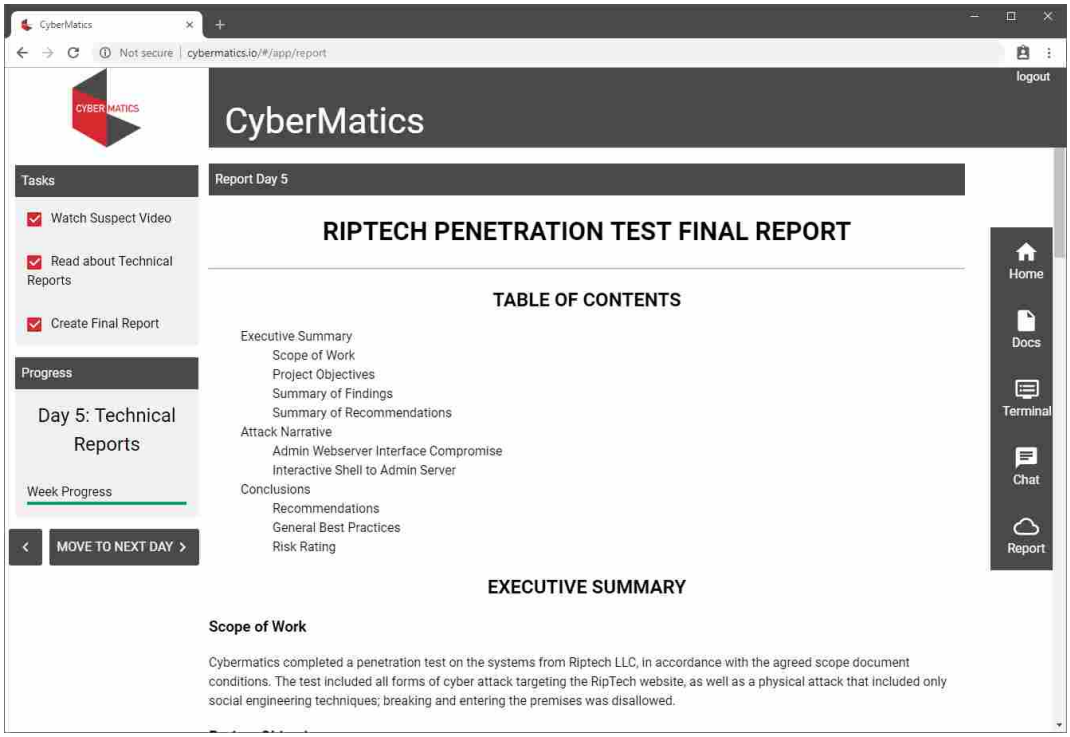

Figure 4.6.5: Final Report

4.6.2 RipTech Website/SQL Injection

We also created a website to represent the company that the Cybermatics team would pentest. This company is named RipTech. RipTech.io was registered and we developed a website that describes the company and provides a login page that the participants can attack with SQL injection. A screenshot of the RipTech.io website is shown in Figure 4.6.6.

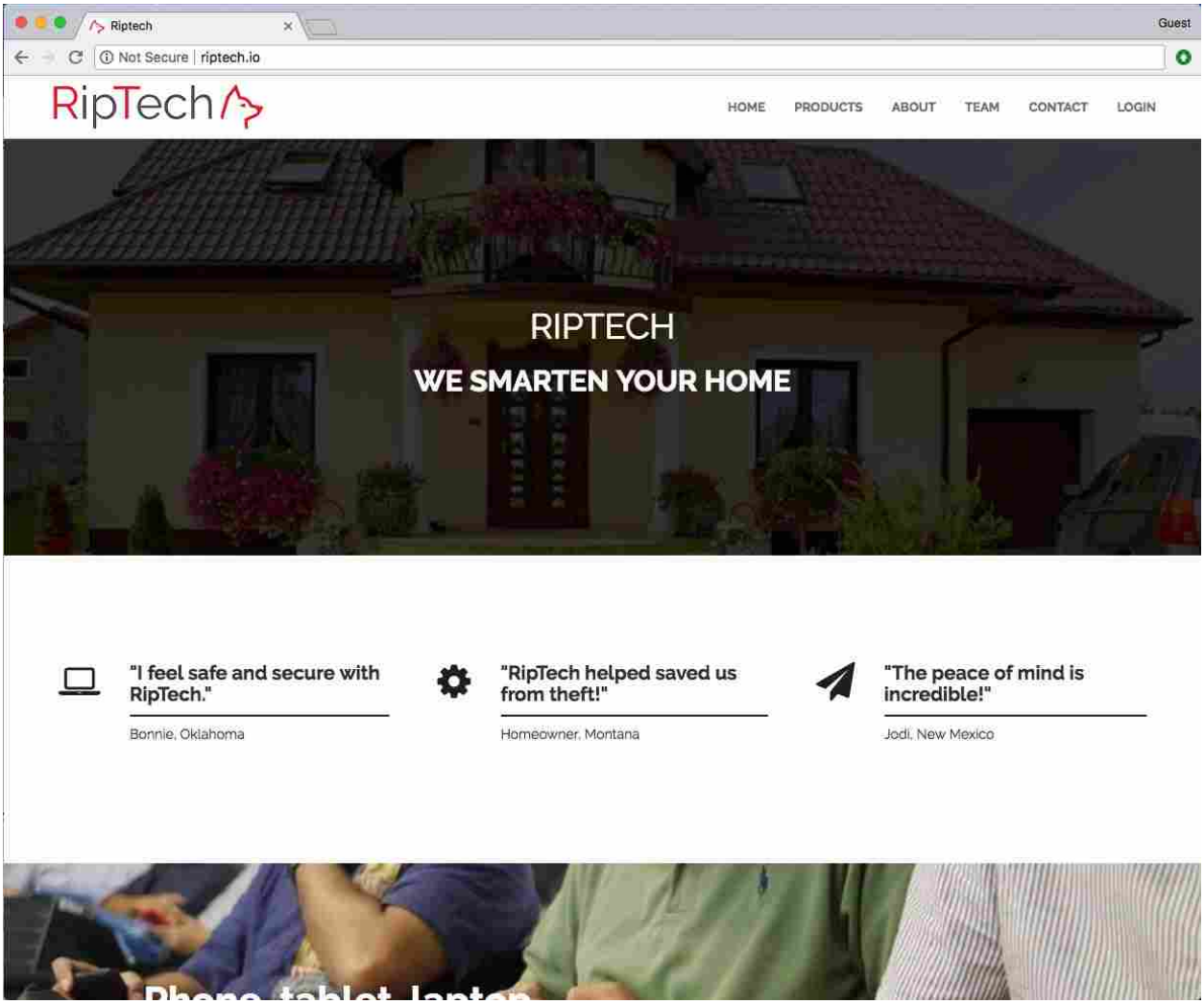

Figure 4.6.6: RipTech Website

The login page for the RipTech website is vulnerable to SQL injection. We do not include an actual database behind the login page, but instead have logic that is hard coded to the different attacks that students use. These attacks are shown to the students in the documentation with some attacks being slightly off from the examples. If one of these hard coded attacks is used, a hard coded response is issued and the student is able to progress with the SQL injection attack. One example of an attack used is shown in Figure 4.6.7.

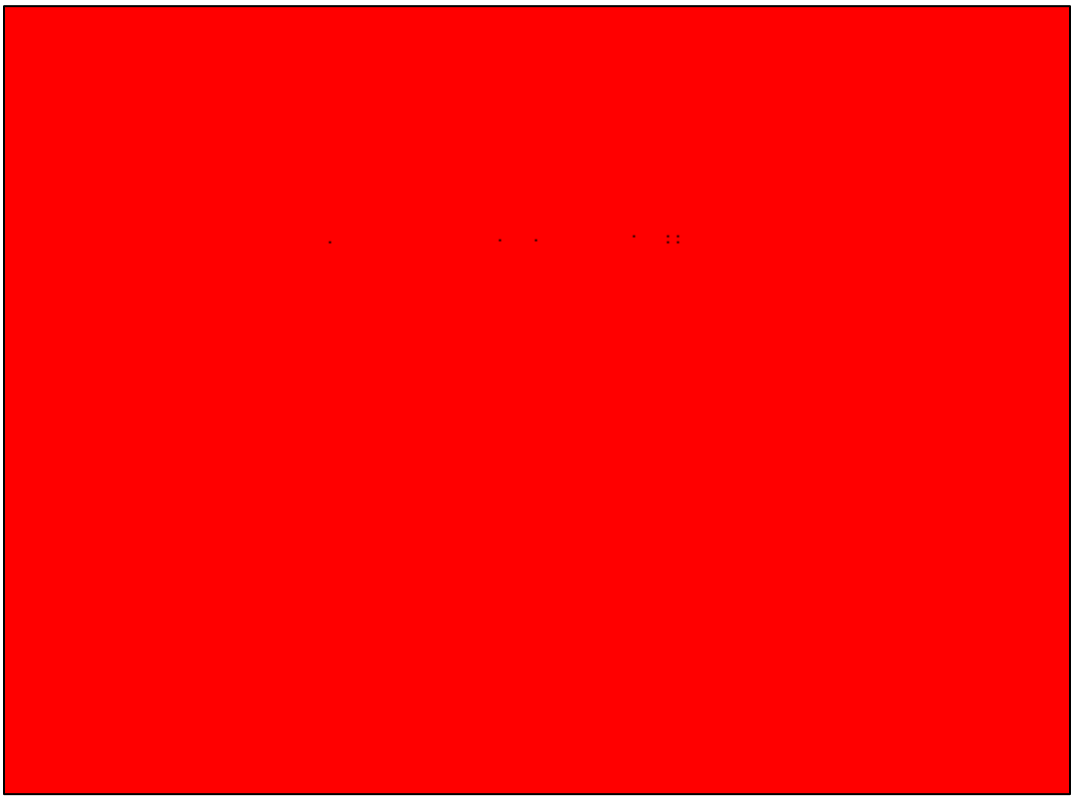

Figure 4.6.7: RipTech Login with SQL Injection

5 FINDINGS

5.1 Survey Overview

A total of 64 students were enrolled in a class, of those 51 (80%) participated in the complete research study including completing both the pre- and post-surveys and the simulation. There were 10 students who completed the post-survey but not the pre-survey. We did our analysis on the 51 that completed both surveys. 43 (74%) of the 51 participants were male, and 8 (16%) of the participants were female. This is consistent with overall enrollments in the IT major. All students were within the 18-28 age range, with one exception who was over 40. Table 5.1.1 shows the year at BYU based on number of earned credits. All students were in an introduction-level class suggesting that they are new to the field of cybersecurity.

Table 5.1.1: Distribution of Participants by Year at BYU Based on Credits

College Year	Amount
# of Freshman	16
# of Sophomore	16
# of Junior	14
# of Senior	5

5.2 Research Question #1

In this section we address the first research question: How does a playable case study affect students' a) likelihood of going into a cybersecurity career, b) intention to continue learning about cybersecurity, and c) confidence in their ability to succeed in a cybersecurity job? How do these correlate with each other?

Table 5.2.1: Pre- and Post-Survey Comparison of Interest, Career Intent, and Confidence

On a scale of 1 to 5, rate your agreement with the following statements:	Pre-survey	Post-survey	Mean	P value
I am interested in cybersecurity	4.29	3.98	-0.31	0.0049
I plan on pursuing a career in cybersecurity	3.31	3.33	0.02	0.8496
I feel confident in my ability to succeed in the cybersecurity field	3.33	3.47	0.14	0.1965

Table 5.2.1 shows the pre- and post-survey results for three high level questions related to interest, career intent, and confidence to be able to succeed in cybersecurity. Surprisingly, interest in cybersecurity dropped. This difference was statistically significant at a 0.05 confidence level. We did a post-hoc analysis on this afterwards which revealed that the likely cause of this was that the pre-survey values were so high, that there was not much room to go higher. The other two were not statistically different. Measuring the impact through a pre- and post-survey may not be very effective in assessing changes in these high-level questions.

Table 5.2.2: Post-Survey Self-Assessment of Simulation Impact

	Yes	No
I intend to continue learning about the topics presented in the simulation	80% (41)	20% (10)
This simulation made me more likely to pursue a career in cybersecurity	73% (37)	27% (14)
The simulation made me more confident in my ability to succeed in a cybersecurity career	76% (39)	24% (12)
I was able to complete the tasks in the simulation effectively	73% (37)	27% (14)

In contrast to the pre- and post-survey comparison results discussed above, students self-reported that the simulation increased their intention to continue learning about cybersecurity, likelihood to pursue a career in cybersecurity, and confidence in their ability to succeed in cybersecurity. These questions were posted as yes/no responses in the post-survey which forced participants to take a position one way or another. They do not measure the size of the impact.

Table 5.2.3: Correlation Between Post-Survey Self-Assessment of Simulation Impact

	Continue Learning	Career	Confident	Complete Tasks
Continue Learning				
Career Intent	69%			
Confidence	31%	59%		
Effective Task Completion	25%	31%	28%	

Table 5.2.3 shows the correlation between the four questions shown in Table 5.2.2. As expected, all correlations between the questions were positive. In other words, those who said

they were able to complete the tasks effectively also said the simulation made them want to continue learning, have a higher likelihood of pursuing a career, and more confident in their skills. Similarly, those who said they did not complete the tasks effectively showed lower scores for the other questions. It is interesting to note how those who felt the simulation made them more likely to pursue a career in cybersecurity also believed it increased their confidence and their desire to continue learning.

Although we did not ask open-ended questions about these specific topics, students did mention related ideas when answering other questions such as, 'How have your perceptions about cybersecurity changed after completing the simulation?' One of the themes mentioned by students was a feeling that cybersecurity was no longer as difficult as previously thought (improved confidence). They often mentioned this with a change in career intent. For example, "cybersecurity is an option now as opposed to before where I thought it would be completely over my head." And, "after being part of this simulation, [it] seems like cybersecurity is something I could do ... and [I am] more likely to go into cybersecurity as a professional." Another mentioned the effectiveness of the simulation itself in cybersecurity education: "I learned a lot about cybersecurity from doing this simulation and I feel like it could definitely be used to teach others about cybersecurity."

5.3 Research Question #2

In this section we address the second research question: Did the simulation change students' understanding of the cybersecurity profession? How did their understanding change?

Table 5.3.1: Pre- and Post-Survey Comparison of Cybersecurity Skills

On a scale of 1 to 5, how important that someone working in cybersecurity would need the following skills to be successful?	Pre-survey	Post-survey	Mean	P value
Leadership skills	4.00	4.24	0.24	0.0325
Ethics	4.45	4.69	0.24	0.0270
Critical thinking	4.88	4.80	-0.08	0.2895
Communication skills	4.55	4.55	0	1
Adaptability	4.78	4.73	-0.05	0.5369
Ability to think outside the box	4.80	4.78	-0.02	0.8211
Problem solving skills	4.92	4.82	-0.10	0.1997
Programming skills	4.16	4.12	-0.04	0.7991
Ability to learn continuously	4.75	4.61	-0.14	0.1965

The two most statistically significant findings from this question were the change in views of leadership skills and ethics in a cybersecurity profession. Both findings were statistically significant at a 0.05 confidence level. It is interesting to note that both leadership skills and ethics were not obvious skills for someone working in cybersecurity before the students completed the simulation. This is possibly because the participants might have only heard about cybersecurity without context. During the simulation, they were able to see how cybersecurity professionals worked together as a team and saw how they interacted with others. They also were able to read over documents, such as the scope document, which put limits on what they were allowed to do.

Table 5.3.2: Themes Identified When Coding Question About Change in Perception of Cybersecurity

Codes Used	Total
Understanding	27
No Change	16
Interest	11
Importance	8
Challenge	8
Concern	6

The main theme participants mentioned after completing the simulation was that of understanding. Participants said they understood more about what cybersecurity professionals did, why they do what they do, and what cybersecurity is in general. For example, one student said,

> "Before the simulation, it seemed like the cybersecurity team was just looking for all the bad things and mistakes the company made but now it seems like more of them trying to help the client in every way they can and keep them safe from threats and loss of data. They're not looking to criticize but rather to catch any mistakes before they cause problems."

Referring to the scope document, a student said, "I thought the companies would just allow the teams to do whatever they wanted to break in." Another realized that "there is a lot of communication required between pentest administrators and clients." Another summed up nicely the general change of opinion:

> "Individuals in cybersecurity don't just sit in a bedroom in their pajamas eating day old pizza hacking without any human interaction. Cybersecurity is a team effort and you have to be able to actively learn things that are relevant to the project. Knowing what it means to be ethical and having a diverse skill set are important to be successful."

Some students had a change of opinion when it came to how challenging a career in cybersecurity would be. Some thought that it would be difficult for them to pursue a career in

cybersecurity before completing the simulation, then after completing it, they found that it was a lot less daunting than previously imagined. For example, one student said that "after being a part of this simulation, this seems like cybersecurity is something I could do." Another said that "rather than being some obscure job description, [cybersecurity] has become much more understandable." Others found it more challenging than previously imagined. For example, one student said, "I think that cybersecurity can be a lot more complicated than I thought because… there are probably so many exploits of the system that it's hard to account for or anticipate them all." Another student was excited that it was more challenging: "I find [cybersecurity] harder than what I thought it would be, but I believe that it poses a challenge that I am excited to face."

Table 5.3.3: Pre- and Post-Survey Comparison of Themes Identified When Coding Question About Responsibilities/Skills of a Cybersecurity Professional

Codes Used	Pre-Survey	Post-Survey
Preventative Security	42	28
Communication	4	21
Ethical	2	16
Knowledgeable	13	14
Programming	2	14
Problem Solving	0	14
Creative Thinking	5	10
Reactionary Security	11	7
Stay Informed	6	3
Attention to Detail	1	2

Before completing the simulation, the majority of participants had a limited understanding of the scope of responsibilities that someone in cybersecurity has. The majority described some sort of preventative security as the dominant responsibility of a cybersecurity professional. They described preventive security responsibilities such as “protecting vital data,” “identifying potential risks,” and “keeping files and systems safe.”

While it is true that preventative security is a major function of the cybersecurity professional, they also emphasized other subjects such as being knowledgeable and reactionary security. After they had completed the simulation, their views changed to be a more well-rounded perspective of the cybersecurity field. One student said, “A cybersecurity professional needs to have leadership ability, extensive computer knowledge, critical thinking, and problem-solving.” Another said, “They need to be able to communicate and work well with others and be good about sharing ideas.”

Ethics was not a major theme that most students mentioned before the simulation, yet it was a top theme after the simulation was completed. One student reflected on ethics and pointed out the scope documents saying that cybersecurity professionals “need to be ethical and follow the rules set out in the scope document.” Another said that a cybersecurity professional “has to be able to know what can be done and what should not be done - ethically, and then he has to follow that ethical code that he has developed in order to be trustworthy and professional in his work.” Another realized the importance of ethically using skills that could otherwise be used illegally by stating that cybersecurity professionals “are paid well but if they were to exploit, they would make so much more.” The importance of trust was brought up by a student when they said that professionals need “to be ethical with the information and to have strong morals and character to be trusted with vital information and role.”

5.4 Research Question #3

In this section we address research question 3: Did the simulation change students' confidence in specific cybersecurity-related skills change? How did their confidence change?

Table 5.4.1: Pre- and Post-Survey Comparison of Self-Confidence in Common Security-Related Tasks

On a scale of 1 to 5, rate your agreement with the following statements:	Pre-survey	Post-survey	Mean	P value
I feel confident in my ability to succeed in the cybersecurity field	3.33	3.47	0.14	0.1965
I feel confident browsing the internet without risk of infection	3.84	3.63	-0.21	0.0780
I feel confident that the passwords I use are strong	3.67	3.47	-0.20	0.1147
I feel confident that I won't be hacked	3.16	3.04	-0.12	0.4015
I feel confident using antivirus and other programs to protect my computer's security	3.71	3.45	-0.26	0.0682
I feel confident updating my computer and my programs to keep them secure	4.14	4.20	0.06	0.6266
I feel confident that I can fix my computer if it is infected	3.37	3.61	0.24	0.0766

There were no statistically significant findings at a 0.05 confidence level for this question. However, there were three at a 0.1 confidence level. Participants generally felt less confident in their ability to browse the internet without risk of infection as well as their ability to use antivirus to protect their computer. This is possibly due to a realization that they are more vulnerable

online than they previously imagined. They also generally said that they felt more confident in fixing their computer if it was infected. This could be due to an increased awareness in their personal security.

5.5 Research Question #4

In this section we address research question 4: How do different design features of a playable case study relate to a feeling of realism? What improvements could be made to the simulation?

Table 5.5.1: Post-Survey Rating of Simulation Features

The following simulation features made the simulation feel more realistic	Post-Survey
The RipTech website	4.71
The terminal	4.54
The documentation	4.15
The storyline	4.00
The Cybermatics portal	3.98
The chat	3.88
The character videos	3.44

Students were asked to rate the above-listed simulation features based on realism on a 1- to 5-point scale after completing the simulation. The RipTech website and the terminal were the top features that students said added to the realism of the simulation. Having a real website in RipTech.io that students could browse to as they would any other website seems to have been a tangible factor that students enjoyed. Students also seemed to enjoy being able to have a terminal built in to the simulation portal that they could interact with easily. The videos were the least

realistic of the simulation features. This follows the same results found when asking what could be improved about the simulation where some students stated that the videos felt cheesy and unrealistic.

Table 5.5.2: Themes Identified When Coding Question About What Participants Liked About the Simulation

Codes Used	Total (both)
Realism	35
Interactive	22
Educational	17
Teamwork	7
Helpful	6
Clarity	6
Experience Level	4
Problem Solving	3
Usability	1

When talking about what they liked about the simulation, 35 of the 51 students mentioned some aspect of realism. They almost always described it as feeling realistic. Students described the simulation as “very real,” “realistic”, and “I really liked how it felt like I was actually performing an SQL injection without having me actually break into a database.” Students mentioned several reasons it felt real. One described how the simulation felt like a real-world encounter, “I liked how the simulation showed a possible project or assignment someone in cybersecurity could be given.” Some described the activities they engaged in including “the ability to hack into a website that seemed very real was a great way of simulating the situation”, and, “being able to navigate a workspace like that in a simulated terminal blew me away.” Others

mentioned aspects related to the user interface, such as the domains being actual websites (e.g., RipTech.io, Cybermatics.io), or the realistic chat. One student said, “The Slack-like chat tab made it feel like I was actually working with the team because I've had to use Slack entirely for a job before.” Another said that they liked “how professional the simulation portal and the connecting website looked, it made it realistic” and that “the videos and the eccentric characters… kept things engaging.” One student that I interviewed after the PCS said that “the videos were funny, and they gave you a purpose to what you were doing that day.”

Students also described the simulation as educational. One student said, “I didn’t even know what cybersecurity was before this.” Another stated that participating in a simulation instead of reading about the subjects online caused more learning to occur: “I learned more from the simulation than I would have reading about it on Wikipedia.” One enjoyed seeing the effects of bad security practices firsthand, “it was very interesting to see how easily a website can lose information if they don't check their inputs and keep them safe.” Others had come into the simulation with the idea that cybersecurity was too difficult of a field for them to succeed in. One of these stated, “I liked this [simulation] because it made me feel like this is something that I could get into. It made cybersecurity less daunting.”

Another topic mentioned was that of being part of a simulated team. Students felt that it added to the experience and made it feel like they had people that they could work with to solve problems. One student said, “It was helpful to chat and get instructions from the team.” Another stated, “It was nice being able to interact with ‘other people’ even if they weren't necessarily real. It allowed me to bounce ideas off of them.” Another liked the “feeling like you had a team.”

Table 5.5.3: Themes Identified When Coding Question About What Participants Thought Could be Improved About the Simulation

Codes Used	Total (both)
Clarity	38
Usability	13
Realism	11
Experience Level	5
Helpful	2
Interactive	0
Educational	0
Problem Solving	0
Teamwork	0

The major desire for improvement was for aspects that broke the realism of the simulation when, for whatever reason, the participants were brought out of the simulation because of something that was confusing, or if something did not work, or if something did not feel real.

Some participants did not like the videos or interacting with the team. One said, “I absolutely hated the videos and I think they should be completely redone. They are incredibly cheesy, and I think they would help people connect to the situation better if it was more serious and less cringy.” Another student that I interviewed stated that the “videos were good in an assignment, but just in general it was a little dramatic.”

While completing the SQL injection section, participants who went a little beyond the scope of the simulation noticed that it was not real SQL injection. The exact commands that the simulation was hard coded to look for would work, but when a participant tried exploring further it would not function as a genuine SQL injection would. One said, “if you put in anything other than exactly what it's looking for, you receive a ‘query failed’ notice… I really couldn't explore beyond the immediate scope of the task.” Hard coding the SQL injection element of the

simulation prevented students from furthering their understanding by not responding correctly to their injection attempts.

The documentation was sometimes the cause of confusion within the simulation. We designed it to be a resource instead of a step by step guide to complete the simulation, but some students wished it had more hints in times when they were stuck. One student related this, but also realized that we did not want to give out all the correct answers: “I think hints or more specific directions for when a person is stuck would be helpful, but I could also see some using the simulation and not learning how to think critically because hints are there to give them all the answers.” Others mentioned that demo videos would have been helpful with some portions of the simulation: “Maybe providing more specified information (specific to the simulation) would be helpful to the user--perhaps in the form of a demo video. Because I have no background in cybersecurity, I had no idea where to begin on a lot of the tasks and it was a little difficult to try to understand all the information on the terminal and try to implement the things that I needed.” Another point that was brought up was the desire for more information than what was provided in the documentation. One student said, “external links or videos [could] help improve the comprehension (especially for those wanting to learn more).”

5.6 Classroom Observation

While observing the class during the simulation, I noticed that participants were most engaged when they were using the terminal or completing the SQL injection task. Some gathered in groups to discuss how to complete a certain task, or to help if someone was struggling. After completing the exercise dealing with the terminal, three or four groups continued to explore the simulated computer system looking for more clues and were excited when they found some. Most questions that the teaching assistants or I answered dealt with usability issues: where

something was, how to use something, or to ask a question about the storyline. Besides those questions, the questions that were asked the most had to do with the SQL injection portion. That part seemed to have a higher learning curve than the other parts of the simulations as more students asked how to complete that part than any other part.

6 DISCUSSION

In this study, we've developed Cybermatics, an authentic playable case study that teaches cybersecurity dispositions, knowledge, and skills to novices. The simulation's primary goals were to find how a playable case study affected participants' career choice, understanding of cybersecurity, and confidence in completing tasks related to cybersecurity. These aspects and more were studied using analysis from a pre- and post- survey, classroom observations, student interviews, as well as data from the simulation itself.

6.1 The Cybermatics Playable Case Study

Cybermatics is the first cybersecurity playable case study created and the second playable case study overall. It was designed to increase the self-efficacy of those who completed it. It was not designed to be competitive in nature, but to help novices increase their understanding of cybersecurity and confidence in their ability to complete cybersecurity tasks. It also included a female team lead to help show that all students regardless of gender can succeed in this field. We found that Cybermatics was effective in increasing the self-reported likelihood of students pursuing a career in cybersecurity. We also saw a self-reported increase in confidence related to cybersecurity. Participants also showed an increased understanding of the importance of leadership skills and ethics in a cybersecurity professional when comparing the pre- and post-surveys. This is important because unlike many existing cybersecurity competitions (e.g.,

picoCTF and other CTFs), Cybermatics exposed students to an authentic team environment that mirrors actual workplace dynamics.

Cybermatics is comparable to the Microcore playable case study in a few ways. Within both playable case studies, the participants interact with a fictional team that helps them throughout the simulation (Balzotti, Hansen, Ebeling, & Fine, 2017). Both Cybermatics and Microcore were created with realism in mind, designed to give players a sense of immersion, and incorporated the This is Not a Game (TINAG) mentality. For example, Cybermatics incorporates a realistic Linux terminal where students perform tasks exactly how they would be performed outside of the simulation. Students also interface with their fictional teams using a Slack-like chat program. Both Cybermatics and Microcore showed strong evidence suggesting that students engaged well with the simulations, though some of the videos and humor in both simulations were disliked by some students (see next section).

Cybermatics can also be compared to the Nephrotex virtual internship focused on engineering design. Both Cybermatics and Nephrotex have been shown to help students learn domain-relevant skills, knowledge, and dispositions in a realistic context (Chesler, Ruis, Collier, Swiecki, Arastoopour, & Shaffer, 2014). They both built confidence in participants' ability to complete domain-related tasks. And both Cybermatics and Nephrotex were successful in developing interest in students to pursue careers in their respective fields. Unlike Cybermatics, Nephrotex requires an instructor or teaching assistant to provide real-time feedback during a class period when the simulation is run. However, both simulations show the power of combining a narrative, authentic activities, appropriate educational scaffolding, and a realistic workplace environment.

6.2 Student Feedback on Cybermatics

When describing what they enjoyed about their experience with Cybermatics, a majority of students stated that it felt realistic. They liked how they were given an authentic scenario that felt like a real-world encounter. In addition, students discussed how the different simulation features such as the terminal and chat features increased the realism of the simulation. As well as being realistic, students also described Cybermatics as educational. One common theme was that students felt that cybersecurity was less daunting than previously imagined. Another theme was students felt that they were able to learn more within the simulation than they would have been able to elsewhere.

When asked what could be improved with the simulation, students reported aspects of the simulation that broke realism. For example, when something was confusing, or if something didn't work, it broke the realism for the students. Another point brought up by students was the quality of the videos included in the simulation. Some felt that the videos were cheesy or dramatic. This is a similar result to what Microcore experienced where students mentioned that the simulation pushed some things too far and felt silly (Balzotti et al., 2017). Clearer documentation was another topic that several students said they wished they had. While there were clear opportunities for improvement, the types of problems that were identified are possible to improve with some effort. Indeed, the team has already begun making improvement for the next iteration of Cybermatics.

6.3 Impact on Students

The Cybermatics playable case study was shown to impact students in various ways. 80% of students said they intend to continue learning about the topics presented in the simulation. When asked in yes/no format, over 70% of students said that the simulation made them more

likely to pursue a career in cybersecurity. However, when asked on a 1- to 5-point scale if they planned to pursue a career in cybersecurity, there was no significant change between the pre- and post-survey results. This may be due to several reasons. It could be that forcing them to decide (i.e., yes or no) rather than choose a neutral response led to the difference. Or perhaps the average did not show a difference because some people moved their scores up, while others moved it down. However, the qualitative results indicate that for at least some students, the experience was important in helping them decide to pursue or at least consider a career in cybersecurity.

When talking about their change in perception of cybersecurity due to the simulation, the main theme identified by students was that of understanding. Students said they better understood the responsibilities and skills necessary for a cybersecurity professional and that those skills felt less daunting for them to be able to accomplish. Most students said they felt more confident in their own abilities to complete cybersecurity-related tasks. Studies have shown that if people have higher career self-efficacy, they will be more likely to pursue that career (Bandura, Barbaranelli, Caprara, & Pastorelli, 2001).

These results can be compared to the results of cybersecurity competitions. In Cybermatics, there was no single simulation winner. All the students were able to complete the simulation in their own time without the pressure of a competitive setting. When unsure of how to proceed, students were able to examine the documentation and educational scaffolding and also ask the teaching assistants or professor for guidance which was freely given as it was not a competition. Competitions can be demoralizing to and can lower the self-efficacy of participants who are not as proficient in the various topics covered (Mirkovic, Tabor, Woo, & Pusey, 2015). In Cybermatics, novices, while possibly taking longer to complete the tasks within the

simulation, can progress and complete the simulation while learning the same principles as more advanced students. Furthermore, Cybermatics helped students see the context in which individual activities (e.g., SQL injection) occur in different team roles. In the broad field of cybersecurity education, while competitions are very useful to hone specific skills and gain experience, simulations such as Cybermatics can be an important complementary approach in the motivation and recruitment of new students.

6.4 Limitations and Future Research

There are several limitations to this study, though we do feel it was successful in generating significant findings that can be useful to others. Cybermatics has only been conducted in one class with one professor. It was a first draft of the simulation and included bugs and other issues that can be fixed and improved for a future run. Some of these hiccups broke the realism for students and can easily be ironed out to prevent future students from experiencing a break in realism. Only 51 students, all in an introductory Information Technology class, participated in this playable case study. And although there was a normal number of female students for the class, there were not enough females to have confidence in findings analyzed by gender.

For future research, this simulation should be run with more students, more gender diversity, and students of different types such as high schoolers. Other playable case studies should also be developed that examine alternative topic areas such as digital forensics or incidence response. Finally, new design techniques can be tested to increase TINAG such as sending real texts from simulation characters or providing students with the use of authentic tools that they would use in the workplace during the simulation. Although there is considerable work to do in order to realize the full potential of playable case studies such as Cybermatics, this thesis suggests that the effort is worthwhile and one that is likely to succeed.

REFERENCES

Baker, M. (2016). Striving for Effective Cyber Workforce Development. Software Engineering Institute, Carnegie Mellon University.

Balzotti, J., Hansen, D., Ebeling, D., & Fine, L. (2017). Microcore: A Playable Case Study for Improving Adolescents Argumentative Writing in a Workplace Context. 10.24251/HICSS.2017.013.

Bandura, A., Barbaranelli, C., Caprara, G., and Pastorelli, C. (2001). Self-Efficacy Beliefs as Shapers of Children's Aspirations and Career Trajectories. Child Development. 72. 187 - 206. 10.1111/1467-8624.00273.

Bonsignore, E., Moulder, V., Neustaedter, C., Hansen, D., Kraus, K., and Druin, A. (2014). Design Tactics for Authentic Interactive Fiction: Insights from Alternate Reality Game Designers. 10.1145/2556288.2557245.

Chesler, N., Ruis, A., Collier, W., Swiecki, Z., Arastoopour, G., and Shaffer, D. (2014). A Novel Paradigm for Engineering Education: Virtual Internships with Individualized Mentoring and Assessment of Engineering Thinking. Journal of biomechanical engineering. 137. 10.1115/1.4029235.

Cheung, R., Cohen, P., Lo, H., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of Cybersecurity Competitions. Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Flushman, T., Gondree, M., and Peterson, Z. (2015). This is Not a Game: Early Observations on Using Alternate Reality Games for Teaching Security Concepts to First-Year Undergraduates. 8th Workshop on Cyber Security Experimentation and Test (CSET 15).

Graham, M., Frederick J., Byars-Winston A., Hunter A., and Handelsman J. (2013). Increasing Persistence of College Students in STEM. Science (New York, N.Y.). 341. 1455-6. 10.1126/science.1240487.

Gredler, M. (1996). Educational Games and Simulations: A Technology in Search of a (Research) Paradigm. In D. H. Jonassen (Ed.), Handbook of research for educational communications and technology (pp. 521-39). New York: MacMillian Library Reference.

Gredler, M. (2004). Games and Simulations and Their Relationship to Learning. Handbook of Research on Educational Communications and Technology, 2nd ed., D. H. Jonassen, Ed. Mahwah, NJ: Lawrence Erlbaum Associates, Inc., pp. 571–581.

Katsantonis, M., Fouliras, P., and Mavridis, I. (2017). Conceptual Analysis of Cyber Security Education Based on Live Competitions. 771-779. 10.1109/EDUCON.2017.7942934.

Kay, D., Pudas, T., and Young, B. (2012). Preparing the Pipeline: The US Cyber Workforce for the Future. Defense Horizons (72): p. 1.

Kolb, D. (2014). Experiential Learning: Experience as the Source of Learning and Development Second Edition. Pearson Education.

Mirkovic, J., Tabor, A., Woo, S., and Pusey, P. (2015). Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015. Summit on Gaming, Games, and Gamification in Security Education.

Raytheon. (2016). Securing Our Future: Closing the Cybersecurity Talent Gap. National Cybersecurity Alliance. Retrieved from https://www.raytheon.com/sites/default/files/cyber/rtnwcm/groups/corporate/documents/content/rtn_335212.pdf

Rowe, D., Lunt, B., & Ekstrom, J. (2011). The Role of Cyber-Security in Information Technology Education. SIGITE 2011. Retrieved from https://doi.org/10.1145/2047594.2047628

Shaffer, D. (2005). Epistemic Games. Innov. J. Online Educ., vol. 1, no. 6, Article 2.

Sullivan, F. (2017). Global Information Security Workforce Study 2017: Benchmarking Workforce Capacity and Response to Cyber Risk. Center for Cyber Safety and Education, $(ISC)^2$, Booz Allen Hamilton, Alta Associates, and Frost & Sullivan.

U.S. Bureau of Labor Statistics. (2018). Information Security Analysts: Occupational Outlook Handbook. Retreived from www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm on Nov 17, 2018.

Vogel, R. (2016). Closing the Cybersecurity Skills Gap. Salus Journal. 4(2): p. 32.

White, K., and Ingalls R. (2016) The Basics of Simulation. Winter Simulation Conferences (WSC). IEEE.

APPENDICES

APPENDIX A. PRE-SURVEY QUESTIONS (11 QUESTIONS)

Q1) Using the following scale (strongly disagree to strongly agree), rate your agreement with the following statements

- I am interested in cybersecurity
- I plan on pursuing a career in cybersecurity
- I feel confident in my ability to succeed in the cybersecurity field
- I feel confident browsing the internet without risk of infection
- I feel confident that the passwords I use are strong
- I feel confident that I won't be hacked
- I feel confident using antivirus and other programs to protect my computer's security
- I feel confident updating my computer and my programs to keep them secure
- I feel confident that I can fix my computer if it is infected

Q2) What is cybersecurity in your opinion?

Q3) What responsibilities/skills does a cybersecurity professional have?

Q4) On a scale of 1 to 5, how important that someone working in cybersecurity would need the following skills to be successful?

- Leadership skills
- Critical thinking
- Communication skills
- Adaptability
- Ability to think outside the box
- Problem solving skills
- Ethics
- Programming skills
- Ability to learn continuously

Q5) On a scale of 1 to 5, how confident are you in your ability to successfully apply each skill listed below?

- Leadership skills
- Critical thinking
- Communication skills
- Adaptability
- Ability to think outside the box
- Problem solving skills
- Ethics
- Programming skills
- Ability to learn continuously

Q6) What is your net id?

Q7) What experience do you have in cybersecurity related work?

Q8) What is your major?

Q9) What is your age?

Q10) What is your gender?

Q11) What is your year in college?

APPENDIX B. POST-SURVEY QUESTIONS (14 QUESTIONS)

Q1) Using the following scale (strongly disagree to strongly agree), rate your agreement with the following statements

- I am interested in cybersecurity
- I plan on pursuing a career in cybersecurity
- I feel confident in my ability to succeed in the cybersecurity field
- I feel confident browsing the internet without risk of infection
- I feel confident that the passwords I use are strong
- I feel confident that I won't be hacked
- I feel confident using antivirus and other programs to protect my computer's security
- I feel confident updating my computer and my programs to keep them secure
- I feel confident that I can fix my computer if it is infected

Q2) The following simulation features made the simulation feel more realistic

- The terminal
- The chat
- The character videos
- The documentation

- The Cybermatics portal
- The RipTech website
- The storyline

Q3) I intend to continue learning about the topics presented in the simulation (yes/no)

Q4) This simulation made me more likely to pursue a career in cybersecurity (yes/no)

Q5) The simulation made me more confident in my ability to succeed in a cybersecurity career (yes/no)

Q6) I was able to complete the tasks in the simulation effectively (yes/no)

Q7) On a scale of 1 to 5, how important that someone working in cybersecurity would need the following skills to be successful?

- Leadership skills
- Critical thinking
- Communication skills
- Adaptability
- Ability to think outside the box
- Problem solving skills
- Ethics
- Programming skills
- Ability to learn continuously

Q8) On a scale of 1 to 5, how confident are you in your ability to successfully apply each skill listed below?

- Leadership skills
- Critical thinking
- Communication skills
- Adaptability
- Ability to think outside the box
- Problem solving skills
- Ethics
- Programming skills
- Ability to learn continuously

Q9) What did you like about the simulation? (free response)

Q10) What could be improved in the simulation? (free response)

Q11) How have your perceptions about cybersecurity changed after completing the simulation? (free response)

Q12) What is cybersecurity in your opinion? (free response)

Q13) What responsibilities/skills does a cybersecurity professional have? (free response)

Q14) What is your net id?