Lab 1 - Phisecure Product Description

Joshua Freeman

Old Dominion University

CS410 Professional Workforce Development I

Professor Janet Brunelle

31 March 2024

Version 1

Table of Contents

1. Introduction
2. Product Description
    2.1. Key Product Features and Capabilities
    2.2. Major Components (Hardware/Software)
3. Identification of Case Study
4. Product Prototype Description
    4.1. Prototype Architecture (Hardware/Software)
    4.2. Prototype Features and Capabilities
    4.3. Prototype Development Challenges
5. Glossary
6. References

1. Introduction

Phishing continues to plague individuals and organizations worldwide, representing one of the most common forms of cyberattacks in today's digital landscape. With an alarming estimate of 3.4 billion malicious emails sent daily (Irwin, 2023), the threat posed by phishing remains ever-present, exploiting human vulnerabilities to infiltrate systems, steal sensitive information, and wreak havoc on unsuspecting victims. In response to this increasing threat, our product, Phisecure, emerges as a beacon of defense and education in the realm of cybersecurity. Designed to empower university students with a comprehensive understanding of phishing tactics, Phisecure serves as a pivotal tool in constructing strong defenses against malicious cyber campaigns. By delving into the intricacies of phishing techniques, students not only enhance their defensive capabilities but also gain practical experience in combating real-world cyber threats. Phisecure offers a dynamic platform where students can engage in immersive learning experiences. Through interactive modules and hands-on simulations, users navigate the complexities of phishing attacks and learn about deceptive tactics. Phisecure represents a leap forward in cybersecurity education, bridging the gap between theory and practice, and empowering the next generation of cybersecurity professionals to navigate the ever-evolving threat landscape with confidence and proficiency.

2. Product Description

Phisecure is a learning tool that will allow students to have a better understanding on how to defend against phishing attacks. Our product is going to be used by universities to give their students a more practical knowledge base in cybersecurity. The learning tool will allow students to create phishing attacks and use them against other students. The other students will learn how to be more proficient at spotting and defending against phishing attacks.

2.1. Key Product Features and Capabilities

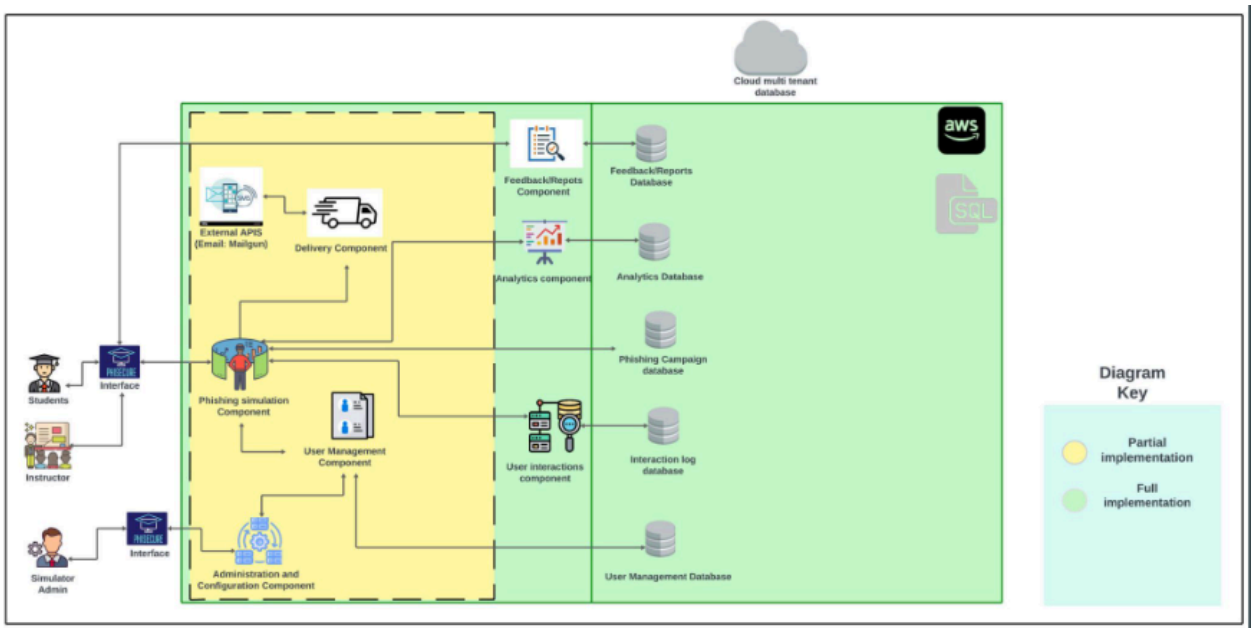
The primary function of Phisecure is giving students the ability to learn how to create and defend against phishing attacks. To facilitate this we will be creating a personalized simulator tool. The tool will cover how to generate a custom phishing attack, the many types of phishing attacks you can create, and how to properly detect and counter those same attacks. After a session is over, both the attacker and the defender will be given a report card detailing their mistakes and feedback on how they can improve. The administrator/teacher will also be given a detailed report on how the students performed. This will allow them to give students personalized feedback on their

mistakes.

Category	Features	Guest	Student	Instructor	Admin	Business Employee	Researcher
User Account Management	User registration		x	x	x	x	x
	Account creation/deletion		x	x	x	x	x
	Login using university credentials		x	x		x	x
	Role-based access control				x		
Phishing simulation	Generate a custom Phishing attack		x	x	x	x	x
	Send phishing attack via email		x	x	x	x	x
	Send phishing attack via sms		x	x	x	x	x
	Send phishing attack via live chat		x	x	x	x	x
	ML generated templates		x	x	x	x	x
	Tutorial	x	x	x	x	x	x
Reporting & Feedback Analytics	Red flags missed		x	x	x	x	
	Links clicked		x	x	x	x	
	Comprosing replies		x	x	x	x	
	Successful attacks		x	x	x	x	
	Most successful platform		x	x	x	x	
	Least successful platform		x	x	x	x	
User interface	Admin dashboard				x	x	
	Student/instructor dashboard		x	x		x	x
	Home page	x	x	x	x	x	x
Sandboxed phishing enviroment	Attack times settings			x	x		x
	Attack environment settings			x	x		x
	Email servers			x	x		x
	Web servers			x	x		x
	Domain setup			x	x		x
	Network isolation			x	x		x

2.2. Major Components (Hardware/Software)

Phisecure will mainly be an application for PCs. Due to this being an educational tool for university students, PCs are already provided in places like the computer lab or library. Phisecure will be created using Python, HTMl, and CSS. We will be using VSCode as our main IDE and SQL will be used for database management. We will be using a cloud based multi-tenant database, this reduces cost while maximizing our resources. The database will be relational due to ease of use, accuracy, and categorizing of data. Our product will also be interacting with a variety of platforms including Discord, Slack, and Microsoft teams.



3. Identification of Case Study

Our case study with Phisecure will be students who are taking cybersecurity classes and want more practical experience. Students will be assigned a role by their instructor: attacker or defender. The attacker will create a fake phishing email and send it to their assigned defender at random. The attacker will be trying to make their fake email look as legitimate as possible. This will occur over a limited period, a week, so the

defender has enough time to see the attack and have a chance to respond. At the end of this period, the attacker and defender will receive a report card. This report will inform them of various statistics, such as click rate, successful/least successful platform, and red flags missed. The instructor will also receive a report on both students, which will allow them to give more in-depth feedback.

4. Product Prototype Description

4.1. Prototype Architecture (Hardware/Software)

4.2. Prototype Features and Capabilities

4.3. Prototype Development Challenges

5. Glossary

Phishing - The fraudulent practice of sending emails or other messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.

Spear Phishing - A type of phishing involving personalization and targeting a specific individual.

Malware - Software that compromises the operation of a system by performing an unauthorized function or process.

Ransomware - A malware designed to deny a user or organization access to files on their computer.

Attack - An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

6. References

Irwin, L. (2023, June 19). *51 must-know phishing statistics for 2023: It governance*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/51-must-know-phishing-statistics-for-2023

Baker, E. (2024, January 23). *Top 10 costs of phishing - hoxhunt*. HoxHunt. http://www.hoxhunt.com/blog/what-are-the-top-10-costs-of-phishing#:~:text=Using%20different%20criteria%2C%20the%20Ponemon,as%20the%20king%20of%20cybercrime.

Stansfield, T. (2023, November 15). *Q3 2023 phishing and malware report*. Vadesecure. http://www.vadesecure.com/en/blog/q3-2023-phishing-malware-report#:~:text=in%20Q3%202023%2C%20Vade%20detected,180.4%20million

Toor, J. (2021, November 2). *Victims penetrated by phishing had conducted anti-phishing training*. Cloudian. https://cloudian.com/press/cloudian-ransomware-survey-finds-65-percent-of-victims-penetrated-by-phishing-had-conducted-anti-phishing-training/

Rezabek, J. (2024, January 24). *How much does phishing cost businesses?*. IRONSCALES. https://ironscales.com/blog/how-much-does-phishing-cost-businesses

Sheng, E. (2023, August 15). *Phishing scams targeting small business on social media including Meta are a "gold mine" for criminals*. CNBC. https://www.cnbc.com/2023/08/15/gold-mine-phishing-scams-rob-main-street-on-social-media-like-meta.html

Steves, M., Greene, K., & Theofanos, M. (2020, September 14). *Categorizing human phishing difficulty: A phish scale*. OUP Academic. https://academic.oup.com/cybersecurity/article/6/1/tyaa009/5905453

Paun, G. (2024, February 20). *Council post: Building a brand: Why a strong Digital Presence Matters*. Forbes. https://www.forbes.com/sites/forbesagencycouncil/2020/07/02/building-a-brand-why-a-strong-digital-presence-matters/

Smith, G. (2024, February 16). *Top phishing statistics for 2024: Latest figures and trends*. StationX. https://www.stationx.net/phishing-statistics/

Alonso, J. (2023, July 18). *Universities warn of increased cyberscams targeting students*. Inside Higher Ed | Higher Education News, Events and Jobs. https://www.insidehighered.com/news/students/safety/2023/07/18/universities-warn-increased-cyberscams-targeting-students

Cisco. (2024, February 22). *What is cybersecurity?*. Cisco. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html