Lab 2 - Phisecure Requirements & Specifications

Joshua Freeman

Old Dominion University

CS411 Professional Workforce Development II

Professor Sarah Hosni

31 October 2024

Version 2

Table of Contents

List of Figures

1. Introduction

Phishing continues to plague individuals and organizations worldwide, representing one of the most common forms of cyberattacks in today's digital landscape. An estimated 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, provides essential defense and education in the realm of cybersecurity. Serving as an educational tool, Phisecure empowers university students with a comprehensive understanding of phishing tactics.

By exploring 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, connecting theory with practical experience it empowers the next generation of

cybersecurity professionals to navigate the ever-evolving threat landscape with confidence and proficiency.

1.1 Purpose

The purpose of this SRS document is to inform the reader on what Phisecure is and how the prototype works.

1.2 Scope

Phisecure is a learning tool that will allow students to have a better understanding of how to defend against phishing attacks. The product is designed 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 become more proficient at spotting and defending against phishing attacks. The primary function of Phisecure is to give students the ability to learn how to create and defend against phishing attacks. To facilitate this, we will be creating a personalized phishing attack. The tool covers how to generate and detect various custom phishing attacks, the many types of phishing attacks you can create, and how to properly detect and counter these attacks. After a session is over, both the attacker and the defender will be given an assessment report detailing their mistakes and feedback areas of improvement . 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.

1.3 Definitions

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.

1.4 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

Phisecure. CS411 Orange Team: Phisecure. (2024, February 5). https://viahub92.github.io/F24-Orange/

1.5 Overview

The remainder of this document will cover the product perspective, product functions, the user characteristics, design constraints, and assumptions and dependencies.

2. Overall Description

Phisecure is a learning tool that is designed to help students understand how to defend against phishing attacks. The product is designed 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. These students will learn how to better recognize and respond to phishing attacks.

2.1 Product Perspective

Phisecure will involve students who are taking ODU cybersecurity classes and want more practical experience. Students will be assigned a role by their instructor: attacker, or defender. The attacker will send a phishing email to a randomly assigned defender. The attacker will attempt to make their phishing email appear as realistic as possible. This exercise will take place over a limited period of one week, giving the defender 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 detailing each student's performance. This report will inform them of various statistics, such as click rate, platform success rate, and missed red flags. The instructor will also receive a

report on both students, which will allow them to give more in-depth feedback. The student can then take this feedback and use it to continuously improve.

2.2 Product Functions

The primary function of Phisecure is to teach students to create and defend against phishing attacks. To facilitate this, we will be creating a personalized simulator tool. The tool will cover how to create custom phishing attacks, the various types of phishing attacks, and how to detect and counter them. 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. The table below goes into more detail about the various features the product will have.

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

2.3 User Characteristics

There will be three main roles that our prototype will utilize: student, instructor, and admin. The student role will be allowed to login, view their dashboard, and send or receive phishing emails. The student dashboard will have an inbox to receive and send the phishing emails. It will also have an area designed to receive reports from their teachers on how well they performed. The teacher role will be presented with a dashboard that shows them a report sending area, analytics on how specific students are performing, and a student assignment area. The administrator will also be presented with a dashboard that has user analytics, a way to manage all of the users, and ways to modify the student and teacher roles.

2.4 Constraints

N/A

2.5 Assumptions and Dependencies

N/A