Lab 2 – Phisecure Requirements & Specifications

Dylan Via

Old Dominion University

CS411W Professional Workforce Development II

Sarah Hosni

22 November 2024

Version 2

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this SRS document is to explain how Phisecure works to developers. This document outlines the intended functionality, constraints, and requirements needed to implement Phisecure effectively. This document ensures that the development team with the project's objectives, allowing a deeper understanding of Phisecure's overall goals and components.

1.2 Scope

Phisecure provides a dynamic educational tool to train students in identifying and responding to phishing attacks. Through customized phishing simulations and hands-on scenarios, students experience phishing attacks in a controlled environment. The system will automatically launch the attacks and develop a performance report based on the student's interactions. Reports will also be generated and sent to the instructors, allowing them to oversee the student engagement and success in the simulations. Phisecure is designed to improve phishing attack awareness by focusing on practical, scenario-based learning.

1.3 Definitions, Acronyms, and Abbreviations

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.

Phishing Campaign – a simulated series of phishing emails sent to students to test their ability to recognize and respond to such threats in a controlled environment.

1.4 References

Team Orange. (2024, October 2). Lab 1 – Phisecure Product Description. Retrieved October 31, 2024 from https://viahub92.github.io/F24-Orange/

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

1.5 Overview

The next sections of this SRS document take a closer look at how Phisecure is designed and what it can do. Section 2 gives an overview of the product, covering its features, who will use it, and any limitations it has. From Section 3 onward, functional and nonfunctional requirements will be discussed.

2. Overall Description

2.1 Product Perspective

Phisecure is an educational platform that uses realistic simulations to teach university students about phishing techniques. It generates and sends phishing messages to help students build detection skills in a controlled environment. The system also tracks how students interact with these messages, giving instructors data to customize training based on each student's and the class's overall performance.

2.2 Product Functions

Key features of Phiesecure:

- Student Questionnaire: A questionnaire the student will fill out on creation of their account. It will record responses to attach tags to the student that will allow the system to identify effective phishing templates to use.
- Phishing Simulation Creation: Automated generation of phishing attacks tailored to the student. Filling in templates that match the tags attached to the student and then sending the attack.
- Performance Tracking: Monitors the students interactions with the simulated attack, this includes opening, replying, and clicking a link attached to the message.
- Performance reports: Generates reports to send to the student, providing feedback based on the results of their interactions. An overall report is generated for the instructor, showing the performance of their students.
- Peer Phishing Module: Students can select another student to generate a simulated attack. They will create their own template for the software to

use in a simulated attack against the selected student. The results will be recorded and reported to both students.

2.3 User Characteristics

Phisecure has three primary user roles:

- Student: Engages with the simulated phishing emails to learn detection strategies.
- Instructor: Monitors the students performance and reviews the reports for class assessments.
- Admin: Oversees the system operations, can manage user accounts, and maintains system integrity.

2.4 Constraints

This software does not protect the student from actual phishing attacks or other cybersecurity threats.

2.5 Assumptions and Dependencies

N/A