Lab 1 - Phisecure Product Description

Hunter Pollock, Ralph Mpanu-Mpanu, Dylan Via, Joshua Freeman, Ethan Barnes, Mustafa Ibrahim

Old Dominion University

CS410 Professional Workforce Development I

Professor Janet Brunelle

29 April 2024

Version 1

Table of Contents

List of Figures

1. Introduction

Phishing is a widespread issue that affects many people. Phishing can be defined as a type of criminal social engineering that is conducted through digital communication channels such as email, voice calls, websites, or text messages. In today's digital age universities are prime targets for phishing related attacks (David, 2019). Phishing makes up about half of cyberattacks against higher education (Oxman, 2023). In 2022, Duke university experienced a phishing campaign which attacked students and tried to bait them into sharing login information with the threat of losing account access (Oxman, 2023).

It is clearly imperative that universities must take phishing threats seriously or face consequences such as financial losses, reputation damage, and data breaches. Because of the social engineering aspect of phishing this results to human error as being one of the top reasons victims fall for phishing attacks. Social engineering can be defined as a scam where the criminal impersonates someone else, a group, or a brand to manipulate the victim to perform a certain action (Oles, 2023). Most serious cyber threats such as ransomware and malware start from phishing attacks due to the low cost and the ability to easily scale (Oles, 2023).

To address these threats universities, need to have a comprehensive strategy to not only educate students and staff using traditional methods. But also, to provide interactive learning where students and university personnel can get more hands-on experience dealing with common phishing attacks.

2. Product Description

Phisecure is an educational software tool that simulates phishing attacks. It provides customized training allowing users to create their own simulations on a variety of platforms. Users begin with creating their own phishing campaign. The campaign will take place in a simulated environment with the goal to target other users and try to get them to interact with an attack. Each campaign will also have a name, description, launch date, end date, and status of the current campaign. In addition, it will have a template for different methods of digital communication to simulate different kinds of phishing venues. Such as email, SMS, and live chat platforms.

2.1 Key Product Features and Capabilities

Figure 1

Features Table

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	Create a phishing campaign		x	x	x	x	x
	Choose a phishing template		x	x	x	x	x
	Choose mode of delivery(email, sms)		x	x	x	x	x
	Target list of recipients		x	x	x	x	x
	Tutorial	x	x	x	x	x	x
Report/Feedback	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
Simulator enviroment	Attack environment settings			x	x		x
	Email simulation server			x	x		x
	Fake web servers and services			x	x		x
	Customizable network configurations			x	x		x
Analytics	Click rate			x	x		x
	Disclosure rate			x	x		x

The features in Phisecure can be broken down into several categories. User management, phishing simulation, reporting/feedback, user interface, simulator environment, and analytics. The core features in the product are the phishing simulation, reports/feedback, and analytics. The phishing simulation is what facilitates the creation of the phishing campaigns, choosing templates and modes of delivery.

Data is collected from users interacting with the campaigns to make sure their following best practices. If they give up sensitive information or compromising data. This data will be collected and stored in the system. Once the simulation is complete feedback will be assessed. Feedback will include red flags missed, links clicked, compromising replies, and most/least successful platforms. This feedback will be used to generate overall reports for student users to show how they did and instructors to assess their students on their performance. This interaction data will also be used to generate insightful analytics such as click rate, disclosure rate, and interaction rate.

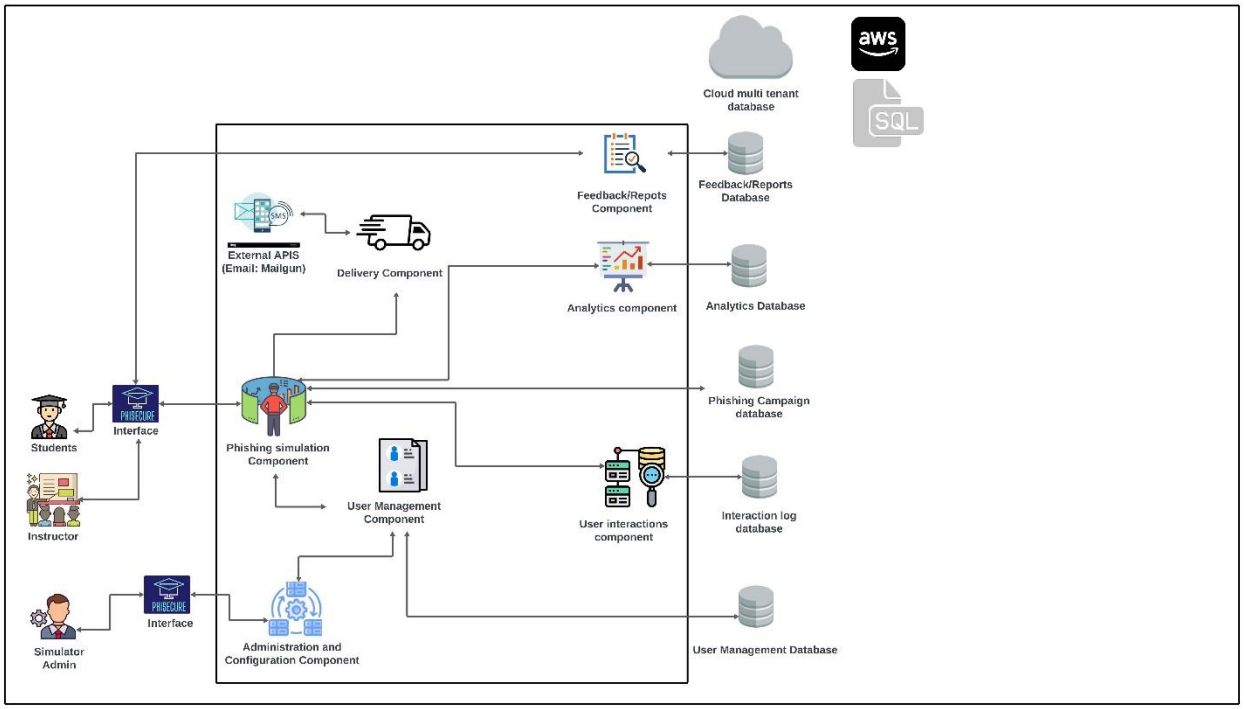
2.1 Major Components (Hardware/Software)

Phisecure will be mainly used as a web application. The frontend is built using the React framework, which is a popular JavaScript library for building user interfaces. It will also use HTML, CSS, and python in conjunction. The backend will utilize the Flask framework used to build web applications in Python. The primary language used for the backend will be Python.

For data storage and management, Phisecure will utilize Amazon RDS (Relational Database Service) and MySQL. Amazon RDS is a managed database service provided by Amazon Web Services (AWS). In addition, the database will be multi-tenanted.

Figure 2

Major Functional Component Design



The key software components in Phisecure design are the phishing simulation component which forms the core, it includes the key logic and algorithms for creating the phishing campaigns and executing them. The user interaction component which will process user interaction metadata. Delivery component which handles delivering the simulated attacks it will leverage external API's such as Twilio, Mailgun, and other live chat API's. User management component which handles users' information such as registration, usernames, passwords, roles. Lastly, the administration and configuration component which will allow simulator admins to configure the simulation environment and perform routine updates.

3. Identification of Case Study

Phisecure will be used as an educational tool in universities. It will be used to educate and prepare students against phishing threats by simulating realistic phishing attacks across multiple communication channels. A case for Phisecure would involve a university such as Old Dominion University. Phisecure would work with administration and current IT security structure to integrate within university curriculum to educate students on best practices and give them hands on experience dealing with phishing.

4. 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.

5. 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

Oxman, Z. (2023, July 13). Protecting Higher Education from Email Attacks. Abnormal Security. Retrieved from https://abnormalsecurity.com/blog/protecting-higher-education-email-attacks

Oles, N. (2023). *How to Catch a Phish*.