ISSN: 2347-6540

International Journal of Latest Research In Engineering and Computing (IJLREC)
Volume 11, Issue 1, Page No.52-60, 2024
www.ijlrec.com

PHISHING CONTROL SIMULATION TOOL

Aman Raj[1], Abhishek Ganguly[2], Farhan Manzoor[3], Aashika Kri. Singh[4]

Student, Computer Science and Engineering, Shivalik College of Engineering, Dehradun, Uttarakhand, India, Iamanraj28@gmail.com[1]

Student, Computer Science and Engineering, Shivalik College of Engineering, Dehradun, Uttarakhand, India, zxganguly.2002@gmail.com [2]

Student, Computer Science and Engineering, Shivalik College of Engineering, Dehradun, Uttarakhand, India, farhanmanzoor2002@gmail.com [3]

Student, Computer Science and Engineering, Shivalik College of Engineering, Dehradun, Uttarakhand, India, Khsuhisingh1085@gmail.com [4]

Abstract :- "PCST" is a phishing framework designed to simulate real-world phishing attacks and assess an organization's susceptibility to such threats. The framework provides security professionals with a platform to create and execute phishing campaigns, thereby identifying vulnerabilities within their systems and educating employees about potential cybersecurity risks. PCST allows users to craft highly realistic phishing emails and web pages, mimicking the tactics used by malicious actors. Through its intuitive interface, users can customize various aspects of their campaigns, including email content, sender information, and landing pages. Additionally, PCST offers detailed analytics and reporting capabilities, enabling users to track campaign engagement and measure the effectiveness of their security awareness training programs. By leveraging PCST, organizations can proactively test their defenses against phishing attacks, identify weak points in their security posture, and implement targeted remediation strategies. Ultimately, PCST serves as a valuable tool in the ongoing effort to enhance cybersecurity resilience and protect sensitive data from unauthorized access and exploitation

Keywords: PCST, Phishing Framework, CyberSecurity, Simulation, Vulnerability Assessment, Email Phishing, Web Phishing, Security Awareness, Analytics, Reporting, Defense Testing, Remediation Strategies, Cyber Resilience, Data Protection

I. INTRODUCTION

Phishing is a prevalent cyber threat that involves deceptive tactics used by malicious individuals or groups to trick unsuspecting users into disclosing sensitive information such as passwords, credit card numbers, or personal identification. These tactics often involve impersonating trusted entities, such as banks, government agencies, or reputable companies, through various communication channels, including email, text messages, social media, or phone calls.

Phishing attacks can take many forms, ranging from simple email scams to sophisticated campaigns that employ advanced social engineering techniques. Common types of phishing attacks include:

Email Phishing: Fake emails that appear to be from legitimate sources, often containing links to malicious websites or attachments designed to install malware on the recipient's device.

Spear Phishing: Targeted attacks aimed at specific individuals or organizations, using personalized messages tailored to the recipient's interests, affiliations, or roles within the organization.

Pharming: Redirecting users to fake websites that mimic legitimate ones, aiming to steal login credentials or financial information.

Vishing: Phishing attacks conducted over the phone, where scammers impersonate trusted entities and attempt to obtain sensitive information through voice communication.

Phishing attacks pose significant risks to individuals, businesses, and society. They can result in financial loss, identity theft, data breaches, and reputational damage. Moreover, phishing attacks are constantly evolving, with attackers employing increasingly sophisticated techniques to bypass security measures and exploit human vulnerabilities.

Importance of Phishing Awareness and Education:

Given the prevalence and evolving nature of phishing attacks, raising awareness and providing education about phishing threats are essential components of effective cybersecurity strategies. Users are often the weakest link in the security chain, as they may inadvertently fall victim to phishing scams due to lack of awareness or training.

Phishing awareness training programs play a crucial role in empowering users to recognize and respond to phishing threats effectively. These programs typically cover topics such as:

- Identifying phishing emails and messages
- Recognizing common phishing tactics and warning signs
- Understanding the consequences of falling victim to phishing attacks
- Best practices for securely handling suspicious emails or messages

By educating users about phishing risks and providing them with the knowledge and skills to identify and mitigate these threats, organizations can significantly reduce their susceptibility to phishing attacks and enhance their overall cybersecurity posture.

Introduction to the PCST:

Phishing simulation tools represent a proactive approach to phishing awareness and education. These tools allow organizations to simulate real-world phishing scenarios in a controlled environment, providing users with hands-on experience in identifying and responding to phishing threats. By conducting simulated phishing campaigns, organizations can assess their employees' awareness levels, measure their response behaviors, and identify areas for improvement.

This project report focuses on PCST, a phishing simulation platform designed to simulate real-world phishing attacks and assess an organization's susceptibility to such threats. PCST provides organizations with a robust framework for conducting simulated phishing campaigns, measuring user responses, and improving overall cybersecurity posture.

PCST offers a range of features to facilitate the creation and execution of phishing simulations and help organizations strengthen their cybersecurity defenses such as:

- **Campaign Creation**: Users can create customized phishing campaigns, including email templates, landing pages, and attachment payloads.
- **Target Groups**: PCST allows users to define target groups within their organization, enabling tailored phishing simulations for different departments or roles.
- **Tracking and Reporting**: The tool provides real-time tracking of email opens, link clicks, and submitted credentials, along with detailed reporting to assess campaign effectiveness.

•**Template Library**: PCST includes a library of pre-built email templates and landing pages, making it easier for users to get started with their phishing simulations.•**Automation**: Users can schedule and automate phishing campaigns, reducing the manual effort required for ongoing security assessments.

- **Integration**: PCST integrates with other security tools and platforms, enhancing its utility within existing security workflows.

II.METHODOLOGY

The methodology section of a project report outlines the approach taken to develop, implement, and evaluate the phishing simulation tool. It provides a detailed description of the processes, techniques, and methodologies used throughout the project lifecycle. Here's a breakdown of key components:

Description of PCST:

PCST is a phishing simulation tool designed to help organizations assess and improve their resilience against phishing attacks. It provides a user-friendly platform for creating, executing, and analyzing simulated phishing campaigns, allowing users to replicate real-world attack scenarios and gauge their organization's susceptibility to phishing threats. At its core, PCST enables users to craft convincing phishing emails and landing pages that mimic legitimate communication from trusted sources. With its intuitive interface, users can easily customize email templates, personalize messages, and create enticing lures to entice recipients to interact with the simulated phishing content. Additionally, PCST offers flexibility in designing multi-stage campaigns, allowing users to sequence multiple phishing emails and landing pages to simulate sophisticated attack chains.

•One of PCST's key features is its robust tracking and reporting capabilities, which provide real- time insights into campaign performance and user engagement. Users can monitor metrics such as email opens, link clicks, and submitted credentials, allowing them to assess the effectiveness of their phishing simulations and identify areas for improvement. Detailed reporting features enable users to generate comprehensive reports for stakeholders, showcasing campaign results and highlighting key findings.

•PCST also supports target segmentation, allowing users to tailor phishing simulations to specific groups or departments within their organization. This enables users to conduct targeted assessments of different user populations and customize phishing campaigns based on their unique characteristics and vulnerabilities.

•Furthermore, PCST emphasizes ease of use and integration, with support for APIs and webhooks that enable seamless integration with existing security tools and workflows. This allows organizations to incorporate PCST into their broader cybersecurity initiatives and leverage its capabilities within their existing infrastructure.

Development Process:

The development process for PCST involves several key stages, including planning, design, implementation, testing, and maintenance. Here's an overview of each stage:

Planning:

Requirements Gathering: We gathers requirements by collaborating with security professionals, penetration testers, and potential users, to understand their needs and objectives for the tool.

- **Goal Definition:** Clear goals and objectives for the project are established, such as creating a user-friendly interface, implementing robust tracking and reporting features, and ensuring compatibility with various email platforms.
- **Technology Selection:** Decisions are made regarding the technologies and frameworks to be used in the development process, taking into account factors such as scalability, performance, and maintainability.

Design:

Architecture Design: The system architecture is designed, outlining the overall structure of the application, including components such as the user interface, backend server, database, and integration points with external services.

- **User Interface Design:** Wireframes and mock-ups are created to design the user interface, focusing on usability, accessibility, and intuitive interaction patterns to enhance the user experience.
- **Database Schema Design:** The database schema is designed to efficiently store and retrieve data related to phishing campaigns, templates, targets, and campaign results.

Implementation:

Frontend Development: The user interface is developed using web technologies such as HTML, CSS, and JavaScript, with frameworks like React.js or Angular.js used to create responsive and interactive interfaces.

Backend Development: The backend server is implemented using a server-side programming language such as Go, Python, or Node.js, with frameworks like Gin, Flask, or Express used to handle HTTP requests, manage authentication, and interact with the database.

Integration Development: Integration points with external services, such as email servers for sending phishing emails and tracking user interactions, are implemented using APIs and SDKs provided by those services.

Testing:

Unit Testing: Individual components of the application are tested in isolation to ensure they function as expected, with automated tests written using frameworks like Jest, Mocha, or Pytest.

Integration Testing: The interaction between different components of the application is tested to verify that they work together correctly, with automated tests covering common use cases and edge cases.

User Acceptance Testing: The application is tested by real users or testers to validate its usability, functionality, and performance against the requirements and expectations defined during the planning stage.

Deployment:

Deployment Strategy: A deployment strategy is developed, outlining the steps and processes for deploying the application to production environments, including considerations for scalability, availability, and security.

Continuous Integration/Continuous Deployment (CI/CD): Automated CI/CD pipelines are set up to streamline the deployment process, with code changes automatically built, tested, and deployed to production environments upon successful validation.

Technologies Used:

PCST is primarily developed using the following technologies:

- **Go (Golang)**: PCST is written in the Go programming language, also known as Golang. Go is a statically typed, compiled language designed for simplicity, efficiency, and concurrency. It is well-suited for building scalable, high-performance applications and services, making it an ideal choice for developing PCST's backend server and core functionality.
- **HTML, CSS, JavaScript**: The user interface of PCST is built using standard web technologies, including HTML for structuring content, CSS for styling, and JavaScript for interactivity. These technologies enable the creation of a responsive and intuitive user interface for managing phishing campaigns, templates, targets, and reporting within the PCST application.
- **React.js**: React.js is a popular JavaScript library for building user interfaces. It is used in PCST to create dynamic and interactive components, such as campaign dashboards, campaign wizards, and result summaries. React.js allows for the efficient rendering of complex user interfaces and facilitates the development of reusable UI components, enhancing the maintainability and scalability of the PCST frontend.

•**Gin**: Gin is a web framework for Go that provides routing, middleware, and utilities for building web applications and APIs. PCST utilizes Gin to handle HTTP requests, define routes, and implement middleware functions for tasks such as authentication, logging, and error handling. Gin's lightweight and fast performance make it well-suited for building the backend server of PCST.

•**SQLite**: SQLite is a lightweight relational database management system (RDBMS) used in PCST for storing campaign data, template configurations, target information, and campaign results. SQLite is embedded within the PCST application, eliminating the need for external dependencies or separate database servers. It provides simplicity, reliability, and portability, making it suitable for small to medium-scale deployments of PCST.

Implementation Details:

Backend Implementation:

•**Go Programming Language**: PCST is primarily implemented in Go (Golang), a statically typed, compiled language known for its simplicity, concurrency features, and performance.

•**Gin Web Framework**: PCST utilizes the Gin web framework, which provides routing, middleware, and utilities for building web applications and APIs in Go. Gin simplifies the implementation of HTTP endpoints, request handling, and middleware functions for tasks such as authentication and logging.

•**Database Management**: PCST uses SQLite as its embedded database management system for storing campaign data, templates, targets, and results. SQLite offers simplicity, portability, and lightweight deployment, making it suitable for small to medium-scale applications like PCST.

•**Email Sending**: PCST integrates with SMTP servers to send phishing emails to targeted recipients. It leverages Go's standard library for SMTP communication and can be configured to work with various SMTP providers and configurations.

Frontend Implementation:

•**HTML, CSS, JavaScript**: The frontend of PCST is built using standard web technologies, including HTML for structuring content, CSS for styling, and JavaScript for interactivity and dynamic behavior.

•**React.js**: PCST utilizes the React.js library for building user interfaces. React.js allows for the creation of reusable UI components, efficient rendering of complex views, and seamless state management, enhancing the responsiveness and usability of the PCST interface.

•**Webpack**: Webpack is used as a module bundler for PCST's frontend assets, including JavaScript, CSS, and other static files. Webpack simplifies the process of managing dependencies, optimizing assets, and generating bundles for deployment.

2.4.3 Authentication and Authorization:

•PCST implements authentication and authorization mechanisms to secure access to its features and functionalities. Users can authenticate using credentials or API keys and are granted appropriate permissions based on their roles and privileges.

•PCST supports role-based access control (RBAC), allowing administrators to define roles with specific permissions and assign users to these roles to control access to sensitive features such as campaign creation, reporting, and configuration.

2.4.4 APIs and Integration:•PCST provides APIs for programmatic access to its functionality, enabling integration with external systems, automation workflows, and custom applications.

•APIs are available for managing campaigns, templates, targets, results, and other aspects of the PCST application. They follow RESTful principles and use JSON for data exchange, providing flexibility and interoperability with various programming languages and frameworks.

2.4.5 Containerization and Deployment:

•PCST can be containerized using Docker for easy deployment and management in different environments. Docker containers encapsulate the application and its dependencies, ensuring consistency and portability across development, testing, and production environments.

•PCST supports deployment on various platforms, including on-premises servers, cloud infrastructure, and container orchestration platforms like Kubernetes. Deployment configurations can be customized to meet specific requirements for scalability, availability, and security.

2.4 Data Collection and Analysis:

Data collection and analysis are critical components of using PCST effectively to assess security awareness, identify vulnerabilities, and improve incident response readiness. Here's how data collection and analysis can be performed with PCST:

Data Collection:

- **Campaign Metrics**: PCST collects various metrics during phishing campaigns, including email opens, link clicks, and submitted credentials. These metrics provide insights into user engagement and susceptibility to phishing attacks.
- **Target Information**: PCST collects data on targeted individuals or groups, including email addresses, job titles, departments, and roles. This information helps in segmenting targets and tailoring phishing simulations to specific audiences.
- **Campaign Configuration**: Data related to campaign settings, such as email templates, landing pages, sending schedules, and payload configurations, are collected to understand the parameters of each phishing campaign.
- **User Responses**: PCST captures user responses to phishing emails, including interactions with landing pages, submission of credentials, and any other actions taken by recipients in response to simulated phishing attempts.
- **Reporting**: PCST generates comprehensive reports summarizing campaign results, including key metrics, graphs, charts, and detailed breakdowns of user responses. These reports provide stakeholders with actionable insights into the effectiveness of phishing simulations.

Data Analysis:

- **Metric Analysis**: Analyze campaign metrics such as email open rates, click-through rates, and conversion rates to assess user engagement and susceptibility to phishing attacks. Identify trends, patterns, and anomalies in the data to understand which types of phishing emails are most effective and which user groups are most vulnerable to attacks.
- **User Segmentation**: Segment users based on demographic information, job roles, departments, or other criteria to analyze how different groups respond to phishing attacks. Compare response rates and susceptibility levels between user segments to identify high- risk areas within the organization.
- **Vulnerability Identification**: Analyze campaign results to identify vulnerabilities in organizational email infrastructure, employee awareness, and incident response procedures. Look for common weaknesses such as employees clicking on suspicious links or submitting credentials to phishing websites.
- **Root Cause Analysis**: Conduct root cause analysis to understand why certain phishing attacks were successful and what factors contributed to their effectiveness. Identify gaps in security awareness training, email filtering, or incident response processes that need to be addressed to mitigate future risks.
- **Benchmarking**: Compare campaign results against industry benchmarks or previous assessments to gauge improvements in security awareness and resilience over time. Use benchmarking data to track progress and set realistic goals for future phishing simulations.

- **Feedback and Iteration**: Gather feedback from stakeholders, including users, security teams, and management, to identify areas for improvement in the PCST campaigns. Use feedback to refine campaign strategies, improve email templates, and tailor training programs to address specific vulnerabilities and weaknesses identified during analysis.
- **Continuous Improvement**: Continuously monitor campaign results and adjust strategies based on ongoing analysis and feedback. Implement iterative improvements to PCST campaigns, security awareness training, and incident response procedures to enhance overall security posture and resilience against phishing attacks.

User Training and Support:

User training and support for PCST are essential components to ensure effective utilization of the tool and maximize its benefits in enhancing organizational security awareness. Here's how user training and support can be provided for PCST:

Training Sessions:

- Conduct training sessions for users, administrators, and security personnel to familiarize them with PCST's features, functionalities, and best practices for conducting phishing simulations.
- Customize training sessions based on the roles and responsibilities of participants, covering topics such as campaign setup, target segmentation, email template design, and result analysis.
- Provide hands-on demonstrations and interactive exercises to give participants practical experience in using PCST to create and execute phishing campaigns.

III. RESULTS AND ANALYSIS

The results and analysis of PCST campaigns provide valuable insights into user behavior, susceptibility to phishing attacks, and the effectiveness of security awareness training efforts. Here's how you can interpret and analyze the results of PCST campaigns:

Email Engagement Metrics:

- **Open Rates:** Measure the percentage of recipients who opened the phishing emails. Low open rates may indicate that email subject lines or sender details need improvement.
- **Click-Through Rates (CTRs):** Calculate the percentage of recipients who clicked on links or attachments in the phishing emails. High CTRs suggest that recipients were persuaded to interact with the phishing content.

Landing Page Interactions:

- **Submission Rates:** Analyze the percentage of users who submitted information (e.g., entered credentials) on the phishing landing pages. High submission rates indicate successful phishing attempts and potential security vulnerabilities.
- **Time Spent:** Monitor the average time spent by users on phishing landing pages. Longer durations may indicate that users are engaged or confused by the content

Credential Harvesting:

- **Credentials Captured:** Identify the number and type of credentials (e.g., usernames, passwords) captured during the campaign. Assess the severity of the risk posed by compromised credentials and prioritize remediation efforts accordingly.

User Segmentation Analysis:

- **Departmental Analysis:** Segment campaign results by department or job role to identify high-risk areas within the organization. Compare response rates and susceptibility levels between different user groups to tailor security awareness training programs.

- **Geographic Analysis:** Analyze campaign results by geographic location to identify regional variations in phishing susceptibility and customize training initiatives accordingly.

Reporting and Visualization:

- **Graphical Representation:** Present campaign results using charts, graphs, and visualizations to facilitate data interpretation and decision-making. Visualize trends, patterns, and anomalies in campaign metrics to identify areas for improvement.
- **Comparative Analysis:** Compare campaign results against baseline metrics, industry benchmarks, or previous assessments to track progress and measure the effectiveness of security awareness initiatives over time.

Actionable Insights and Recommendations:

- **Risk Mitigation Strategies:** Develop actionable recommendations for mitigating identified risks and vulnerabilities, such as enhancing security awareness training, implementing multi-factor authentication, or improving email filtering mechanisms.
- **Training and Education:** Use campaign results to tailor security awareness training programs, phishing simulations, and educational materials to address specific areas of weakness and reinforce best practices among employees.
- **Policy and Procedure Enhancements:** Review and update organizational policies, procedures, and incident response plans based on insights gained from PCST campaigns to improve incident detection, response, and recovery capabilities.

IV. CONCLUSION

In conclusion, PCST stands as a robust and versatile phishing simulation tool that plays a crucial role in enhancing cybersecurity awareness and resilience within organizations. Throughout this project report, we have explored the evolution of phishing attacks, the importance of phishing awareness, and the need for effective simulation tools like PCST to mitigate risks and strengthen defenses. PCST offers a comprehensive suite of features and functionalities designed to streamline the process of creating, executing, and analyzing phishing campaigns. Its intuitive user interface, customizable templates, advanced targeting options, and powerful reporting capabilities empower organizations to conduct realistic and effective phishing simulations tailored to their specific needs and objectives. Through the implementation of PCST, organizations gain valuable insights into user behavior, susceptibility to phishing attacks, and areas of vulnerability within their infrastructure. By analyzing campaign results, identifying trends, and prioritizing remediation efforts, organizations can proactively address security gaps, enhance security awareness, and build a culture of cyber resilience. However, it's essential to acknowledge the challenges and limitations associated with PCST, such as legal and ethical considerations, technical expertise requirements, and platform limitations. By addressing these challenges and continuing to innovate, PCST can evolve to meet the emerging needs of organizations and adapt to evolving cybersecurity threats effectively. In the future, we envision PCST expanding its capabilities through integration with emerging technologies, automation features, and enhanced reporting and analysis tools. By embracing these future directions and staying true to its core mission of empowering organizations to defend against phishing attacks, PCST will continue to play a pivotal role in safeguarding digital assets and protecting against evolving cyber threats.

V. ACKNOWLEDGEMENT

We gratefully acknowledge some of the open-source projects on phishing tools for providing meteorological data, valuable information, and kind help for the completion of this study.

REFERENCE

1. CISA (Cybersecurity & Infrastructure Security Agency). (n.d.). Phishing. Retrieved from https://www.cisa.gov/phishing

2. Open Source Security Testing Methodology Manual (OSSTMM). (n.d.). Retrieved from http://www.isecom.org/mirror/OSSTMM.3.pdf

3. SANS Institute. (n.d.). SANS Security Awareness Phishing Resources. Retrieved from https://www.sans.org/security-awareness-training/resources/phishing

4. The National Institute of Standards and Technology (NIST). (n.d.). Phishing Campaign Assessment. Retrieved from https://www.nist.gov/itl/small-business-cybersecurity/phishing-campaign-assessment

5. Verizon. (2021). 2021 Data Breach Investigations Report (DBIR). Retrieved from https://www.verizon.com/business/resources/reports/dbir/

6. Women's Society of Cyberjutsu. (n.d.). Phishing Detection and Response. Retrieved from https://womenscyberjutsu.org/content.aspx?page_id=22&club_id=969866&module_id=321701

7. Wombat Security. (n.d.). State of the Phish. Retrieved from https://www.infosecinstitute.com/state-of-the-phish/