IBM Innovation Centre for Education

PHEMESOFT Software That Matters

YENEPOYA
(DEEMED TO BE UNIVERSITY)

YENEPOYA INSTITUTE OF ARTS, SCIENCE, COMMERCE AND MANAGEMENT
(A constituent unit of Yenepoya Deemed to be University)

PROJECT SYNOPSIS

Simulated Phishing Campaign for Employee Training

BACHELOR OF COMPUTER APPLICATION
(IoT, Ethical Hacking, Cyber Security and Digital Forensics)

SUBMITTED BY:-
NAME: Hizan Rahman
REG NO: 22BCIECS042
LH-28

GUIDED BY:
Mr. Shashank – IBM SME

INDEX

INTRODUCTION:

Phishing attacks are one of the most prevalent and effective cyber threats, targeting employees to gain unauthorized access to confidential data. These attacks often involve fraudulent emails, messages, or websites that mimic legitimate sources to deceive users into revealing sensitive information, such as passwords, financial details, or company secrets. Many organizations face security breaches due to a lack of employee awareness and preparedness. Traditional training methods often fail to engage employees effectively, leading to poor knowledge retention.

This project aims to develop a simulated phishing campaign to educate employees on different phishing tactics, strengthen their awareness, and reduce susceptibility to cyber threats. By providing hands-on experience through real-world phishing scenarios, employees will become more vigilant in recognizing and avoiding potential cyber threats.

LITERATURE SURVEY:

Research studies indicate that phishing attacks account for a significant portion of cybersecurity breaches, with an increasing number of sophisticated phishing campaigns being reported globally. Various cybersecurity reports from organizations such as **Verizon** and **IBM** highlight that human error is one of the leading causes of security incidents. Traditional cybersecurity awareness programs often rely on lectures, presentations, and policy documents, which may not effectively engage employees.

Simulated phishing campaigns have emerged as a more effective solution, offering interactive and practical learning experiences. Companies that implement simulated phishing tests and continuous awareness programs have seen a marked reduction in successful phishing attempts. Studies suggest that repeated exposure to phishing simulations helps employees build better recognition patterns and response mechanisms, ultimately improving overall cybersecurity resilience within an organization.

METHODOLOGY:

The simulated phishing campaign will be executed in the following phases:

1. **Requirement Analysis:** Identify various phishing techniques such as spear phishing, whaling, smishing, and vishing. Research common attack methods and their impact on organizations to design realistic phishing scenarios.
3. **Design & Development:** Develop a simulated phishing campaign that mimics real phishing attacks. The campaign will include multiple phishing email templates, malicious website replicas, and fake login pages to test employee responses.

4. **Analysis & Reporting:** Assess employee susceptibility to phishing attacks by analyzing collected data. Generate reports detailing employee performance, common mistakes, and areas requiring improvement.
5. **Training & Awareness:** Assess employee susceptibility to phishing attacks by analyzing collected data. Generate reports detailing employee performance, common mistakes, and areas requiring improvement.

FACILITIES REQUIRED:

Software Tools:

- **Social Engineering Toolkit (SET):** To simulate social engineering attacks and phishing scenarios.
- **Phishing Frenzy:** To automate and manage phishing campaigns effectively.
- **Wireshark:** For network analysis and monitoring user responses during simulations.

Networking:

A secure and stable internet connection to facilitate the deployment and tracking of phishing campaigns.

Human Resources:

A dedicated team of cybersecurity experts, developers, content creators, and analysts to design, implement, and monitor the simulated phishing campaign.

REFERENCES:

- **[1] Mitnick, K. D., & Simon, W. L. (2002).** ***The Art of Deception: Controlling the Human Element of Security*****. John Wiley & Sons.**
- **[2] Hadnagy, C. (2010).** ***Social Engineering: The Art of Human Hacking*****. Wiley.**
- **[3] NIST, SANS, and OWASP REPORTS.**