**1. Overview & Objective**

This report outlines the execution of a simulated phishing campaign designed to assess employee awareness and improve organizational security training. The goal was to identify susceptibility to social engineering attacks using phishing emails.

**2. Scope & Tools Used**

The simulation targeted employees across various departments within the organization. The primary tool used was the Social Engineering Toolkit (SET) on a Kali Linux environment. The campaign focused on email-based credential harvesting using cloned login pages.

**3. Methodology & Commands Used**

**Step-by-Step Process with Commands:**

**Step 1: Launch SET**

sudo setoolkit

**Step 2: Navigate SET Menu**

1) Social-Engineering Attacks

2) Website Attack Vectors

3) Credential Harvester Attack Method

2) Site Cloner

**Step 3: Clone Target Site**  
Enter a URL to clone (Google):

**https://accounts.google.com**

Then, provide your local or external IP address to host the phishing page.

**Step 4: Send Phishing Email via SET Mass Mailer**  
Navigate to:

**1)** Social-Engineering Attacks

**5)** Mass Mailer Attack

Use this module to craft and send realistic phishing emails that contain links to your cloned login page.

**Step 5: Monitor and Collect Data**  
Harvested credentials and logs are stored in:

/var/www/html

/root/.set/reports

**4**. **Phishing Email Design**

Emails were crafted to appear as legitimate password reset requests from the IT department. The email contained a call to action and a link to the cloned site, urging users to 'verify' their account credentials.

**6. Results & Analysis**

* Emails Sent:
* Open Rate:
* Click Rate:
* Credential Submissions:

Common behavior: Users clicked links within minutes of receiving the email.

Logs were analyzed to determine peak interaction times and common departments vulnerable to phishing.

7. **Key Findings**

* A notable percentage of users clicked on suspicious links.
* Some employees submitted their login credentials.
* Lack of awareness about phishing indicators was evident.
* Technical controls like MFA and email filters were either absent or insufficient.

**8. Recommendations**

* Introduce mandatory phishing awareness training.
* Implement technical controls such as SPF, DKIM, and DMARC.
* Enforce organization-wide Multi-Factor Authentication (MFA).
* Conduct regular phishing simulations to reinforce awareness.
* Establish a protocol for reporting suspected phishing emails.

**Conclusion**

This phishing simulation highlighted key vulnerabilities in employee awareness and technical defenses. By acting on the provided recommendations, the organization can greatly reduce its exposure to real-world phishing threats.