Experiment 3: Simulating a Phishing attack and detection

Aim:

To simulate a phishing attack in a controlled environment and implement detection techniques to identify and mitigate phishing attempts.

Objectives:

1. To understand the concept of phishing and its impact on users
2. To simulate a phishing email or webpage to study attacker methodology
3. To analyse phishing indicators such as suspicious URLs, sender spoofing, and abnormal requests
4. To use tools and techniques for detecting phishing attempts
5. To create awareness about prevention strategies against phishing

Tools Required:
1. Kali linux (for creating phishing pages with tools like SET- Social Engineering Toolkit)
2. Browser (to test phishing webpage)
3. Email Client (to simulate phishing email delivery)
4. Wireshark (optional- for monitoring traffic)
5. URL scanning tools (e.g., VirusTotal, PhishTank)

Algorithm:
1. Start Kali Linux and launch the Social Engineering Toolkit (SET)
2. Select the Social Engineering Attacks option
3. Choose Website Attack Vectors and then Credential Harvester Attack Method
4. Clone a legitimate login page (e.g., Gmail, Facebook- only for educational/demo purposes)
5. Host the cloned page on the local machine
6. Access the phishing page via browser to simulate victim interaction
7. Enter dummy credentials on the phishing page.
8. Observe and capture the credentials on the attacker's terminal
9. Use URL analysis tools (VirusTotal/PhishTank) to test detection of the phishing URL
10. Demonstrate how awareness and automated detection prevent phishing success.

Procedure:

1. Setup Environment

- Launch Kali Linux in VirtualBox/VMware. This ensures a safe, isolated environments

2. Start SET tool:

- Open terminal and type:

Sudo setoolkit

This loads the Social Engineering Toolkit used for phishing simulations

3. Select Attack Type:

- Choose 1) social Engineering Attacks 2) Website Attack Vectors 3) Credential Harvester
- This prepares a fake login page to capture credentials

4. Clone Target Website

- Enter a URL of a legitimate site (e.g., https://accounts.google.com) for cloning
- The tool creates a phishing replica of the page

5. Host Phishing Page:

- The cloned page is hosted locally (e.g., http://192.168.1.100)

6. Simulate Victim Access

- Open the phishing URL in a browser and enter dummy credentials
- SET captures the entered username and password in terminal

7. Detection Phase:

- Use wireshark to analyse unusual traffic redirections
- Paste the Phishing URL in VirusTotal or PhisTank to check blacklistin

8. Prevention Measures

- Demonstrate awareness steps:
- Checking SSL certificates
- Hovering over links to reveal suspicious domains
- Using browser phishing filters

Sample Output

1. Screenshot of SET terminal capturing credentials
2. Screenshot of phishing page opened in browser
3. Screenshot of VirusTotal/PhisTank flagging the phishing URL

Result

Phishing attack was successfully simulated and credentials were captured using the cloned webpage and the phishing attempt was detected through URL scanning tools and traffic analysis.

Innovative Approach

Students extend this experiment by developing a browser script/extension that automatically warns user when suspicious domains or non- HTTPS login pages are visited, bridging awareness with technical defense.

Pre-Viva Questions

1. What is Phishing and why it is dangerous?
2. What are common signs of a phishing email or webpage?
3. Name any two tools used for simulating phishing attacks.
4. How does HTTPS help in preventing phishing?
5. What is the role of user awareness in phishing prevention?

Post –Viva Questions

1. How were credentials captured during the phishing simulation?
2. What differences did you notice between the phishing page and the original?
3. How can phishing URLs be detected automatically?
4. Why is phishing considered a social engineering attack?
5. Suggest two real-world mitigation strategies against phishing?