**Social Engineering Attack Project: Credential Harvesting via Phishing Introduction to Social Engineering**

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybersecurity, attackers use psychological tactics to trick individuals into divulging confidential information or performing actions that compromise security. These attacks often involve phishing emails, deceptive websites, or impersonation to achieve their objectives.

**Objective of the Attack**

The primary goal of this project is to demonstrate how a social engineering attack can be executed using the Credential Harvester method. This involves setting up a fake website to collect user credentials and crafting a phishing email to lure the victim into entering their information.​

**Tools and Environment**

* **Operating System**: Kali Linux​
* **Tool**: Social Engineering Toolkit (SET)​
* **Target**: Unsuspecting user with a Gmail account​

**Step-by-Step Attack Execution**

**Step 1: Setting Up the Credential Harvester**

1. **Launch Kali Linux**: Boot into the Kali Linux environment.​
2. **Open SET**: Navigate to the Social Engineering Toolkit.​

A screenshot of a computer

AI-generated content may be incorrect.

1. **Select Attack Type**:
   * Choose "Social Engineering Attacks" (Set 1).​

A screenshot of a computer

AI-generated content may be incorrect.

1. **Choose Attack Vector**:
   * Select "Website Attack Vectors" (Set 2).​

A screenshot of a computer

AI-generated content may be incorrect.

1. **Select Attack Method**:
   * Choose "Credential Harvester Attack Method" (Set 3).​

A screenshot of a computer

AI-generated content may be incorrect.

1. **Select Site Cloning Method**:
   * Opt for "Web Templates" (Set 1).​

A screenshot of a computer

AI-generated content may be incorrect.

1. **Configure IP Address**:
   * The tool will automatically detect and set your Kali Linux IP address. Press Enter to confirm.​
   * If you have the IP address for the fake website you want the user to be directed to, you can also use this

A screenshot of a computer

AI-generated content may be incorrect.

1. **Choose Website Template**:
   * Select "Google" (Set 2) to clone the Google login page.​

A screenshot of a computer

AI-generated content may be incorrect.

The tool will now host a fake Google login page on your Kali Linux machine, waiting for victims to access it.​

A screenshot of a computer screen

AI-generated content may be incorrect.

**Step 2: Crafting the Phishing Email**

1. **Open Gmail**: Log into your Gmail account.​
2. **Change Display Name:**

Go to settings and navigate to Accounts and Import, then click edit info on send email as and change display name to “**Google Support**” so this doesn’t raise suspicion when the victim receives the email

1. **Compose a New Email**:
   * **Subject**: "Urgent: Google Account Suspension Notice"​
   * **Body**:

Dear Spectre,

Your Google account has been suspended due to suspicious activity. Click the link below to unlock it. If you do not respond within 24 hours, your account will be permanently deleted.

Sincerely,

Google Support Team

**Step 3: Embedding the Malicious Link**

1. **Inspect Email Content**:
   * Right-click on the email body and select "Inspect" to open the developer tools.​

A screenshot of a computer

AI-generated content may be incorrect.

1. **Edit as HTML**:
   * Locate the section containing the email text.​
   * Modify the HTML to embed the malicious link:​

html

CopyEdit

<a href="http://172.30.147.114">here</a>

* + This creates a hyperlink labelled "here" that directs the victim to the fake login page hosted on your Kali Linux machine.​

A computer screen with text on it

AI-generated content may be incorrect.

A white background with black text

AI-generated content may be incorrect.

**Step 4: Sending the Phishing Email**

* Send the crafted email to the target user.​

**Step 5: Harvesting Credentials**

* Monitor the SET tool's terminal for incoming connections.​
* When the victim clicks the link and enters their credentials on the fake page, the information will be captured and displayed in your terminal.​

A screenshot of a computer

AI-generated content may be incorrect.

**5. Conclusion**

This project illustrates how social engineering attacks exploit human psychology rather than technical vulnerabilities. By creating a convincing phishing email and a realistic fake login page, attackers can deceive users into revealing sensitive information. Understanding these tactics is crucial for developing effective cybersecurity awareness and defence strategies.