**Social Engineering Simulation Report**

**1️ Objective**

The goal of this task was to understand how social engineering attacks (specifically phishing) are performed and how to simulate them safely using the **Social-Engineer Toolkit (SET)**.  
This helps highlight the human factor in cybersecurity and develop practical defensive measures.

**2️ Tools Used**

* **Social-Engineer Toolkit (SET)** — open-source Python toolkit for social engineering simulations.
* **Virtual Machine** — Kali Linux or Parrot OS for ethical testing.
* **Test victim** — a separate virtual machine or browser to test the phishing page.

**3️ Attack Simulation**

**✅ Steps Performed:**

1. **Installed SET**
2. sudo apt update
3. sudo apt install set
4. **Launched SET**
5. sudo setoolkit
6. **Selected attack method:**
   * 1. Social-Engineering Attacks
     2. Website Attack Vectors
     3. Credential Harvester Attack Method
     4. Site Cloner
7. **Cloned a real website:**  
   Example: [https://accounts.google.com](https://accounts.google.com/)
8. **Hosted the fake site locally:**
   * Entered my local IP address for the phishing server.
   * SET created and served the cloned page.
9. **Visited the phishing page on a test machine:**
   * Submitted fake credentials.
   * Verified that credentials were captured and displayed in the SET terminal.

**4️Observation**

* The cloned page looked identical to the real login page.
* If a user did not carefully check the URL, they could easily be tricked.
* All entered credentials were captured in plain text.

**5️ Countermeasures**

|  |  |  |  | **Defense** | **Description** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| 1️ |  |  |  | **Multi-Factor Authentication (MFA)** | Even if credentials are stolen, attackers cannot log in without the second factor. |
| 2️ |  |  |  | **Email Security Gateways** | Block suspicious phishing emails using advanced filters. |
| 3️ |  |  |  | **SPF, DKIM, DMARC** | Prevent attackers from spoofing trusted domains. |
| 4️ |  |  |  | **User Awareness Training** | Educate staff to check sender addresses, hover over links, and report suspicious emails. |
| 5️ |  |  |  | **Web/DNS Filtering** | Block access to newly registered or suspicious domains. |
| 6️ |  |  |  | **SIEM Monitoring** | Detect unusual login behavior and brute-force attempts. |
| 7️ |  |  |  | **Clear Reporting** | Ensure employees know how to report phishing attempts quickly. |

**6️ Lessons Learned**

* Social engineering is **often the easiest attack vector** — technology alone cannot stop it.
* Simulating phishing helps organizations test real awareness.
* Countermeasures must combine **technical controls**, **employee training**, and **process improvements**.

**7️ Files Attached**

* Screenshots of:
  + SET menu.
  + Cloned phishing page.
  + Terminal output showing captured data.

**8️ Conclusion**

This lab demonstrated the risk of phishing and credential harvesting in a **safe lab environment**. It showed how attackers can easily trick untrained users and why **multi-layered defense** is critical for real-world organizations.