### **Lab 1- Credential Harvesting Using Site Cloning Lab**

**What Was Learned:**This lab provided a practical understanding of how attackers can harvest user credentials through a cloned website. By using the Social Engineering Toolkit (SET), the process of creating a convincing phishing attack and capturing sensitive information like usernames and passwords was demonstrated.

**Key Learnings:**

1. **Cloning Websites for Phishing:**
   * Learned how attackers replicate legitimate websites to create deceptive login pages.
   * Observed how cloned sites can convincingly mimic trusted brands, increasing the likelihood of user interaction.
2. **Using the Social Engineering Toolkit (SET):**
   * Gained hands-on experience with SET, a tool that automates the creation of phishing sites.
   * Configured the tool to clone a target website by entering the local machine’s IP address and the site’s URL.
3. **Capturing and Analyzing Credentials:**
   * Discovered how POST requests from a cloned site are logged in SET.
   * Retrieved plaintext usernames and passwords from the tool's terminal output.

**Takeaways:**

* **Awareness of Phishing Risks:** Highlighted the ease with which attackers can clone websites, emphasizing the importance of cautious web browsing.
* **Technical Insight:** Gained a deeper understanding of how phishing tools operate, including their reliance on social engineering techniques.
* **Ethical Practices:** Recognized the importance of ethical use of such methods for identifying vulnerabilities and strengthening cybersecurity defenses.

This lab reinforced the need for education and technical defenses to protect against credential harvesting attacks.