-

**TTSET GLOBAL**

**CREDENTIAL HARVESTING ETICAL HACKING**

July 30,2025

**NKENYI JOYCELINE .N**

TTSET25G030

**CYBERSECURITY**

**Mr. Tante**

This project demonstrates a phishing attack using SEToolkit on Kali Linux by cloning websites

Like Facebook and Google .It highlights the attack setup, execution, risks involved, and methods to prevent phishing.

Table of Contents

[Table of contents](#_Toc204967992) **[1.](#_Toc204967992)**

[1.1. Title 1](#_Toc204967993)**[.](#_Toc204967993)**

[1.2. Objective](#_Toc204967994) **[1.](#_Toc204967994)**

[1.3 .Lab Setup](#_Toc204967995) **[1.](#_Toc204967995)**

[1.4. Tools used 1](#_Toc204967996)**[.](#_Toc204967996)**

[1.5. Execution steps](#_Toc204967997) **[1.](#_Toc204967997)**

[1.6. Output examples](#_Toc204967998) **[1.](#_Toc204967998)**

[1.7. Risks 1](#_Toc204967999)**[.](#_Toc204967999)**

[1.8. Defense Mechanisms](#_Toc204968000) **[1.](#_Toc204968000)**

[1.9. Solution](#_Toc204968001) **[1.](#_Toc204968001)**

**1.2. Objective**

This report explains the phishing attack demonstration we carried out in class using Kali Linux and the Social-Engineer Toolkit (SEToolkit). The purpose of the exercise was to understand how attackers use phishing techniques to trick users into revealing their credentials and how we can identify and prevent such attacks.

**1.3. Lab Setup**

The phishing attack demonstration was conducted in a controlled lab environment using virtual machines and isolated networks to ensure no real systems or data were affected. The setup included the following components:

**1.3.1. Hardware & Virtualization**

A host computer with at least 8 GB RAM and 50 GB storage.

VirtualBox (or VMware) installed on the host computer to run virtual machines.

**1.3.2. Virtual Machines**

* Kali Linux (Attacker Machine): Used as the primary attack platform.
* Pre-installed with penetration testing tools, including the Social-Engineer Toolkit (SEToolkit).
* Assigned a local network IP address (e.g., 192.168.x.x).

**Victim Environment:**

* A browser on the host machine or a separate virtual machine (e.g., Windows 10).
* Used to simulate a victim accessing the cloned phishing pages.

**1.3.3. Network Configuration**

* VirtualBox NAT or Bridged Adapter network configuration to ensure the attacker machine and victim environment could communicate internally.
* All activity was restricted to the lab environment to prevent accidental exposure to the internet.

**Note:** The phishing experiment was conducted using Kali Linux in VirtualBox on a host machine. SEToolkit was used as the main tool, and a cloned Google/Facebook login page was served locally using an IP address from ifconfig. The phishing link was accessed within the same machine using a web browser.

**1.4. Tools Used**

* Kali Linux
* Social-Engineer Toolkit
* VirtualBox
* Chrome Browser
* Visual Studio Code

**1.5. Executive Steps**

⚠ All actions were performed under supervision with written approval as part of the internship training. No real systems or data were targeted.

The steps followed are listed below:

**Step 1: Launch SEToolkit**

* + Opened Kali Linux terminal.
  + Navigated into the toolkit folder: cd social-engineer-toolkit
  + Started the toolkit: sudo setoolkit
  + Accepted terms and waited for the **SET>** prompt

**Step 2: Selected Attack Type**

* Chose option 1: Social Engineering Attacks
* Then chose the option 2: Website Attack Vectors
* Then followed by option 3: Credential Harvester Attack Method
* Finally, chose option 2 : Site Cloner for Facebook for Google

**Step 3: Cloned a Legitimate Website**

* Entered the IP address of the Kali Linux machine.
* Entered the URL of the site to clone:

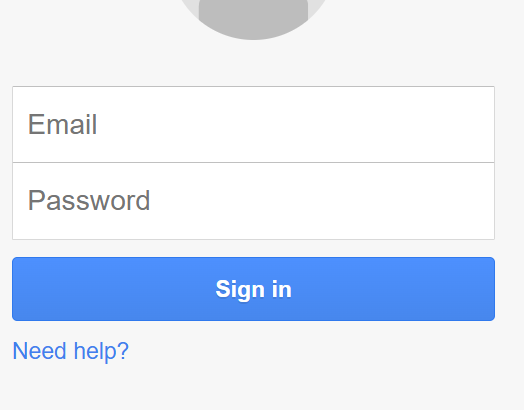
**Google login**: **<https://.google.com>**

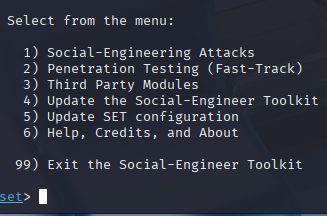
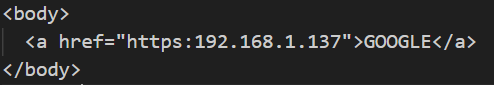
**Facebook login**: https://facebook.com

* SEToolkit cloned the selected website to our machine.

**Step 4: Capture Test Credentials**

* When a test user entered dummy credentials on the cloned page, the credentials were captured by SEToolkit and displayed in the terminal log.
* This showed us how attackers can steal login details using phishing techniques.

**1.6. Output Examples**



Clone login page

SEToolkit menu Google Form



The captured Credentials

**1.7. Risks**

* During the demonstration, we learned how to distinguish legitimate websites from fake ones.
* Check the URL/domain carefully: Attackers often use misspelled domains or extra words (e.g., gooogle-login.com), so avoid look-alike domains and misspellings
* Don’t rely on HTTPS alone: Fake sites can also use SSL certificates too.
* Look for design inconsistencies: Poor logos, broken links, or unusual layouts are warning signs.
* Use password managers: They only auto-fill on the correct domain ie, they do not auto-fill credentials on fake sites.

**1.8. Defense Mechanisms**

* Do not click suspicious links; type the address manually.
* Enable multi-factor authentication (MFA) on all accounts.
* Use a password manager to detect fake domains.
* Report suspicious emails or links to the IT/security team.
* Always verify a website’s URL before entering credentials.

**1.9. Conclusion**

This internship exercise gave me hands-on exposure to phishing techniques, helping me understand how attackers trick users and how to prevent such attacks. The knowledge gained will help me recognize phishing attempts, secure systems, and educate others on safe online practices.