Cyber Security: Lab 4: Social Engineering

Social Engineering

The term **"social engineering"** is derived from the words **"social"** and **"engineering,"** where **"social"** refers to personal, professions, and our day-in-day-out lives. On the other hand, **"engineering"** involves comprehensive processes to complete a work such that the defined goal is met. In other words, it is a set of methods.

When social and engineering is combined, we get social engineering, which involves intrusion based on human interaction. It is a non-technical intrusion in which a person is often tricked into breaking the general security guidelines already set in an institution.

**Social Engineering Toolkit**

Social engineering toolkit is a **free and open-source tool** which is used for social engineering attacks like **phishing, sending SMS, faking phone,** etc. It is a free tool that comes with Kali Linux, or we can download and install it directly from **Github.** The Social Engineering Toolkit is designed and developed by a programmer named **Dave Kennedy.** Security researchers and penetration testers use this tool to check cybersecurity issues in systems all over the world. The goal of the social engineering toolkit is to perform attacking techniques on their machines. This toolkit also includes website vector attacks and custom vector attacks, which allow us to **clone any website, perform phishing attacks.**

**Features of Social Engineering Toolkit**

The following are the features of the social engineering toolkit:

* Social Engineering Toolkit is **free** and **open source.**
* Social Engineering Toolkit is portable, which means we can quickly switch attack vectors.
* Social Engineering Toolkit supports integration with third-party modules.
* Social Engineering Toolkit is already installed in our Kali Linux, but we can also download and install it from **Github.**
* Social Engineering Toolkit is a **multi-platform** tool; we can run it in **Windows, Linux,** and **Unix.**
* Social Engineering Toolkit contains access to the **Fast-Track Penetration Testing platform.**
* Social Engineering Toolkit offers various attack vectors like **Website Attacks, Infection Media Generator, Website Attacks,** etc.

**Uses of Social Engineering Toolkit**

There are various uses of social engineering toolkit:

1. Web Attack
2. Mass Mailer Attack
3. Phishing Attacks
4. Create a Payload and Listene

Example of Google Phishing page- one kind of social engineering attack done through fake links over mail, sms)

Perform Google and Twitter Phishing

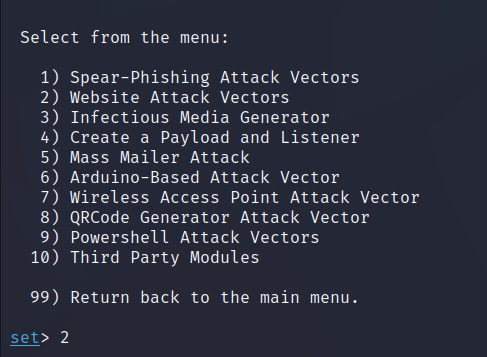
# Working with Social Engineering Toolkit in Kali Linux.

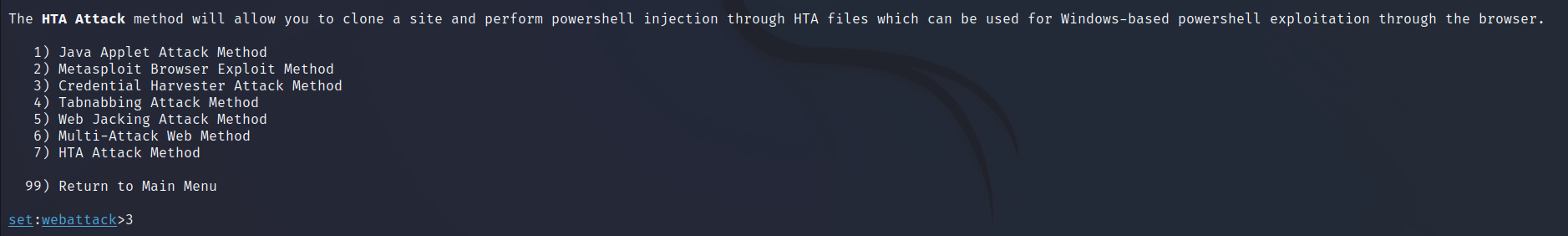
## Activity-1: Clone Google and Twitter homepage using *set*.

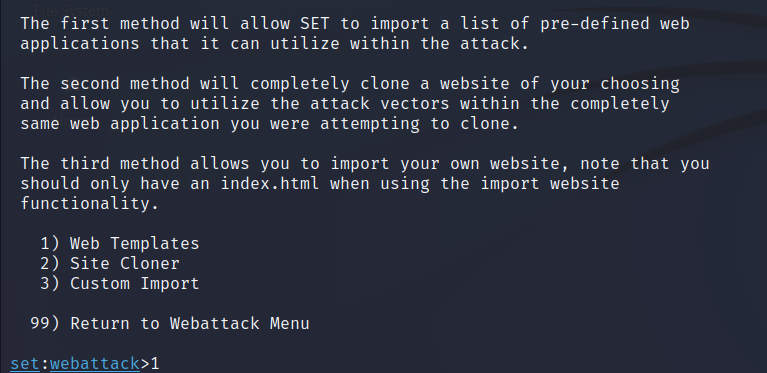
## Open Kali linux

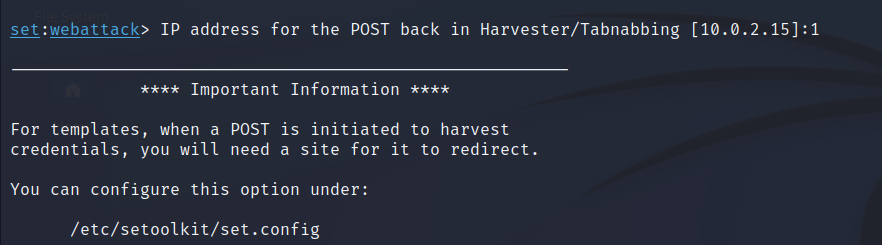
## Go to Applications-> Social Engineering Tools-> Social Engineering Tool Kit (root)

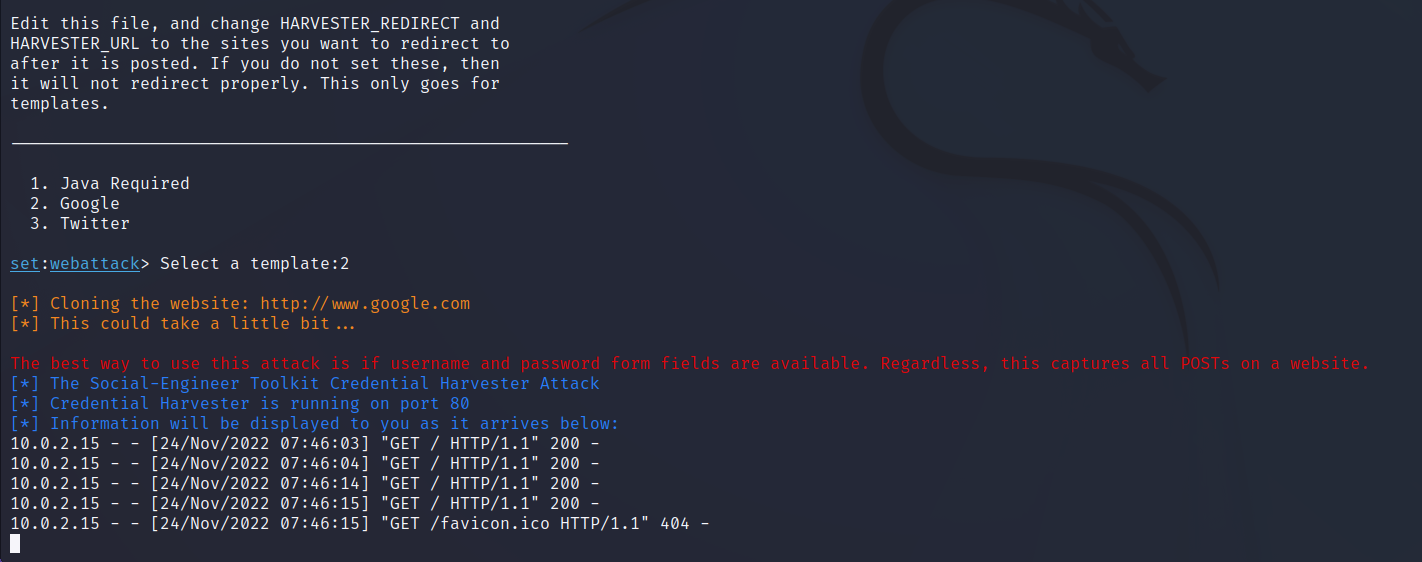
## Password for kali: kali











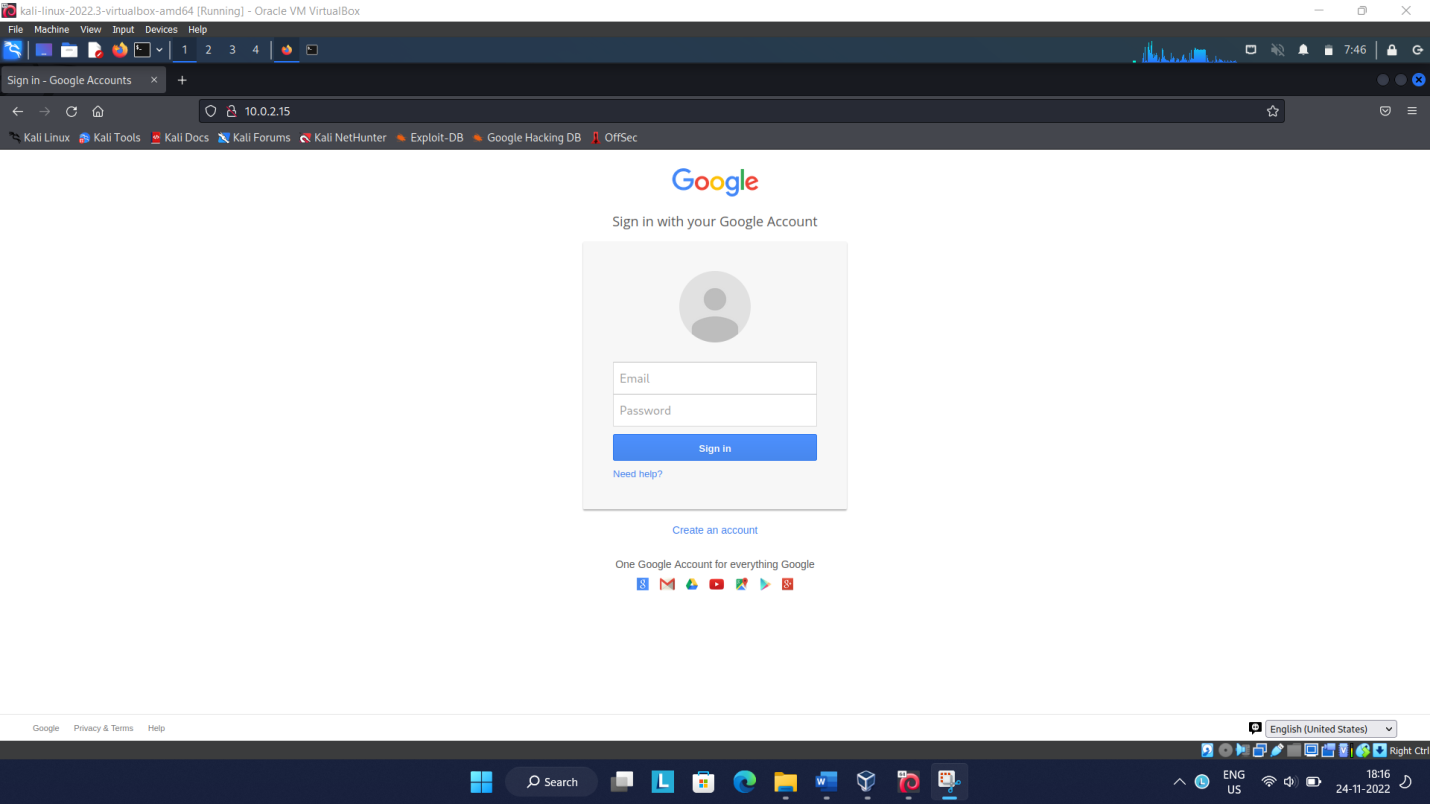


Image 1: cloned Google Sign In page

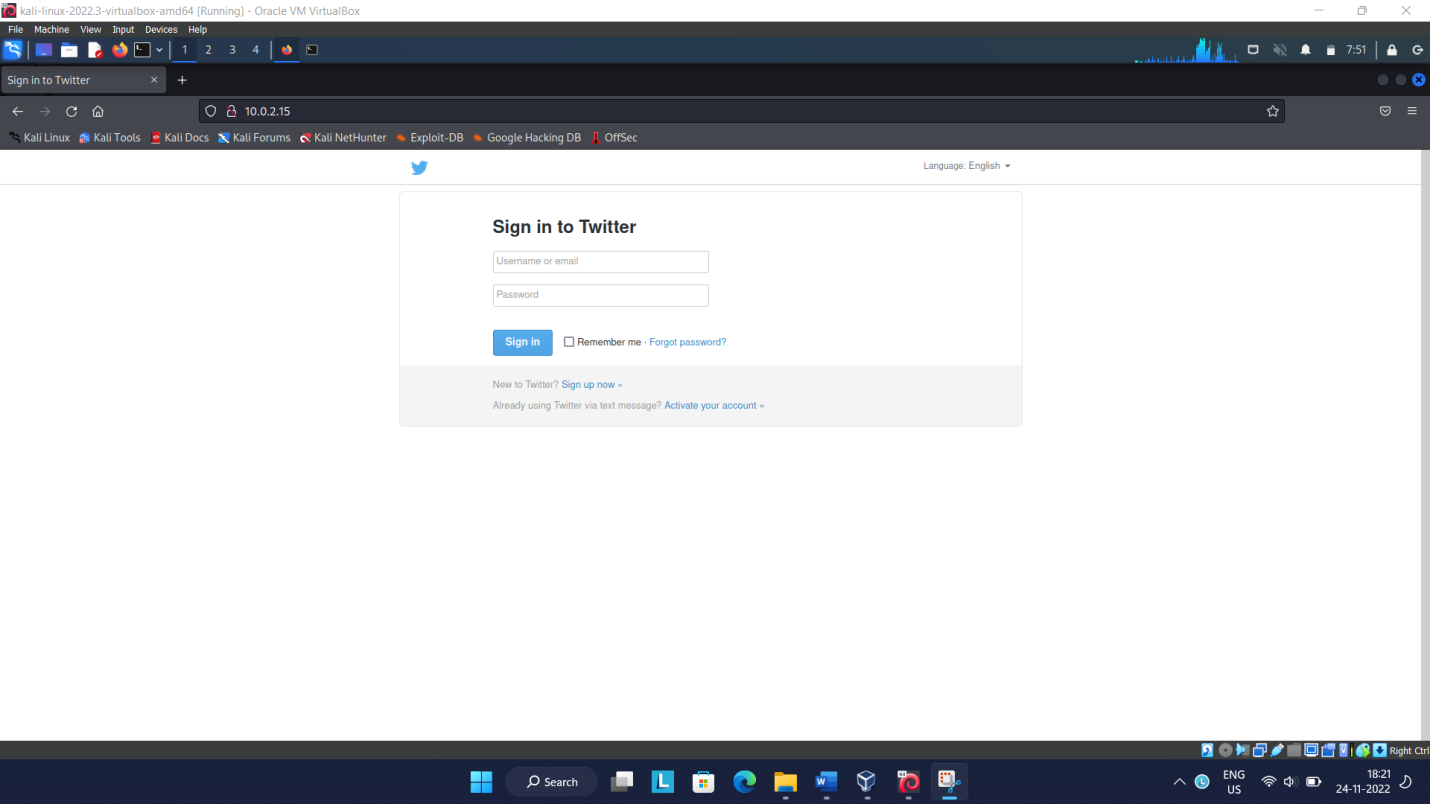


Image 2: Cloned Twitter Sign In page