|  |  |
| --- | --- |
| **Ex. No. 6** | **Phishing using Social Engineering Tool** |
| **Date of Exercise** | 11/10/23 |

**Aim:**

The objective of this experiment is to obtain target credentials of social accounts using Social Engineering Toolkit.

**Description:**

Social Engineering Toolkit is a preinstalled tool available in Kali, a linux distributed OS. The Social-Engineer Toolkit (SET) was created and written by Dave Kennedy, the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET provides an interface using a menu with options to choose from. It allows selecting particular attacks in areas such as spear-phishing, mass mailing, WiFi, QR, and more. Based on the selected attack it will ask for related details. The provided input is then used by SET to start a tool like Metasploit to initiate the related attack.

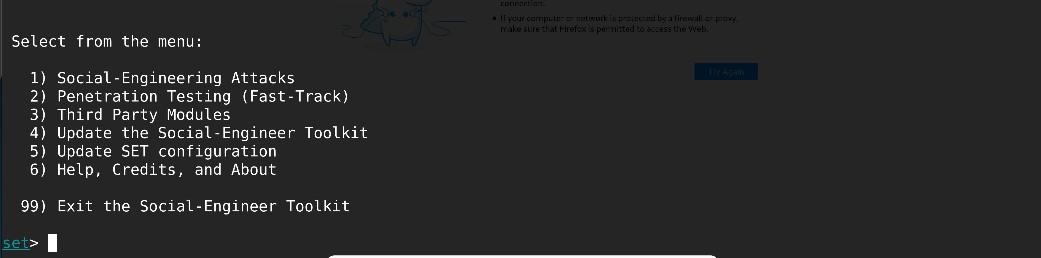
**Steps:**

SET can be used in Kali machine in a virtual machine, for experiment purpose the target machine can be our host machine or directly open the link from browser in Kali.

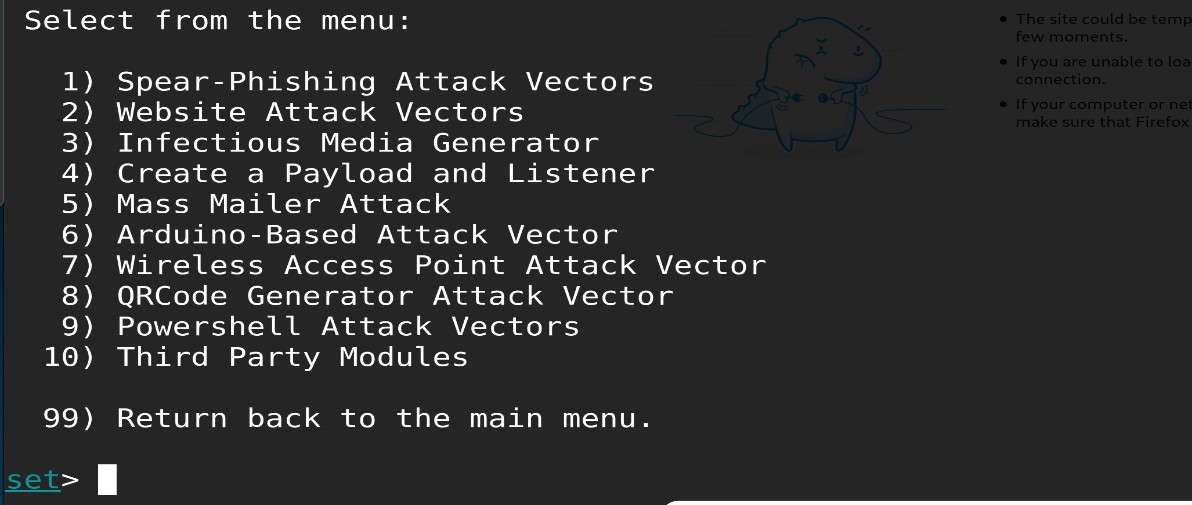
Step 1. Open Kali in Virtual Box.

Step 2. Open Social Engineering Toolkit (SET) from application menu or use setoolkit command in terminal.

Step 3. Select 1. Social Engineering in options.



Step 4. Select 2 for Website Attack Vendors



Step 5. Select 3 for Credential Harvester.

Step 6. Select 2 Site Cloner

Step 7. Enter the IP address for listening, the IP address for the listening host can be found using ifconfig in new tab, use inet for listening host.

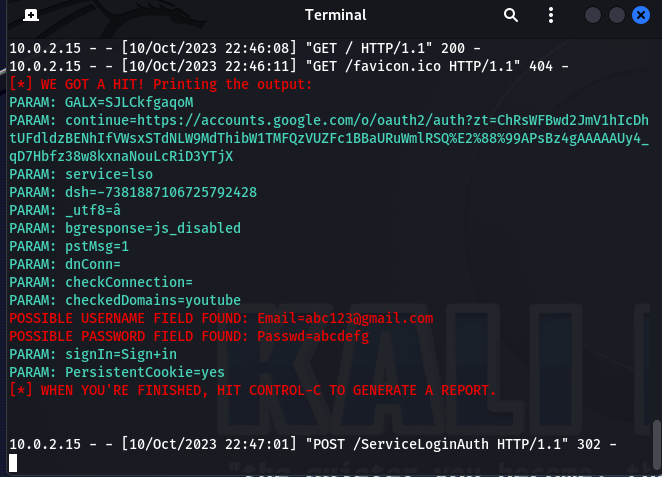
Text  Description automatically generated

Step 8. Enter the URL for site cloning, in this experiment we are using facebook login page.

Step 9. When the above page appears, set started to steal credentials, to open the phishing site, type the listening IP address in the browser.

**Output:**

Phishing page loaded in the Target browser.



Phished Credentials appear in the terminal.

**Result:**

We have successfully cloned Facebook login page and used it for phishing the details of user.