Credential Harvesting Using Site Cloning (SET)

Lab Objective: Learn how to harvest credentials using a cloned website.

Lab Purpose: Credential harvesting is the process of gathering sensitive information on a target—such as passwords or the answers to secret questions—without them knowing that this information is being captured.

Lab Tool: Kali Linux Lab

Topology: You can use Kali Linux in a virtual machine for the purpose of this lab.

Lab Walkthrough:

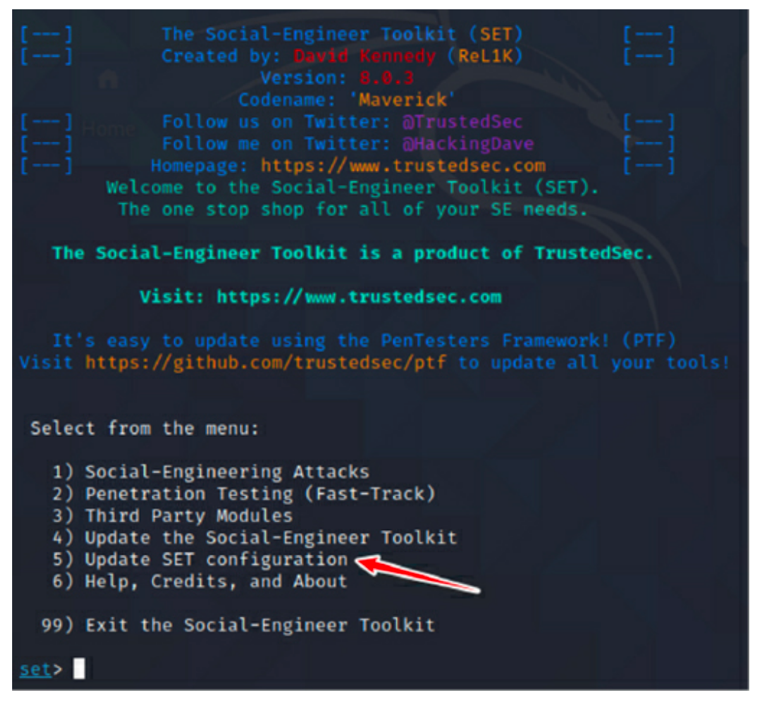
*Task 1:*

The first step is to boot your virtual machine and get Kali Linux up and running. Once this is complete, open a terminal and start the “SET: Social Engineering Toolkit” by typing as “root” user:

setoolkit

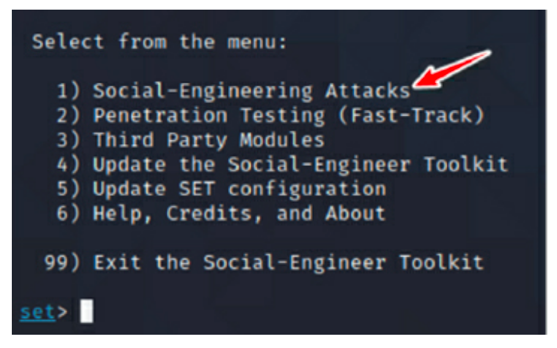
When “Do you agree to the terms of service [y/n]” message appears, type “Y”.

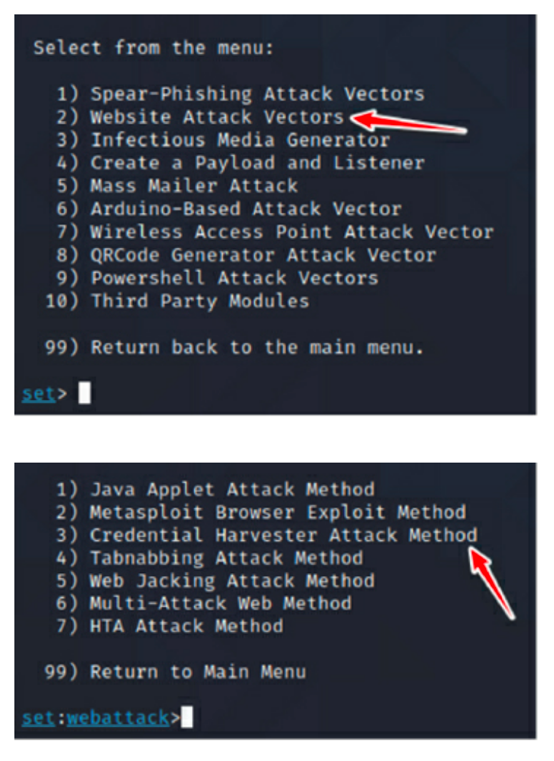
First, update SET utility to get latest features. Choose option 5.



*Task 2:*

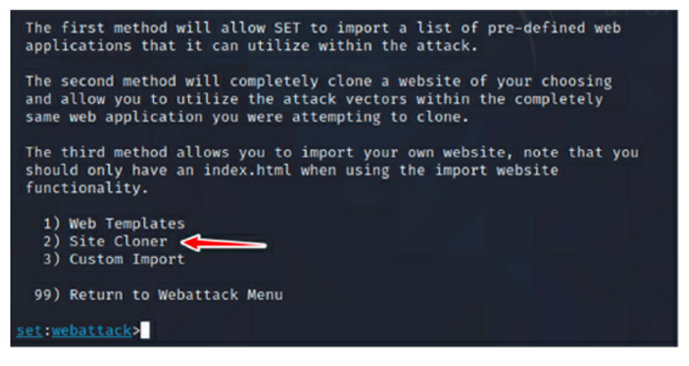
From the main menu, choose option 1 for “Social-Engineering Attacks”, then choose option 2 to select “Website Attack Vectors”. You will then be presented with the following screen asking you which kind of website attack you want to conduct. Choose option 3, the “Credential Harvester Attack Method”.



**

*Task 3:*

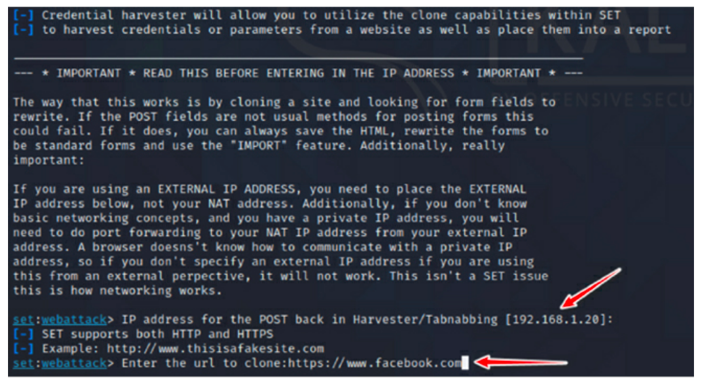
The next menu will ask you which method you’d like to choose to harvest a victim’s credentials. We will be cloning a site in this lab, so choose option 2 “Site Cloner”.

**

*Task 4:*

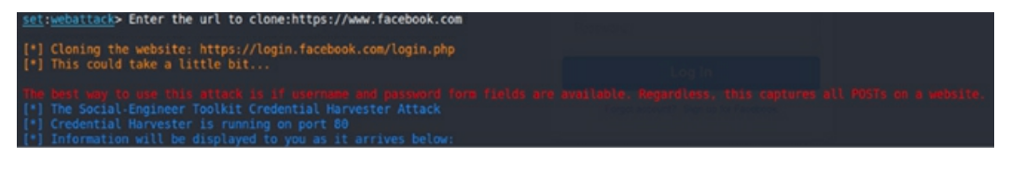
SET will ask you for your IP address so that it can send the POST requests from the cloned website back to your machine. Normally, SET can detect your IP address automatically. If your Kali node has many IP addresses, you can find the desired one by opening a new terminal and typing “ifconfig”.

Once you tell SET that you would like to clone a website, it will then ask you for the URL of the site you wish to clone. You can enter any site you like. For this lab, I will be using https://www.facebook.com.

**

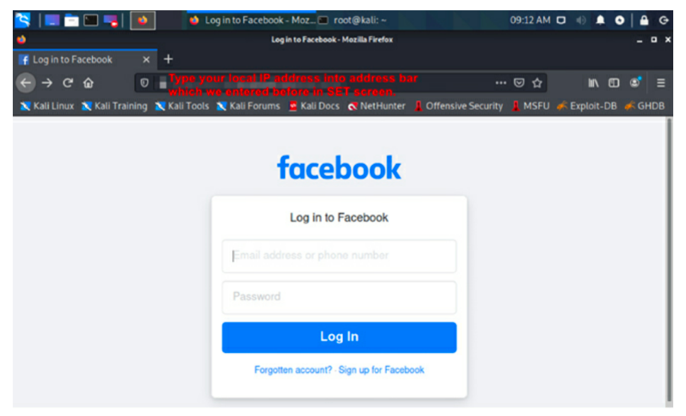
*Task 5:*

Once the URL is entered, SET will clone the site and display all the POST requests of the site back to this terminal. It is now time to navigate to the cloned site.

**

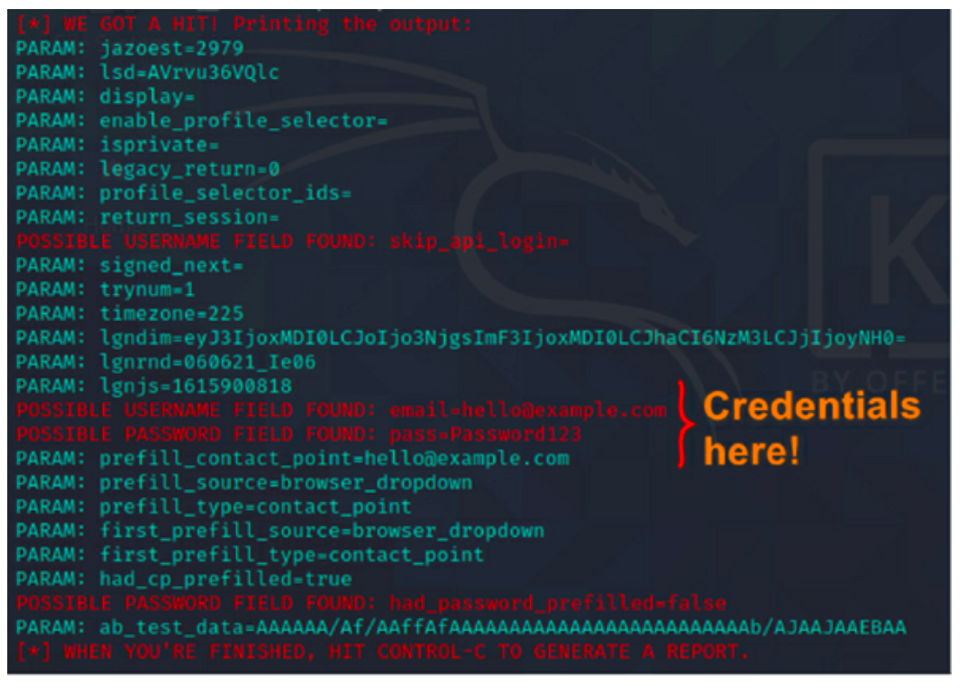
*Task 6:*

To get to the cloned site, open Firefox in your Kali machine and enter your local IP address into the browser. You will then be able to view the cloned login page for Facebook. Enter a random username and password into the fields and press Log In.

**

*Task 7:*

Finally, go back to the terminal where SET is running. You will see lots of text from the numerous POST requests being sent from the cloned site. Scroll down until you see the values “username” and “password”. You should be able to see the username and password you entered into the cloned site in cleartext.

**