Security+[SY0–601] Lab Walkthrough

Lab 1 — Credential Harvesting Using Site Cloning

Hassen Hannachi

June 8, 2025

Contents

List of Figures

1 Introduction

Credential harvesting is the process of gathering sensitive information on a target such as credit card details or passwords, without them knowing that this information is being captured.

2 Environment Setup

To get hands-on experience in preparation for the CompTIA Security+ exam [SY0–601]. All the labs use free tools. I STRONGLY recommended that these exercises be conducted within a virtualized environment [1], such as VMware or VirtualBox, to prevent potential security risks to personal computing systems .[2].

3 Lab Walkthrough

3.1 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 Social Engineering Toolkit by typing: ***sudo setoolkit***. From this menu, choose ***option 5*** for ***Update SET cofiguration***

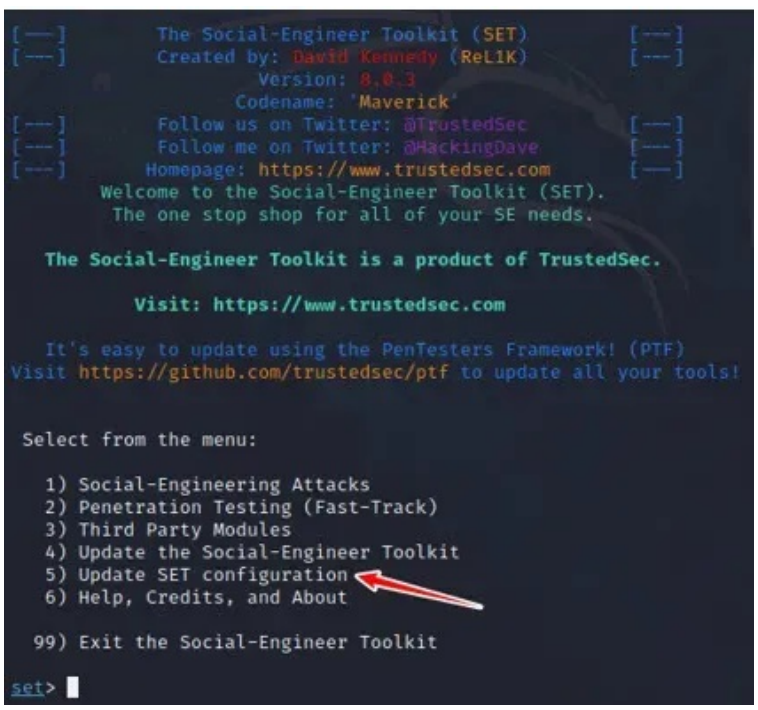

Figure 1: social engineering toolkit

[1]You can use Kali Linux in a virtual machine for the purpose of this lab.
[2]NEVER configure these labs at work using your employers' PCs

3.2 Task 2

From the first menu, choose option 1 for Social -Engineering Attacks. From the next menu, choose option 2 for 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.

Figure 2: credential harvester

3.3 Task 3

The next menu will ask you which method you want to choose to harvest a victim's credentials. In this lab we will be cloning a site, so choose option 2.

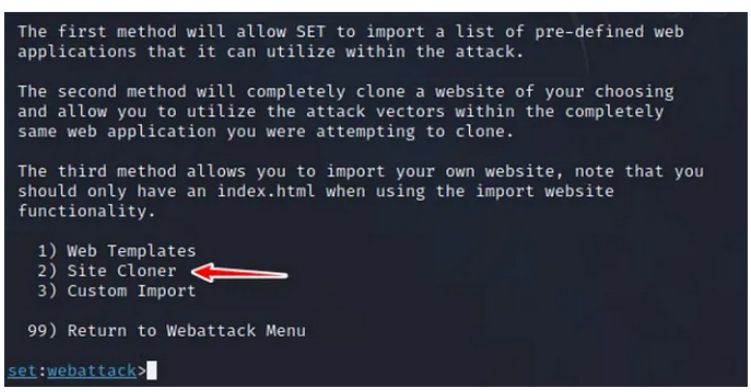

Figure 3: site cloner

3.4 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. For the purpose of this lab, enter your Kali machine's local IP address. This can be found 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, but for this lab I will be using https://www.facebook.com.

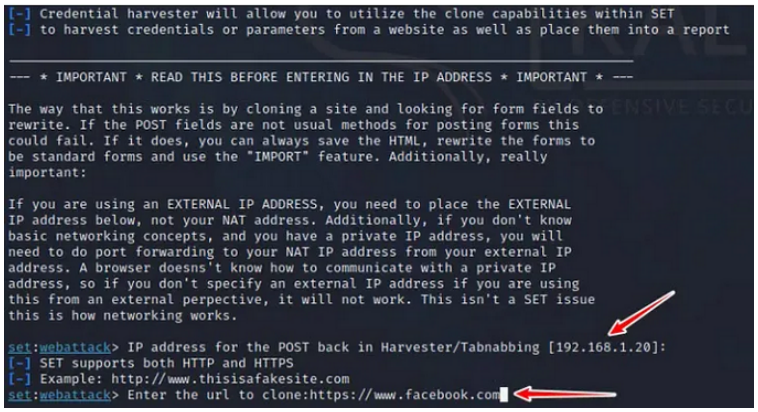

Figure 4: clone website url

3.5 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.

Figure 5: POST requests

3.6 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.

3.7 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

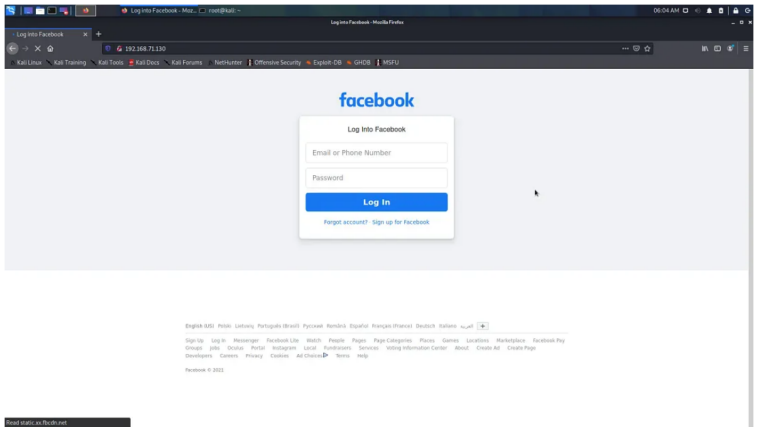

Figure 6: cloned site

values username and password. You should be able to see the username and password you entered into the cloned site in cleartext.

Figure 7: credentials in cleartext

4 Conclusion

In this lab, we successfully demonstrated a credential harvesting attack by cloning legitimate websites, a technique commonly used in phishing campaigns. By replicating the look and feel of trusted platforms (e.g., bank login pages or webmail portals), attackers can trick users into submitting sensitive data such as usernames and passwords.