## Lab 08: Credential Harvesting via Site Cloning using SET in ParrotOS

### Scenario

CyberNova Solutions, a multinational technology firm managing confidential client contracts and financial transactions, has recently observed an increase in phishing-style cyberattacks targeting its employees. While robust defenses such as intrusion detection systems and endpoint protection are in place, human error remains a critical vulnerability.

To evaluate employee awareness and the company’s resilience against social engineering, CyberNova’s security team has planned a red team assessment. The aim is to simulate a convincing fake login page, trick a user into entering credentials, and demonstrate how attackers can use stolen login details to further infiltrate systems.

In this controlled exercise, the red team will use the Social-Engineer Toolkit (SET) on ParrotOS to clone a legitimate website, host it locally, and capture any credentials submitted by the victim. This simulation will provide valuable insight into potential weaknesses and help enhance cybersecurity awareness.

### Solution

You have been engaged as a certified security practitioner to carry out a phishing simulation. The objective of this exercise is to clone a legitimate-looking website using the Social-Engineer Toolkit (SET) site cloner feature, host the cloned site on the attacker's machine, and capture any login credentials entered by the victim. The demonstration will include launching the Social-Engineer Toolkit in ParrotOS, navigating to the Website Attack Vectors menu, selecting the Credential Harvester Attack Method, and then choosing the Site Cloner option. You will enter the attacker machine’s IP address to host the cloned site and observe how credentials are captured in real-time.

By completing this lab, you will gain practical experience in phishing simulation techniques and understand how attackers use deceptive web pages to harvest sensitive information. SET, being a widely used open-source framework for simulating social engineering threats, provides a convenient Credential Harvester module that demonstrates how attackers can collect sensitive data from unsuspecting users, which can subsequently be exploited to escalate further attacks.

**Note:** In this lab, the attacker machine (ParrotOS) uses the IP address. Replace these with your own IP addresses when performing the lab.

|  |
| --- |
| 1. Turn on **ParrotOS** virtual machine. Open a **Terminal**, and execute the **sudo su** command to run programs with root privileges. Execute the following command: **setoolkit** to launch **Social-Engineer Toolkit.** If a **Do you agree to the terms of service [y/n]** question appears, enter **y** and press **Enter**.    2. First, update the SET utility to get the latest features. Choose **option** **5**.    3. From the **SET main menu**, select **option 1: Social-Engineering Attacks**.    4. From the next menu, select **option 2:** **Website Attack Vectors**.    5. When prompted to choose the type of website attack, select **option 3: Credential Harvester Attack Method**.    6. The next menu will ask you which method you would like to choose to harvest a victim’s credentials. We will be cloning a site in this lab, so choose **option 2**: **Site Cloner.**    7. 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 ParrotOS has many IP addresses, you can find the desired one by opening a new terminal and typing **ifconfig.** Type your ParrotOS **IP address** and press **Enter**.    8. Once you tell **SET** that you would like to clone a website, it will then prompt you to enter the URL of the site you wish to clone. You can enter any site of your choice. For this lab, I will be using: **http://testphp.vulnweb.com/login.php**  This is a deliberately vulnerable web application created for security testing and demonstration purposes. It will allow us to safely showcase the cloning process without targeting a real-world, production website.    9. 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.    10. To get to the cloned site, open **Firefox** in your ParrotOS machine and enter your **local IP address** into the browser. You will then be able to view the cloned login page for **testphp.vulnweb.com**.      11. Enter a random **username** and **password** into the fields and press **Log In**.    12. 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 **username** and **password** values. You should be able to see the username and password you entered into the cloned site in clear text. |