Social Engineering Attacks with Social Engineering Toolkit (SET) and Browser Exploitation Framework (BeEF)

Note: These labs are performed based on the lab works provided in "Module 4: Social Engineering Attacks" in the "Ethical Hacking" Course provided by CISCO.

A social engineering attack is a psychological manipulation technique used by cybercriminals to deceive people into giving up sensitive information or performing actions that compromise security.

Lab 1- Exploring the Social Engineer Toolkit (SET)

Social Engineering Toolkit (SET) can be used to launch numerous social engineering attacks. In this lab, we will perform the following actions.

1. Launch SET and explore the toolkit
2. Clone a website to obtain user credentials
3. Capture and view user credentials

The following resources will be required to perform this lab.

- Kali VM customized for Ethical Hacker course
- Internet access

Part 1: Launching SET and Exploring the Toolkit

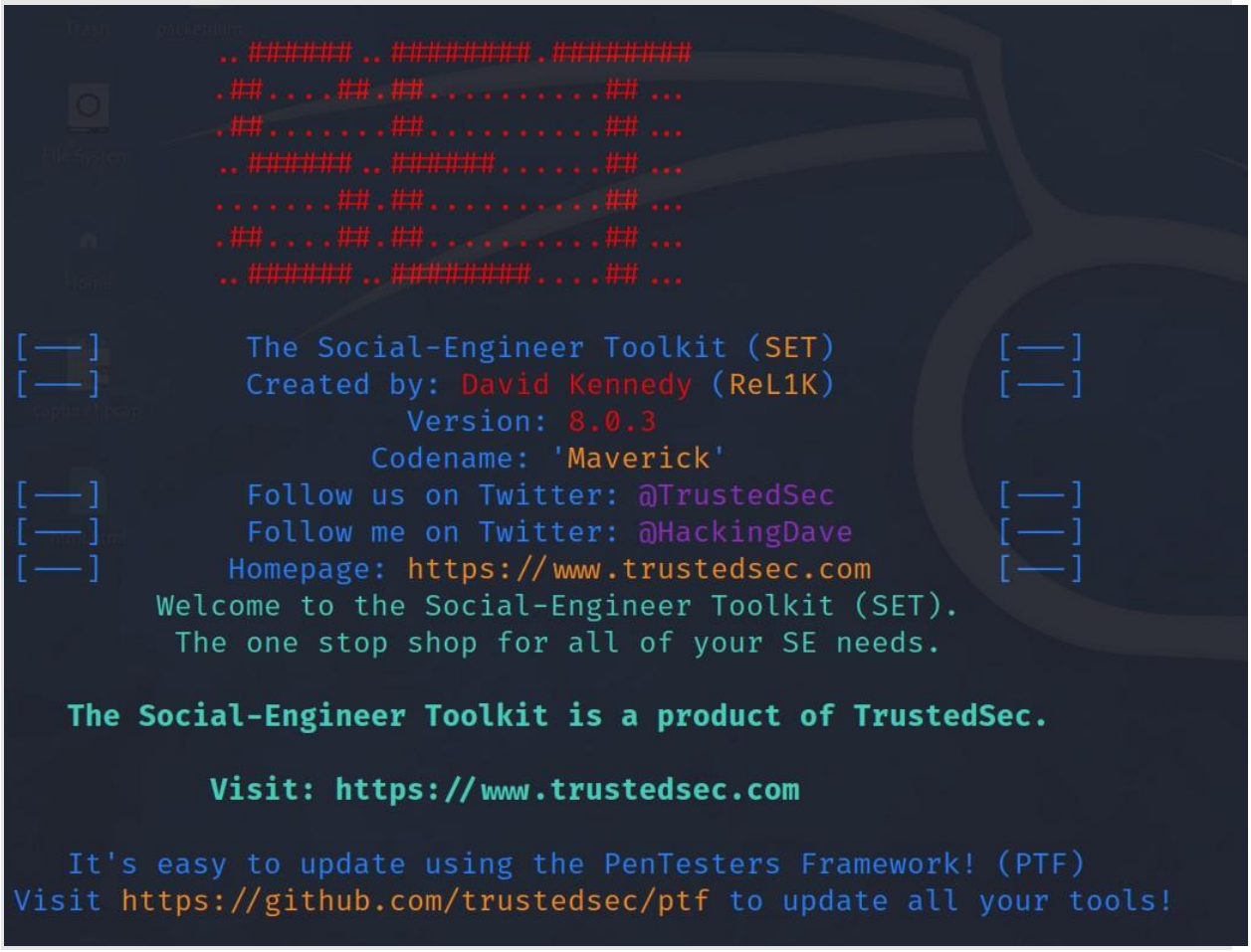
a. At first, start Kali Linux using the username kali and the password kali. Open a terminal session from the menu bar at the top of the screen.

b. To run the SET as root, use the ***sudo -i*** command to obtain persistent root access.

```
$ sudo -i
```

c. Now, enter the command ***setoolkit*** to load the social engineering toolkit. Alternatively, we can run the Social Engineering Toolkit from the **Applications > Social Engineering Tools > Social Engineering Toolkit (root)** option on the Kali menu.

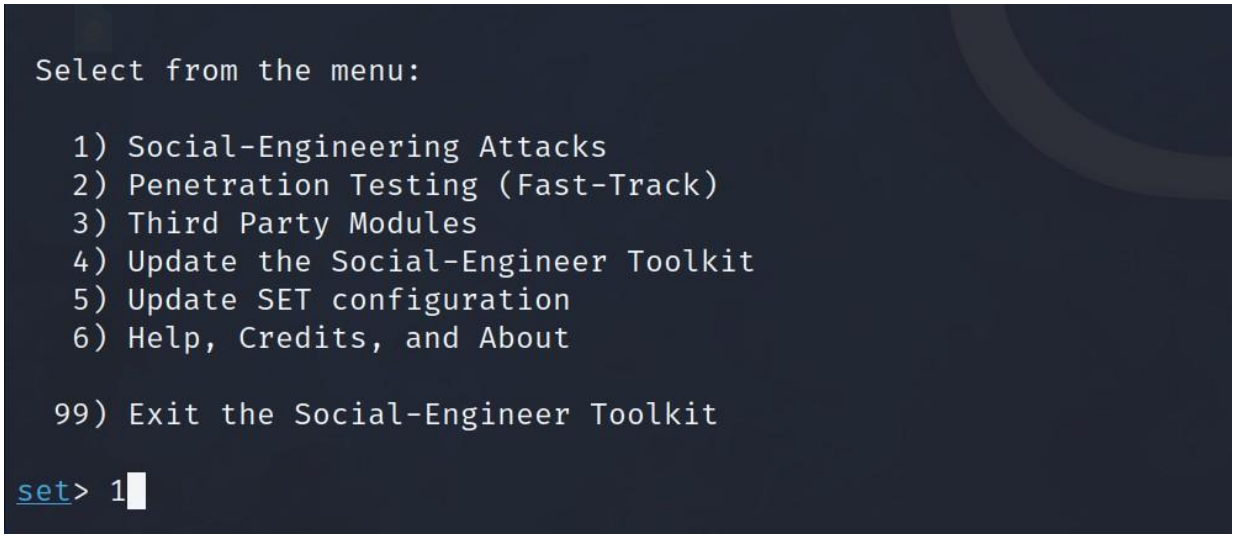
```
# setoolkit
```



d. If the disclaimer appears, enter y to accept the terms of service provided.

e. Now the initial SET menu will be displayed.

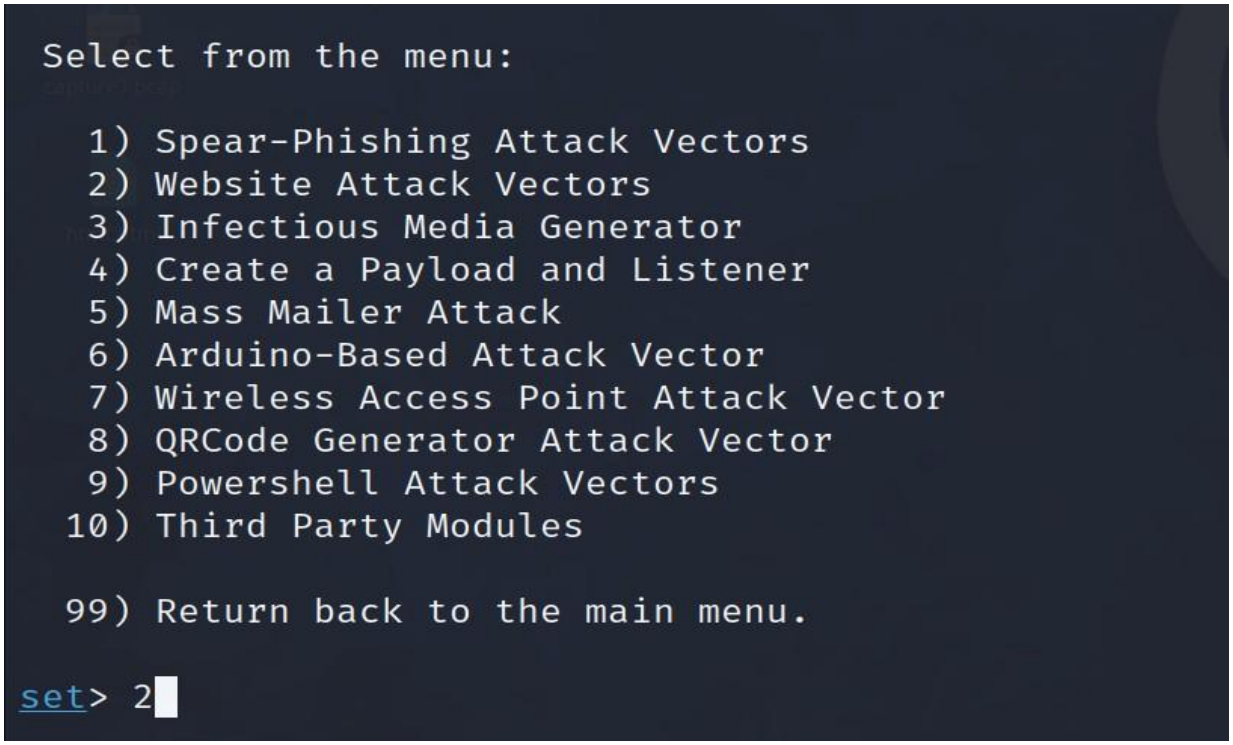
f. After the SET menu appeared, enter 1 to select the 1st option from the menu and press Enter to access the Social-Engineering Attacks submenu.



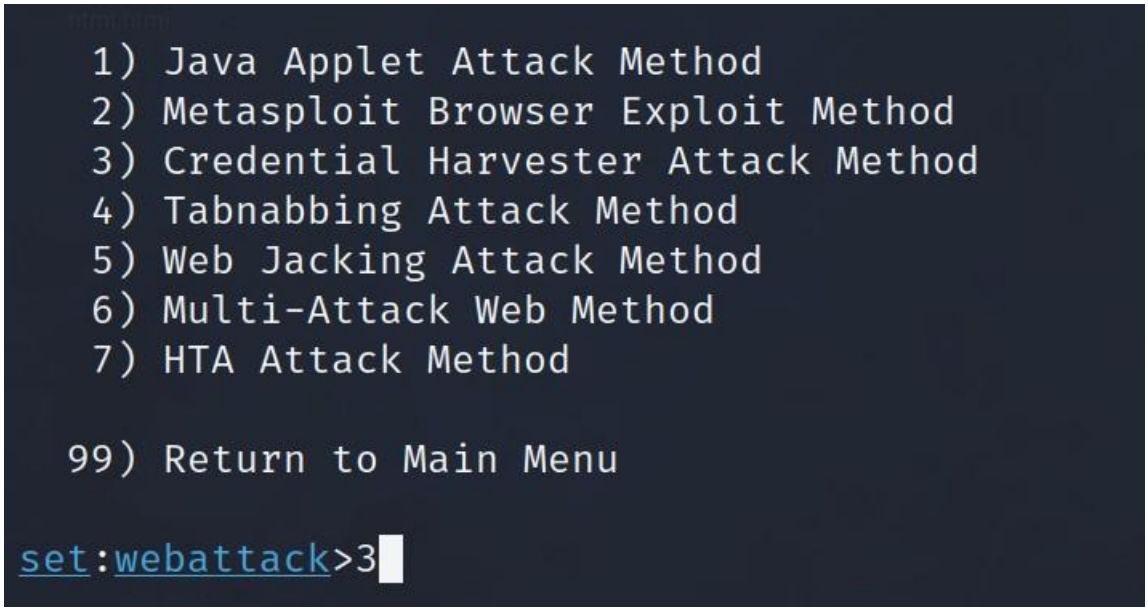
g. We can select each option to see a brief description of each exploit and what the tool does for each option. We can use CTRL-C or enter 99 to return to the main menu.

Part 2: Cloning a website to Obtain User Credentials

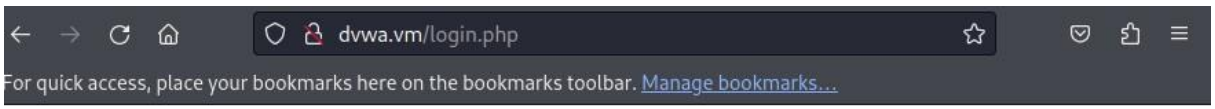
a. After launching the **Social-Engineering Attacks** submenu as given in part 1, choose the second option, **"Website Attack Vectors".**



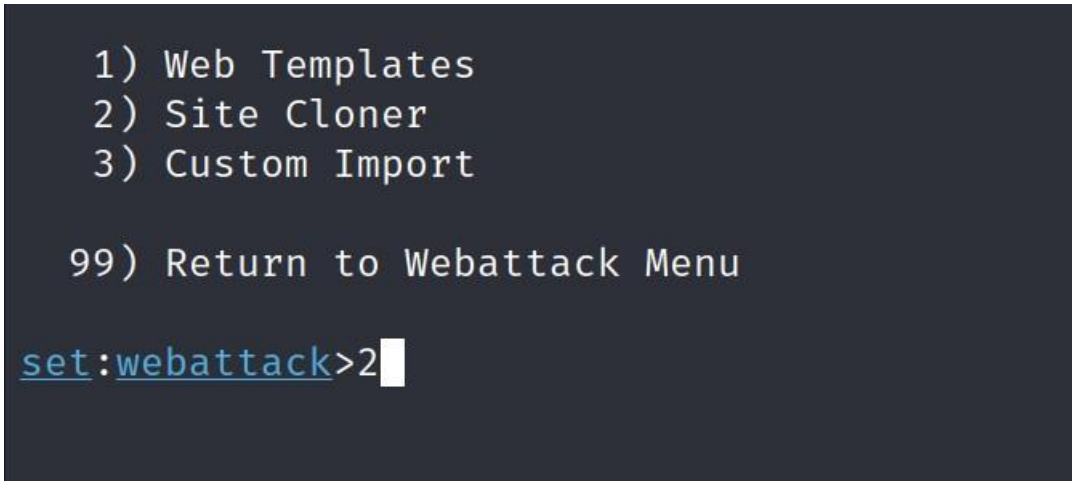
b. Now, select the third option, **“Credential Harvester Attack Method”** from the menu.



c. Open the Kali Firefox browser, and enter the URL **http://DVWA.vm/**. The login screen will appear. If the URL is not found, enter **http://10.6.6.13/** to access the web server using its IP address.



d. Now we have to return to the terminal session and select the second option, **“Site Cloner”** from the **“Credential Harvester Attack Method”** menu.



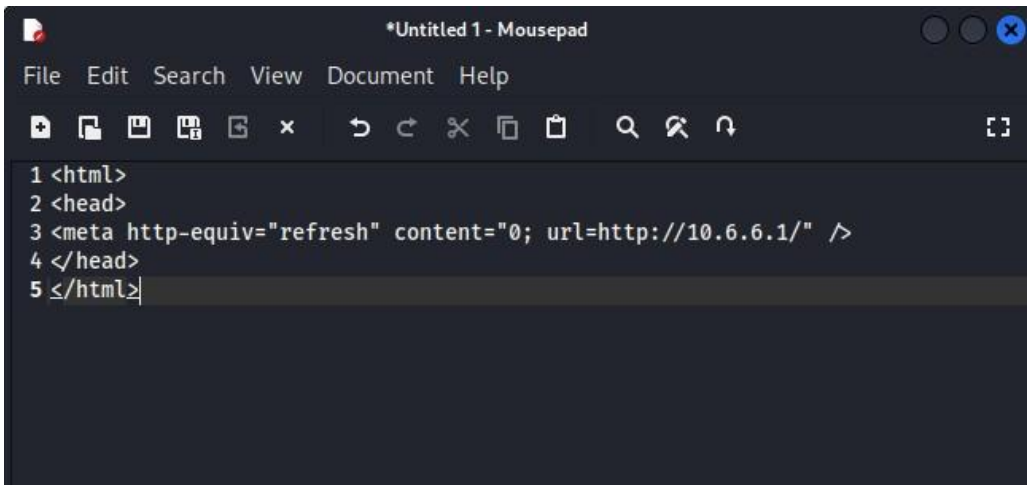
e. Enter the IP address **10.6.6.1** at the prompt.

f. Next, enter the URL of the DVWA website **http://DVWA.vm** for cloning.

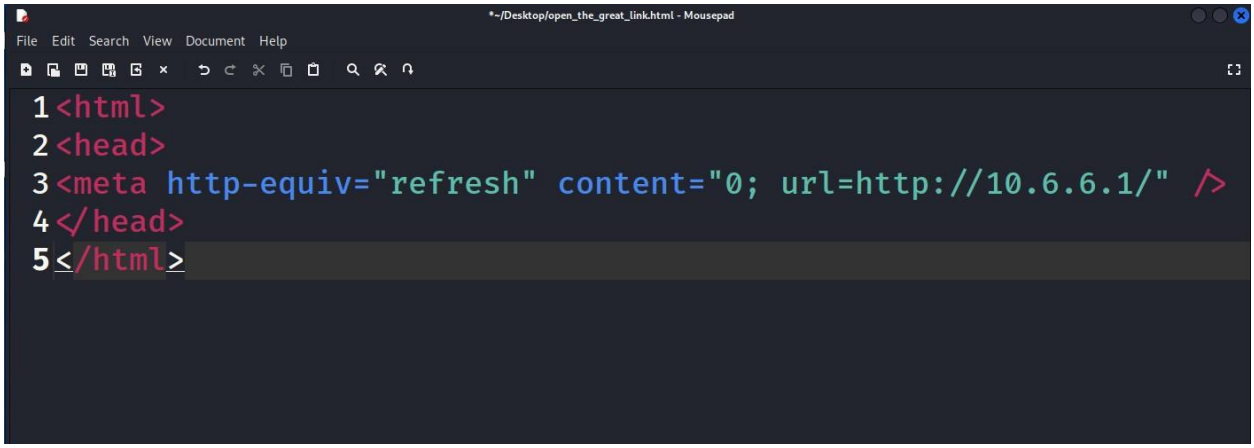
Part 3: Capturing and Viewing User Credentials

a. To set up for capturing and viewing the user credentials, we have to create the social engineering exploit. To do this, open the Kali Linux Mousepad text editor by selecting **Applications > Favorites > Text Editor** from the menu, and then enter the HTML code provided below into the text editor.

```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```

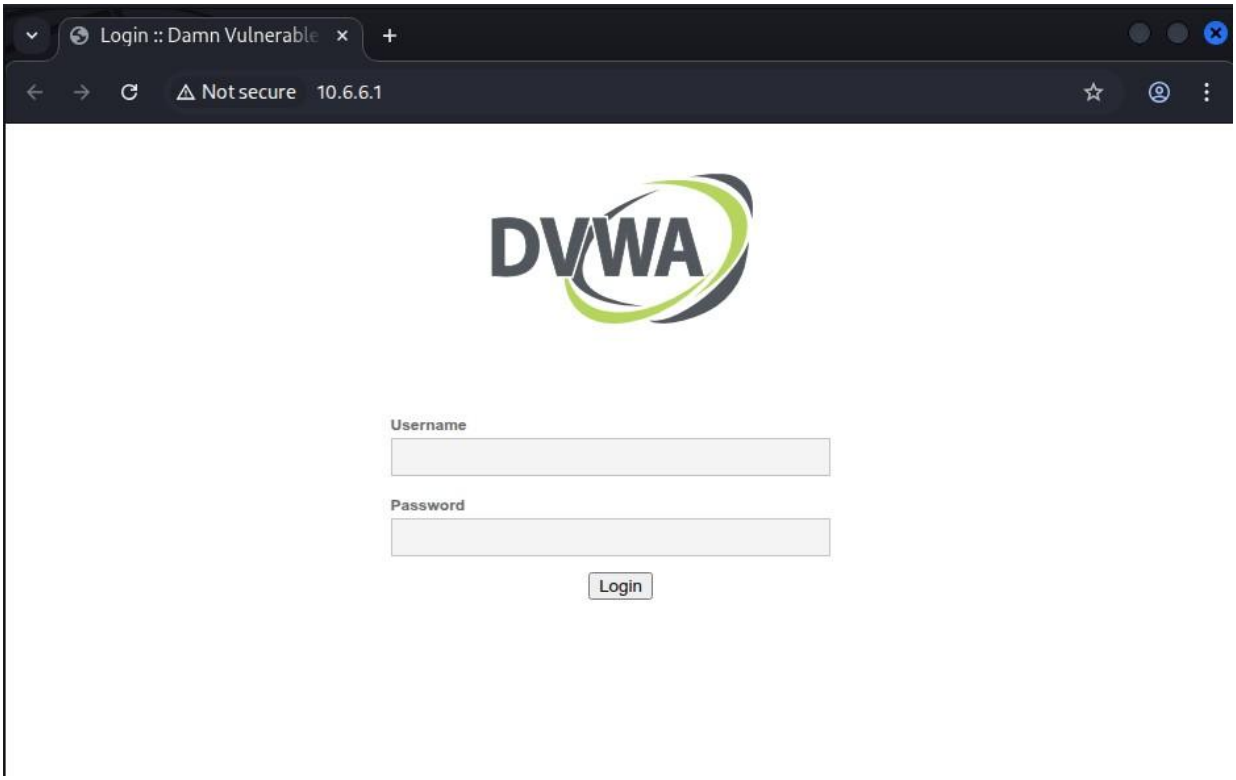


b. Next, save the file in the **/home/kali/Desktop** folder with the appropriate name (i.e., **open_the_great_link.html**) and save it.



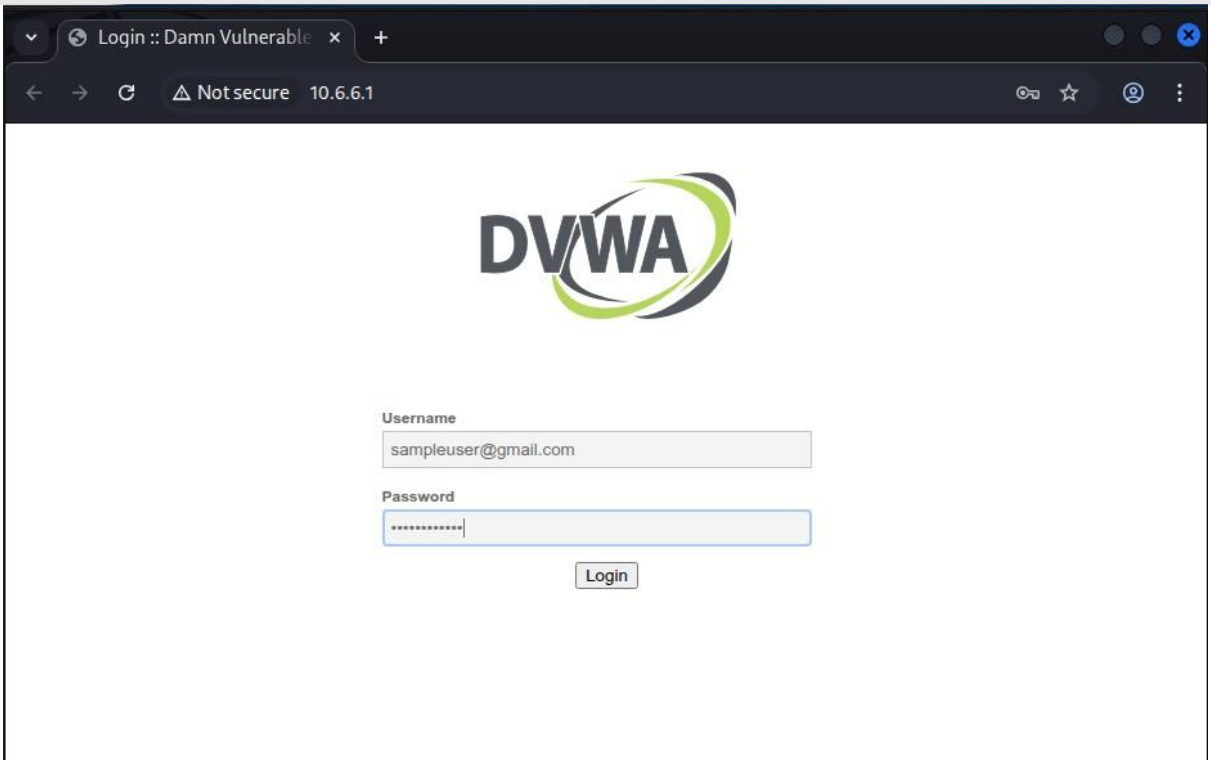
c. Close the text editor.

d. Now, double-click the desktop icon for the **open_the_great_link.html** page. It should be the same DVWA login page that was viewed in step c of part 2.

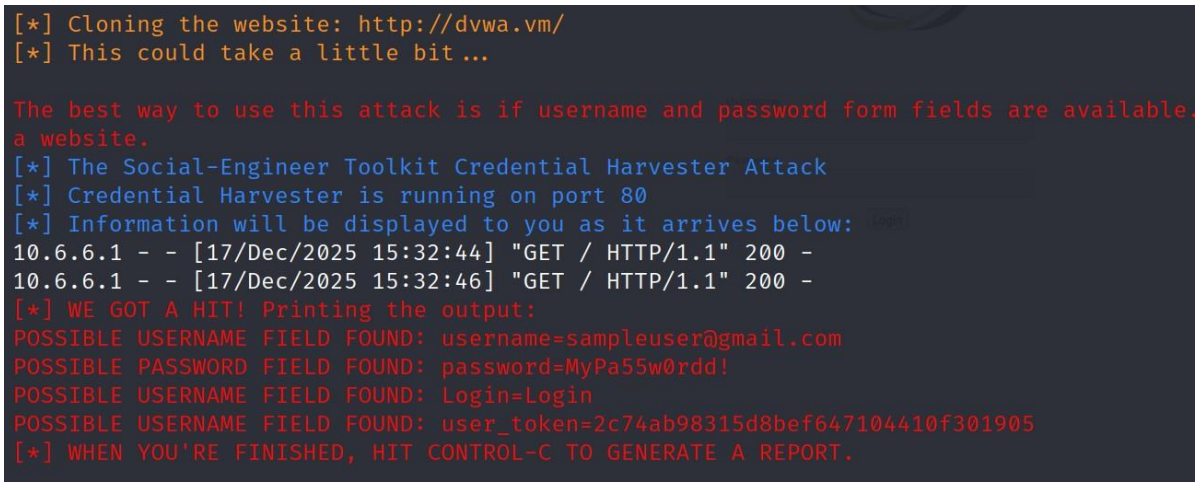


e. Next, enter the Username and Password in the fields and click Login to send the form.

Username: sampleuser@gmail.com
Password: MyPa55w0rdd!



f. Now we have to return to the terminal session that is running the SET application. We will see the output from the login attempt.



g. Enter **CTRL-C** to save the report in XML format that can be used in other penetration testing applications.

h. Press Enter to exit from the **seotoolkit** and see the information that is saved in the file generated by the tool.

i. By default, the generated file will be located in the following path.

```
/root/.set/reports/
```

j. Enter the file location with the use of cd command as below.

```
cd /root/.set/reports/
```

k. List the files using the ls command and use the cat command to see the information within the file.

Lab 2- Using the Browser Exploitation Framework (BeEF)

Browser Exploitation Framework (BeEF) is an application that runs in the browser, which allows taking control of target browsers that visit a malicious web page created by the attacker.

In this lab, we will complete the following actions:

- Load the BeEF GUI Environment
- Hook the Local Browser to Simulate a Client-Side Attack
- Investigate BeEF Exploit Capabilities

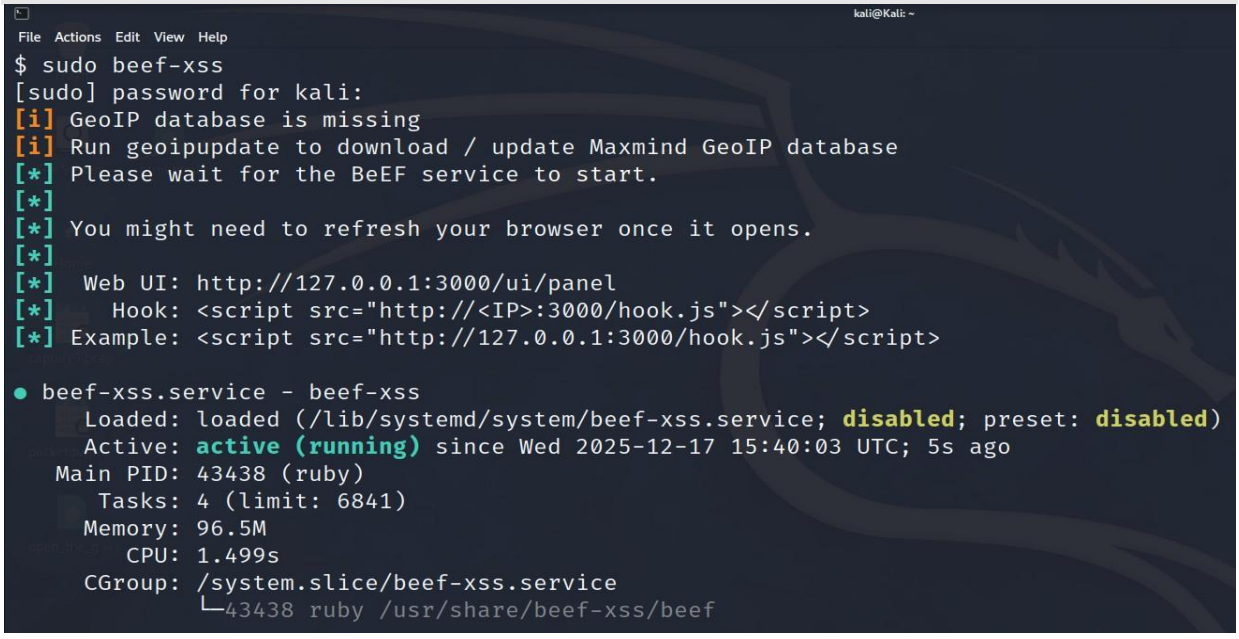
The following resources will be required to perform this lab.

- Kali VM customized for Ethical Hacker course
- Internet access

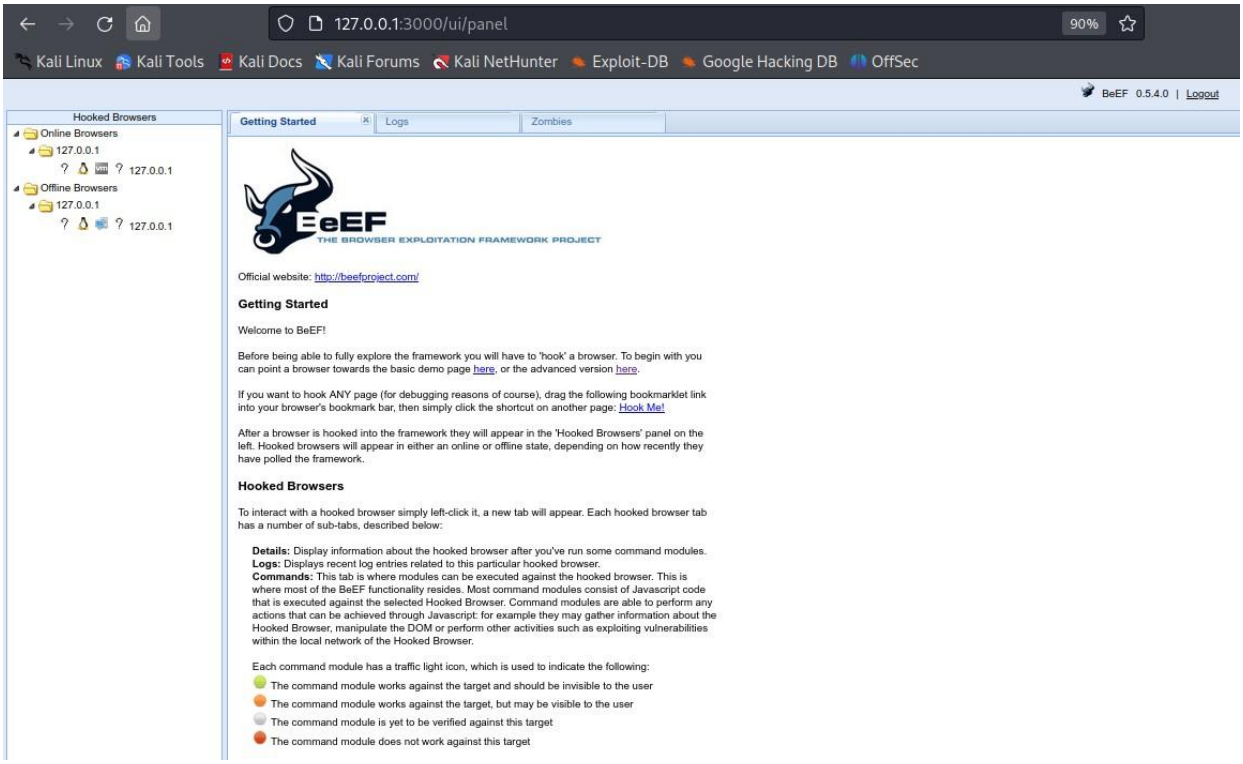
Part 1: Load the BeEF GUI Environment

a. We can load the BeEF GUI environment in two ways. The first one is opening the BeEF application from the Kali **Application > All Applications > BeEF** located in the Start Menu. OR, it can be launched with the use of a command **"beef-xss"** in the terminal.

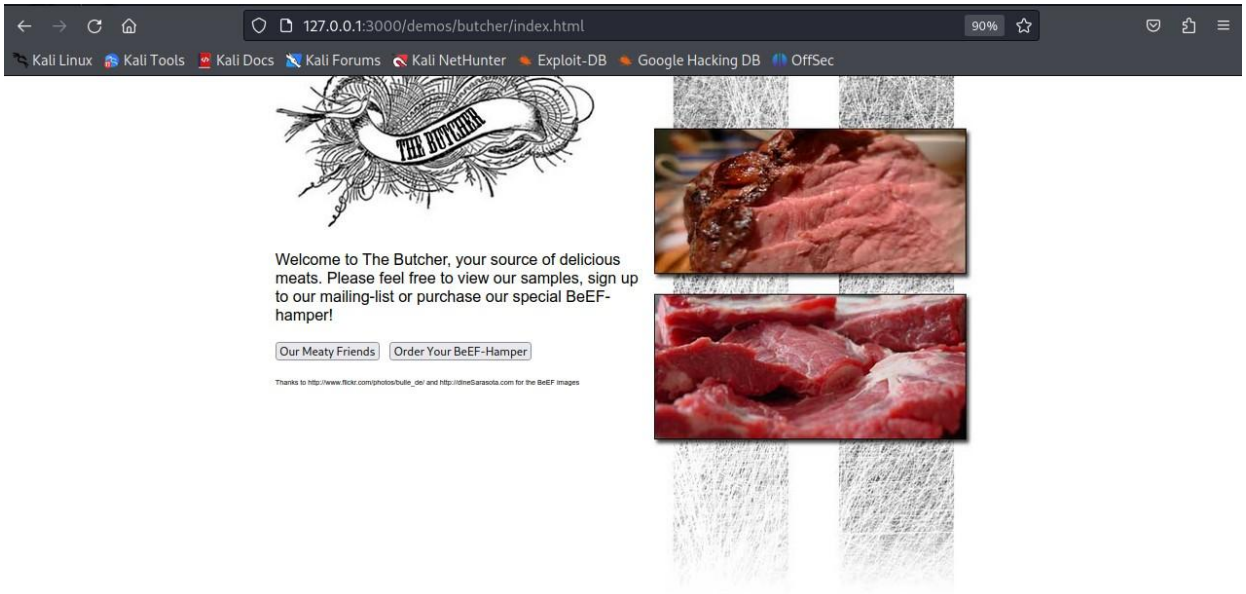
```
$ sudo beef-xss
```



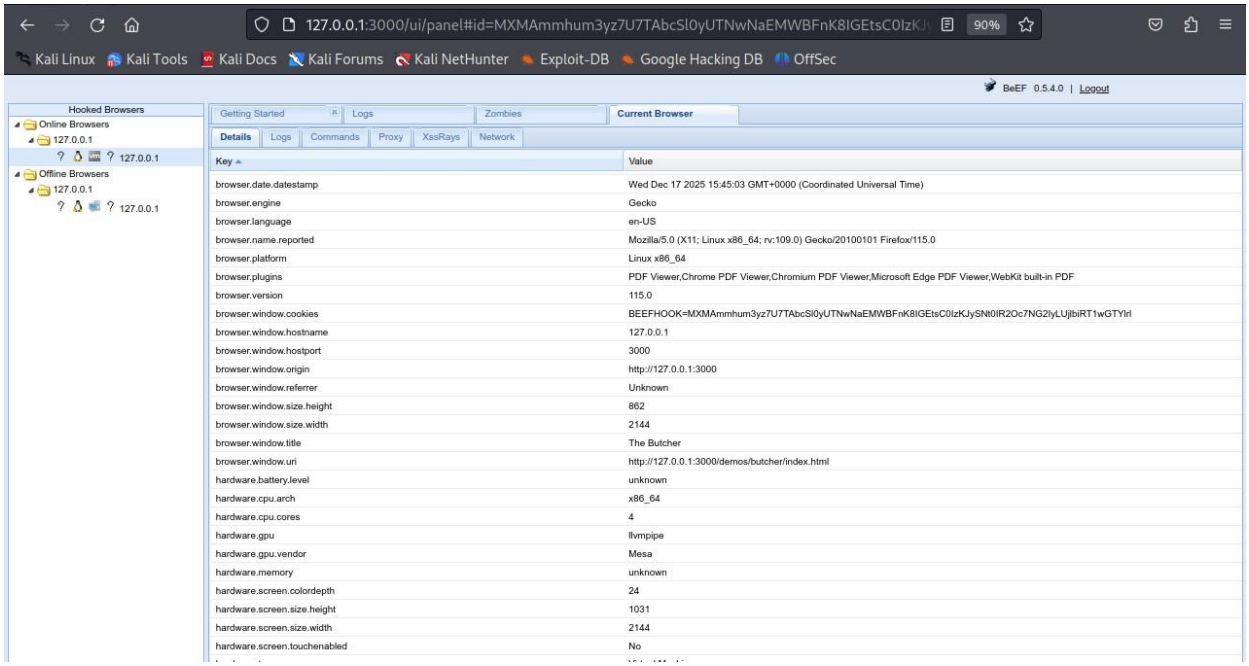
b. If we are running the BeEF for the first time, we will be prompted to change the password for the BeEF user. Enter mynewbeef as the password.
c. Now we will see the BeEF interface after a browser window opens automatically. If it does not, open Firefox from the menu bar and enter **http://127.0.0.1:3000/ui/authentication** as the URL.
d. Next, log in to BeEF with the username beef and the password mynewbeef.



e. After successfully logging in, open a new tab in the Firefox browser and enter the following URL in the browser address bar and press Enter.
http://127.0.0.1:3000/demos/butcher/index.html.



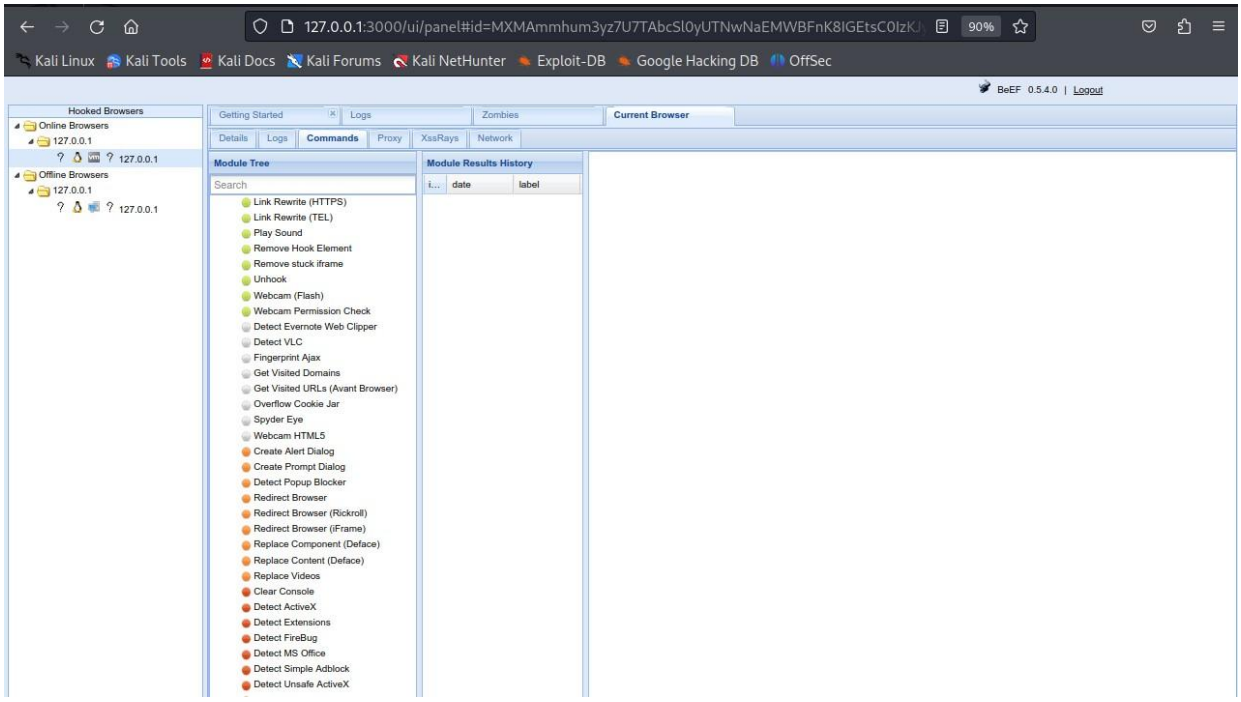
f. We can view the source code for the HTML page using the shortcut key **CTRL-U** in Firefox.
g. Now we have to return to the browser window that contains the BeEF Control Panel. We can view that the information in the Hooked Browsers panel on the left side of the screen has changed.
h. Click the entry listed under **Online Browsers**.
i. We can view what information BeEF knows about the target user's computer and browser from the Details tab.



Part 2: Investigate BeEF Exploit Capabilities

a. To investigate the BeEF exploit capabilities, click the **Commands** tab, where modules can be executed against the target browser.

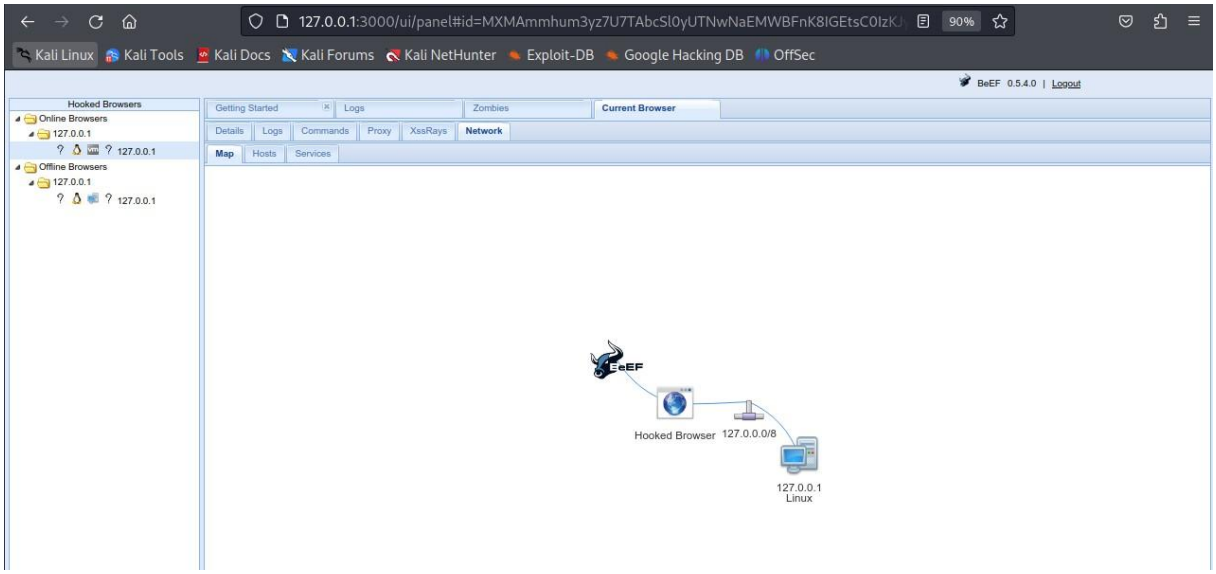
b. Next, expand the command categories in the Module Tree pane. The color-coded icons are referred to as "**traffic lights**".



c. Each command module has a traffic light icon, which is used to indicate the following:

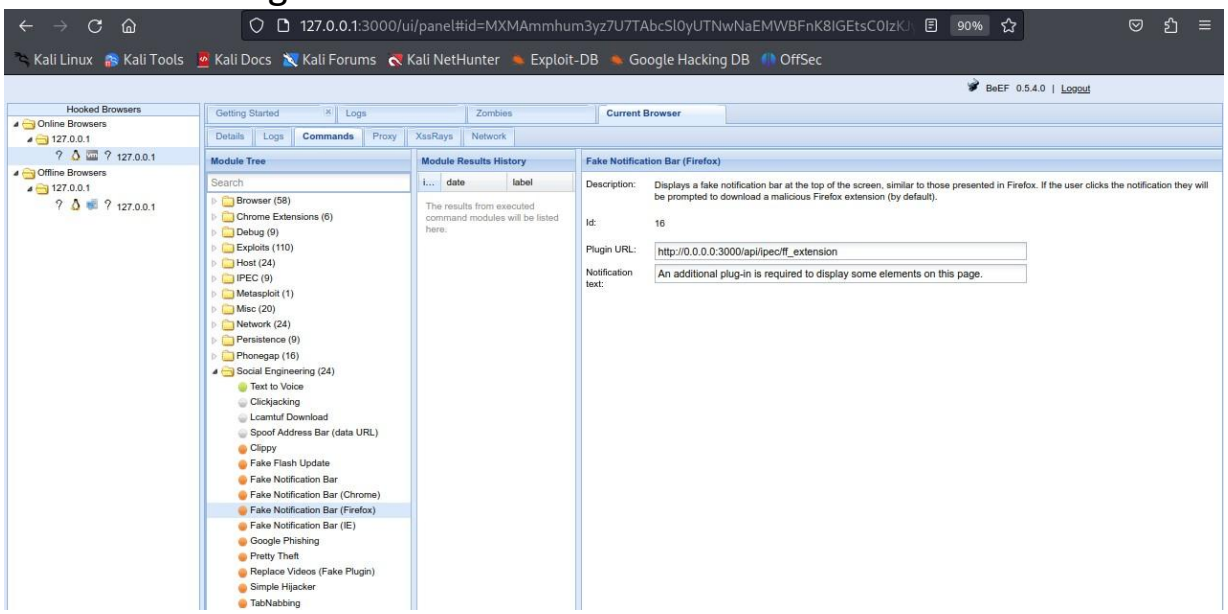
- Green: The command module works against the target and should be invisible to the user.
- Orange: The command module works against the target but may be visible to the user.
- White: The command module is yet to be verified against this target.
- Red: The command module does not work against this target.

d. Click the **Network** tab to create a network map displaying the current network topology.



e. Now, click the **Commands** tab in the **BeEF Control Panel**. Scroll down and open the **Social Engineering** category.

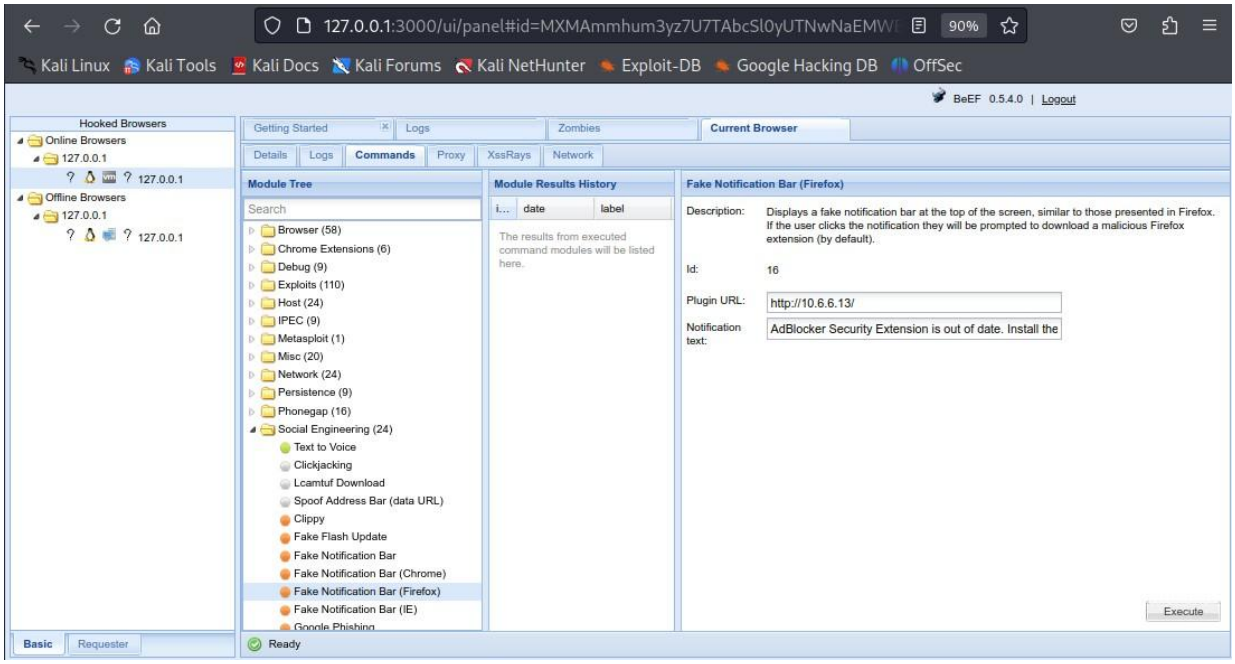
f. Next, select the **Fake Notification Bar (Firefox)** choice from the module list. The default URL for the malicious plug-in is listed along with the message that will be shown on the browser window.



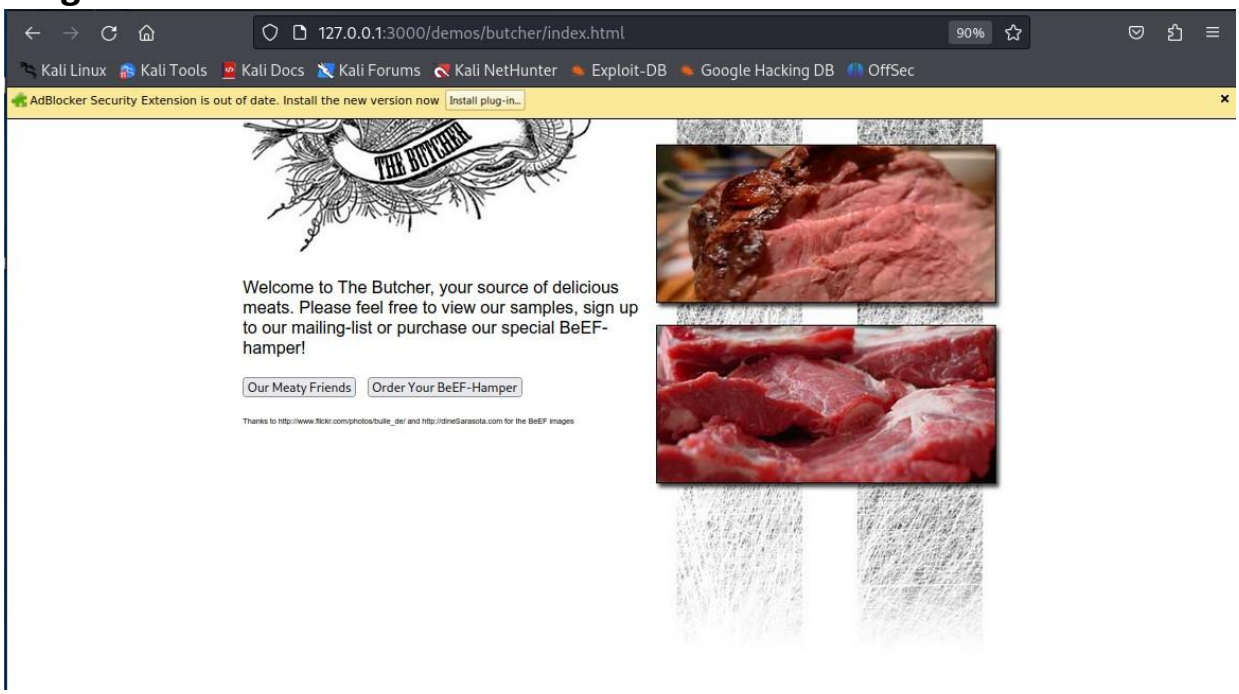
g. This exploit will cause an alert to display on the browser. If the user clicks the install button for the fake plug-in, they will be directed to the URL provided.

h. Change Plugin URL to **http://10.6.6.13/.** This URL redirects the user to the login screen for the DVWA virtual server. The URL can point to any webpage, either locally stored or on the network.

i. In a live penetration testing environment, this would be a cloned website, a malicious application download, or a webpage containing a malicious script.
j. Change the alert text to say **AdBlocker Security Extension is out of date**. **Install the new version now**. Now click **Execute** to send the alert to the hooked browser window.



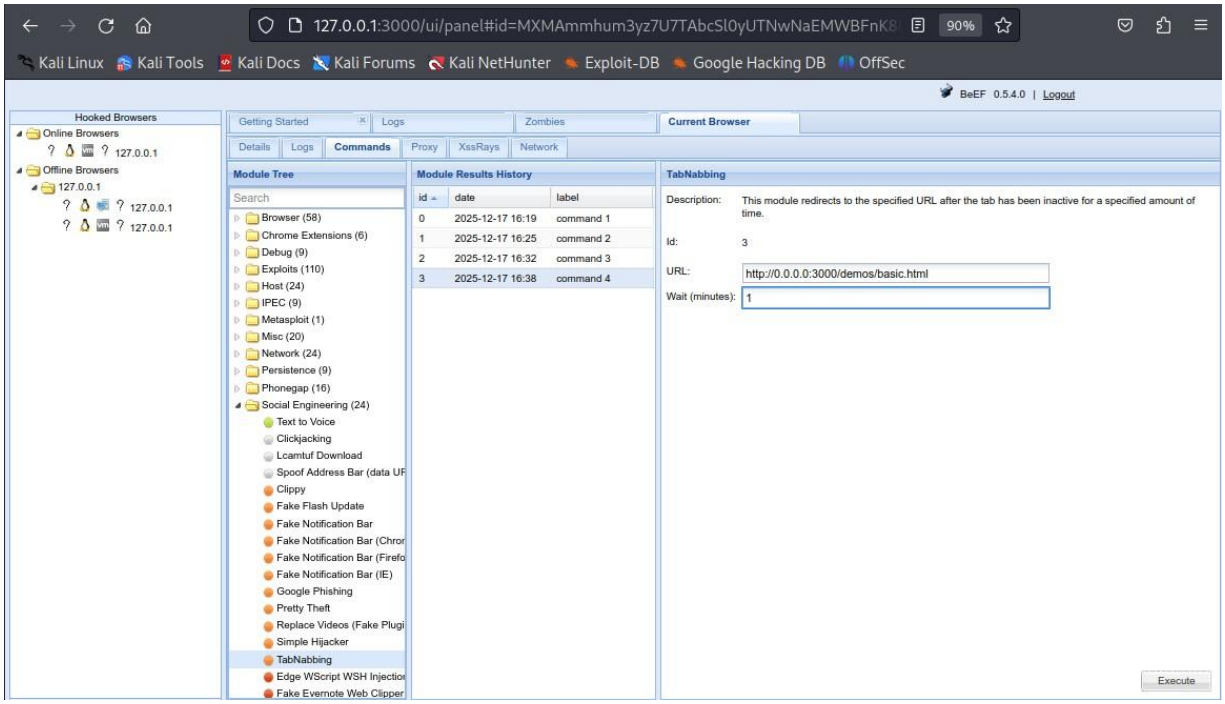
k. Next, return to the browser tab that displays The Butcher fake web page. An alert message is in the Firefox banner area. Click the **Install Plug-in** button on the alert banner.



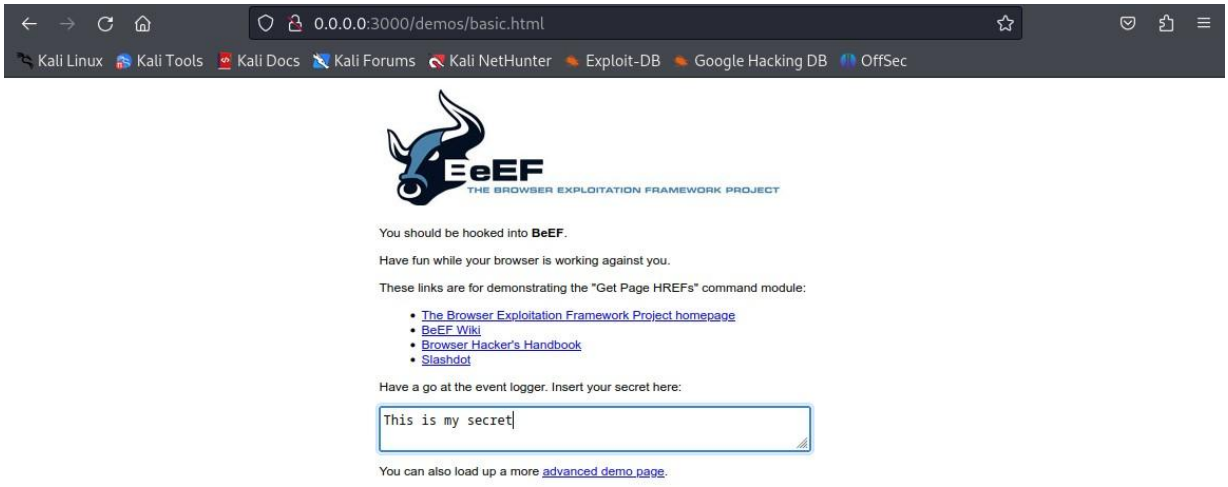
Part 3 - Use TabNabbing to Display a Malicious Website

TabNabbing is a function that redirects the user to a different URL if a browser tab of a hooked browser is idle for a specified length of time.

a. Open a new tab and navigate back to The Butcher web page located at **http://127.0.0.1:3000/demos/butcher/index.html**.
b. Return to the **BeEF Control Panel** Tab. Select the instance listed under the **Online Browsers** in the **Hooked Browsers** panel.
c. Then open the Commands tab and expand the **Social Engineering** category. Scroll down and select **TabNabbing**.
d. Next, change the number of minutes to 1 and click the Execute button to start the exploit. This will remain idle for at least one minute.



e. Now, return to the tab that displayed the Butcher web page.
f. In the box at the center of the BeEF Basic Demo screen, type **“This is my secret”.** Return to the BeEF Control Panel tab.



g. With the entry under Online Browsers selected, select Logs from the menu bar.