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

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:

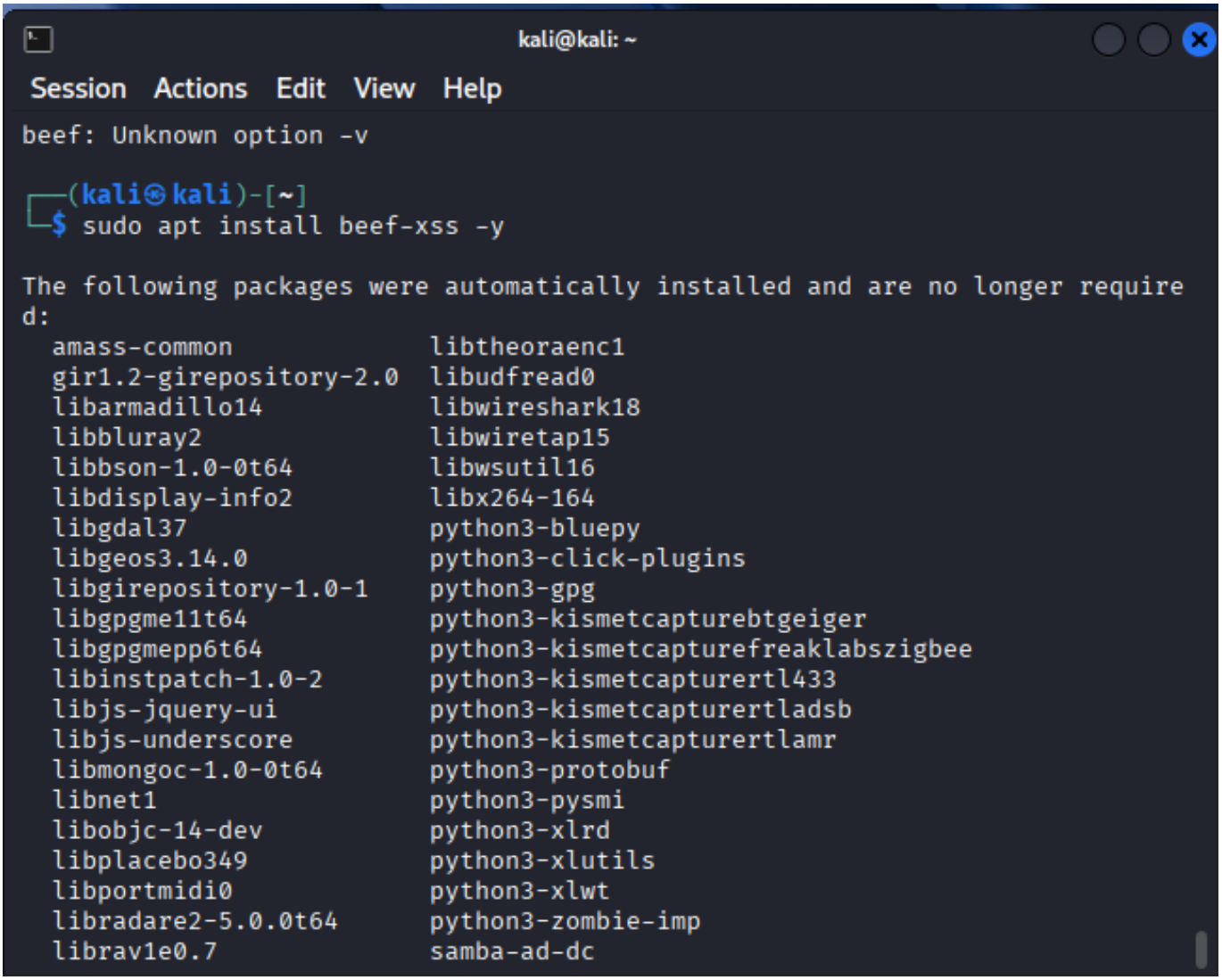
Update and upgrade the machine using command:

sudo apt update && sudo apt upgrade -y

Step 3:

Install BeEF on Kali using:

sudo apt install beef-xss -y

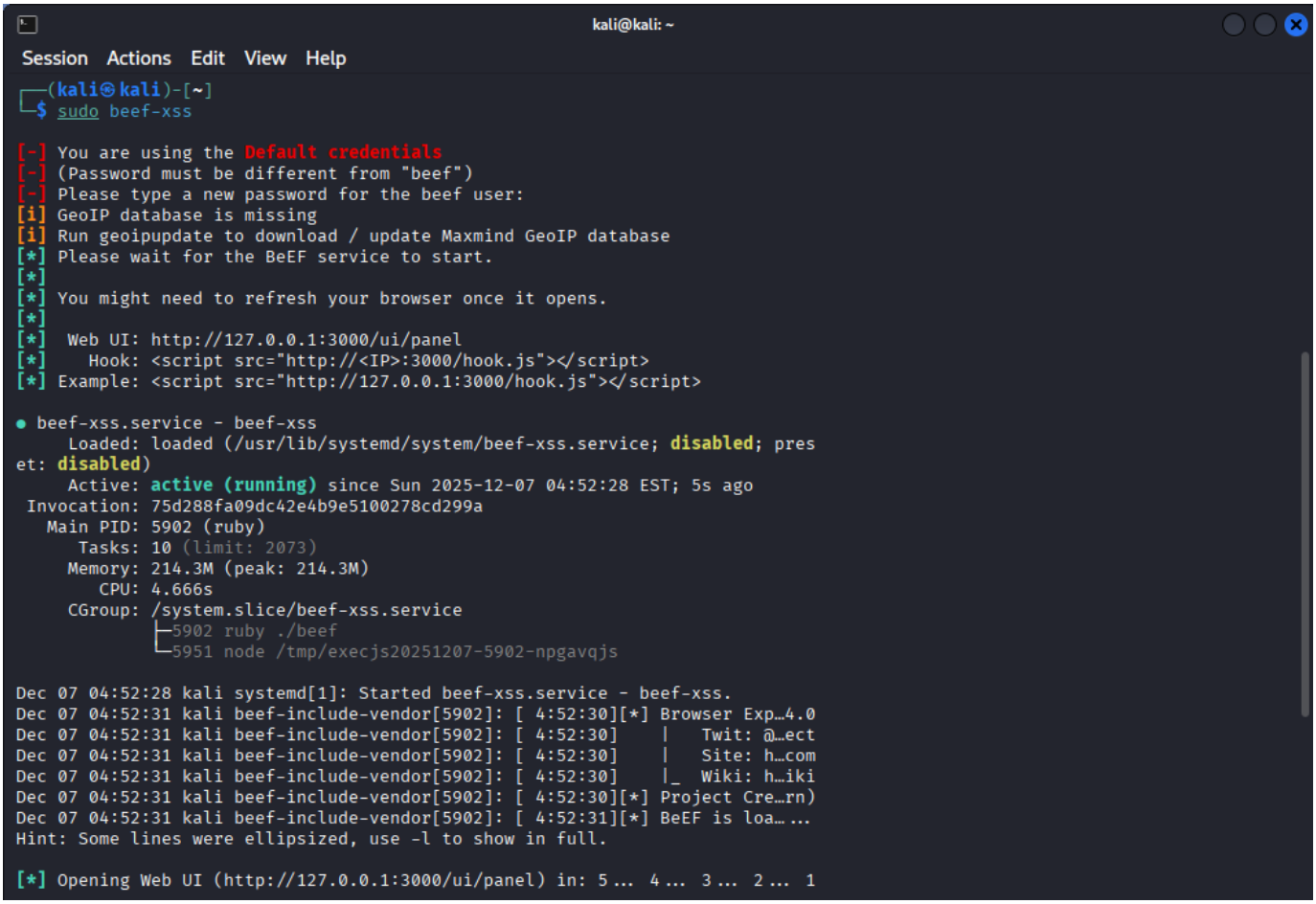


As we are running this project just for learning we can run it localy while to execute this on a real enviorment using online linux server so that you can pass the intendent user link directly making it obfustucated.

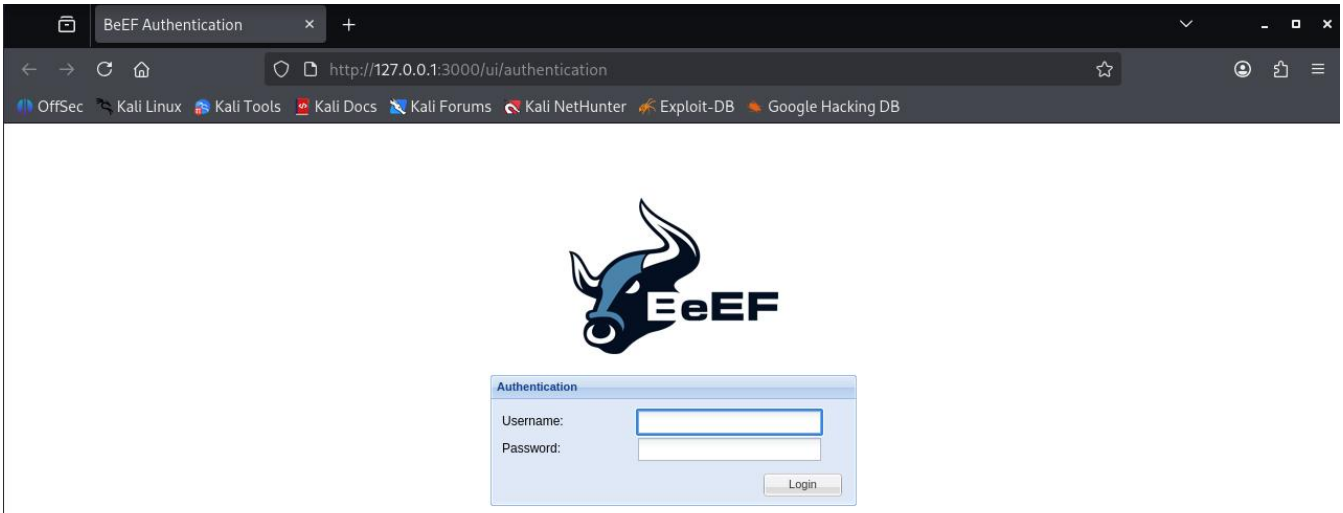
Now to start the BeEF run:

sudo beef-xss

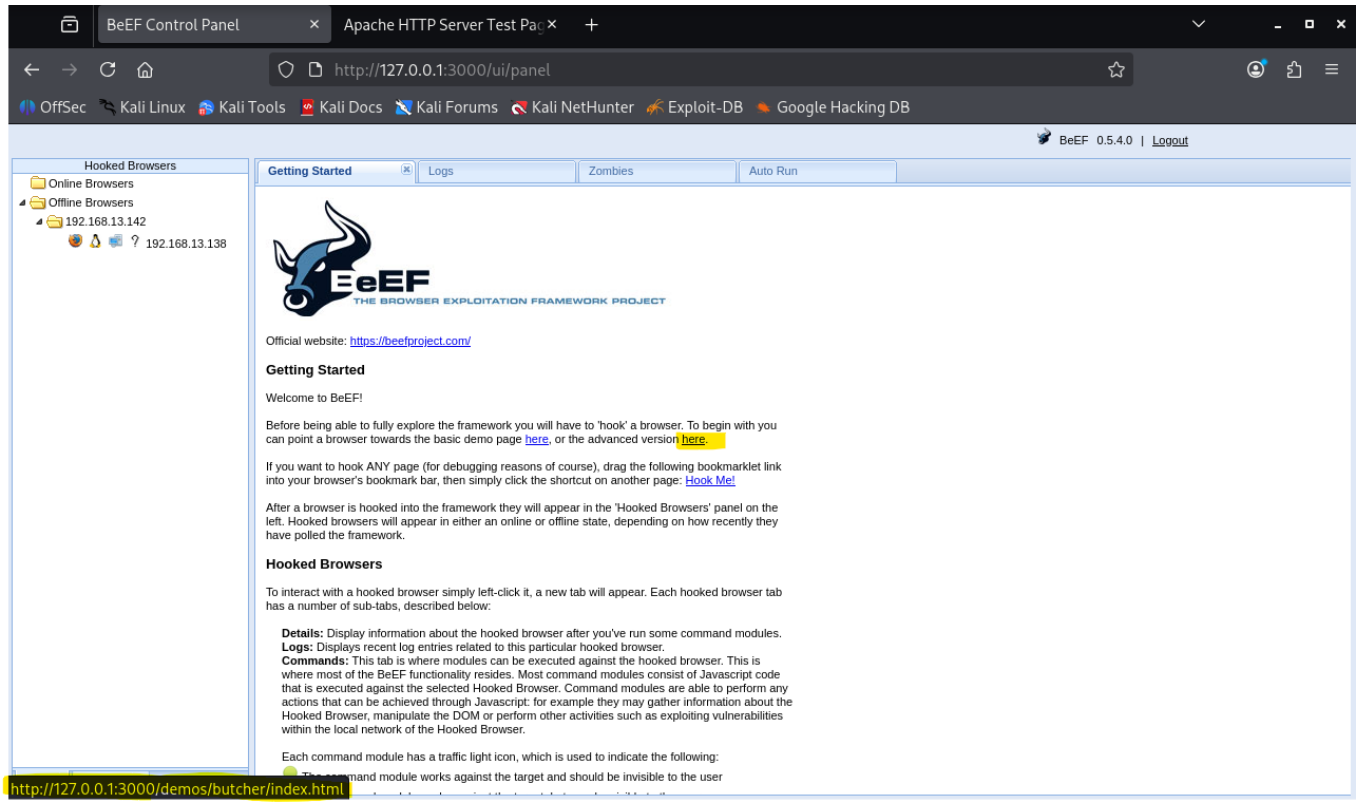
Then enter a new password to be ahead if asked for default login credential type beef for username and password.



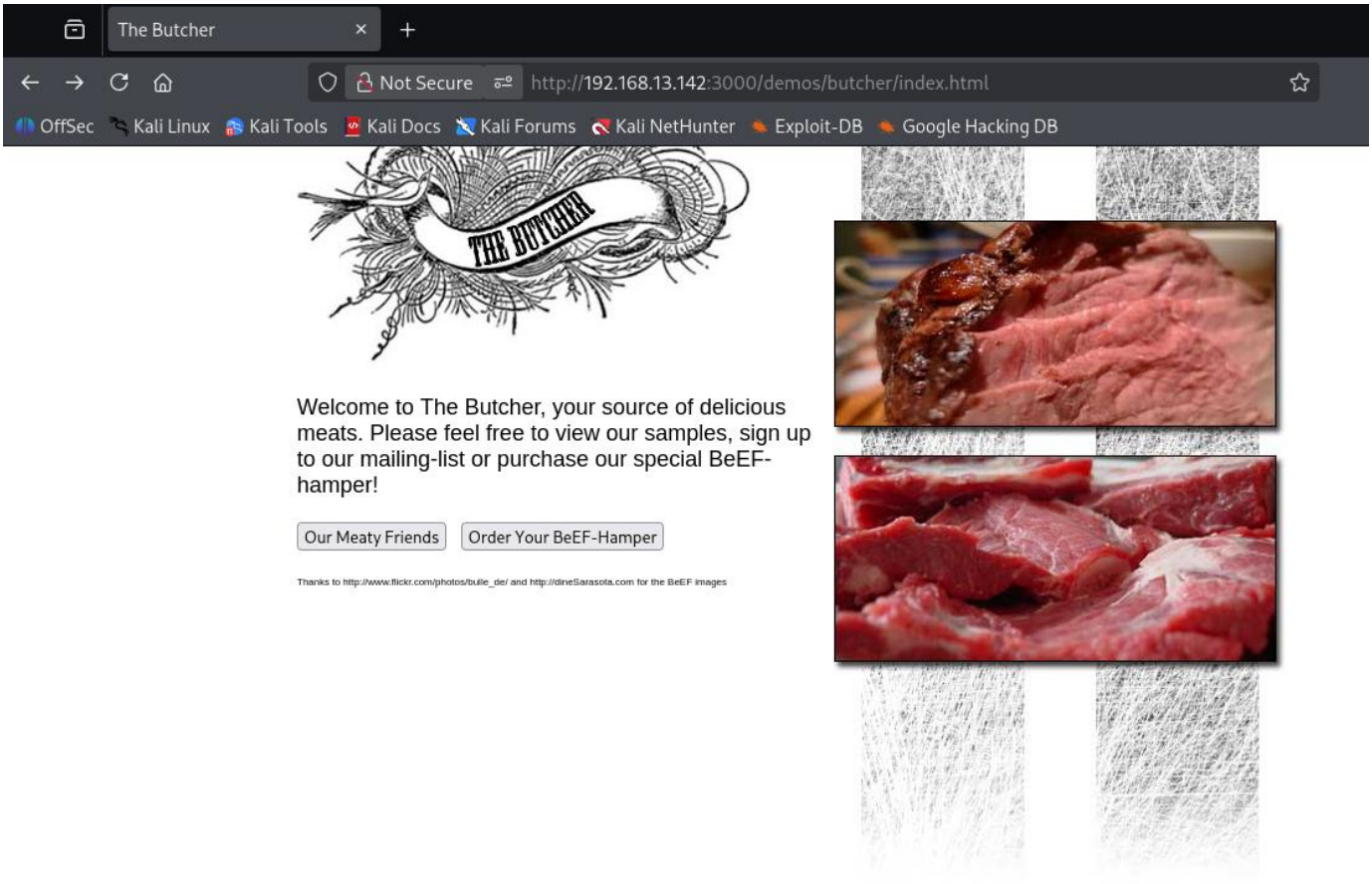
Once done you will see a Webpage opened on a port 3000 login with username and password you set.



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.

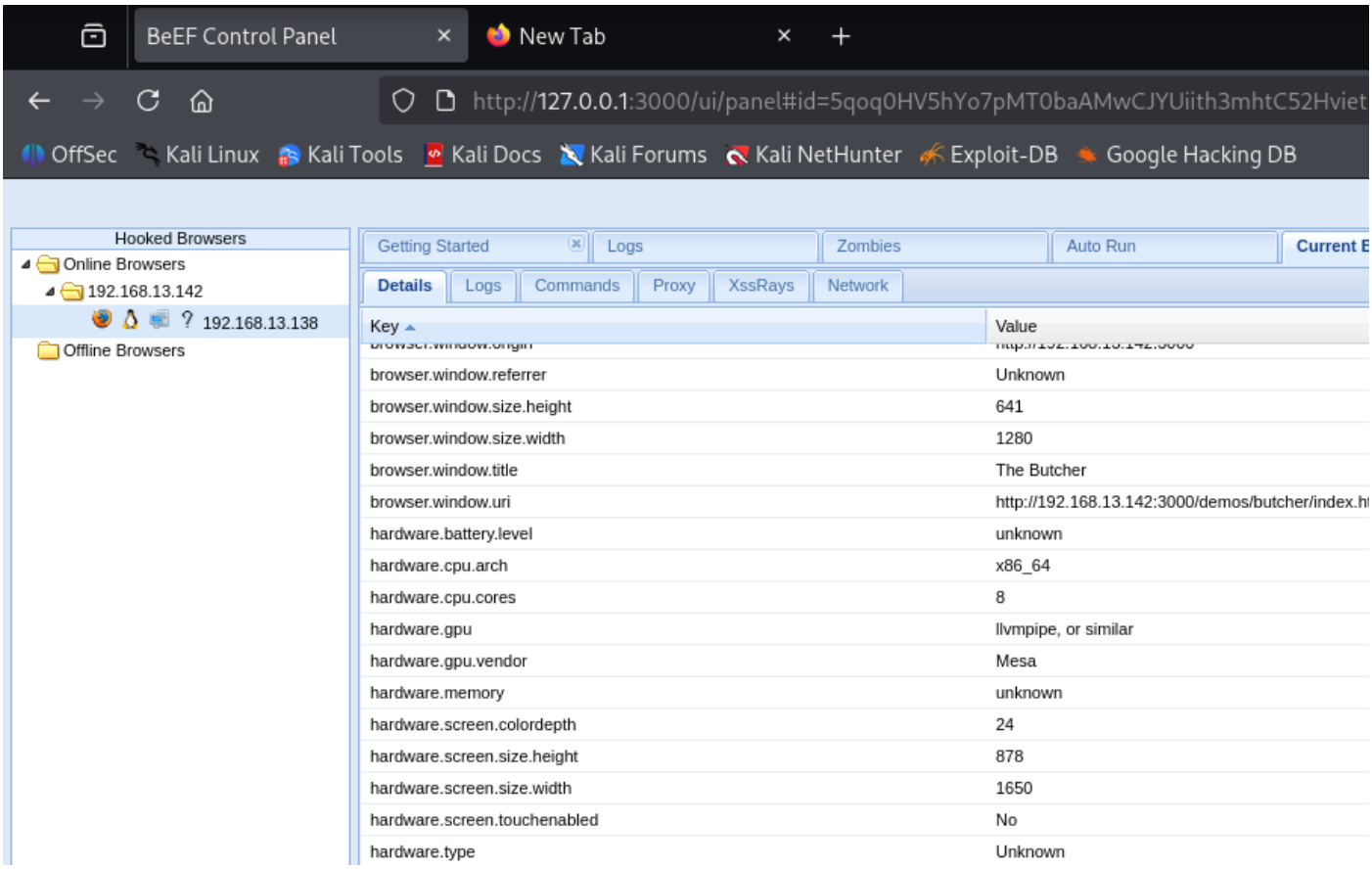


To open it on different machine, edit the localhost address with your actual kali Ip as shown in screenshot below:

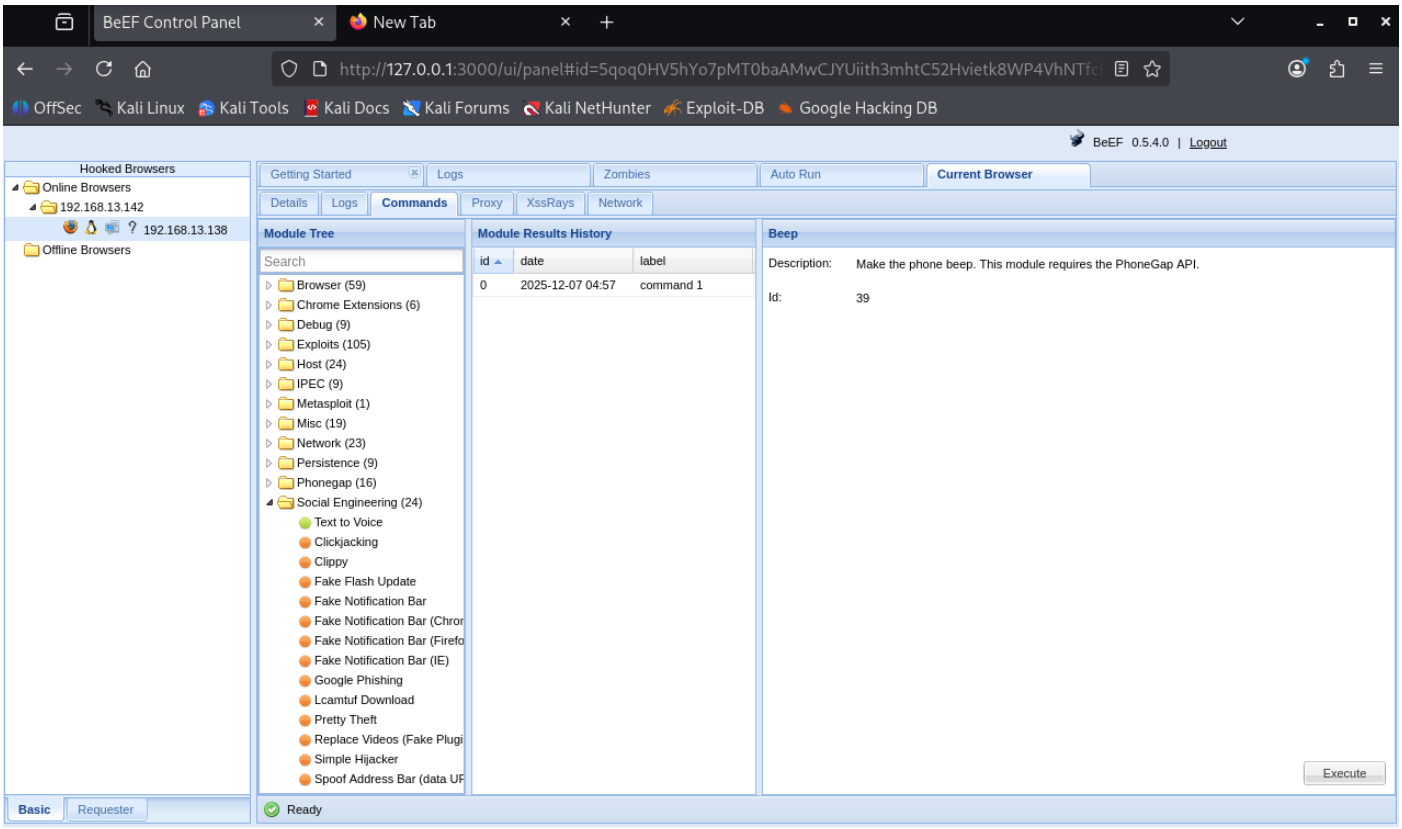


Attack report

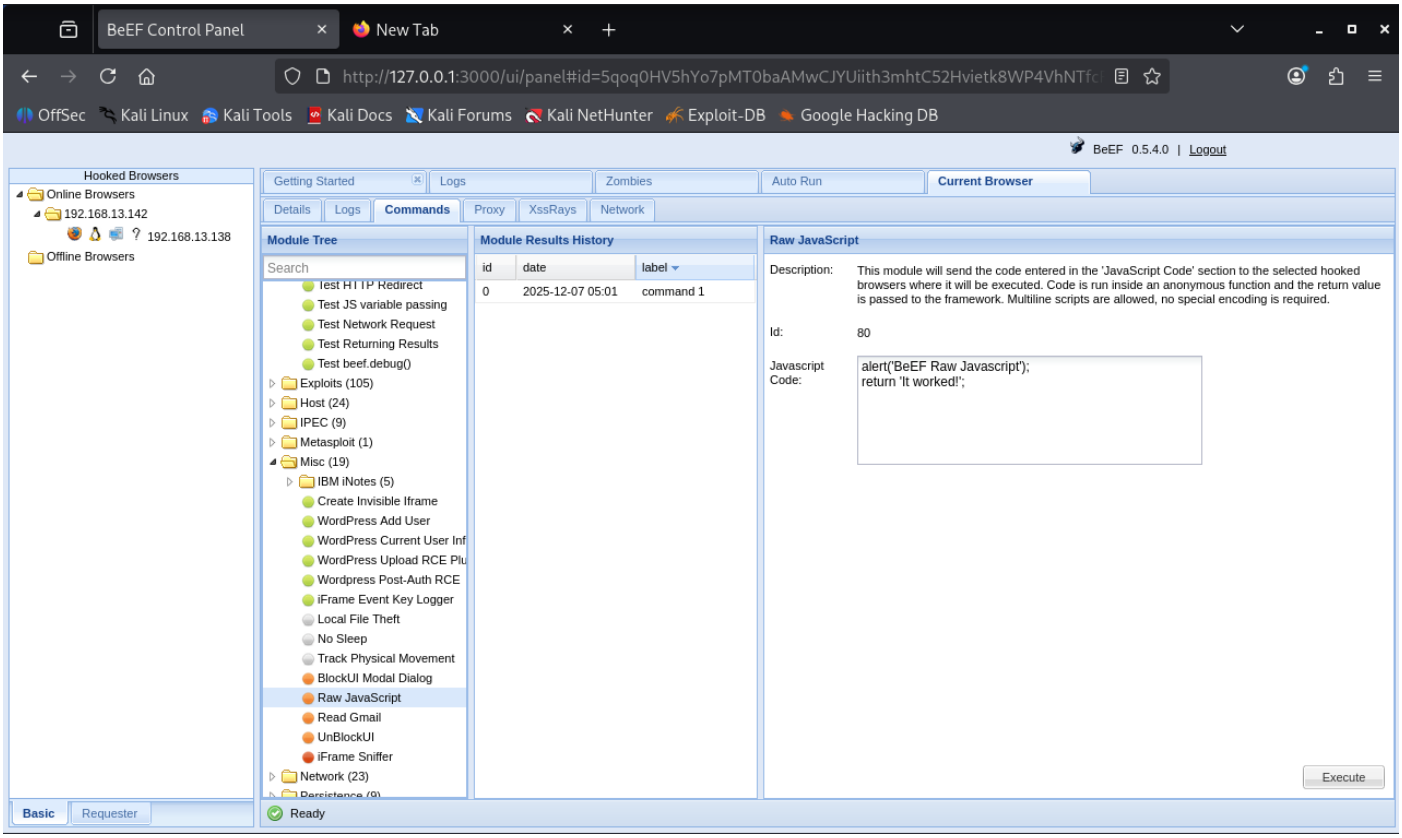
Once the intendent user opens the webpage you are all set now you got the powers, Move back to the beEF portal and open the online browsers and you see a list of browser you have control on and you will see all the details including the what machine it is open on its IP address, screen size and more.



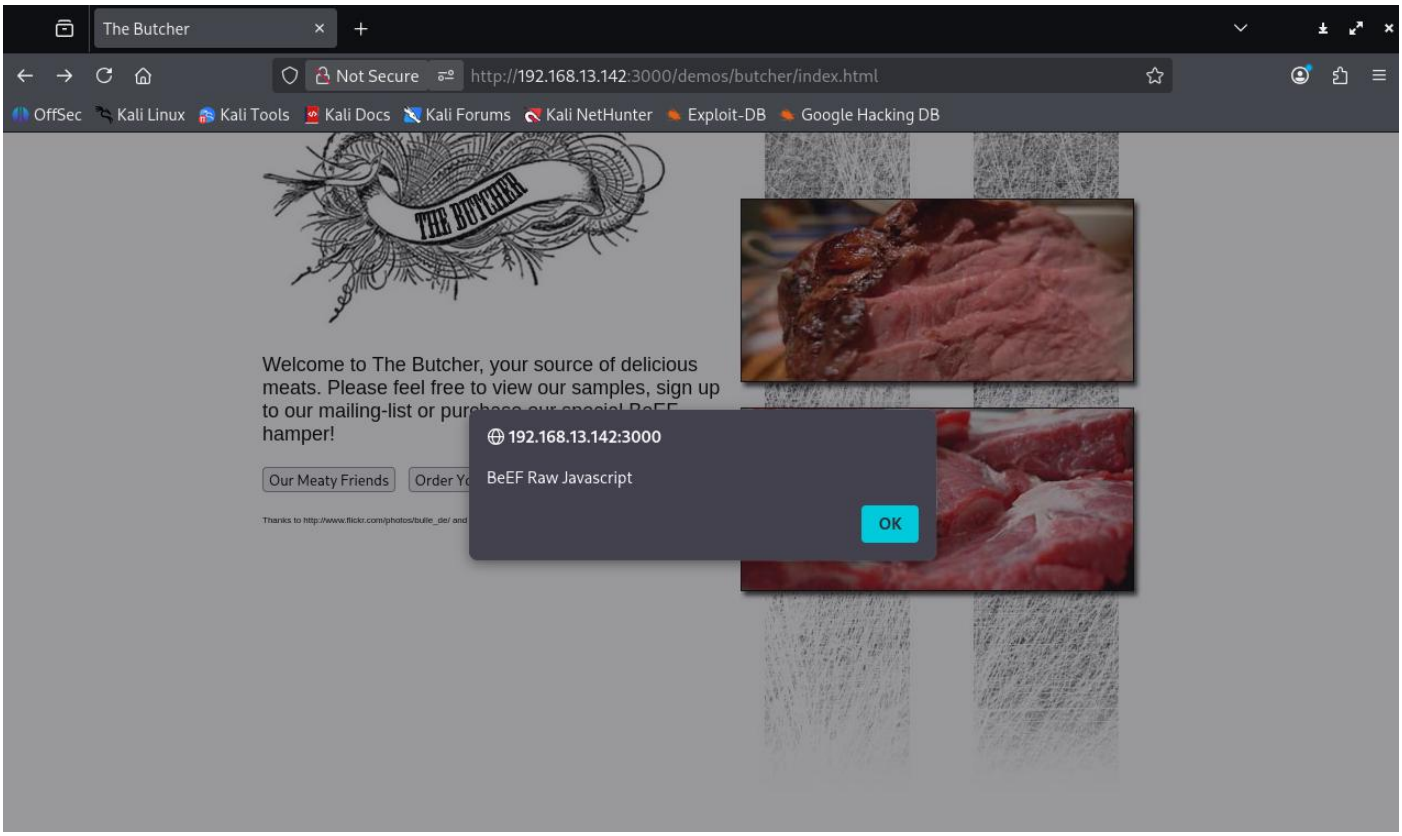
Now move to command tab and you will find a whole lot of prebuilt attack on that as shown below:



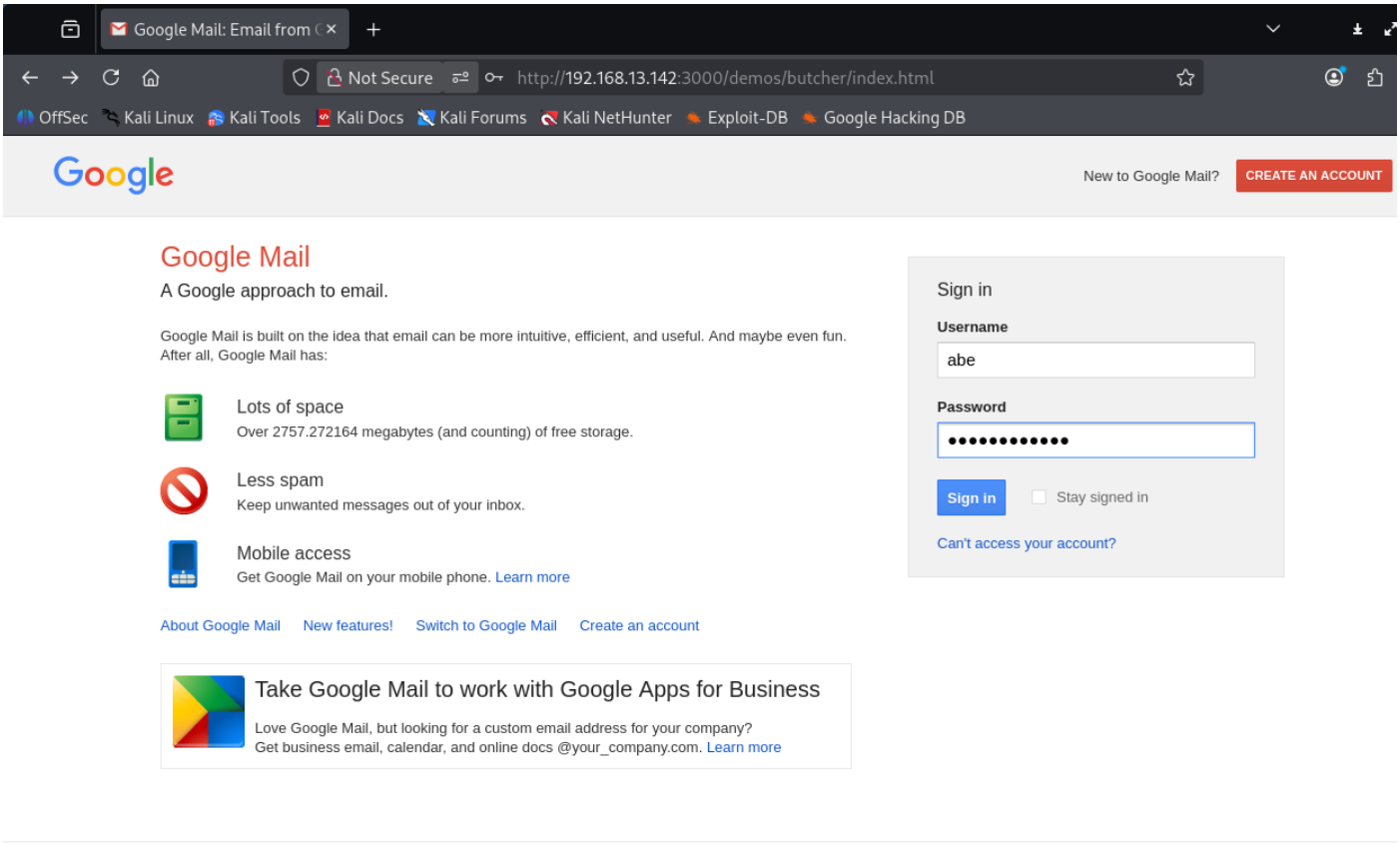
Let’s try to alert a user using a java message box. Go to Misc directory and select Raw JavaScript and you will see a JavaScript code option write you script there and hit execute. I have keep it simple as it is for lab purpose.



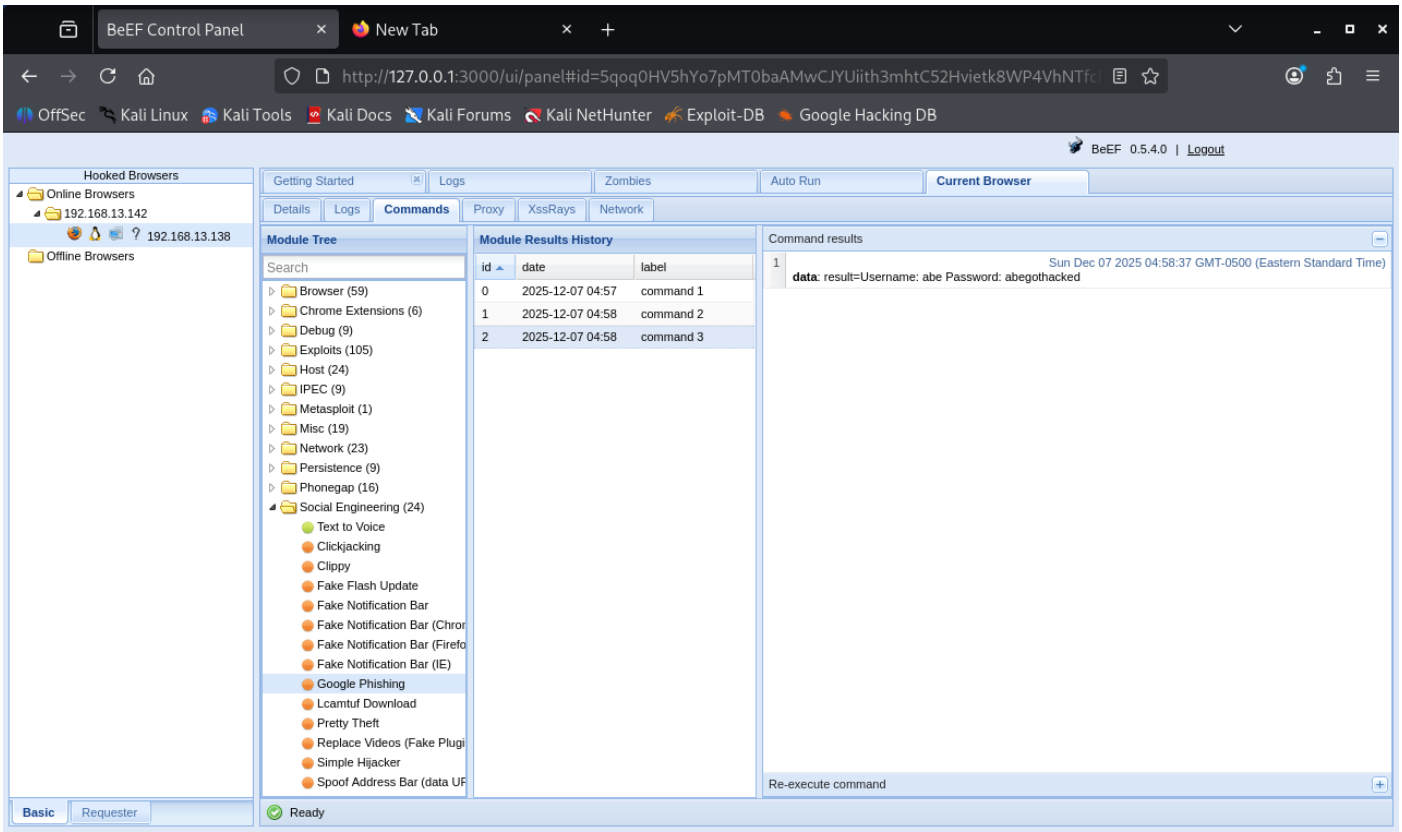
Once you hit execute you will see the output on the machine:



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.