The Browser Exploitation Framework (BeEF)

What is BeEF?

BeEF, short for the Browser Exploitation Framework, is an open-source tool that allows security professionals and researchers to conduct targeted attacks against web browsers. It operates by hooking into a victim's browser, enabling the attacker to monitor the victim's activities, gather information, and execute commands within the context of the browser.

Let see what it is all about.

- First lets install beef in our kali machine.

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

- Launch Beef.

```
beef-xss
```

- Alright to use it we will save a website template and place it in our /var/www/html folder.
- Lets add our Beef hook inside the index.html file.
- Now that we have done with the setup, we just have to send our server IP link to the victim.
- Once the victim has clicked on the link, we got the entry in our Web panel.
- We can see the Operating System and Browser information of our target.
- Next see the commands we can execute on the target, once it is hooked. We have a lot of commands here and all are divided in some categories like Browser, Chrome Extension and much more.
- So if we look into the Getting started section, there is a description for each command.
- Let see the Browser ones first.

This was just an introduction to the BEEF framework, this framework is really cool at what it does and this is not limited to just hooking browsers, we can also use it to inject URL on the network traffic too. But that's out of scope for this module now.

Combining BEEF with your other Client Side attacking technique will give us an extra edge over defenders, gaining almost full control over them.