

Forum:[Hack Forums](#)

Thread: [Introduction to BeEf](#)

Freddy Kru?ger - January 19, 2017, 6:35 am

What is BEeF?

When skids are asked what they use to hack Metasploit is the usual answer, mostly because they don't know any other way to do it. BEeF (I don't know what the lower-case e is for) stands for Browser Exploitation Framework is the equivalent to Metasploit for Browsers. In the land of Web-borne and mobile exploitation, BeEF focuses on one backdoor which is the web browser.

How is BeEF used for hacking?

Before being able to use BeEF's framework one must first "Hook" a browser, BeEF provides a hook URL that can be used. A popular way of Hooking a target is usually by putting the hook script into your webpage. After the target is "hooked" you can begin using the BeEF framework's many commands, including using metasploit.

Running BeEF:

The first thing you're going to have to do is CD to where BeEF is located, on Kali you can do this by inputting the code below:

Code `cd /usr/share/beef-xss` then run the BeEF script

Code `./beef`

This is the console output that should pop up after you run the script.

I know it's a bit confusing but I'll elaborate, Hook UI is the interface where commands are sent and your list of zombies is viewed, we'll be looking into that in a bit. First we're going to talk about the hook URL which is what hooks the victim's browser. Below I'll put an example of some web code which should hopefully clarify how this hook URL is used.

The above is an example of me injecting my hook url into an html page, I am sure this is not the only way to get someone to run your shit, Google or get creative with it.

The BeEF Interface:

Opening the BeEF UI URL will greet you with a browser interface and a log-in screen, the default username and password are both "beef". After logging in you'll be led to the interface where commands can be sent to hooked browsers.

What the interface looks like. ([Click to View](#))

One very important detail to look at is the traffic light system that BeEF uses to tell you what exploits work on the victim. Green means that you can use this exploit on the victim without him knowing.

Orange means you can use an exploit but it may be visible to the target.

Red means the exploit CANNOT be used against the target.

Grey means the target hasn't been measured on this particular exploit.

Conclusion:

That concludes our introduction to BeEF, I hope you learned something from this thread as I had a lot of fun making it. I don't usually contribute shit because I'm lazy but hopefully that will change.

Additional Reading: [BeEF's Website](#)

[BeEF'S Github Page](#)

[BeEF's Wiki](#)

[Using BeEF with Metasploit](#)

Happy Hacking!

Freddy Kru?ger - April 28, 2017, 12:45 am

Giving this a nice bump, not one reply damn.

/Ninja - April 30, 2017, 3:35 am

Good share man. Beef is a neat tool that is included with kali but i have noticed not a whole lot of people use it or really understand it at least the people i know. Excluding seasoned or professional pentesters. it is a very useful tool if you know how to use it.

Glad its being introduced. Also nice job including other reading to go a long with it and increase peoples knowledge on the tool

Dr. Gonzo - April 30, 2017, 9:36 am

Solid intro man. I've been meaning to start using this with XSS. Things like this rarely get much attention because the users on this forum generally lack the foresight to really stop and try to understand things.

/Ninja - April 30, 2017, 12:56 pm

(Apr 30, 2017 09:36 AM)Veridian Wrote: [\[CITE\]](#) Solid intro man. I've been meaning to start using this with XSS. Things like this rarely get much attention because the users on this forum generally lack the foresight to really stop and try to understand things.

Agreed every one wants a click and pwn process... no one takes the time to learn the in and out of a tool or a specific attack vector.

Freddy Kru?ger - May 2, 2017, 12:26 am

Thank you very much for the feedback, I appreciate it.

Lewd - May 2, 2017, 12:30 am

I like this idea.. why is there no replies we must BUMP!

Stop cry - May 2, 2017, 2:04 am

what is this mistake <http://www.img-share.eu/f/images/353/iOa8oHkD.png>

Mr. Robot - May 2, 2017, 2:05 am

Not a bad little tutorial

(May 2, 2017 02:04 AM)Stop cry Wrote: [\[CITE\]](#) what is this mistake
<http://www.img-share.eu/f/images/353/iOa8oHkD.png>

Remove the space
cd /usr/share/beef-xss

You are using CD to get into the folder /usr/share/beef-xss

The way you have it is trying to CD into a folder and run an argument -xss which isn't anything.

// Also OP - BeEF is just Browser Exploitation Framework with Be=Browser and EF= Exploitation Framework

Freddy Kru?ger - May 2, 2017, 11:32 pm

(May 2, 2017 02:05 AM)Mr. Robot Wrote: [\[CITE\]](#) Not a bad little tutorial

Remove the space
cd /usr/share/beef-xss

You are using CD to get into the folder /usr/share/beef-xss

The way you have it is trying to CD into a folder and run an argument -xss which isn't anything.

// Also OP - BeEF is just Browser Exploitation Framework with Be=Browser and EF= Exploitation Framework

Thanks for the enlightenment and the feedback. ?

mecklenburg - May 6, 2017, 5:40 pm

Im working hard to understand beef. I practiced on my own browser in the virtual box. The main thing I dont get is how to hook other browsers. Obviously much more to learn, any tutorials and tips are appreciated

Freddy Kru?ger - July 17, 2017, 6:46 am

(May 6, 2017 05:40 PM)mecklenburg Wrote: [\[CITE\]](#) Im working hard to understand beef. I practiced on my own browser in the virtual box. The main thing I dont get is how to hook other browsers. Obviously much more to learn, any tutorials and tips are appreciated
Here's a nice example of how to hook other browsers.

ripen - July 18, 2017, 8:19 pm

Very informative tutorial , thanks . Also great format!