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.

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.[1] https://www.youtube.com/watch?v=N9Wv7kvlXAY

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!!

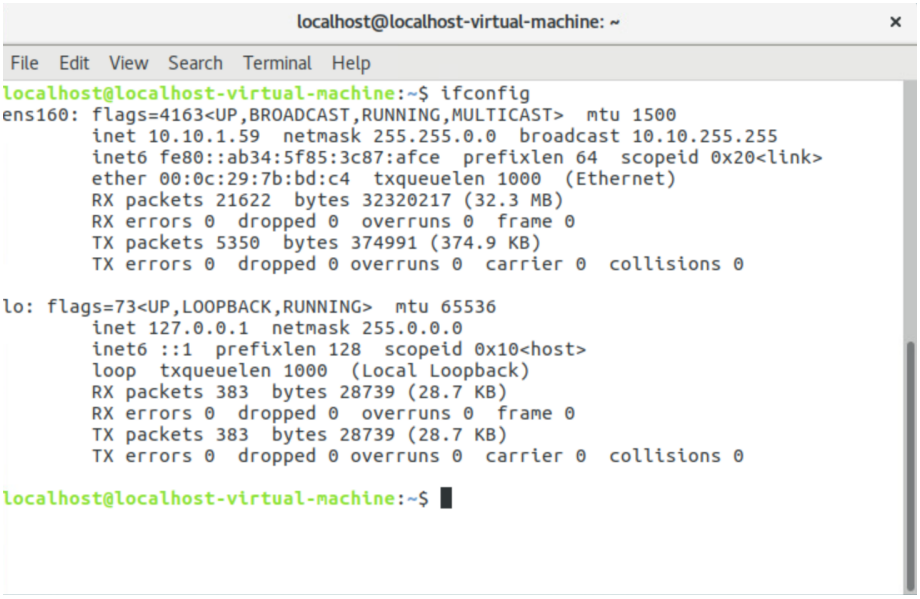
Instructor Note:

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
```

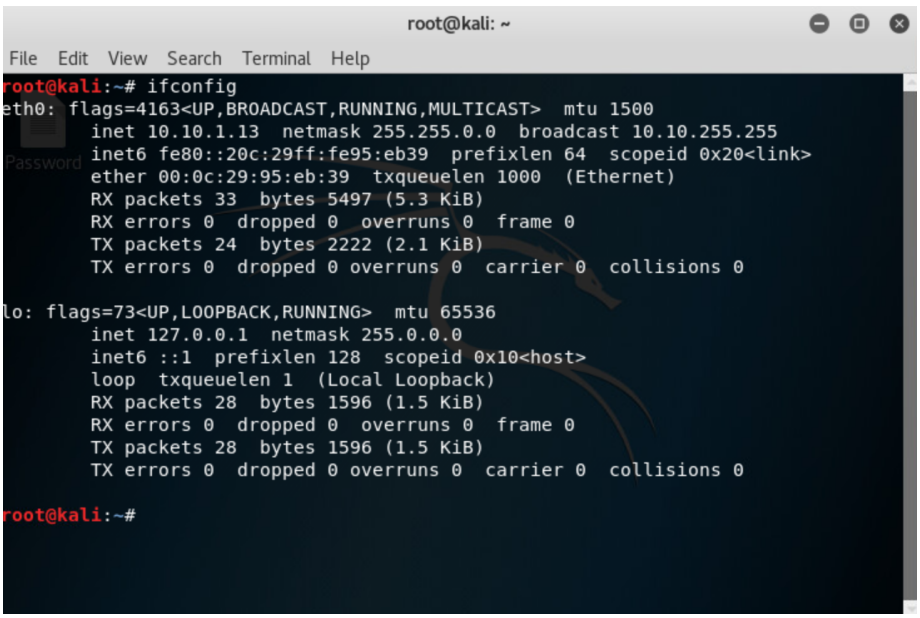
The visual below highlights the results of the 'ifconfig' command being executed on the target machine.



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.

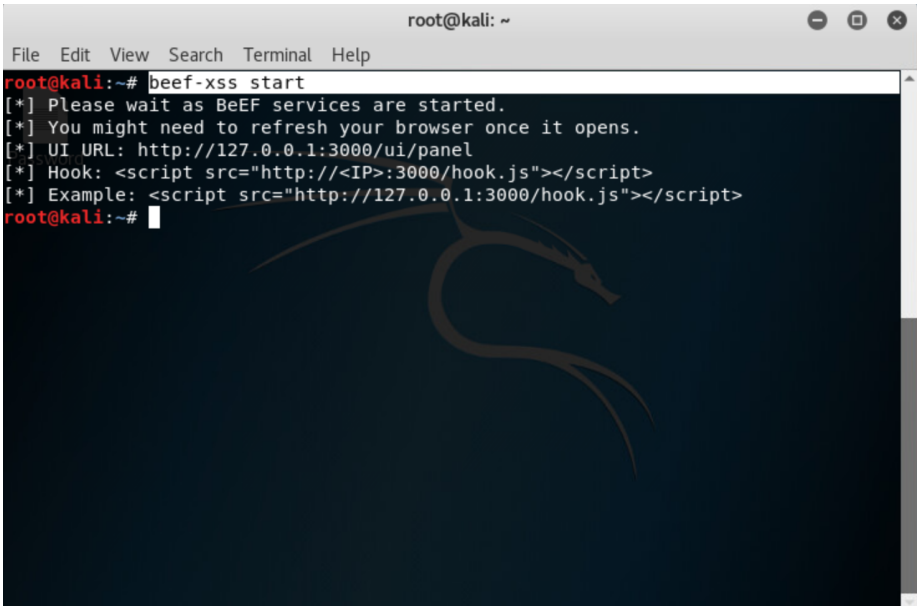


From the visual above, we can see that the IP address of the network interface is 10.10.1.13. This is the IP address for the cyber operator that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Ubuntu and Kali Linux virtual machines.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

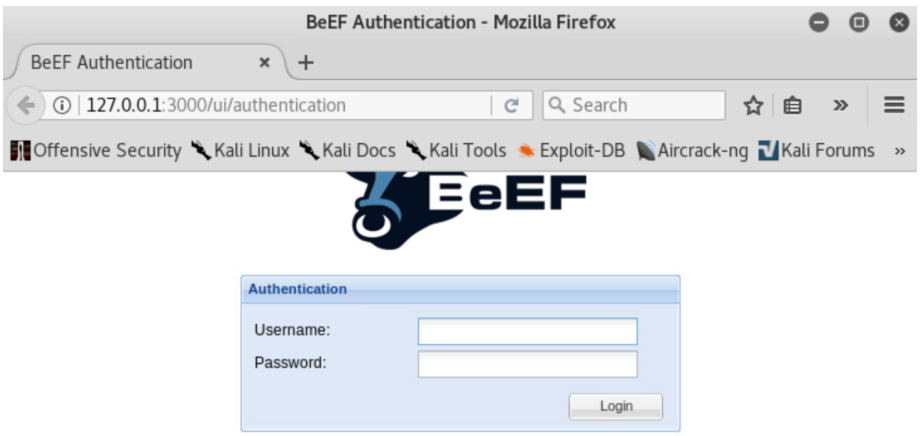
Browser Exploitation Framework (BeEF) Operation

Start the Browser Exploitation Framework

```
beef-xss start
```

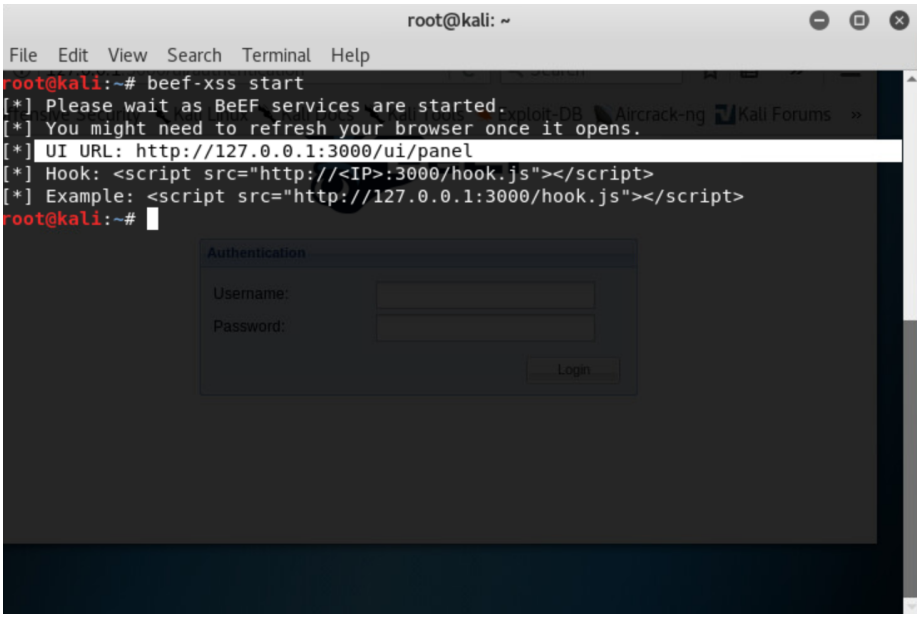


Wait a moment while the web browser is automatically opened to an authentication page.



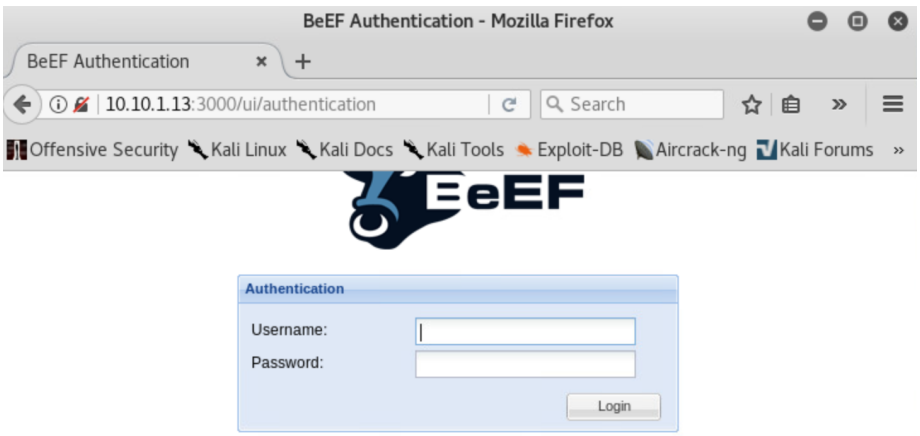
If the web browser does not automatically open, launch it by typing the **UI URL** automatically generated when you started the BeEF.

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



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.

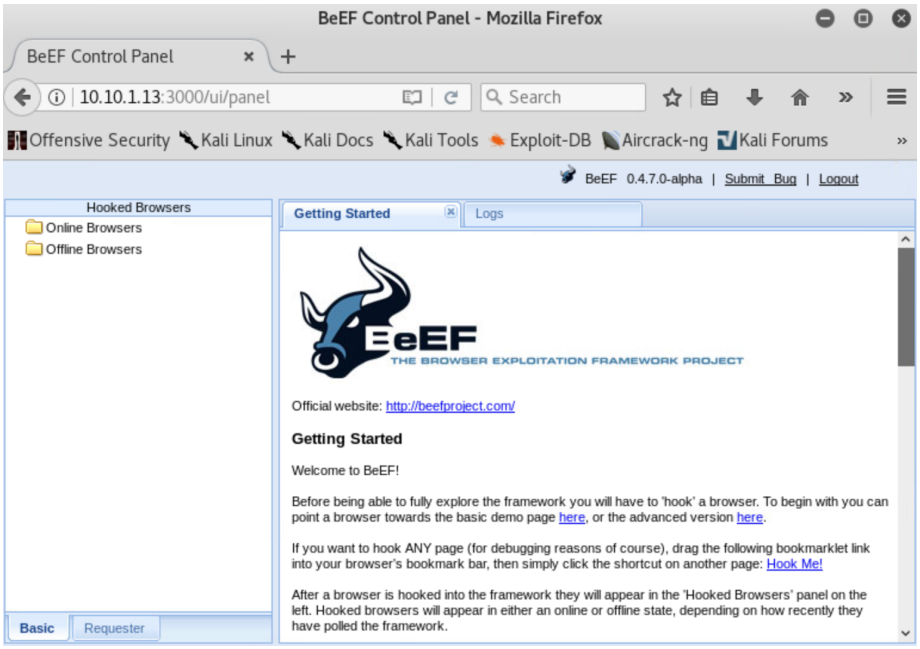
```
http://10.10.1.13
```



Authenticate using the default credentials:

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

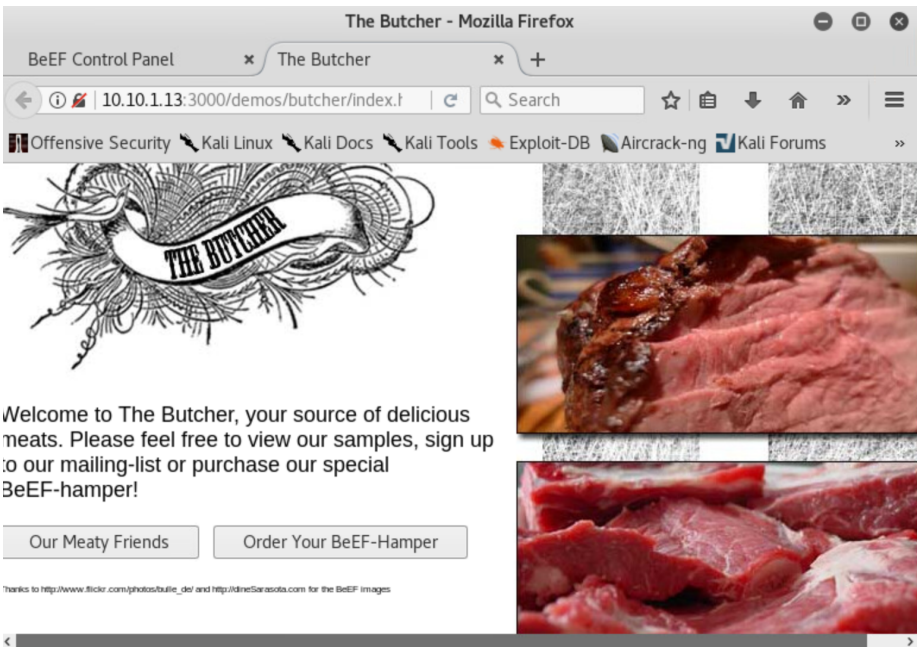
If successful, the following BeEF Control Panel should be visible in the web page of the cyber operator Kali Linux VM.



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

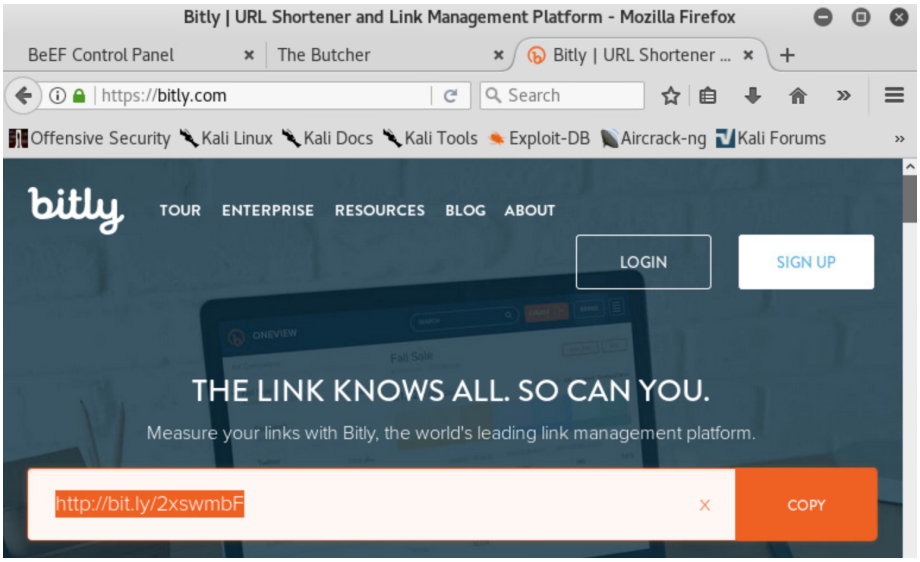
It should open a web page about 'the butcher'.

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



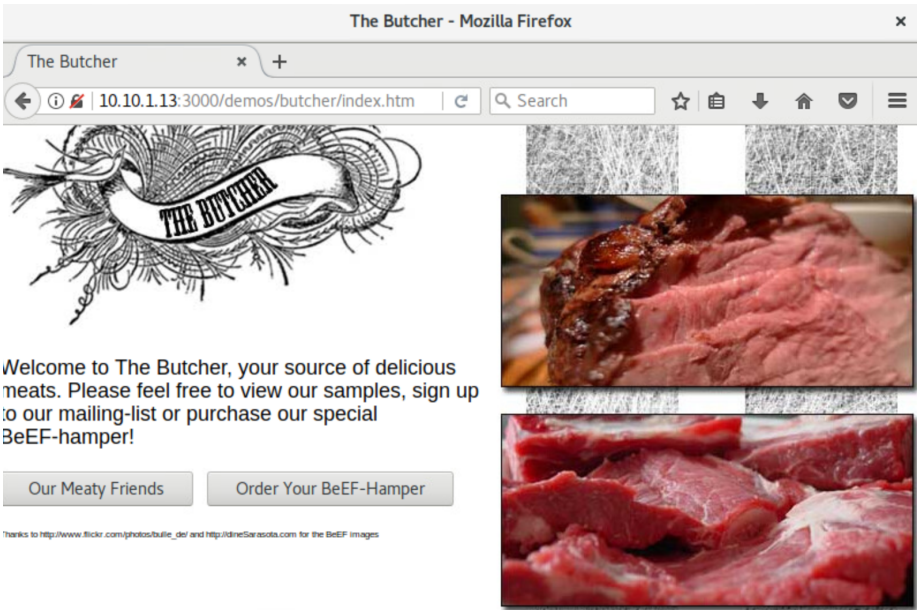
Before we have our target visit the web page, we need to obfuscate the link.

Use a service such as Bitly to obfuscate the link.

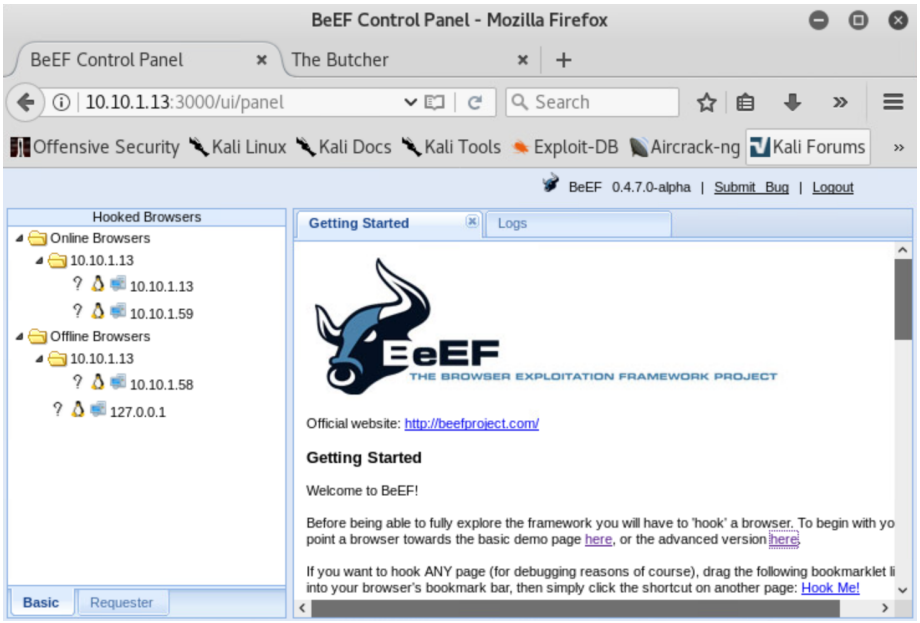


Open the target VM, and then open a web browser.

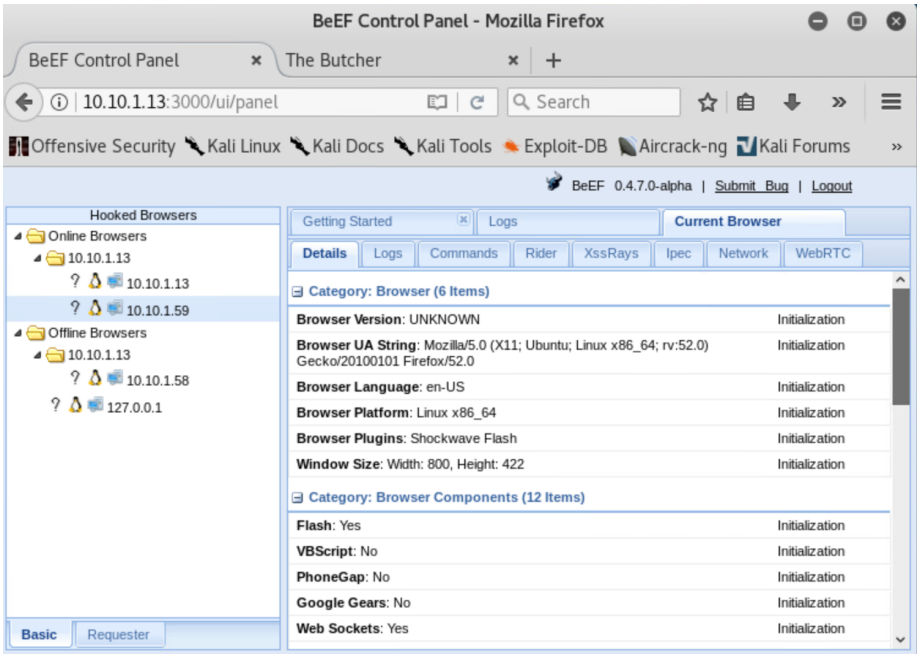
Type in the obfuscated URL in the web browser address bar.

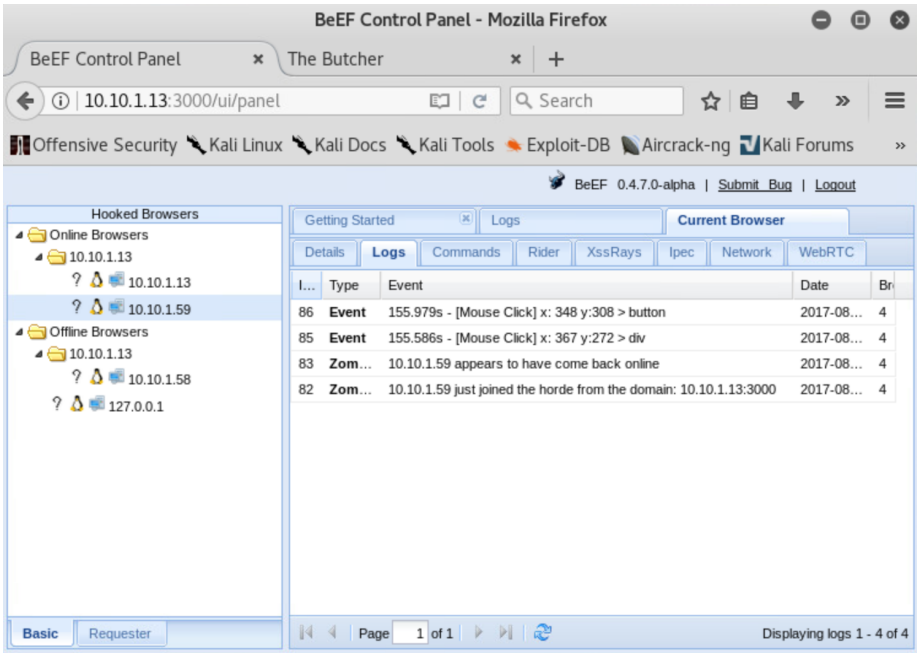


The target VM IP address should now appear under the **Online Browsers** folder on the offensive cyber operator Kali Linux VM.

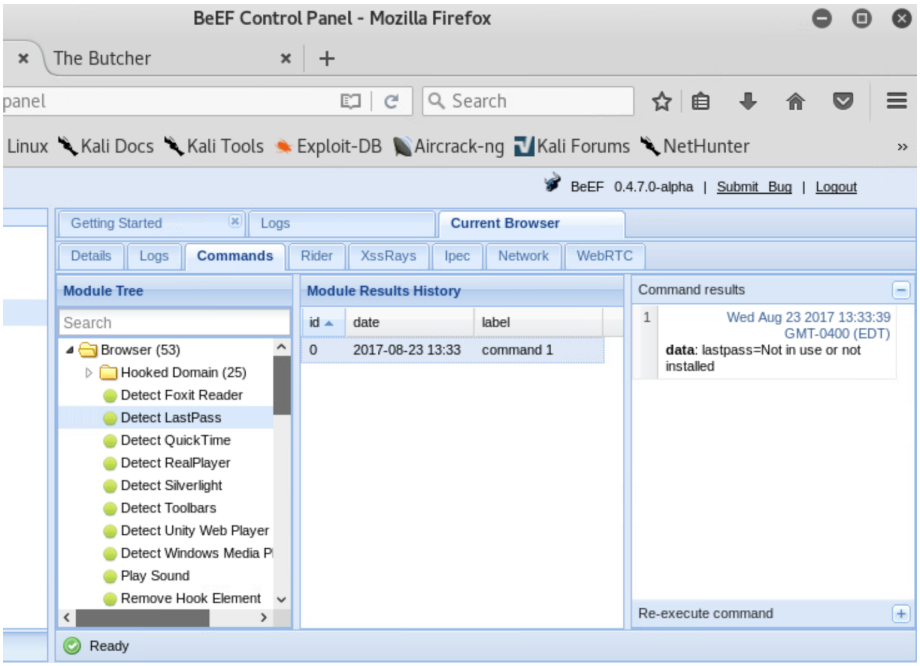


MIDN should take a screenshot of the Details and Logs tab.

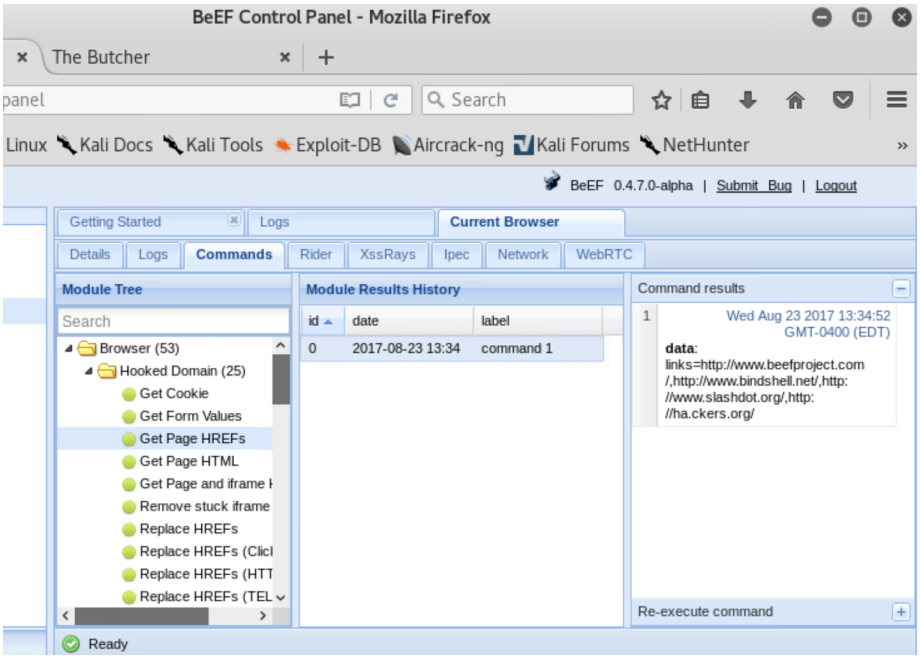




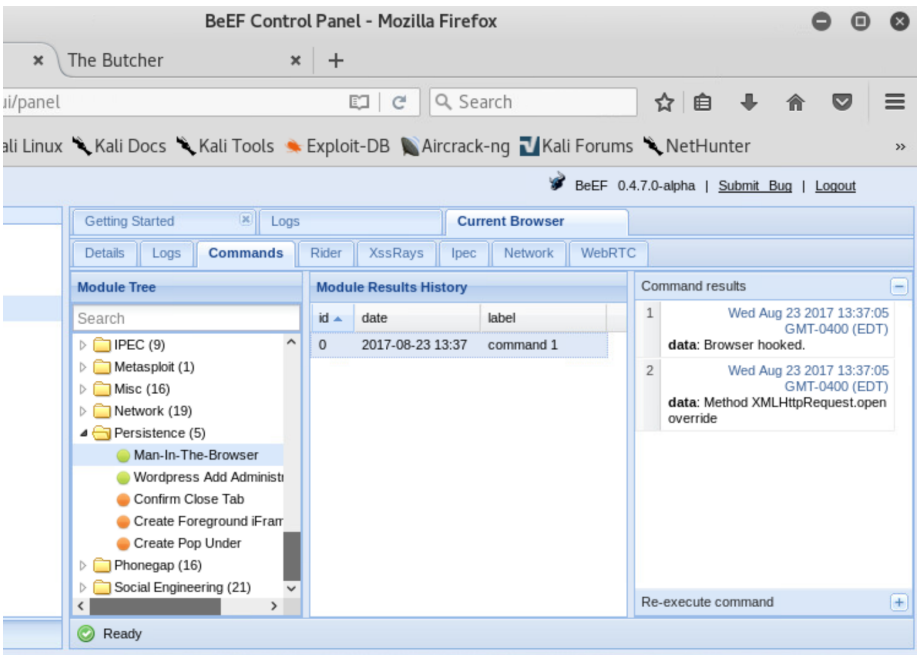
MIDN should now visit and take a screenshot of the LastPass Browser Command to determine if passwords are stored.



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