



ETHICAL HACKING LAB SERIES

Lab 12: Client Side Exploitations

Material in this Lab Aligns to the Following Certification Domains/Objectives		
Certified Ethical Hacking (CEH) Domains	Offensive Security (PWK) Objectives	SANS GPEN Objectives
13: Hacking Web Applications	13: Client Side Attacks	6: General Web Application Probing

Document Version: 2016-03-09

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC² is a registered trademark of EMC Corporation.

Contents

Introduction	3
Objective	3
Pod Topology	4
Lab Settings	5
1 Hooking Browsers with BeEF Framework.....	6
2 Client Exploitation with BeEF Framework	10

Introduction

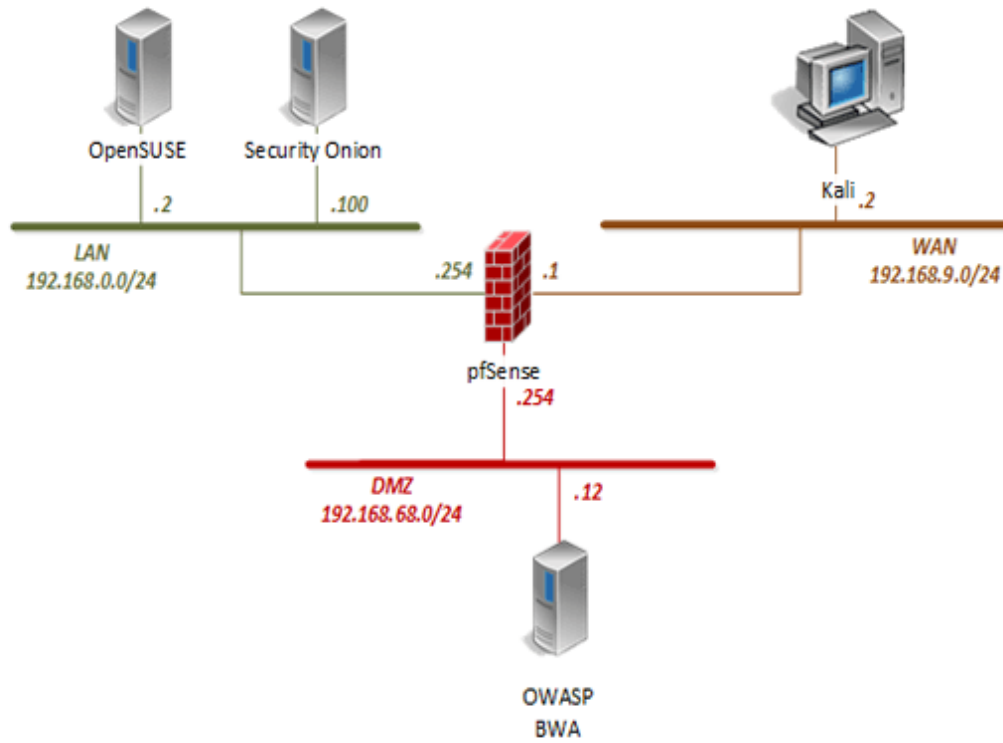
Browsers are susceptible to exploitation and can be used to gain access to the computer system and network. In this lab, we will use the BeEF framework to specifically target the browser and exploit the browser.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Hooking Browsers with BeEF Framework
2. Client Exploitation with BeEF Framework

Pod Topology



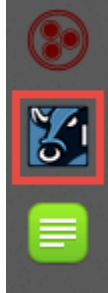
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali Linux	192.168.9.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

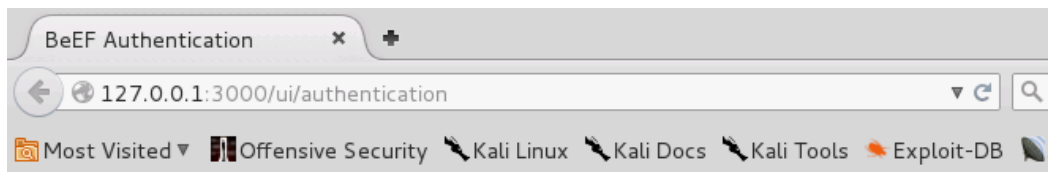
1 Hooking Browsers with BeEF Framework

1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Click **Next**.
4. Enter `toor` as the *password*. Click **Sign In**.
5. Open the *BeEF Framework* by clicking on the **BeEF** icon located on the left panel.



Wait about 1-2 minutes until a web browser appears with a *BeEF* login page.

6. Login with `beef` as the *username* and `beef` as the *password*. Click **Login**.



Authentication

Username:

Password:

7. Notice on the left panel the local host address is listed. Working with BeEF, a victim is needed to hook their browser. In the middle pane, there are two demo links, click on the **here** hyperlink to navigate to the *BeEF Basic Demo* page.



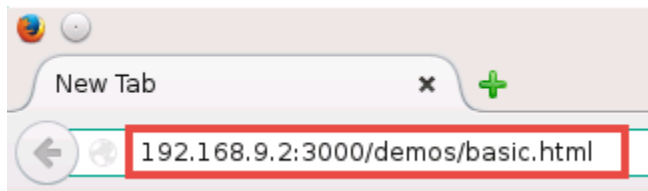
Official website: <http://beefproject.com/>

Getting Started

Welcome to BeEF!

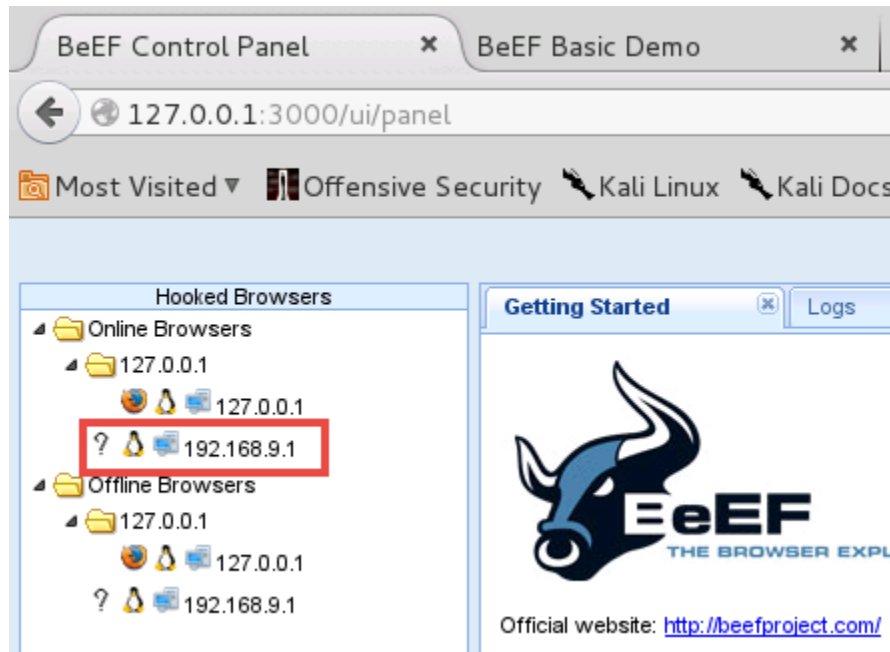
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#), or the advanced version [here](#).

8. Leave the *BeEF Demo* page open and navigate to the **topology** page. Click on the **OpenSUSE** VM icon.
9. Login with **osboxes** as the *username* and **osboxes.org** as the *password*. Press **Enter**.
10. Once logged in, launch *Firefox* by clicking on the **Firefox** quick launch icon located on the bottom panel.
11. When viewing the *Firefox* browser, enter **192.168.9.2:3000/demos/basic.html** into the address field. Press **Enter**.

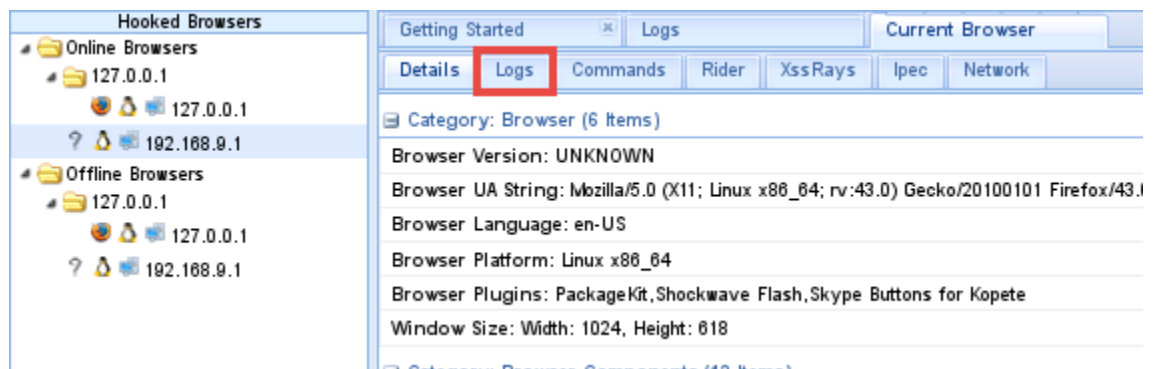


12. Leave the Firefox browser opened and navigate back to the **Kali** VM.
13. Make sure to view the **Iceweasel** browser and click on the **first tab**, which should be the **BeEF Control Panel**.

14. Notice on the *Hooked Browsers* list towards the left, a new online browser appears. Click on **192.168.9.1**.

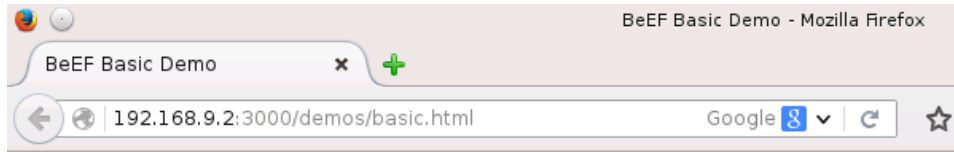


15. Once the hooked browser is selected, notice the given information in the middle pane. It appears that the browser that is hooked is running *Firefox* version 43 based on the *Browser UA String*. Click on the **Logs** tab.



16. Generate some events so they can be analyzed on the *Logs* tab. Navigate back to the **OpenSUSE** VM.

17. While viewing the *Firefox* browser, type **secret** into the *Insert your secret here:* text field. Press **Enter**.



You should be hooked into **BeEF**.

Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module

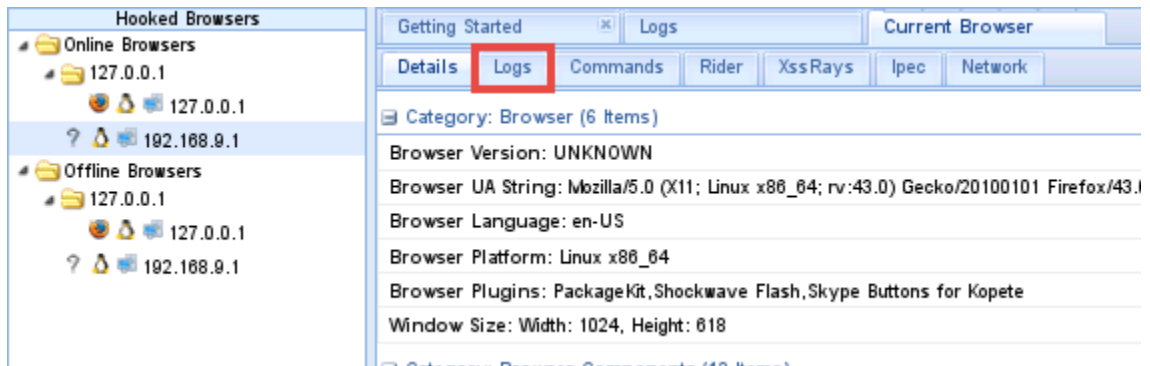
- [The Browser Exploitation Framework Project homepage](#)
- [ha.ckers.org homepage](#)
- [Slashdot](#)

Have a go at the event logger.

Insert your secret here:

You can also load up a more advanced demo page [here](#)

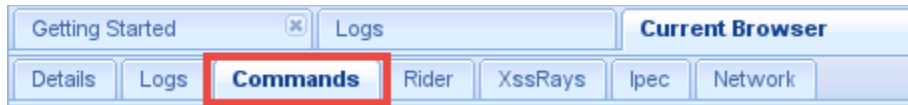
18. Navigate back to the **Kali** VM.
19. While viewing the **BeEF Control Panel** tab, press the **F5** key to refresh the page.
20. Click on **192.168.9.1** from the *Hooked Browsers* pane underneath *Online Browsers*.
21. In the middle pane, click on the **Logs** tab.



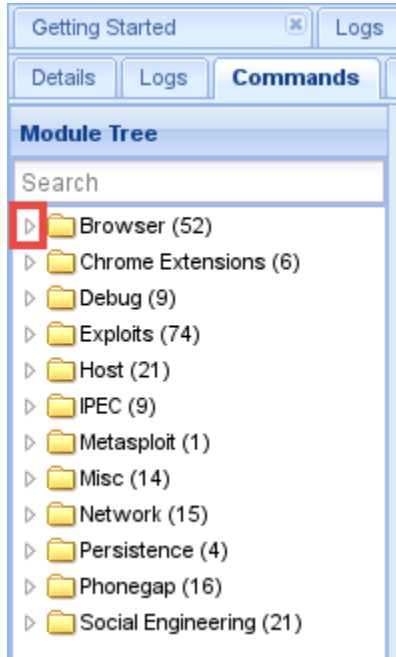
Notice some events are shown here, including captured keystrokes.

2 Client Exploitation with BeEF Framework

1. Click on the **Commands** tab in the middle pane.

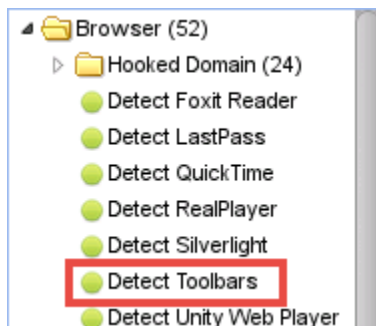


2. In the *Module Tree* pane, expand the **Browser** inventory.



Once expanded, notice the different colors presented. The color *green* means that those commands can be used, the color *orange* means that the commands may not work and the color *red* means that the commands do not work against the current browser.

3. From the same pane, click on **Detect Toolbars**.



- Once selected, click the **Execute** button located on the bottom right corner.

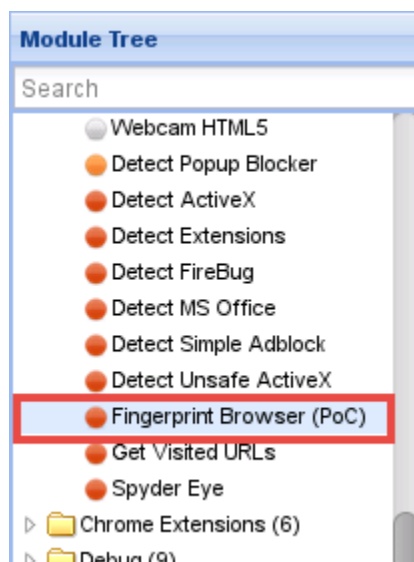


- Notice the *Module Results History* pane populates. Click on the **command 1** result.

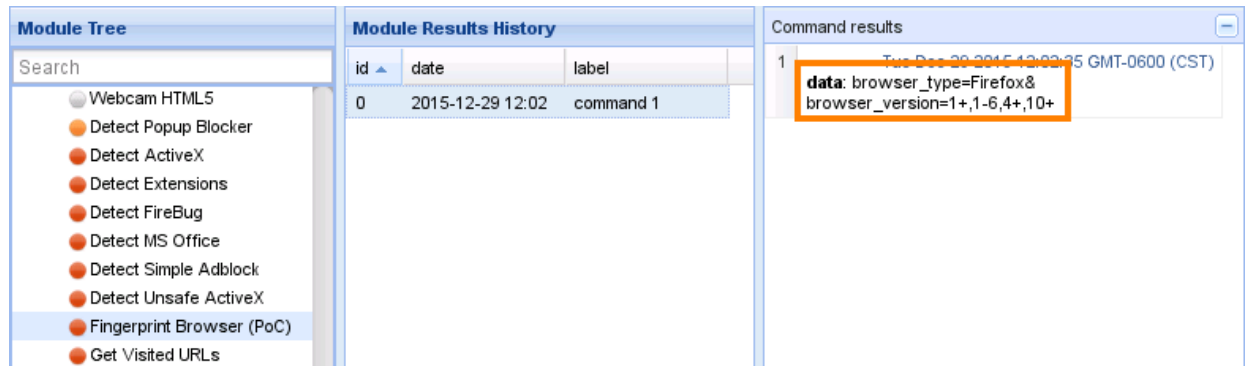
Module Results History		
id	date	label
0	2015-12-29 11:50	command 1



- Notice in the *Command results* pane that no toolbars have been detected.
- Focus on the *Module Tree* pane and select **Fingerprint Browser (PoC)**.



8. Once selected, click the **Execute** button.
9. Notice the *Module Results History* pane populates. Select the **command 1** entry.
10. The given results show that the hooked browser has been successfully fingerprinted.



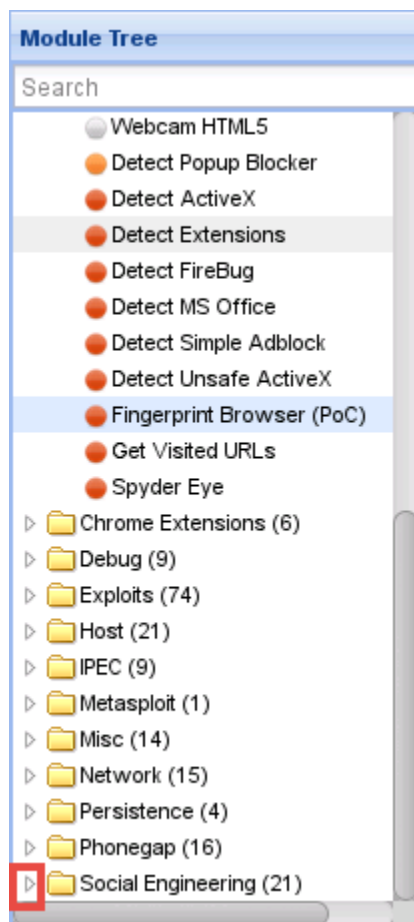
The screenshot displays three panes from the application interface:

- Module Tree:** A list of modules with 'Fingerprint Browser (PoC)' selected and highlighted in blue.
- Module Results History:** A table with columns 'id', 'date', and 'label'. It contains one entry:

id	date	label
0	2015-12-29 12:02	command 1
- Command results:** A pane showing the results of the selected command. It displays a timestamp 'Tue Dec 29 2015 12:02:25 GMT-0600 (CST)' and a data block:

data: browser_type=Firefox&
 browser_version=1+,1-6,4+,10+

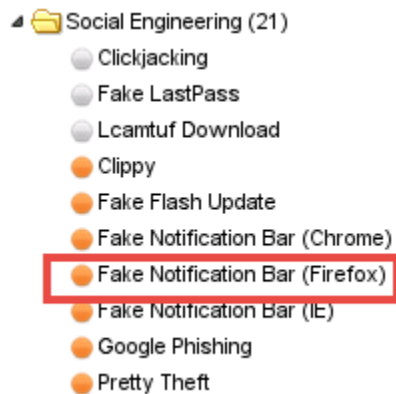
11. In the *Module Tree* pane, expand the **Social Engineering** inventory.



The screenshot shows the 'Module Tree' pane with a search bar at the top. A list of modules and folders is displayed. The 'Social Engineering (21)' folder is expanded, indicated by a red rectangle around the folder icon and its name. The expanded list includes:

- Webcam HTML5
- Detect Popup Blocker
- Detect ActiveX
- Detect Extensions
- Detect FireBug
- Detect MS Office
- Detect Simple Adblock
- Detect Unsafe ActiveX
- Fingerprint Browser (PoC)
- Get Visited URLs
- Spyder Eye
- Chrome Extensions (6)
- Debug (9)
- Exploits (74)
- Host (21)
- IPEC (9)
- Metasploit (1)
- Misc (14)
- Network (15)
- Persistence (4)
- Phonegap (16)
- Social Engineering (21)

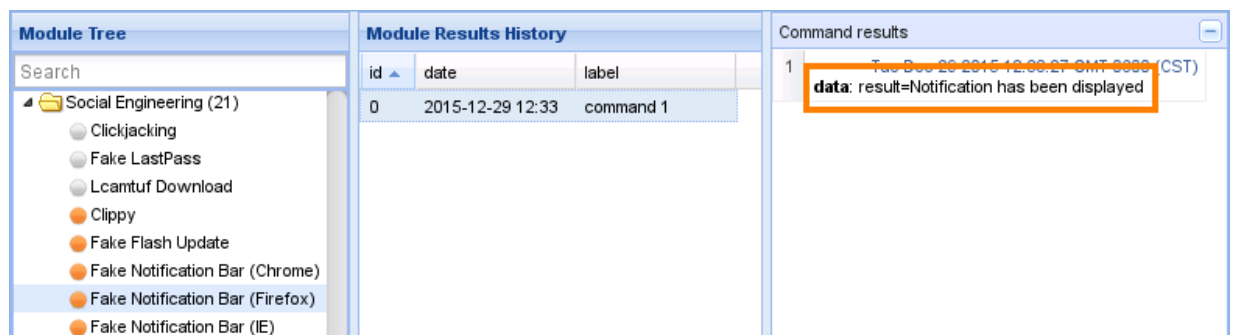
12. Select **Fake Notification Bar (Firefox)** from the same pane.



13. Once selected, click the **Execute** button.

14. The *Module Results History* pane should populate, click the **command 1** entry.

15. Notice the result indicates that a notification has been displayed. Switch to the **OpenSUSE VM**.

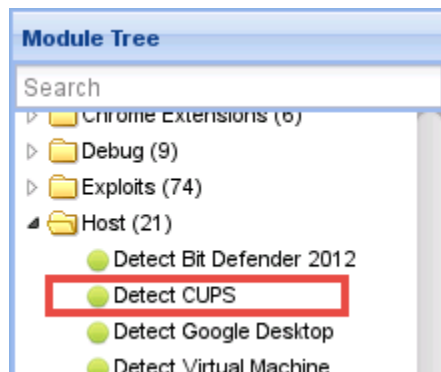


16. Focus on the **Firefox** web browser and notice a notification is present, asking to install a plug-in. Don't install the plug-in.

17. Navigate back to the **Kali VM**.

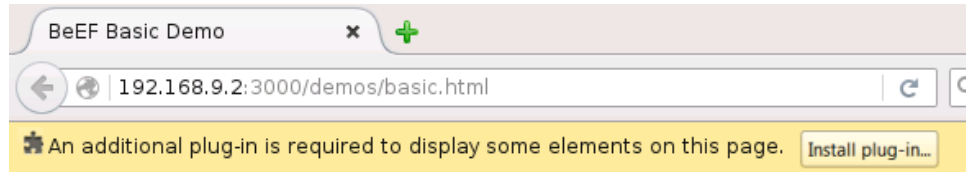
18. Using the *BeEF Framework*, expand the **Host** inventory item in the *Module Tree* pane.

19. Select **Detect CUPS** from the same pane.



20. Click the **Execute** button.

21. The *Module Results History* pane should populate, click the **command 1** entry.
22. Notice the result indicates that CUPS has been installed. Switch to the **OpenSUSE VM**.
23. While viewing the **BeEF Basic Demo** tab on the *Firefox* window, click the **here** link found after "You can also load up a more advanced demo page".



Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module

- [The Browser Exploitation Framework Project homepage](#)
- [ha.ckers.org homepage](#)
- [Slashdot](#)

Have a go at the event logger.

Insert your secret here:

You can also load up a more advanced demo page [here](#)

24. Once the webpage redirects, click the **Order Your BeEF-Hamper** button.



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/bulle_de/ and <http://dineSarasota.com> for the BeEF images

25. Notice that a few text fields appear. Fill in each text field using the information below:

- Name: Sally
- Phone: 000-000-0000
- Address: 234 S Lane
- Credit Card: 6011000990139424

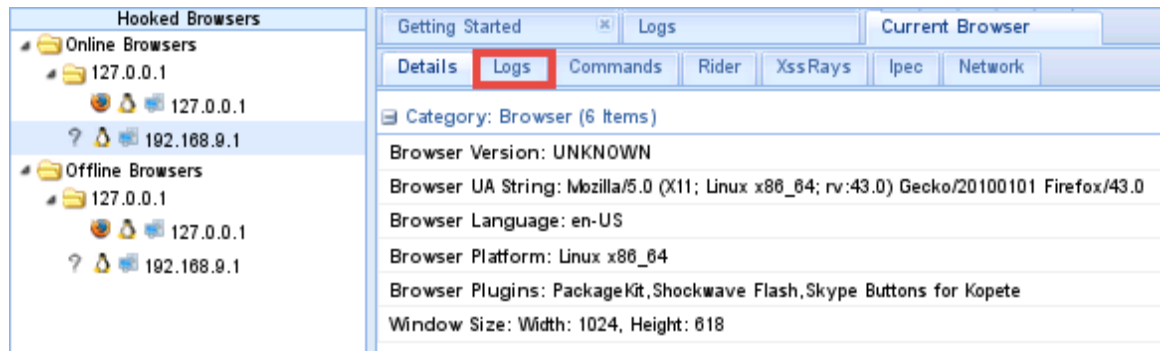
26. Click the **Buy buy!** button.

27. Switch to the **Kali** VM.

28. While viewing the *BeEF Control Panel* tab, press **F5** to refresh the page.

29. Click on **192.168.9.1** from the *Hooked Browsers* pane underneath *Online Browsers*.

30. In the bottom middle pane, click on the **Logs** tab.



Notice the captured keystrokes from the hooked browser.

31. Close the **Kali** and **OpenSUSE** PC viewers.