Network Penetration Testing Methodology-Internal

6 Hr 33 Min Remaining

Instructions Resources Help  100%

Exercise 23: Penetration Testing Vulnerable Machines and Creating a Botnet

Scenario

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-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester 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 the 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.

The objective of this lab is to help students learn how to:

* Use the Browser Exploitation Framework (BeEF)
* Establish a botnet of vulnerable machines

**Lab Duration**: **25** Minutes

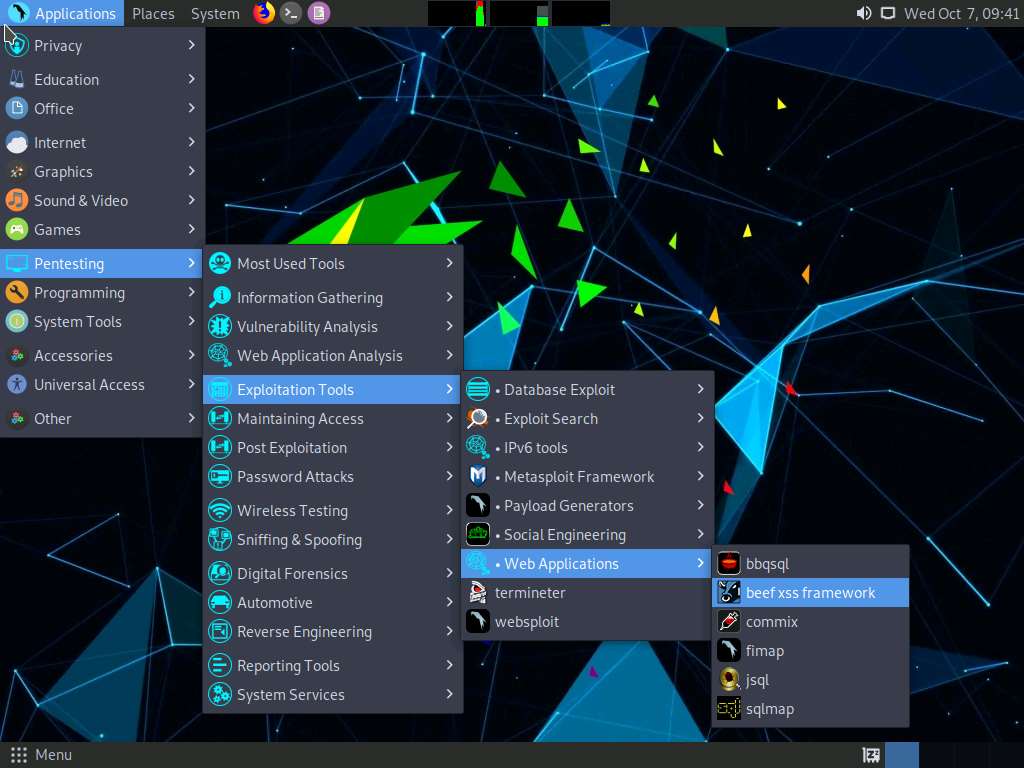
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



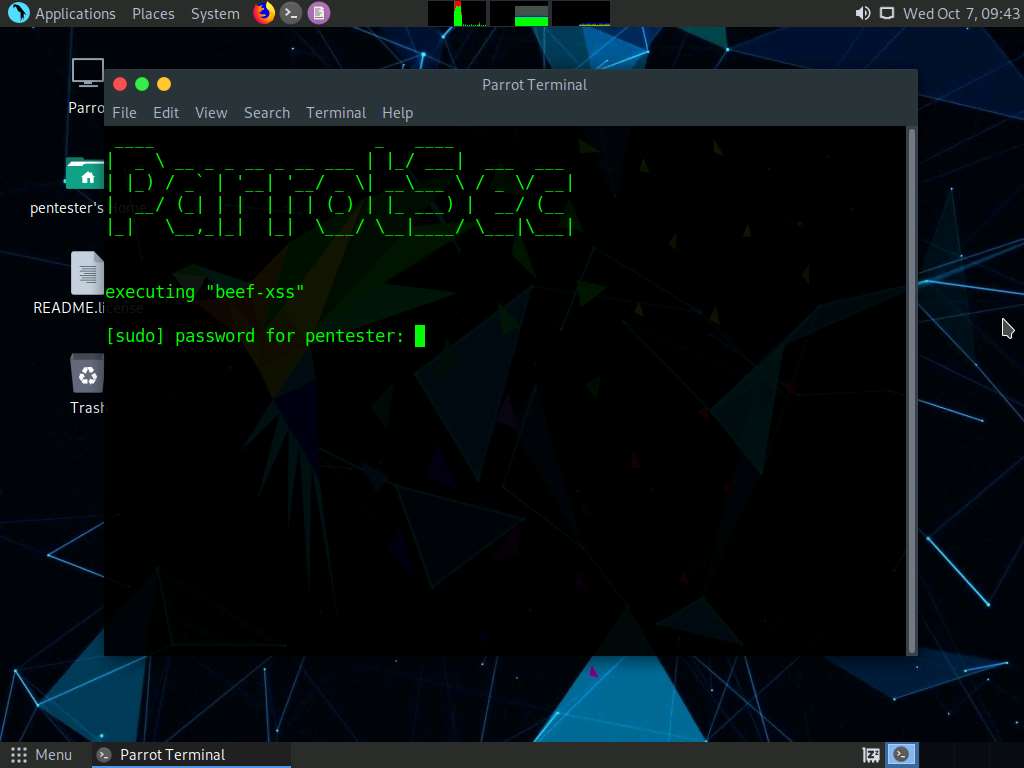
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



1. Launch BeEF framework. Navigate to **Applications** | **Pentesting** | **Exploitation Tools** | **Web Applications** | **beef xss framework**.



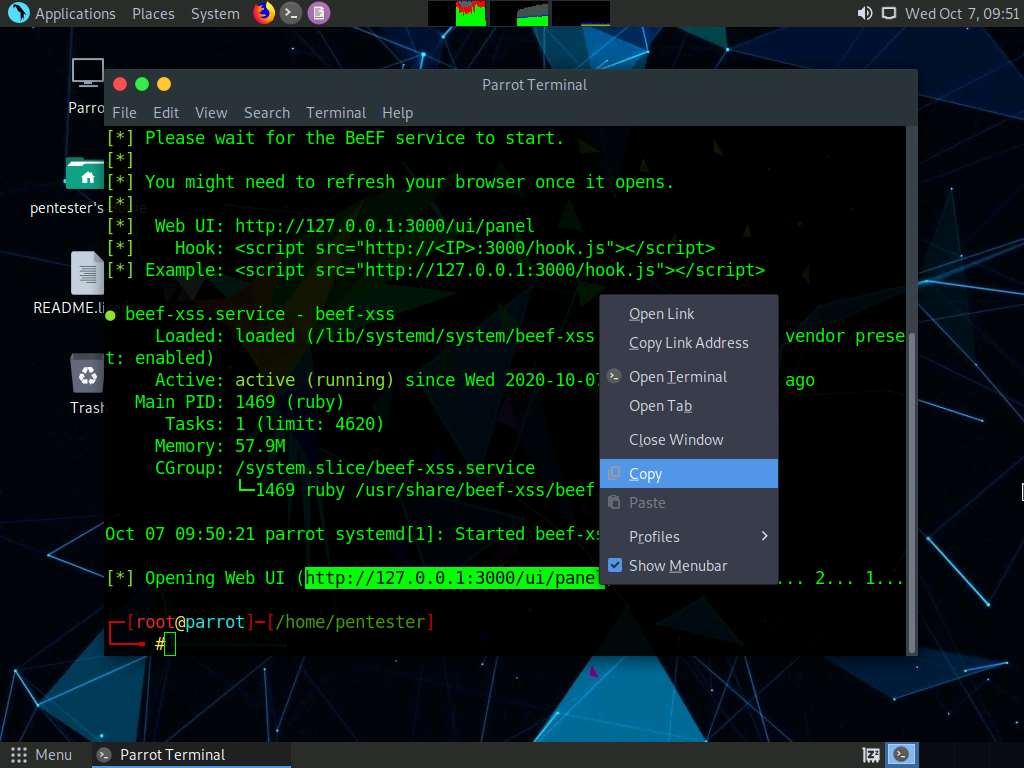
1. Type **toor** and press **Enter**.



1. Please type a new password prompt appears, type the password of your choice. In this exercise we are typing password as **test**.

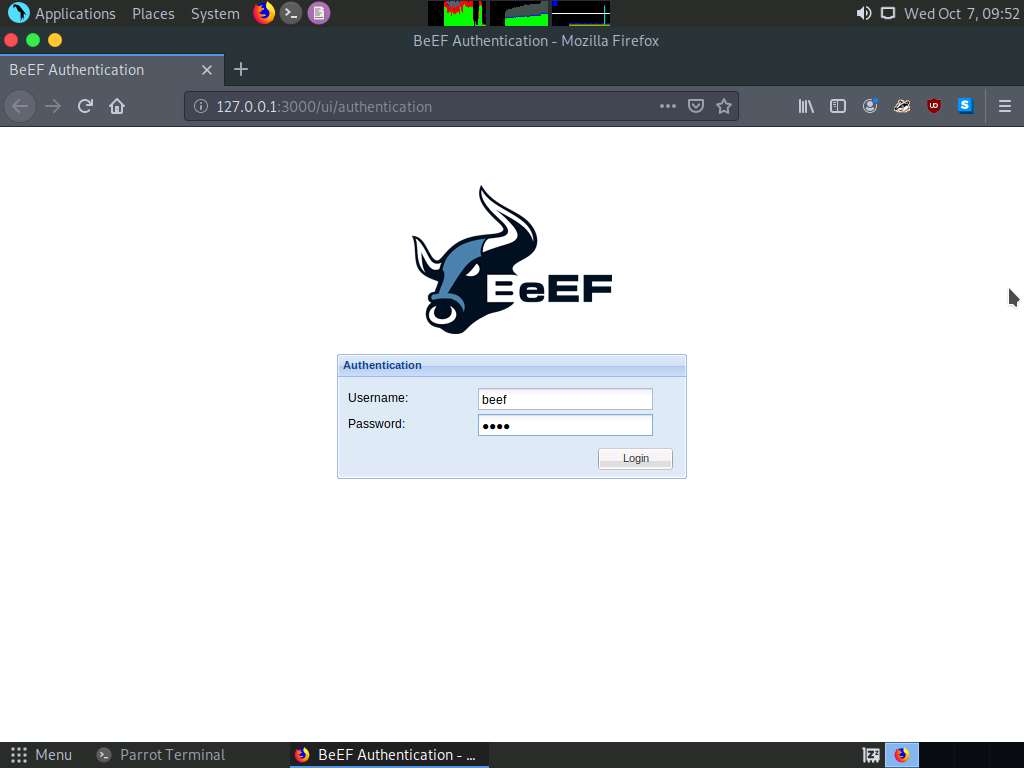


1. Copy the link **http://127.0.0.1:3000/ui/panel**. You will have to access this page in a web browser and log in to it. Minimize the terminal window

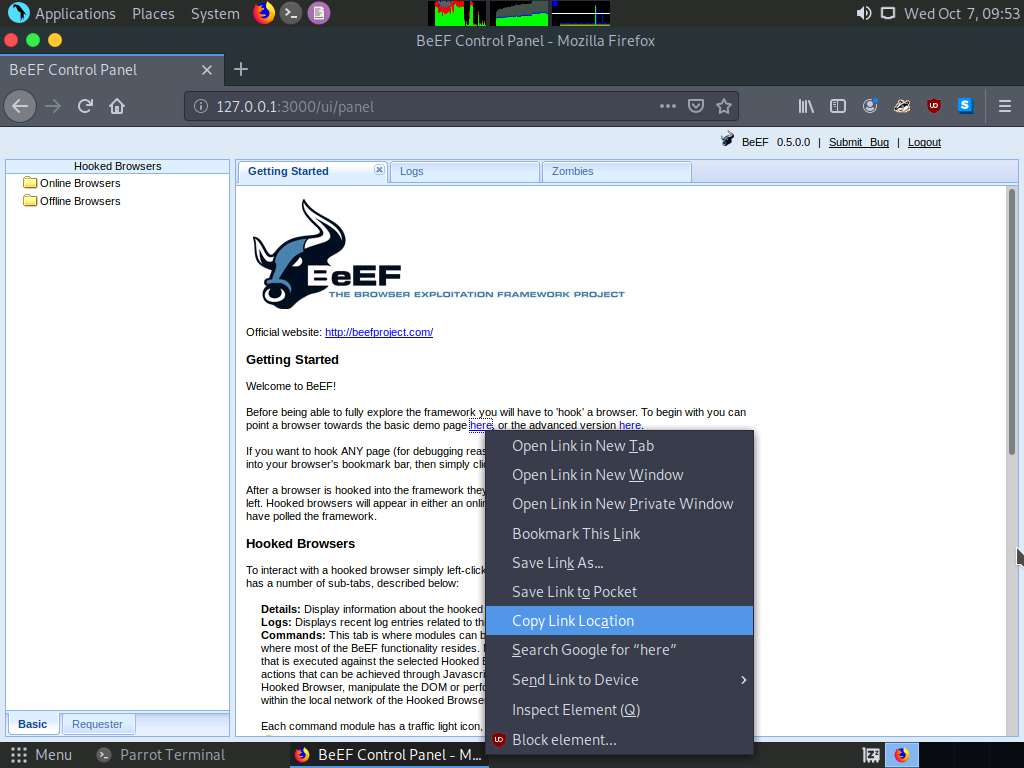


1. Click **Firefox** icon from the menu bar and paste the copied URL in address bar of the browser and press **Enter**. BeEF login page appears on the browser. Enter the following credentials to log in to the web application and click the **Login** button:

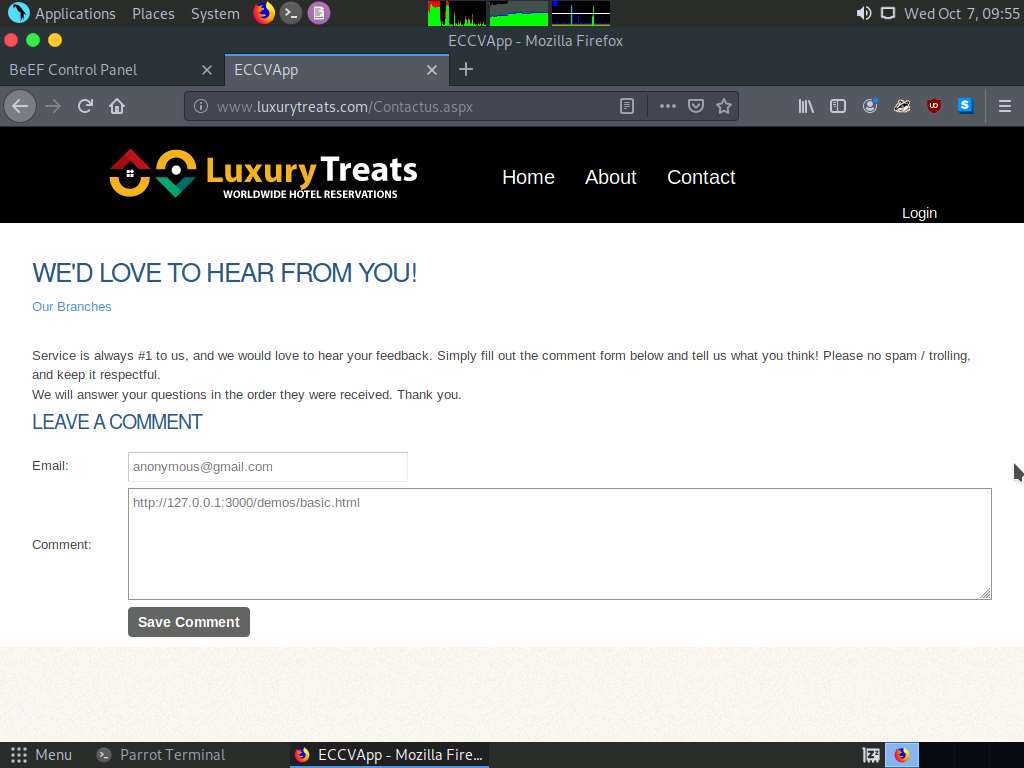
Username: **beef**  
Password: **test**

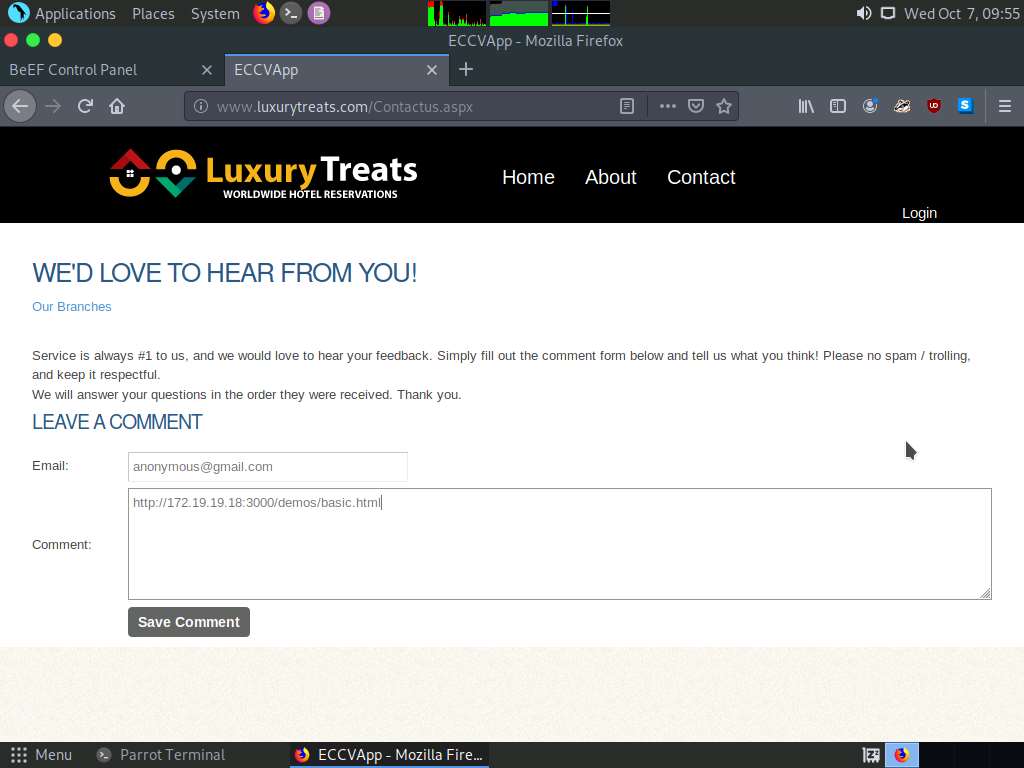


1. The BeEF home page appears on the browser window. Under the **Getting Started** section, you will observe two "here" links. Right-click the first **here** link and select **Copy Link Location**. Now, you need to paste the link in the **Contact Us** page of **LuxuryTreats** website.

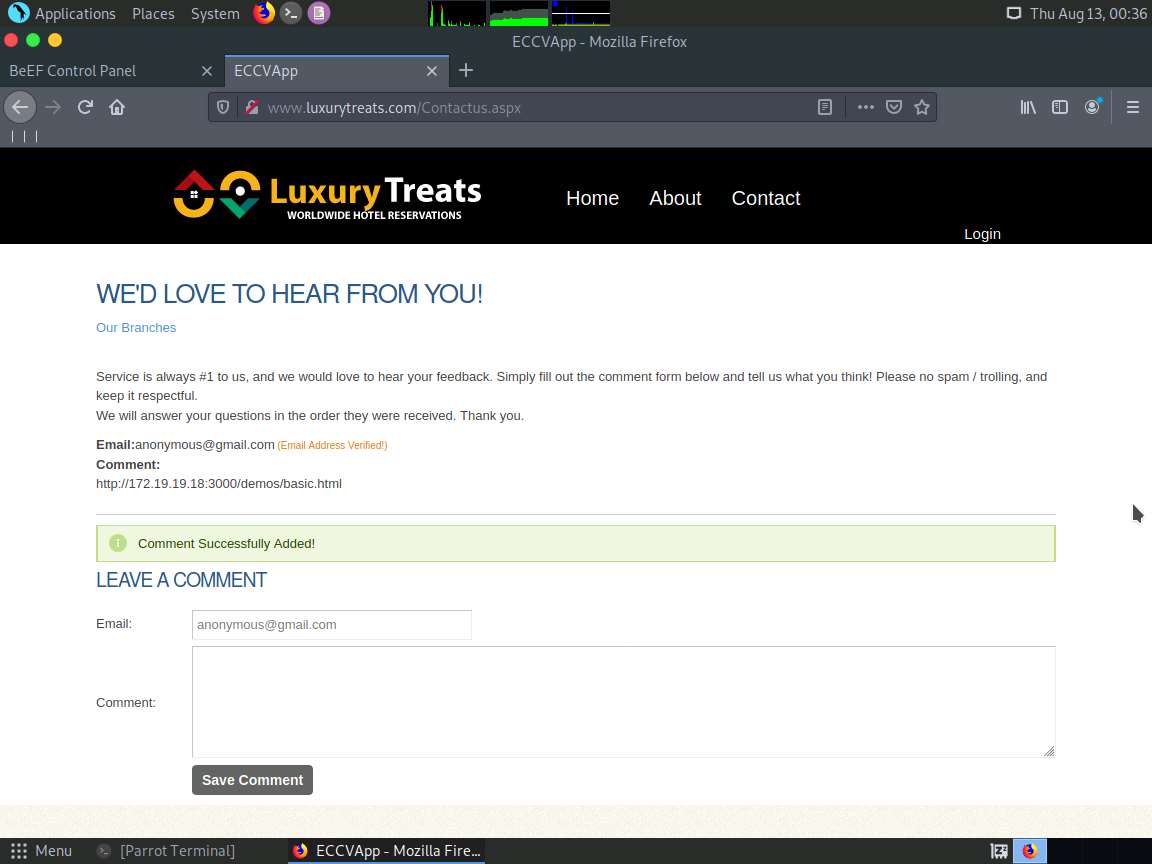


1. Now, open a new tab in the web browser and browse the webpage **http://www.luxurytreats.com/Contactus.aspx**.
2. **Contact Us** page appears; type a fake email in the **Email** field, paste the link (**http://127.0.0.1:3000/demos/basic.html**) copied from the BeEF framework in the **Comment** field. Replace **127.0.0.1** with the IP address of the Parrot machine i.e., **172.19.19.18** and click **Save Comment**.





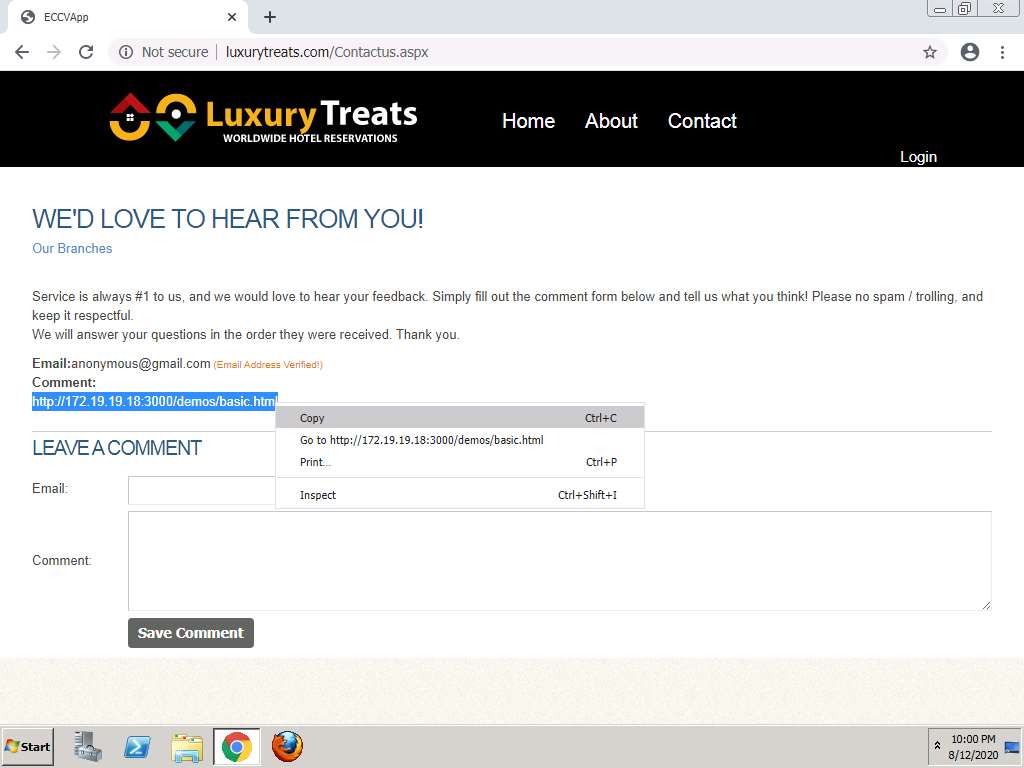
1. A comment link is posted on the page. Now, browse the webpage from other machines and open the URL **http://172.19.19.18:3000/demos/basic.html**. As soon as you open the webpage, the browser exploitation framework running in this machine attains connection with the machine. This way, a botnet will be created.



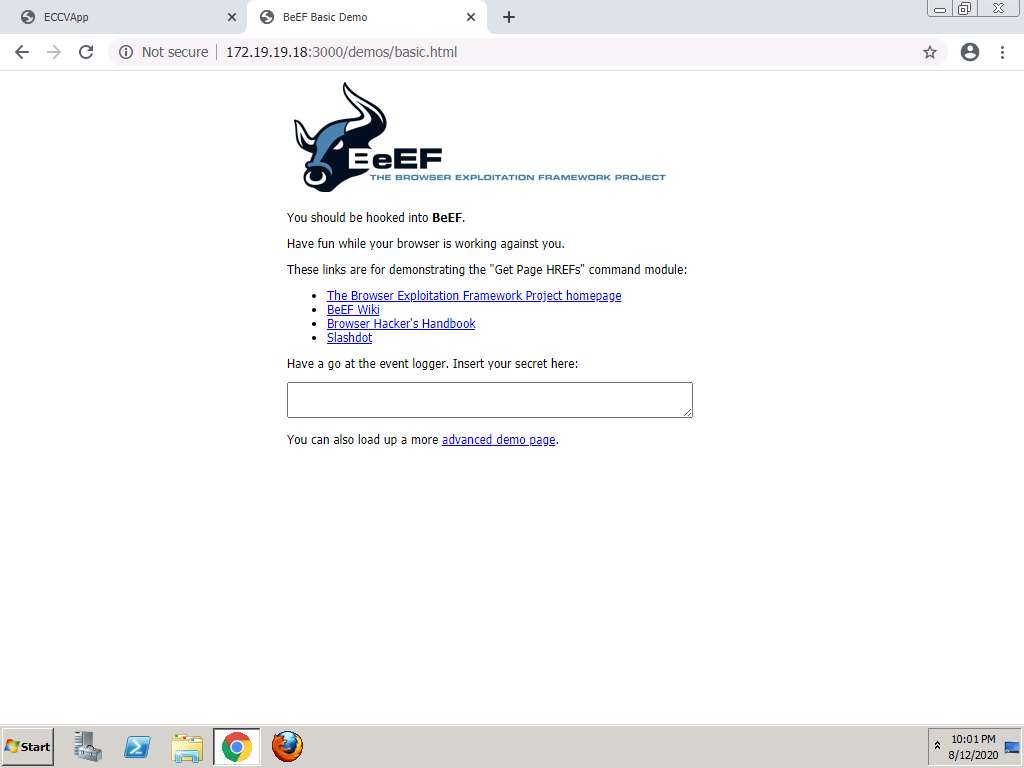
1. Log on to the **Database Server** machine, by clicking @lab.VirtualMachine(DatabaseServerSubnetB).SelectLink. Click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10) and then click Pa$$w0rd to login.



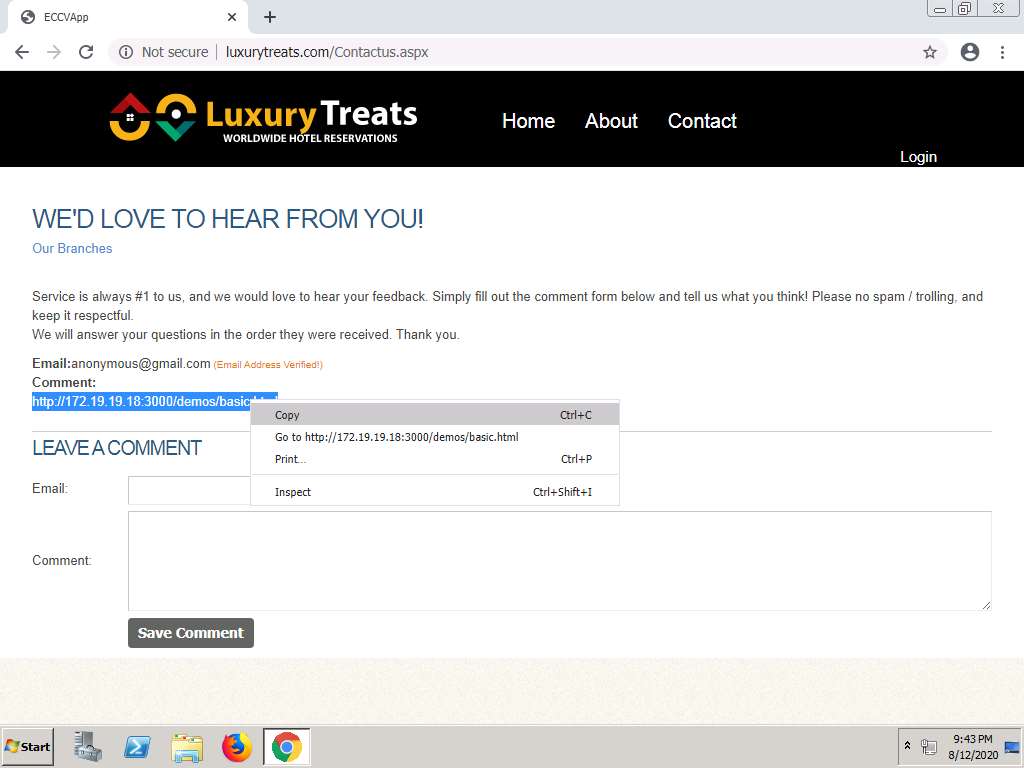
1. Launch Google chrome and browse the URL http://www.luxurytreats.com/Contactus.aspx. You will observe the Browser Exploitation Framework link in the **Comment** field. Copy the link.



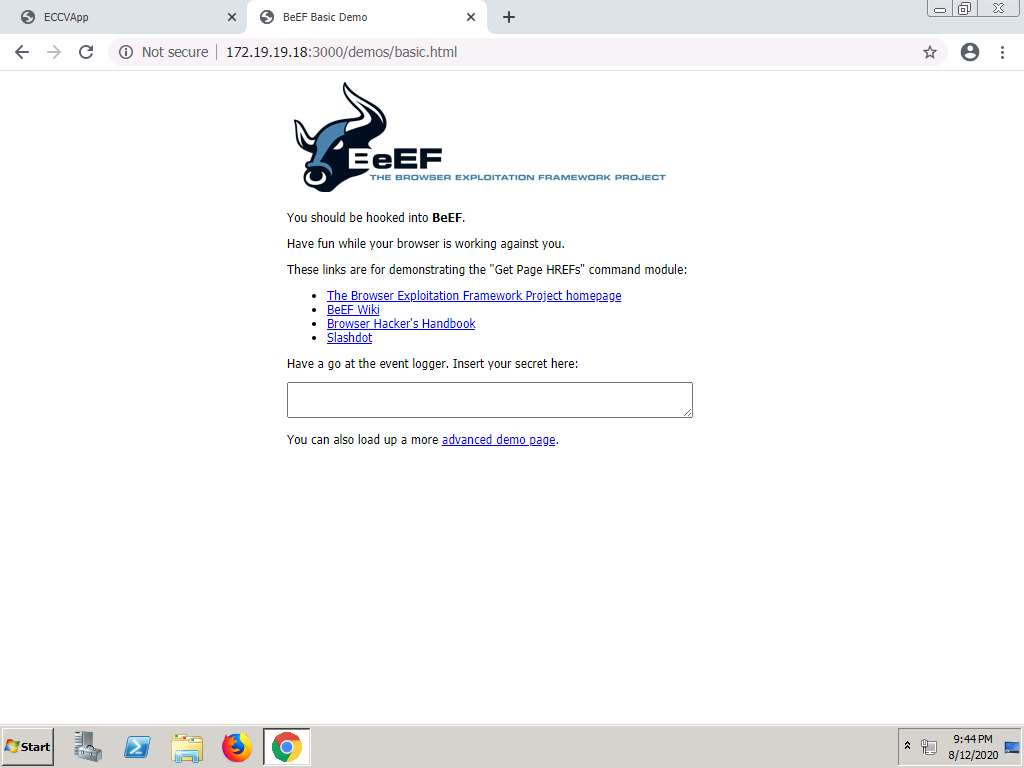
1. Open a new tab, paste the URL and press **Enter**. As soon as you open this webpage, BeEF running in **Parrot** machine establishes a connection with this machine.



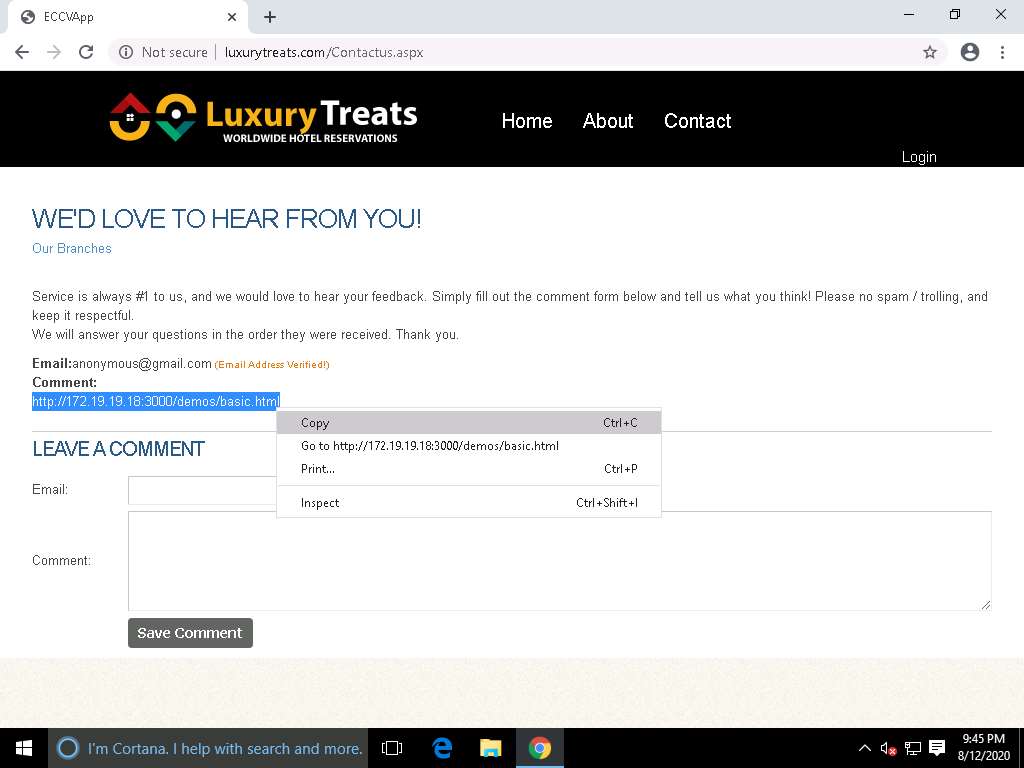
1. Select **Advertisement Dept** from the **Resources** pane, log in to it. Launch **Chrome** web browser and browse the URL http://www.luxurytreats.com/Contactus.aspx. You will observe the Browser Exploitation Framework link in the **Comment** field, copy the link.



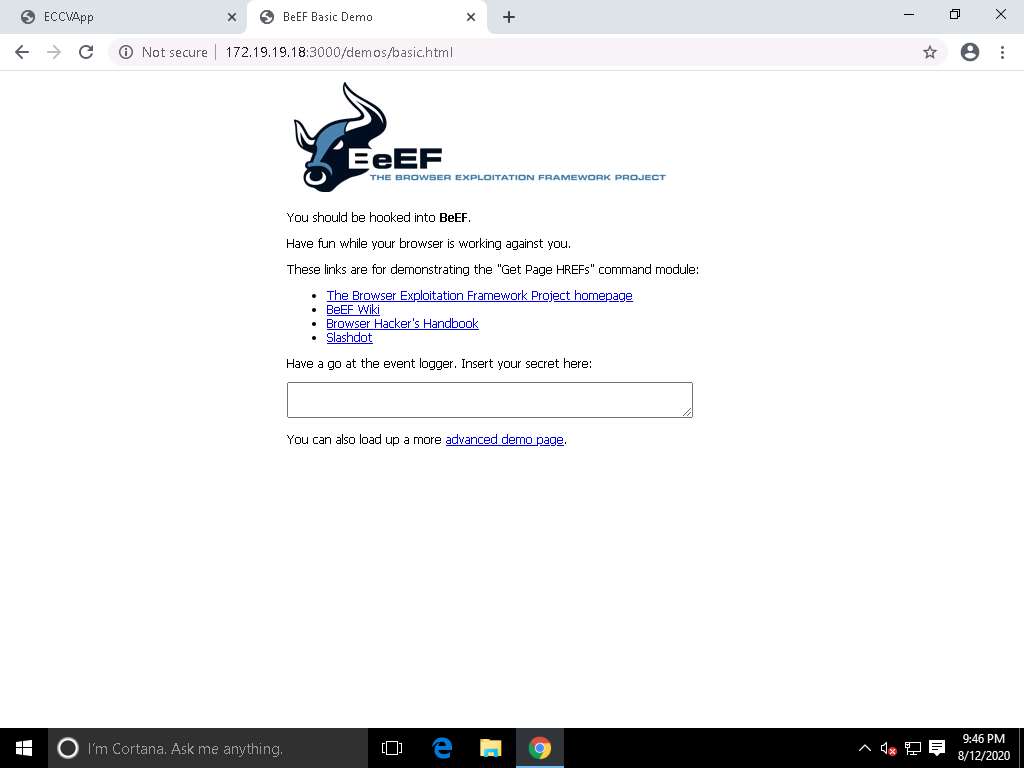
1. Open a new tab, paste the URL and press **Enter**. As soon as you open this webpage, BeEF running in the **Parrot** machine establishes a connection with this machine.



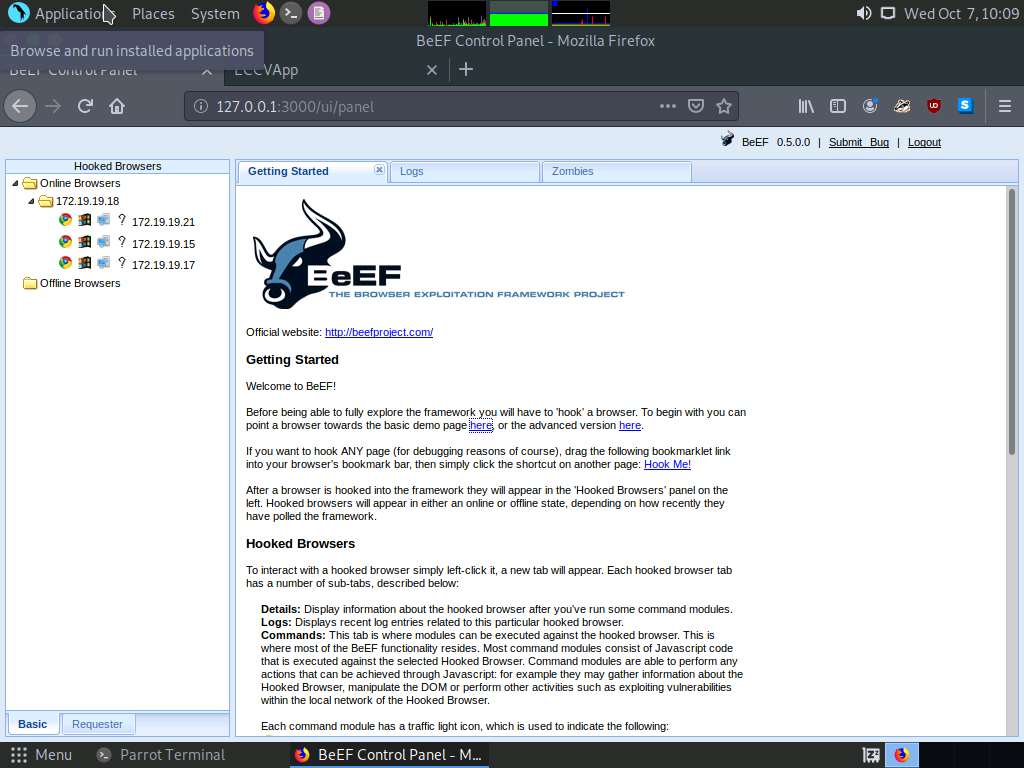
1. Select **Sales Department** from the **Resources** pane and log in to it using the credentials **Admin**/**test@123**. Once you login to the machine, if a **Network** banner appears at the right side corner of the Desktop, click **Yes**. Launch Chrome web browser and browse the URL http://www.luxurytreats.com/Contactus.aspx. You will observe the Browser Exploitation Framework link in the **Comment** field, copy the link.



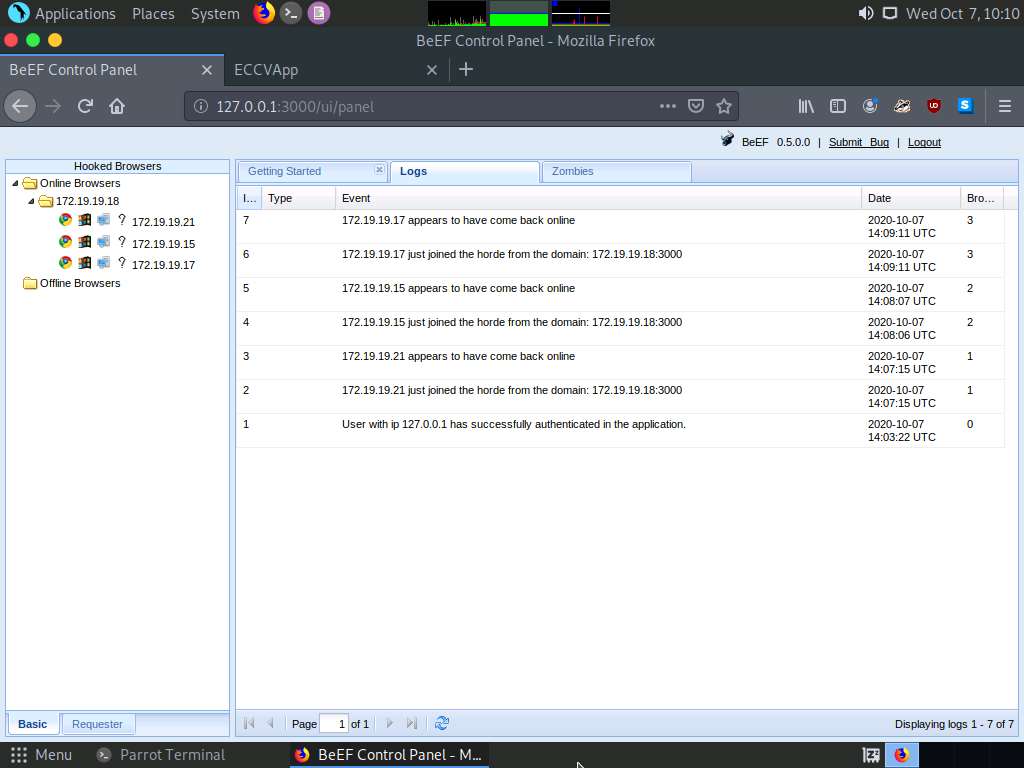
1. Open a new tab, paste the URL and press **Enter**. As soon as you open this webpage, BeEF running in the **Parrot** machine establishes a connection with this machine.



1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10), switch to the tab in which you are logged in to BeEF and click **Logs** tab.



1. You will observe that all the three machines **Database Server**, **Advertisement Dept** and **Sales Department** are connected to the Browser Exploitation Framework (BeEF) by observing the logs. You can observe them even in the left pane under the **172.19.19.18** directory (under **Online Browsers**).



1. This way, if anyone visits the page, BeEF gains access to their machines.

In this lab, you have learned how to:

* Use the Browser Exploitation Framework (BeEF)
* Attain Credentials of a user account in plain text
* Establish a botnet of vulnerable machines