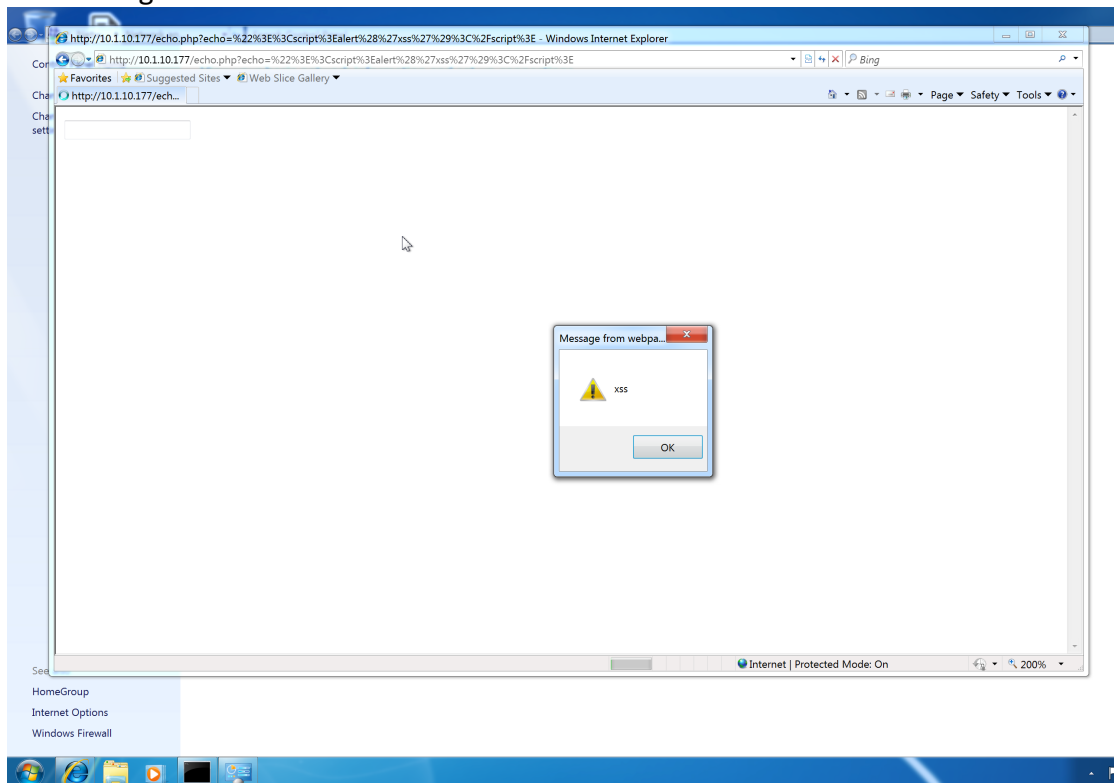


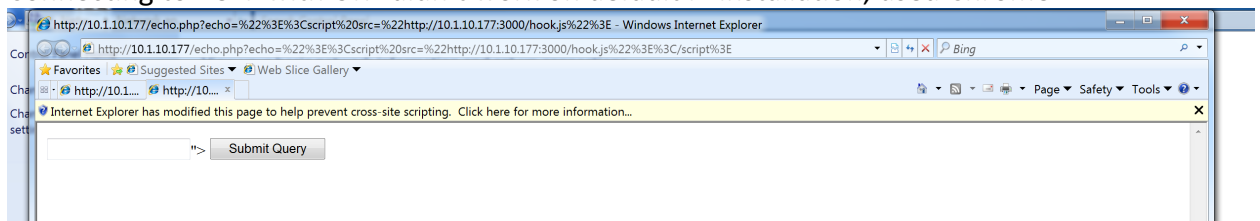
HW7

Default installation of Internet Explorer blocked the XSS, default install of Chrome did not

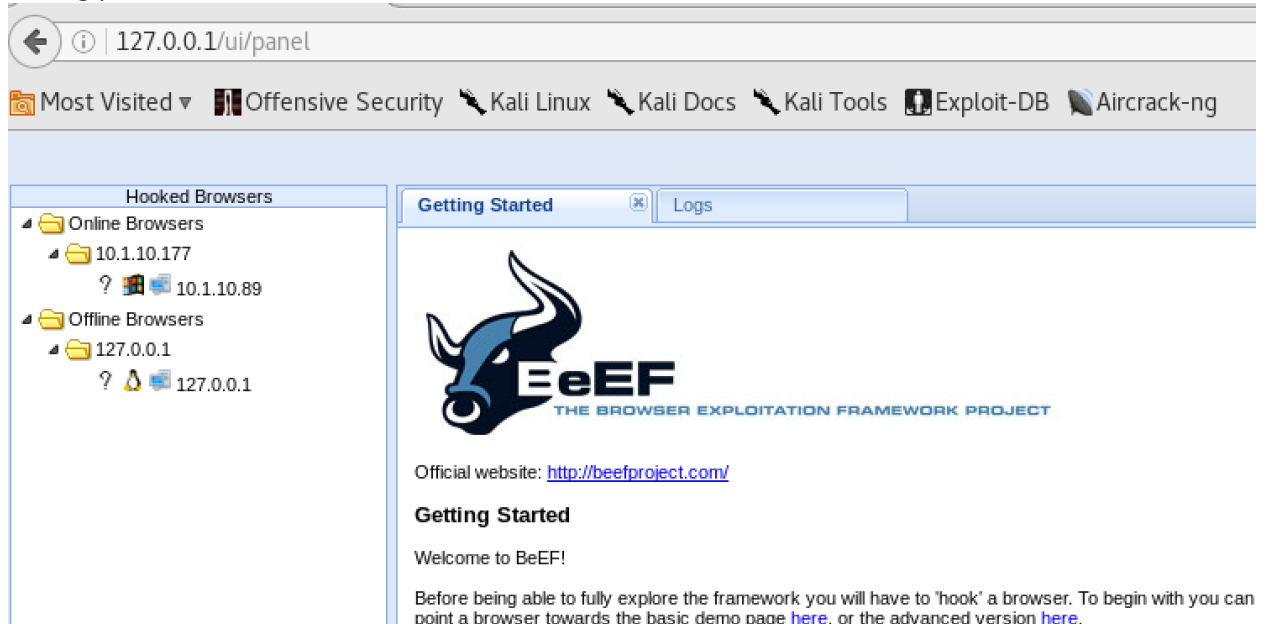
1) Connecting to BeEF from Windows



2) Connecting to BeEF with URL didn't work on default IE installation, used Chrome



3) Listing poisoned browser connected to BeEF




127.0.0.1/ui/panel

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Hooked Browsers

- Online Browsers
 - 10.1.10.177
 - 10.1.10.89
- Offline Browsers
 - 127.0.0.1
 - 127.0.0.1

Getting Started Logs

 **EeEF**
THE BROWSER EXPLOITATION FRAMEWORK PROJECT

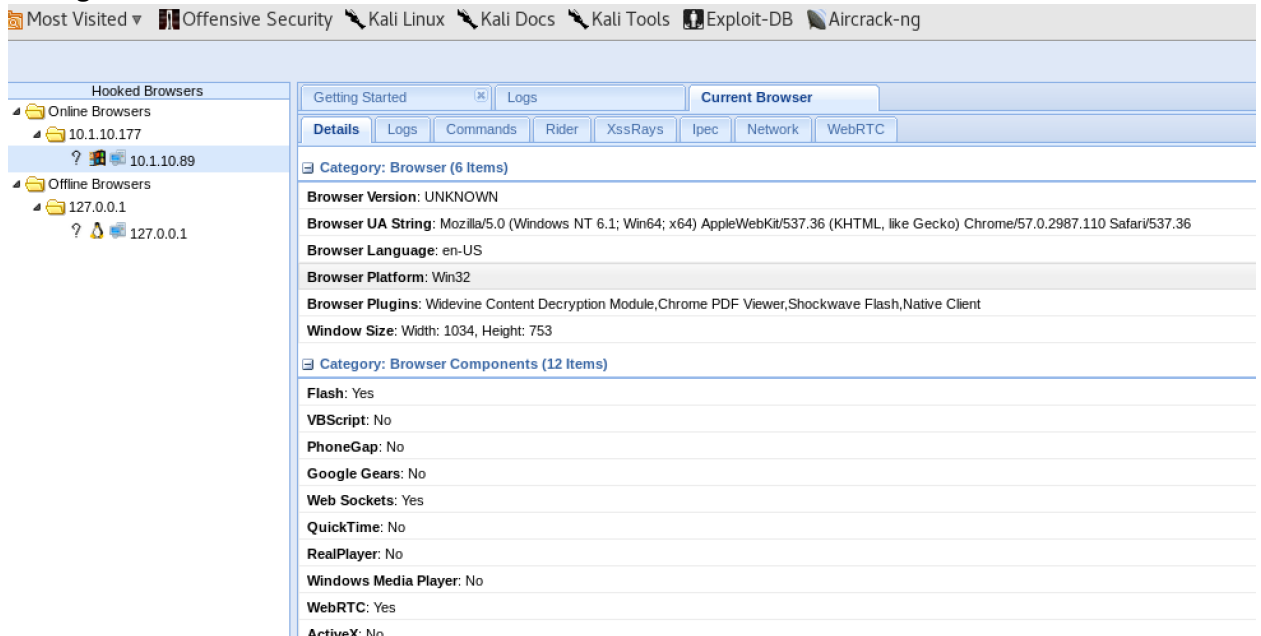
Official website: <http://beefproject.com/>

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](#).

4) Listing browser info and commands that can be executed



Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Hooked Browsers

- Online Browsers
 - 10.1.10.177
 - 10.1.10.89
- Offline Browsers
 - 127.0.0.1
 - 127.0.0.1

Getting Started Logs **Current Browser**

Details Logs Commands Rider XssRays Ipec Network WebRTC

Category: Browser (6 Items)

Browser Version: UNKNOWN

Browser UA String: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.110 Safari/537.36

Browser Language: en-US

Browser Platform: Win32

Browser Plugins: Widevine Content Decryption Module, Chrome PDF Viewer, Shockwave Flash, Native Client

Window Size: Width: 1034, Height: 753

Category: Browser Components (12 Items)

Flash: Yes

VBScript: No

PhoneGap: No

Google Gears: No

Web Sockets: Yes

QuickTime: No

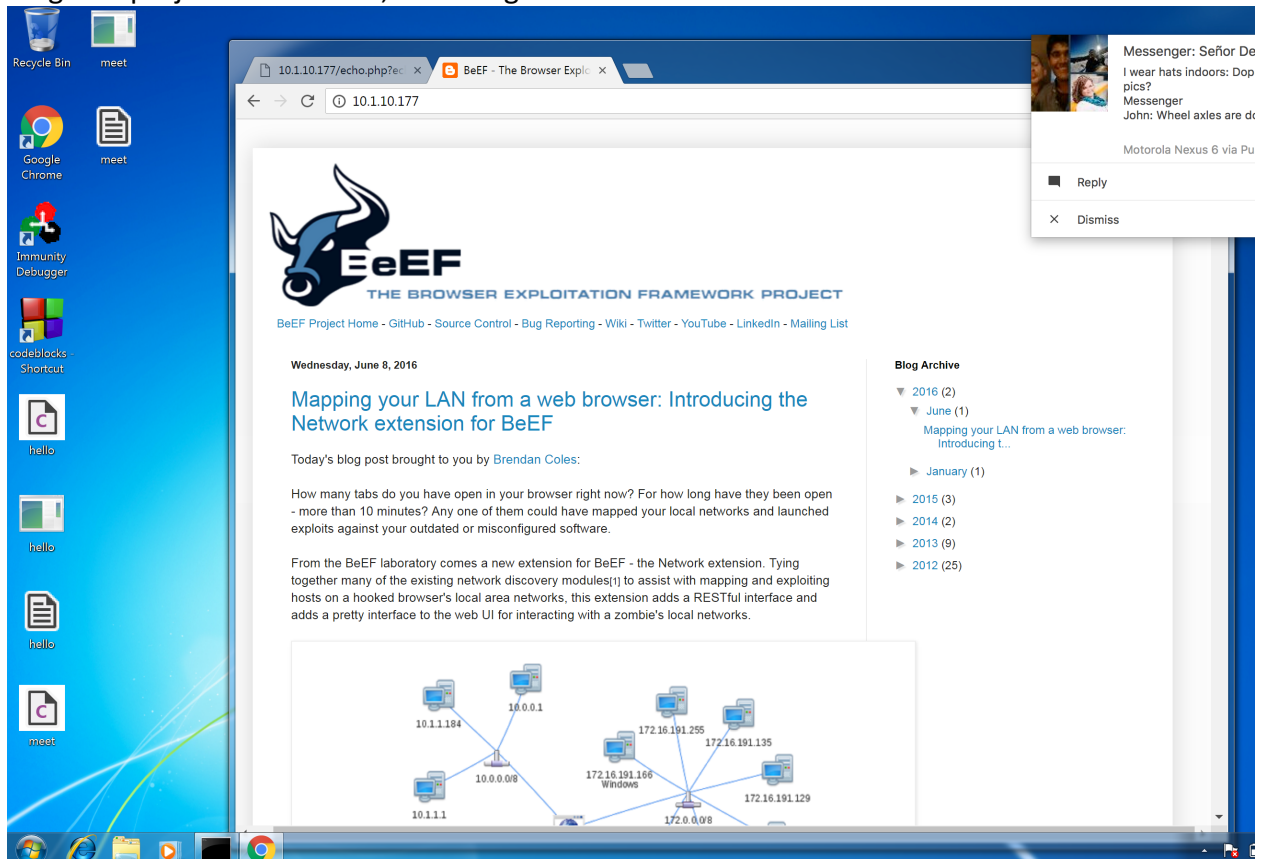
RealPlayer: No

Windows Media Player: No

WebRTC: Yes

ActiveX: No

5) Blog.beefproject.com cloned, accessing from windows



6) Output from DNS spoofing using Ettercap

