

# Beef - Invadindo navegadores sem ser notado

8 de julho de 2015 / [Guilherme](#)

Beef é uma ferramenta de código aberto usada na invasão de browsers, a qual realiza testes de penetração em navegadores de forma silenciosa e sem que a vítima baixe nada. Ela é bem comum em sistemas desenvolvidos para pentest como o Kali Linux, Parrot, Backbox entre outros. Isso não significa que todas as pessoas que usam esses sistemas saibam de sua existência e como ela funciona.

Ela não é uma exclusividade de sistemas de pentest, pode ser instalado em qualquer distribuição linux. Mo meu caso, usarei no ubuntu 14.10. Talvez em uma outra ocasião eu farei um tutorial de como instalá-lo no ubuntu, nesse eu mostrarei o uso devido a não encontrar nenhum bom conteúdo sobre isso em Português.

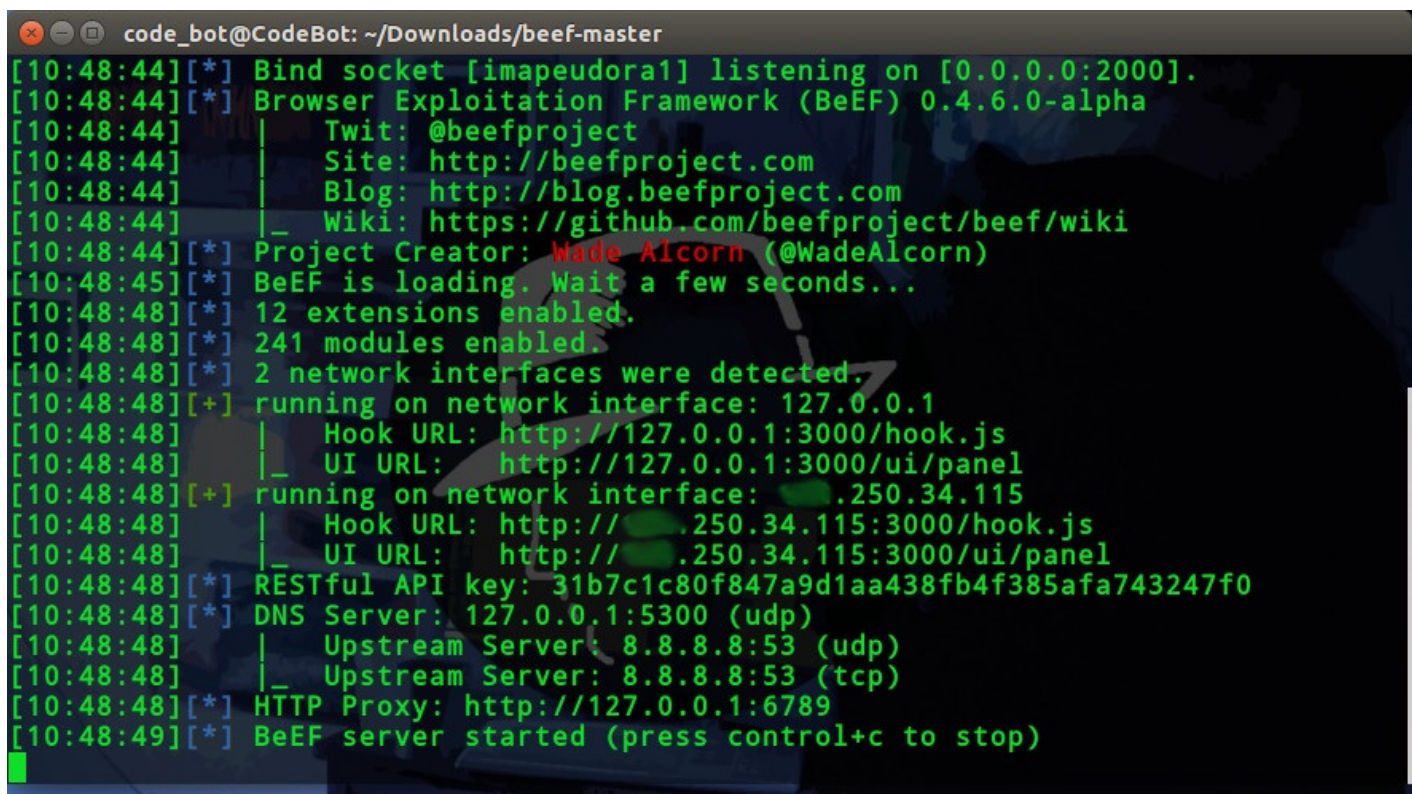
Como a maioria aqui usa sistemas de pentest, siga os comandos abaixo para entrar na pasta onde fica o Beef

```
cd /usr/share/beef-xss
```

Depois para executá-lo, dê o comando:

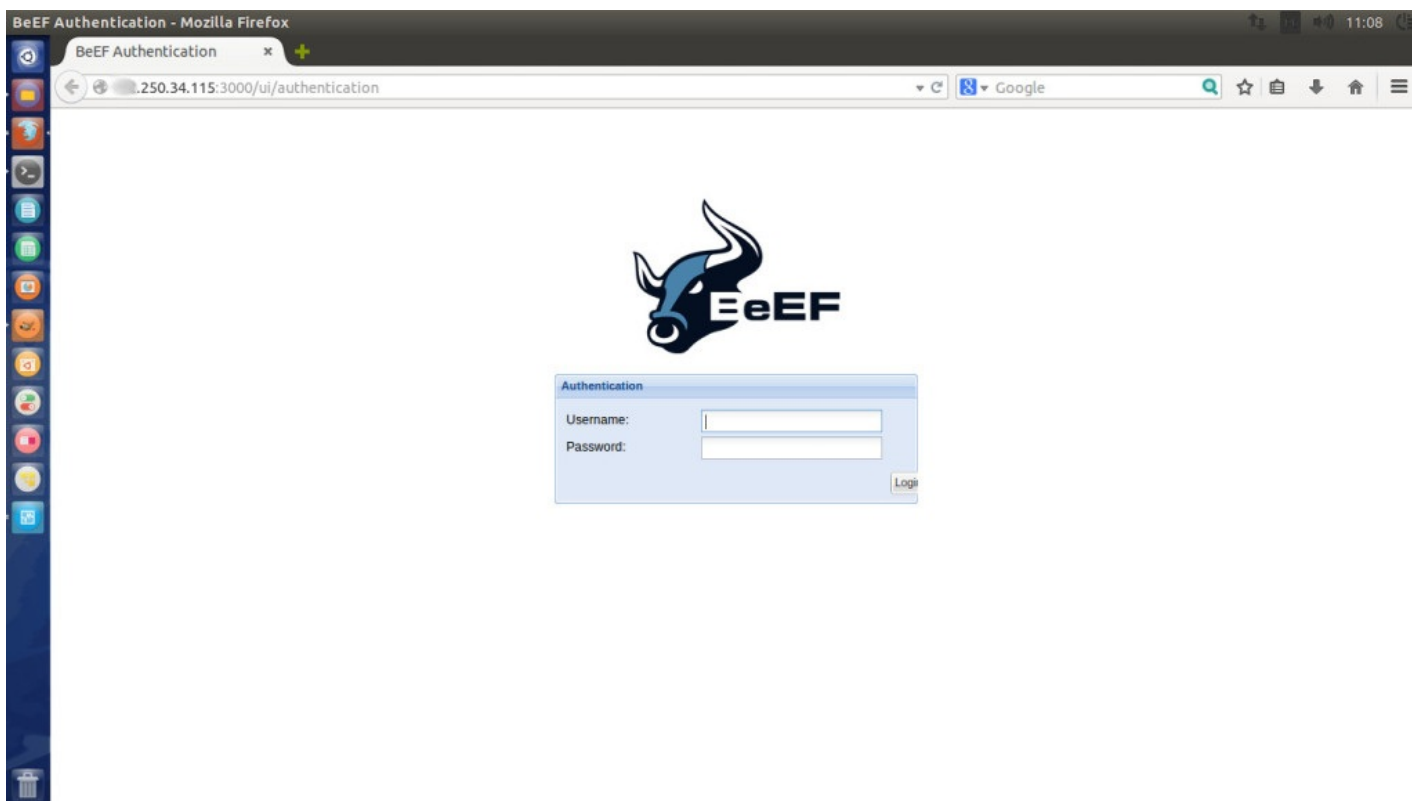
```
./beef
```

Sua próxima tela terá que ser esta:

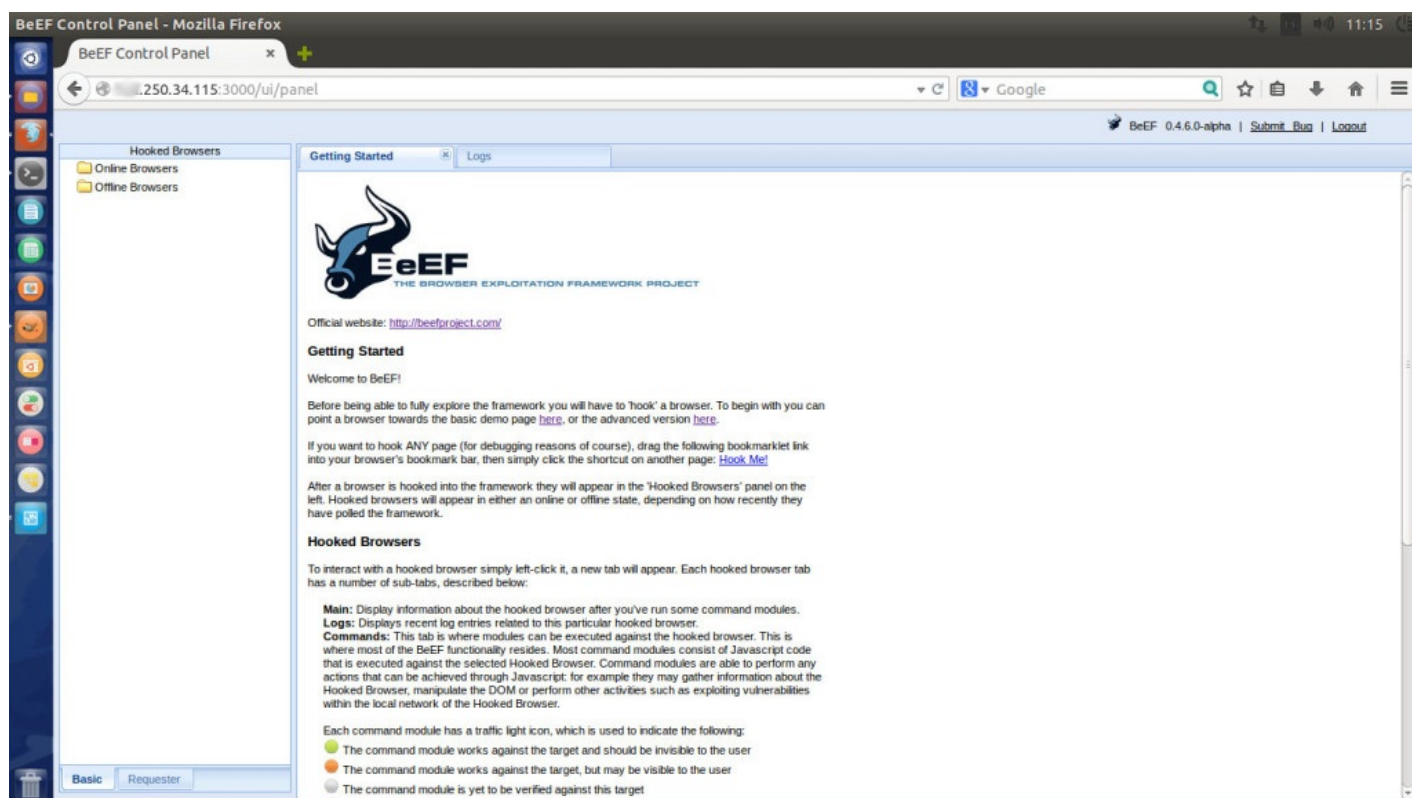
A terminal window titled 'code\_bot@CodeBot: ~/Downloads/beef-master' displays the output of running the Beef framework. The logs show the framework version (0.4.6.0-alpha), project creator (Wade Alcorn), and various enabled components like 12 extensions and 241 modules. It also lists detected network interfaces and the URLs for the hook and UI panel. The final line indicates the BeEF server has started and can be stopped with Ctrl+C.

```
code_bot@CodeBot: ~/Downloads/beef-master
[10:48:44][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[10:48:44][*] Browser Exploitation Framework (BeEF) 0.4.6.0-alpha
[10:48:44] |   Twit: @beefproject
[10:48:44] |   Site: http://beefproject.com
[10:48:44] |   Blog: http://blog.beefproject.com
[10:48:44] |_  Wiki: https://github.com/beefproject/beef/wiki
[10:48:44][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[10:48:45][*] BeEF is loading. Wait a few seconds...
[10:48:48][*] 12 extensions enabled.
[10:48:48][*] 241 modules enabled.
[10:48:48][*] 2 network interfaces were detected.
[10:48:48][+] running on network interface: 127.0.0.1
[10:48:48] |   Hook URL: http://127.0.0.1:3000/hook.js
[10:48:48] |_  UI URL:   http://127.0.0.1:3000/ui/panel
[10:48:48][+] running on network interface: 250.34.115
[10:48:48] |   Hook URL: http://250.34.115:3000/hook.js
[10:48:48] |_  UI URL:   http://250.34.115:3000/ui/panel
[10:48:48][*] RESTful API key: 31b7c1c80f847a9d1aa438fb4f385afa743247f0
[10:48:48][*] DNS Server: 127.0.0.1:5300 (udp)
[10:48:48] |   Upstream Server: 8.8.8.8:53 (udp)
[10:48:48] |_  Upstream Server: 8.8.8.8:53 (tcp)
[10:48:48][*] HTTP Proxy: http://127.0.0.1:6789
[10:48:49][*] BeEF server started (press control+c to stop)
```

Na linha onde temos `http://xxx.250.34.115:3000/ui/panel` é onde o nosso painel do Beef está, copie e cole no seu navegador.

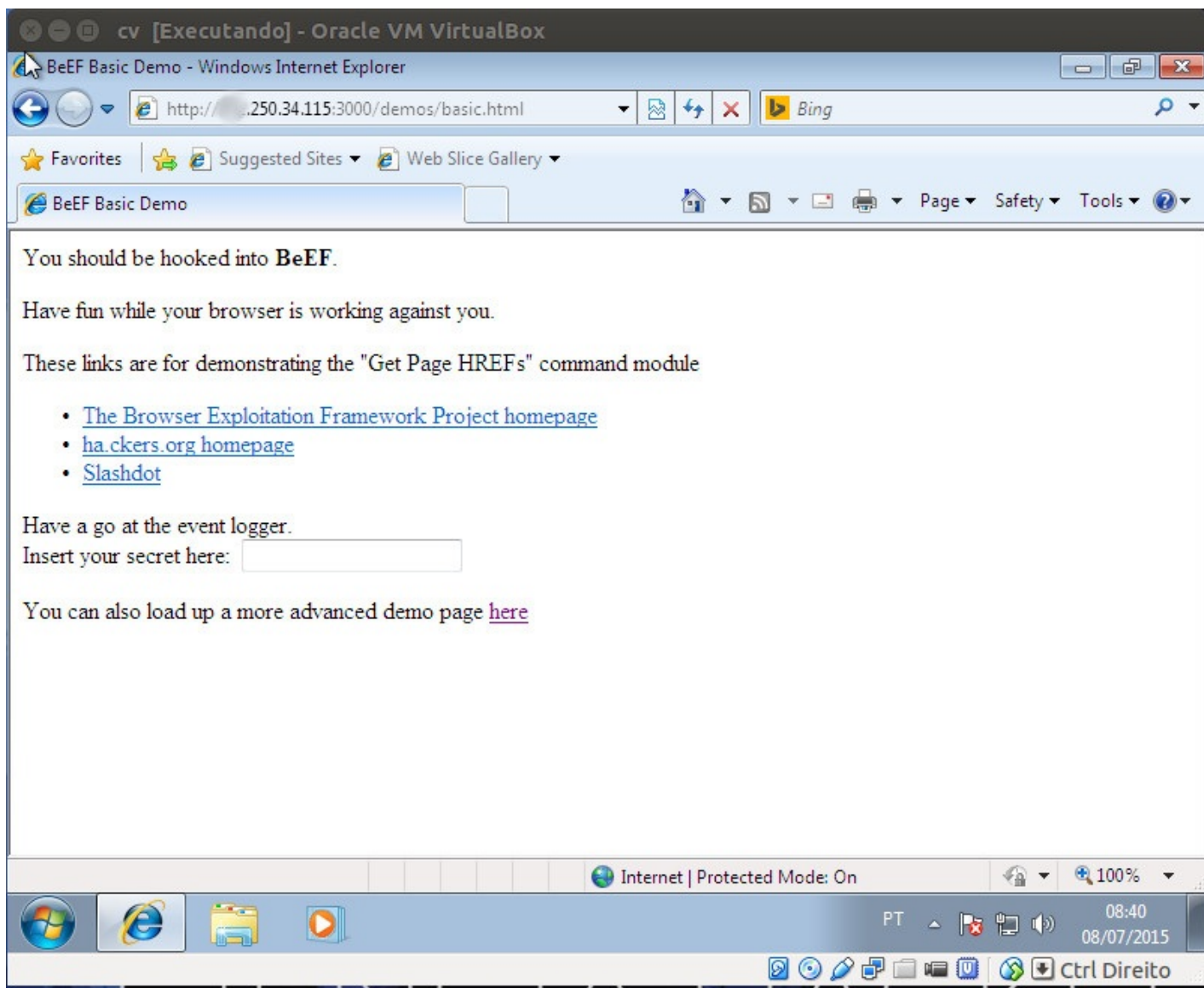


Nessa tela ele nos pede login e senha. Por padrão, coloque *login:beef* *password:beef* e clique em *login*.

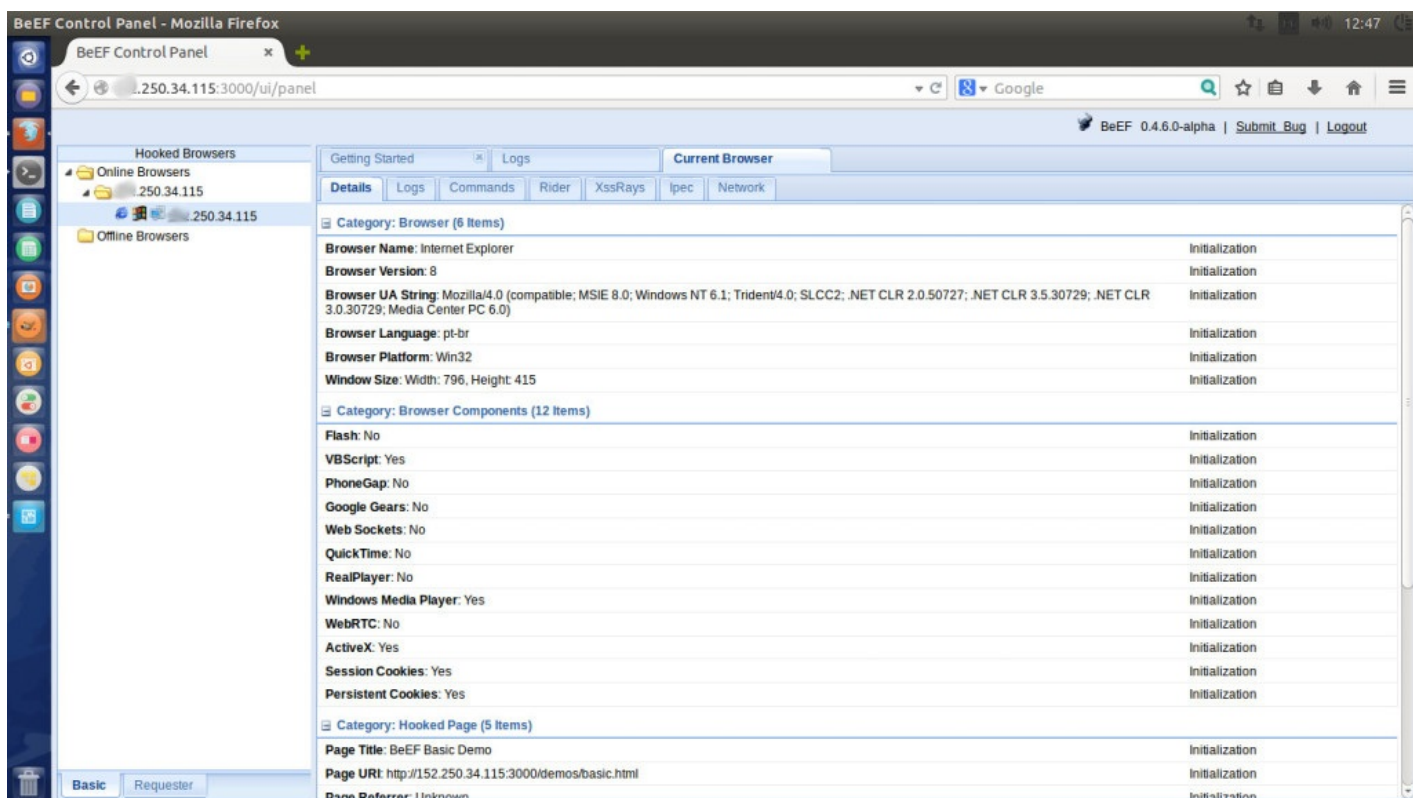


Para testar, eu vou usar uma máquina virtual rodando Windows 7 Ultimate e com o navegador Internet Explorer, para pegar vítimas em rede própria (pois invadir pessoas que você não tem permissão não é legal né rsrs) use o seguinte link:

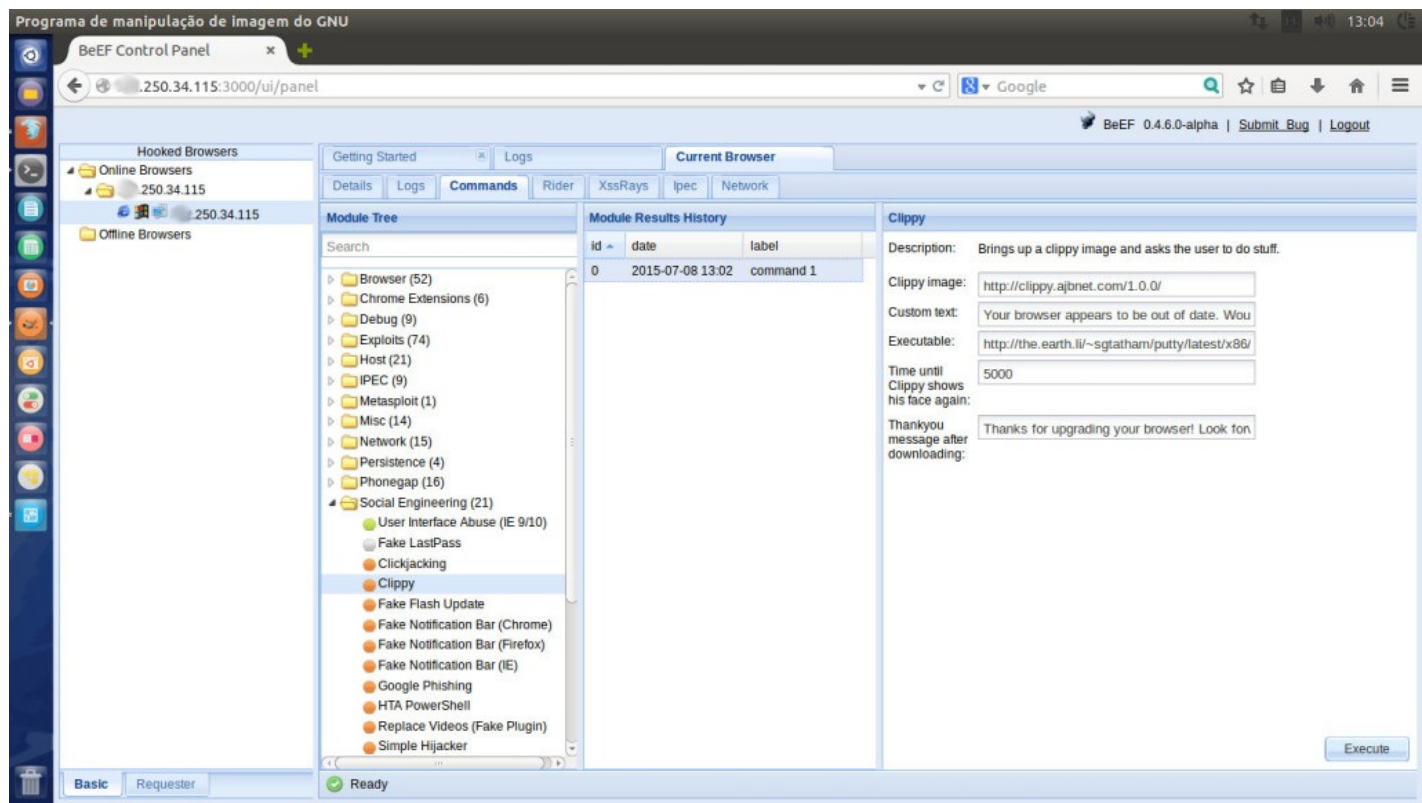
<http://seuip:3000/demos/basic.html>



Essa janela será exibida. Inicialmente, você vai pensar que abriu uma página e agora? Agora é só se divertir! Se você observar no painel do Beef, uma nova conexão será exibida com o IP e as principais informações do computador alvo.

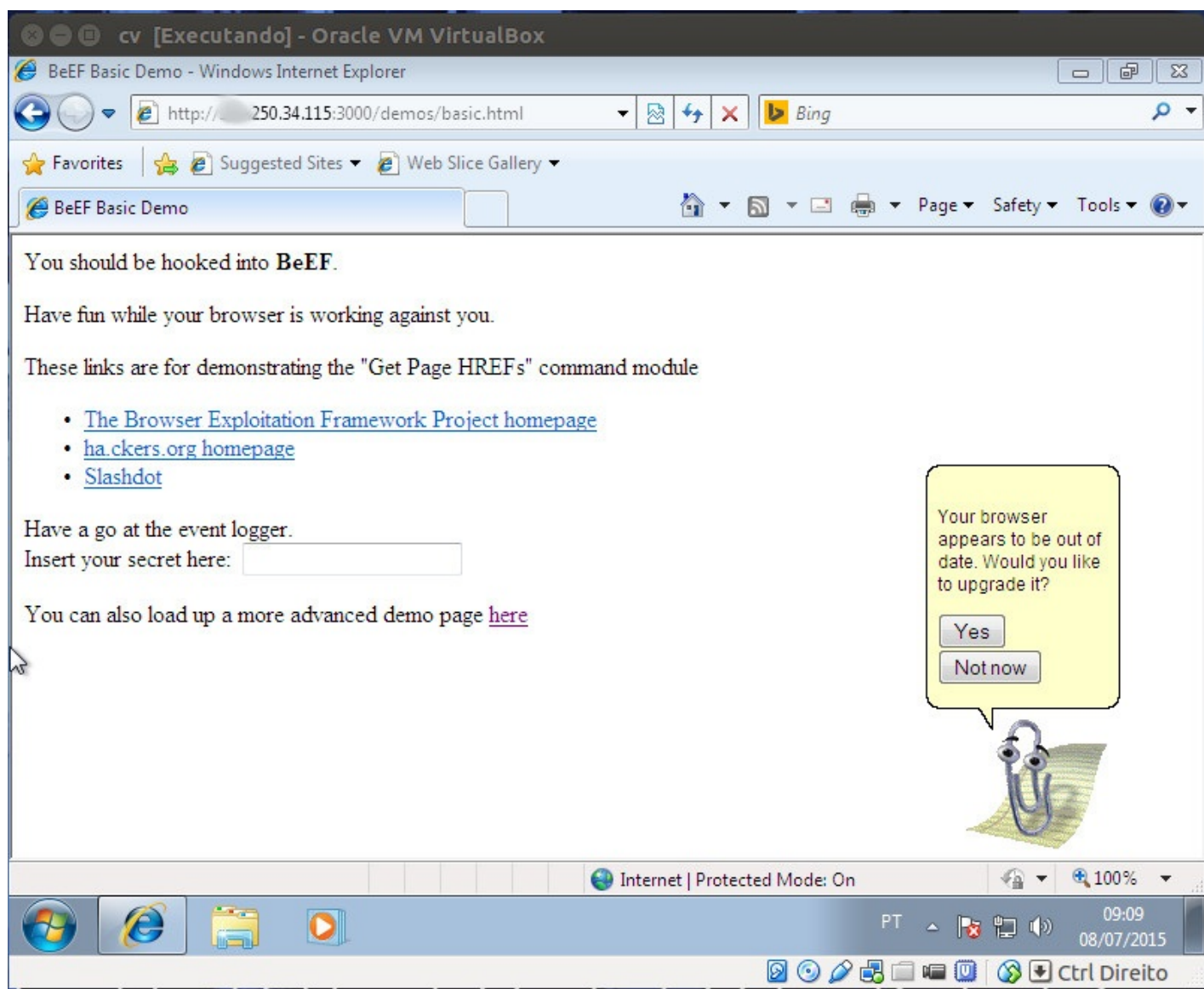


Como podem ver, temos todas as informações do sistema. No caso, se você fizer uma invasão em outro computador (Não recomendável) vai ver as informações do alvo.



Agora é só diversão, temos vários commands, aqui mostro um que é bem simples, claro você pode explorar as outras opções e conseguir coisas bem mais valiosas \$\$.





Aqui está o resultado do comando.

Até a próxima!

.....