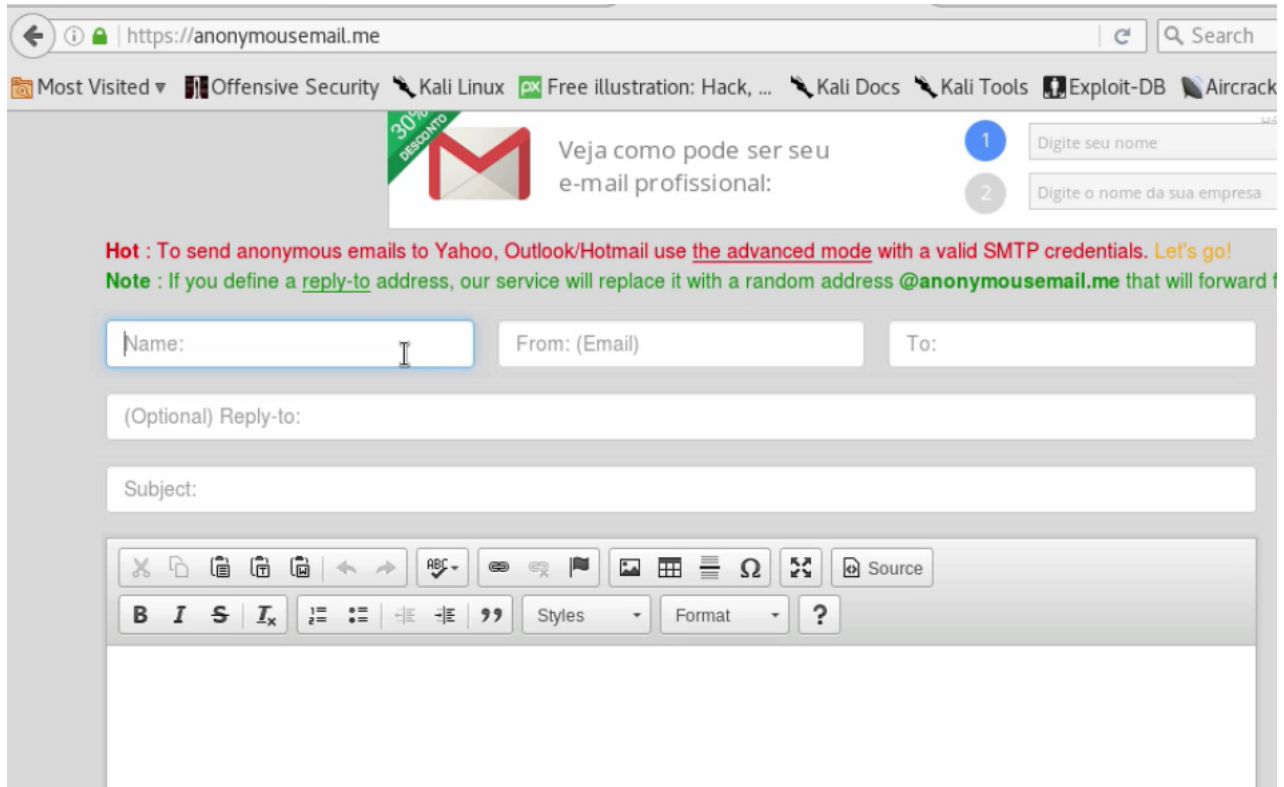


Melhorando engenharia social com e-mail

Transcrição

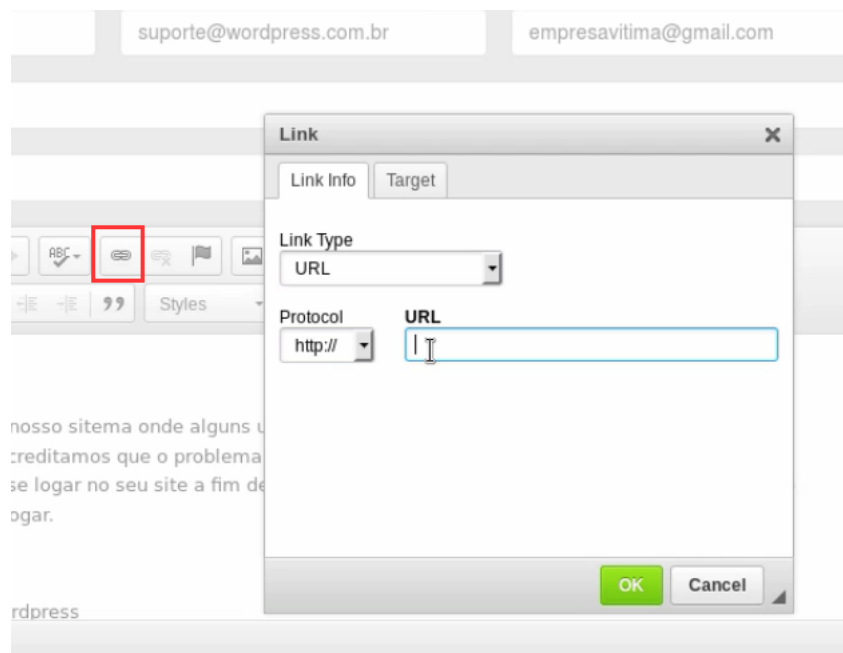
Outra forma de enviar um e-mail é utilizando alguns sites. Um dos servidores disponíveis é o Anonymous email:



The screenshot shows the homepage of anonymousemail.me. The browser's address bar displays the URL. The page features a navigation bar with links to 'Most Visited', 'Offensive Security', 'Kali Linux', 'Free illustration: Hack, ...', 'Kali Docs', 'Kali Tools', 'Exploit-DB', and 'Aircrack'. A prominent banner for Gmail with a '30% desconto' (30% discount) tag is visible. Below the banner, there are instructions in red and green text: 'Hot : To send anonymous emails to Yahoo, Outlook/Hotmail use the advanced mode with a valid SMTP credentials. Let's go!' and 'Note : If you define a reply-to address, our service will replace it with a random address @anonymousemail.me that will forward'. The main form includes fields for 'Name:', 'From: (Email)', 'To:', '(Optional) Reply-to:', and 'Subject:'. Below these fields is a rich text editor with various icons for text formatting (bold, italic, underline, strikethrough, bulleted list, numbered list, indent, outdent, link, unlink, quote, unquote) and a 'Source' button.

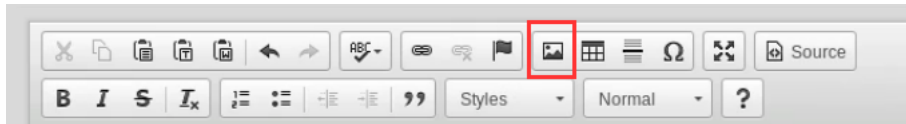
Assim que acessamos o site, basta preencher o formulário acima com as informações pedidas: o endereço de quem receberá a mensagem, o e-mail fictício de quem envia, o assunto e o conteúdo.

Para referenciar um link podemos clicar no botão mostrado na imagem abaixo e preenchemos a seguinte janela:

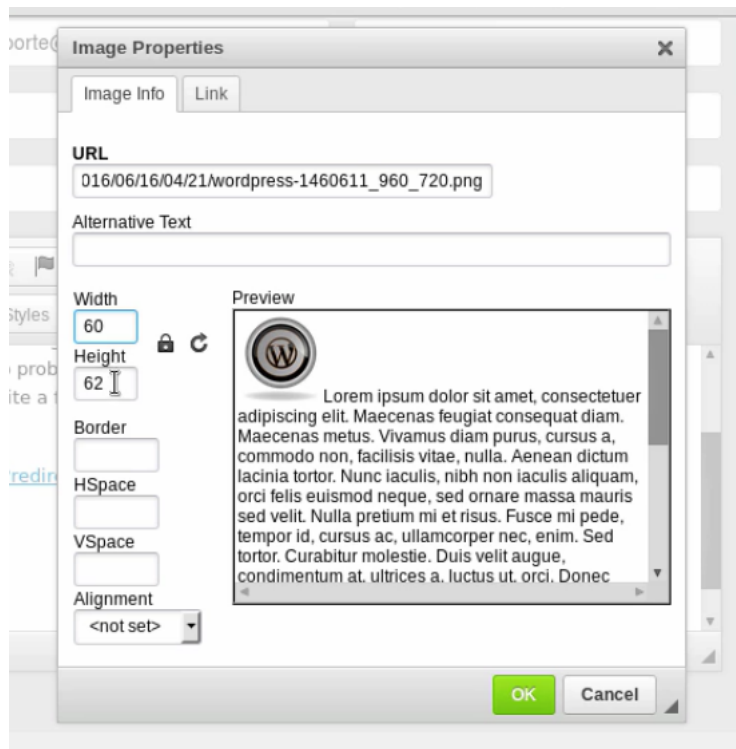


The screenshot shows a 'Link' dialog box with two tabs: 'Link Info' and 'Target'. The 'Link Info' tab is active. It contains a 'Link Type' dropdown menu set to 'URL'. Below this, there are 'Protocol' and 'URL' fields. The 'Protocol' dropdown is set to 'http://'. The 'URL' field is empty and has a text cursor. At the bottom of the dialog are 'OK' and 'Cancel' buttons. In the background, a text editor is visible with a red box highlighting the 'Link' icon in the toolbar.

Nesse formulário inserimos a URL parcialmente verdadeira o que gera um link que acrescentamos no corpo do e-mail. Adicionamos também um logotipo para que a mensagem ganhe credibilidade, utilizamos o seguinte ícone:



Ao clicar no botão abre-se o seguinte formulário no qual acrescentamos a URL da imagem e ajustamos as dimensões dela:



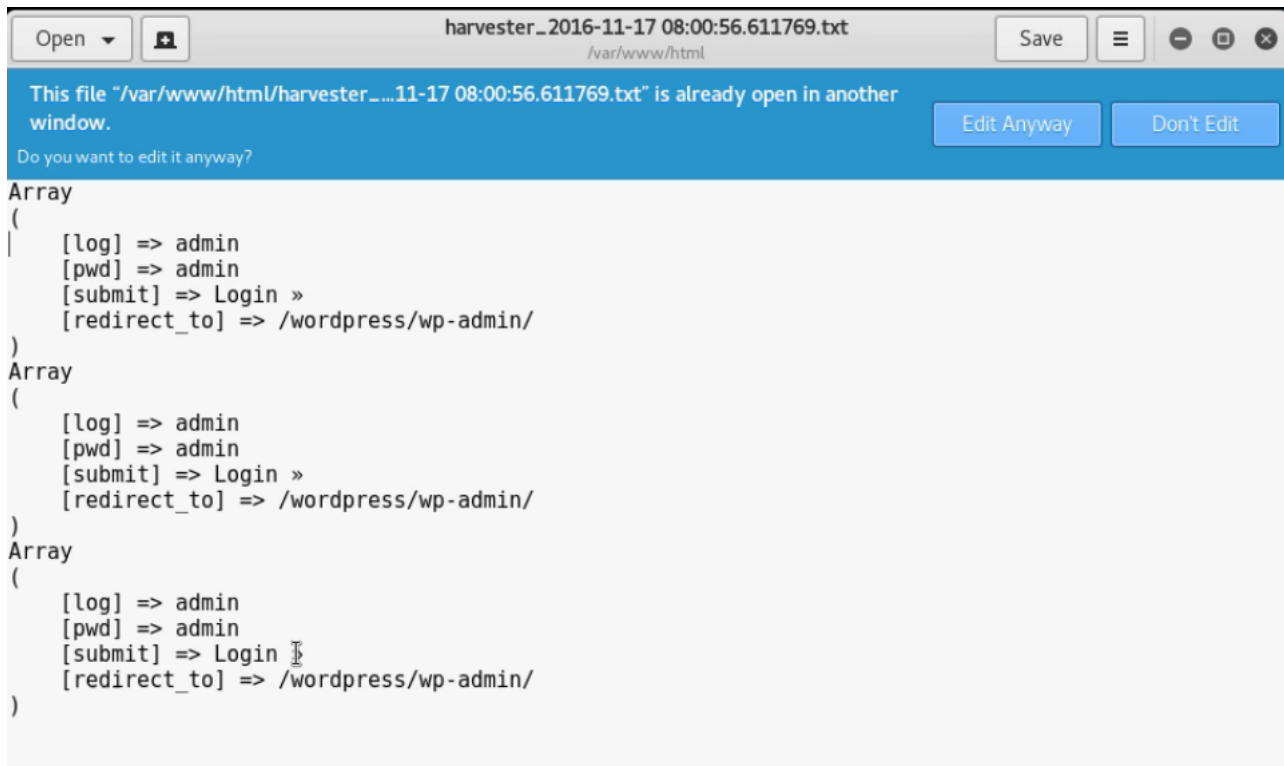
Finalmente, para enviar o e-mail basta dar um *check* na caixa que encontra-se bem embaixo na página dizendo que não somos um robô e clicamos em *Send Email*.

Vamos acessar o gmail do usuário e verificar que a mensagem é efetivamente recebida. Temos o seguinte:



O e-mail parece estar correto, ademais, transmite maior confiança do que o primeiro que enviamos. Se clicarmos no link da mensagem seremos redirecionados para a página que leva a URL falsa.

Supondo que o usuário preencha seus dados na página falsa, podemos verificá-los através do "Computer > var > www > html", no arquivo "harvest-2016-11-17". Teremos o seguinte:



```
harvester_2016-11-17 08:00:56.611769.txt
/var/www/html

This file "/var/www/html/harvester_2016-11-17 08:00:56.611769.txt" is already open in another window.
Do you want to edit it anyway? Edit Anyway Don't Edit

Array
(
    [log] => admin
    [pwd] => admin
    [submit] => Login »
    [redirect_to] => /wordpress/wp-admin/
)
Array
(
    [log] => admin
    [pwd] => admin
    [submit] => Login »
    [redirect_to] => /wordpress/wp-admin/
)
Array
(
    [log] => admin
    [pwd] => admin
    [submit] => Login »
    [redirect_to] => /wordpress/wp-admin/
)
```

O *username* e a *password* do usuário!

Ou seja, nós utilizamos um link verdadeiro para redirecionar a página e dessa forma, conseguimos acesso aos dados da vítima! Então, percebe o quão perigoso é esse tipo de ataque!