Esteganografia com Steghide Linux

15 de maio de 2015 / s0ph0s

Existe diversas formas de comunicação segurança dentro do *hacking*, uma delas é a *esteganografia*. Ela permite que nós enviemos mensagens ocultas para outra pessoa com o fim de manter uma comunicação segura. No uso computacional, seria você esconder uma mensagem dentro de um anexo (seja uma imagem, musica, video) para enviar a um destinatário a qual usaremos a ferramenta ***Steghide*** que possibilita a utilização desse recurso.

História da esteganografia

A esteganografia não é dos tempos de hoje, já vem do tempo dos Egípcios onde se comunicavam pela escrita desenvolvida chamada de hieróglifos. Outro caso era que alguns reis mandavam raspar as cabeças de escravos para tatuar as mensagens nelas, e depois que o cabelo crescesse, o rei mandava o escravo pessoalmente com a mensagem. Com o passar da historia foi evoluindo até os dias de hoje, que é muito utilizado no meio computacional.

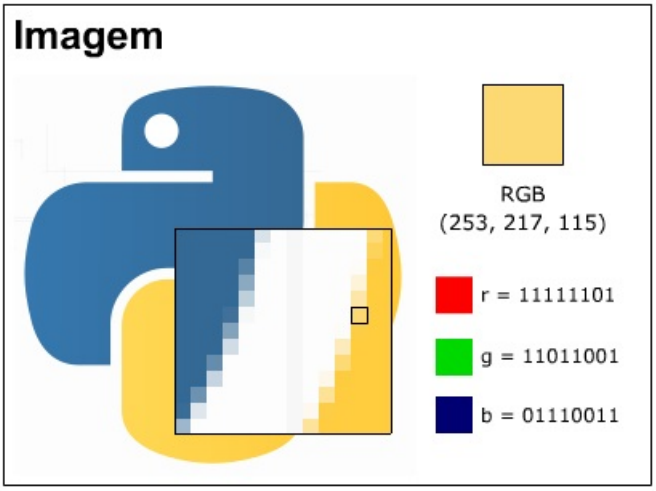
Meios que se aplicam e quem a utiliza

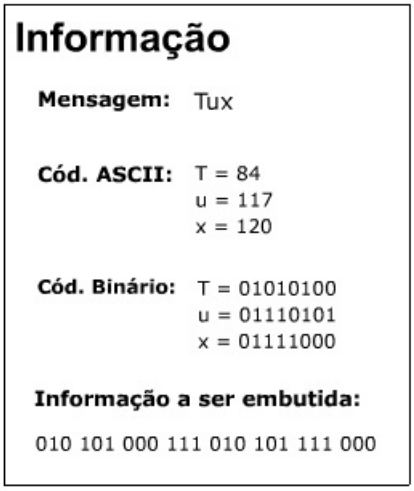
Ela é aplicada muito nos dias de hoje mesmo sendo pouco falada, é utilizada principalmente no meio dos *hackers que* utilizam essa técnica para enviar mensagem uns para os outros, com a finalidade de evitar uma interceptação de qualquer indivíduo (como governo ou outra entidade), garantindo que só o destinatário que saiba como abrir a mensagem oculta. Outros meio que se aplica é no meio penal onde juízes ou autoridades da leis utilizam assinaturas digitais para uso dela, e também temos os exemplos mais simples como uso de tintas de canetas invisíveis (lidas com ultra violeta).

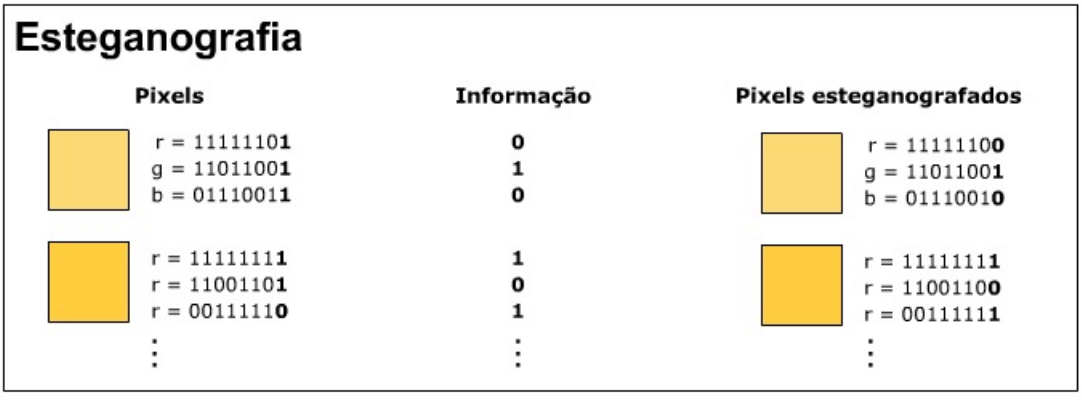
Entendendo o processo de alteração

Uma das formas que o algoritmo é utilizado, é que ele pega o bit menos significativo do arquivo (seja uma imagem, música, vídeo,etc) e altera ele, indexando um novo valor no conteúdo da mensagem dele. Permitindo a mensagem indexada seja comprimida nesses bits, por isso existe uma limitação de alguns tipos de extensões no uso dela.

Como vemos no gráfico abaixo:







Esteganografia x Criptografia

Existe uma confusão quando falamos do assunto de esteganografia, muitos confundem o uso dela com a criptografia. Lembrando que a criptografia tem o conceito de cifrar a mensagem, transformando o conteúdo dela (sem que entendam o significado da cifra) que fica de modo aparente a existência dela. Já no caso da esteganografia, ela tem o objetivo de esconder o conteúdo da mensagem, sem que ninguém perceba que existe algo oculto no arquivo ou que se quer exista uma mensagem.

Implementando a esteganografia com Steghide

O **Steghide** é uma ferramenta que permite a implementação da estegonografia, por meio da qual conseguimos pegar um anexo e indexar nossa mensagem dentro dela, sem que ninguém perceba que ela exista. Essa ferramenta também oferece recursos extras que nos dão maior segurança no envio da mensagem como:

- compressão de dados.
- criptografia dos dados incorporados.
- checagem de integridade automática usando checksum.

Ele utiliza a criptografia AES de 128 bits (sendo a mais segura nos dias de hoje) por padrão mas você pode incrementar outra criptografia nesse processo, suportando as extensões dos arquivos JPEG, BMP, WAV e AU no anexo a ser utilizado, mas no conteúdo de seu anexo pode ser qualquer uma.

Para dar um exemplo prático sobre a implementação da ferramenta vamos utilizar o exemplo seguinte: Temos uma imagem (*pinguim.jpg*) e temos um arquivo texto a ser enviado para um amigo (*secreto.txt*) então usamos o seguinte comando:

```
# steghide embed -ef secreto.txt -cf pinguim.jpg -sf novo_pinguim.jpg
```

Logo em seguida ele pedirá para inserirmos uma senha, então você confirmará ela duas vezes seguidas. Note que ele irá gerar outra imagem idêntica a imagem *pinguim.jpg* sem desfigurar nada nela, sendo que a olho nu não podemos identificar nenhuma mensagem oculta ou alteração desse conteúdo.

Original

Totalmente esteganografada

Agora para fazer o processo reverso, ou seja, de decifrar a mensagem seguimos o seguinte exemplo:

```
# steghide embed -ef secreto.txt -cf pinguim.jpg -sf novo_pinguim.jpg
```

E insira a senha qual foi inserida anteriormente para descriptografar a mensagem, pronto agora temos a nossa mensagem. Note que a segurança desse processo vincula que o destinatário além de saber a senha, tem que saber nome do arquivo (mensagem) a ser extraído, garantindo maior confidencialidade.

Caso queira ver esse processo em vídeo com a explicação e uso da ferramenta, confira abaixo.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com, ou ative o JavaScript caso ele esteja desativado em seu navegador.