Lab - Usando Esteganografia

Objetivos

Use a esteganografia para ocultar um documento num ficheiro JPEG.

Contexto/cenário

Steghide é um programa de esteganografia de código aberto que oculta dados em vários tipos de ficheiros, tais como ficheiros de áudio e imagem. Você irá ocultar um ficheiro de dados dentro de um ficheiro de imagem.

Recursos necessários

- Um PC com o Ubuntu 16.04 Desktop LTS instalado no VirtualBox ou numa máquina virtual VMware.

Passo 1: Abra uma janela de terminal no Ubuntu.

a. Inicie uma sessão no Ubuntu usando as seguintes credenciais:

Utilizador: **cisco**

Palavra-passe: **password**

b. Clique no ícone do terminal para abrir um terminal.

Passo 2: Execute Steghide.

a. No prompt de comandos, introduza o seguinte comando para mudar para o diretório **Downloads**:

```
cisco@ubuntu:~$ cd Downloads/
```

b. Execute **libreoffice secret.odt &** no prompt.

```
31cisco@ubuntu:~/Downloads$ libreoffice secret.odt &
```

Qual é a messagem em **secret.odt**?

_____

c. Feche o ficheiro **secret.odt** quando terminar.

d. Execute **gimp keyboard.jpg &** no prompt para ver o ficheiro de imagem

```
cisco@ubuntu:~/Downloads$ gimp keyboard.jpg &
```

e. Feche o ficheiro **keyboard.jpg** quando terminar.

f. No prompt de comandos, introduza o seguinte comando:

```
cisco@ubuntu:~/Downloads$ steghide embed -cf keyboard.jpg -ef secret.odt
```

Este comando pega o ficheiro jpeg chamado “keyboard.jpg” e usa-o como um suporte para incorporar o documento, **secret.odt**, nele.

g. Quando for solicitada uma frase-senha, use **Cisco**. Digite a frase-senha novamente quando solicitada.

```
cisco@ubuntu:~/Downloads$ steghide embed -cf keyboard.jpg -ef secret.odt
Enter passphrase:
```

h. Você embebeu o ficheiro **secret.odt**, no ficheiro de imagem, keyboard.jpg.

i. Abra os ficheiros, **secret.odt** e **keyboard.jpg**. Esses ficheiros mudaram? _____

Passo 3: Verifique o ficheiro oculto.

a. Digite o seguinte comando no terminal.

```
cisco@ubuntu:~/Downloads$ steghide info keyboard.jpg
```

```
cisco@ubuntu:~/Downloads$ steghide info keyboard.jpg
"keyboard.jpg":
  format: jpeg
  capacity: 11.9 KB
Try to get information about embedded data ? (y/n)
```

b. Digite **y** no terminal. (Não pressione **Enter**).

c. Introduza a frase-senha **Cisco** e pressione **Enter**.

d. Os resultados abaixo mostram que o ficheiro, secret.odt, está cifrado e compactado.

```
Enter passphrase:
  embedded file "secret.odt":
    size: 8.1 KB
    encrypted: rijndael-128, cbc
    compressed: yes
cisco@ubuntu:~/Downloads$
```

Passo 4: Extraia o ficheiro oculto.

a. Digite o seguinte comando no terminal.

```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
```

```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
```

b. Introduza a frase-senha, **Cisco**, e pressione **Enter**.

c. Introduza **e** quando solicitado a substituir o ficheiro existente **secret.odt** com o novo ficheiro extraído **secret.odt**.

```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
Enter passphrase:
the file "secret.odt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.odt".
```

d. Você extraiu o ficheiro. Abra o ficheiro extraído **secret.odt** com o LibreOffice.

Você poderia abrir o ficheiro? A mensagem secreta é a mesma de antes?

_____

Referências

Steghide: http://steghide.sourceforge.net/