Lab - Use Steganography to Hide Data

Objectives

Use steganography to hide a document within a JPEG file.

Background / Scenario

The advantage of steganography over cryptography is that the secret message does not attract any special attention. No one would ever know that a picture contained a secret message by viewing the file either electronically or in hardcopy. In this lab, you will use Steghide, an open-source steganography program, to hide a data file within an image file.

Required Resources

PC with the **CSE-LABVM** installed in VirtualBox

Instructions

Step 1: Open a terminal window in the CSE-LABVM.

a. Launch the **CSE-LABVM**.

b. Double-click the **Terminal** icon to open a terminal.

Step 2: Review the files that will be used for steganography.

a. Enter the **cd Downloads/** command to change to the **Downloads** directory, and then list the contents of the directory.

```
cisco@labvm:~$ cd Downloads/
cisco@labvm:~/Downloads$ ls -l
total 472
drwxr-xr-x 8 cisco cisco   4096 Jan 27 01:30 jcryptool
drwxrwxr-x 3 cisco cisco   4096 Mar 18 18:11 john
-rw-rw-rw- 1 cisco cisco 455357 Mar 22 16:10 keyboard.jpg
drwxrwxr-x 6 root  root    4096 Mar 18 17:46 lynis
-rw-rw-r-- 1 cisco cisco   9912 Mar 22 16:13 secret.odt
cisco@labvm:~/Downloads$
```

You will hide the contents of the secret.odt file inside the keyboard.jpg file.

b. Enter the **libreoffice secret.odt &** command to open the "secret.odt" file in LibreOffice.

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

What is the message in the **secret.odt**?

c. Click **File** > **Exit LibreOffice** to quit LibreOffice and close the file.

d. In the terminal window, press **Enter** to get a new command prompt, and the enter command **gimp keyboard.jpg &** to open the "keyboard.jpg" file in GIMP.

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

e. Click **File** > **Quit** to quit GIMP and close the file.

f. In the terminal window, press **Enter** to get a new command prompt.

Step 3: Use Steghide to embed the content of the secret.odt file inside the keyboard.jpg file.

a. At the command prompt, enter the following **steghide** command. When prompted for a passphrase, use **Cisco**. Re-enter the passphrase when prompted.

```
cisco@labvm:~/Downloads$ steghide embed -cf keyboard.jpg -ef secret.odt
Enter passphrase: Cisco
Re-Enter passphrase: Cisco
embedding "secret.odt" in "keyboard.jpg"... done
cisco@labvm:~/Downloads$
```

b. Open the files, **secret.odt** and **keyboard.jpg**.

Did these files change?

Step 4: Verify the secret.odt is hidden in the keyboard.jpg file.

Enter the **steghide info keyboard.jpg** command, type **y** at the prompt, and enter the passphrase **Cisco**, and then press **Enter**.

```
cisco@labvm:~/Downloads$ steghide info keyboard.jpg
"keyboard.jpg":
  format: jpeg
  capacity: 26.6 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase: Cisco
  embedded file "secret.odt":
    size: 9.7 KB
    encrypted: rijndael-128, cbc
    compressed: yes
cisco@labvm:~/Downloads$
```

Step 5: Extract the secret.odt file from the keyboard.jpg file.

a. Enter the **steghide extract -sf keyboard.jpg** command, enter the passphrase Cisco, and then type **y** at the prompt.

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

b. Open the extracted **secret.odt** file with LibreOffice.

Could you open the file? Is the secret message the same as before?

Answer Key

Step 1: Open a terminal window in the CSE-LABVM.

Step 2: Review the files that will be used for steganography.

What is the message in the **secret.odt**?

The secret document

Step 3: Use Steghide to embed the content of the secret.odt file inside the keyboard.jpg file.

Did these files change?

No. The files did not change.

Step 4: Verify the secret.odt is hidden in the keyboard.jpg file.

Step 5: Extract the secret.odt file from the keyboard.jpg file.

Could you open the file? Is the secret message the same as before?

The file can be opened, and the message is the same as before.