Lab – Using Steganography

Objectives

Use steganography to hide a document within a JPEG file.

Background / Scenario

Steghide is an open source steganography program that hides data in various types of files such as audio and image files. You are going to hide a data file within an image file.

Required Resources

- PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine

Step 1: Open a terminal window in Ubuntu.

a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**

b. Click on the terminal icon to open a terminal.

Step 2: Run Steghide.

a. At the command prompt, enter the following command to change to the **Downloads** directory:

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

b. Enter **libreoffice secret.odt &** at the prompt.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

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

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

c. Close the **secret.odt** file when done.

d. Enter **gimp keyboard.jpg &** at the prompt to view the image file

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

e. Close the **keyboard.jpg** file when done.

f. At the command prompt, enter the following command :

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

This command takes the jpeg file called “keyboard.jpg” and uses it as a carrier to embed the document, **secret.odt**, into it.

g. When prompted for a passphrase, use **Cisco**. Re-enter the passphrase when prompted.

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

h. You have embedded the document, **secret.odt**, into the image file, keyboard.jpg.

i. Open the files, **secret.odt** and **keyboard.jpg**. Did these files change?

Step 3: Verify the hidden file.

a. Type the following command in 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. Type **y** at the prompt. (Do not press **Enter**).

c. Enter the passphrase **Cisco** and press **Enter**.

d. The results below shows that the file, secret.odt, is encrypted and compressed.

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

Step 4: Extract the hidden file.

a. Type the following command in terminal.

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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

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

b. Enter the passphrase, **Cisco**, and press **Enter**.

c. Enter **y** when prompted to overwrite the existing **secret.odt** file with the new extracted **secret.odt** file.

```
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. You have extracted the file. Open the extracted **secret.odt** file with LibreOffice.

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

References

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

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.