Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 6, June 2021, pg.90 – 96

Steganography Using Bin-Walk Tool & Its Overview

Pooja Gaikwad[1]; Priyanka Ghumare[2]; Gayatri Chaudhari[3]; Sayali Nikam[4]; Rupali Murtdak[5];Assistant Prof. Umakant Mandawkar[6]

[1]Department of Computer Science, Sandip University, India
[2]Department of Computer Science, Sandip University, India
[3]Department of Computer Science, Sandip University, India
[4]Department of Computer Science, Sandip University, India
[5]Department of Computer Science, Sandip University, India
[6]Department of Computer Science, Sandip University, India

[1] poojasgaikwad.32@gmail.com; [2] ghumarepriyanka1999@gmail.com; [3] gayatrichaudhari85@gmail.com; [4] sayalinikam454@gmail.com; [5] murtadaksiddhi7@gmail.com; [6] umakant.mandawkar@sandipuniversity.edu.in

DOI: 10.47760/ijcsmc.2021.v10i06.010

Abstract— In this paper, a detailed overview on steganography & its Types, tools, techniques is conducted to study and look over them. This research involves the steganography using binwalk tool in the Necromancer. Necromancer is the vulnerable virtual machine, in order to gain the root access of VM (Virtual Machine) there are 11 flags to collect on the way, Few flags are found by using the Binwalk tool, to know the hint behind image, so we have used an Image steganography in one of flag of Necromancer. Flags are nothing but any encrypted code. Steganography refers to the act of camouflage the secret data within any image, audio, video in order to avoid the detection. The secret data is then extracted at its destination. The use of steganography are often combined with encryption as an additional step for hiding or protecting data.

Keywords— Steganography, Information security, Information Hiding, cryptography, Necromancer

I. INTRODUCTION

Can you visualize that if there can be the capability and power to hide & conceal data in plain sight? Well it is possible, Yes. Steganography is the art of hiding secret information to prevent the detection of message that is hidden. Actually a word “Steganography” means concealing information or data within other non-secret text or data. This word comes from Greek, “Steganographia”, which is combination of two words stegano & graphia, stegano means covered, graphia means writing. This is how steganography word is established. There are various types of steganography like image Steganography, text Steganography, audio Steganography, video Steganography etc.

Well in the world of information Security, The usage of steganography combines encryption as an additional step for concealing or protecting the data. This paper will also provide different types, tools & techniques of steganography.

II. WHAT IS STEGANOGRAPHY?

Steganography is the technique of hiding secret data, non-secret, file or message in order to avoid detection. The secret data is then extracted at its destination. The use of steganography is often combined with encryption as an additional step for hiding or protecting data.

Techniques Used in Steganography

There are three Techniques used in steganography:-

1) -Least Significant Bit
2) -Palette Based Technique
3) -Secure Cover Selection

1. *Least Significant Bit*

   In Least Significant bit technique, when the attacker identifies the information about the least significant bit in the image and with their secret message. In this case, malicious activity i.e. Malicious code. The targeted downloads files, they introduce the malware into their computer which allows the attacker access to this device and the hack begins and generate the malicious code. In this activity, first of all we have to identifies the information of the bit of image with the secret code and we crack the malicious activity. It is used for large amount of data like image, audio, text and to carry out hidden exchanges.

2. *Palette Based Technique*

   In Palette Based Technique, It also uses significant bit images as malware. Here, first of all attackers first encrypt the message and then hide the file. A large portion of this image is available in palette-based formats, like as GIF and PNG. In that there are two methods is to hiding the message in palette-based images. Embedding message into the palette. Embedding into the image data i.e. malicious code. When attacker attacks the file before that encrypt it and then hide it. It converts the huge data but this data only in GIF and PNG format and then encrypt it and it convert it into the embedded message into Palette. Criminals generally used data to hide the information and communicate with other criminals.

3. *Secure Cover Selection*

   In Secure Cover Selection, in that cyber criminals compares the block images into the specific malware. Existing cover selection methods for steganography cannot resist steganalysis. It is a secure cover selection method which is able to resist steganalysis and single object steganalysis. This is a really complex technique where the cyber criminals compare the blocks of the carrier image to the blocks of their specific malware. If an image with the same blocks as the malware is found, it is a secure cover selection. It is used for ethical hackers also. These are just a few methods by which black hat hackers. Black hat hackers also compare the data in the block of image and then malware will be found. It allows attackers to operate in stealth mode while conducting a serious attack mode. Secure Cover selection method includes the deployment of security patches, updating software, and educating end-users.

III. TYPES OF STEGANOGRAPHY

1. Image

The process of hiding the secret message in an image file is called as image steganography. It has certain limitations like you cannot contain a large amount of data in an image because it may shown as that image contains the suspicious data. It is the process of hiding a secret message within a larger one in such a way that someone cannot understand the contents of the hidden message. Steganography attempts to hide the existence of communication.
Image steganography refers to hiding data i.e. text, images or audio files in another Video file or Image. The current project aims to use steganography for a picture with another image using spatial domain technique. This hidden information or data can be retrieved or achieve only through proper decoding technique.
As the name suggests, Image Steganography refers to the method of hiding data within a picture file. The image selected for this purpose is named the cover-image and therefore the image obtained after steganography is named the stego-image.
Hiding the data or information by using the cover object as the image is known as image steganography. In digital steganography, images are widely used cover source because there are an enormous number of bits present within the digital representation of a picture. There are tons of the ways to cover information inside a picture. Most common approaches include:

- Least Significant Bit Insertion
- Encrypt and Scatter
- Coding and Cosine Transformation
- Redundant Pattern Encoding
- Masking and Filtering

2. Text

We can hide secrete data in text file. This method lacks robustness and isn't that much efficient in hiding the data. It can be easily detected or exposed by the eyes of intruders. Text steganography is a technique of hiding secret text message inside another text as a covering message or generating a cover message related with the original secret message. Text Steganography is hiding information or data inside the text files. It involves things like changing words within a text, changing the format of existing text, generating random character sequences or using context-free grammars to generate readable texts. Different techniques used to hide the data in the text message are:

- Format Based Method
- Linguistic Method
- Random and Statistical Generation

3. Video

The process of hiding the secret message in an Video file is known as Video steganography. Video Steganography is far more safe and efficient as compared to that of the image and text steganography. Steganography can embed large amount of data in frames of the video and audio. In Video Steganography you'll hide quite

data into digital video format. The advantage of this sort may be a great deal of knowledge are often hidden inside and therefore the incontrovertible fact that it's a moving stream of images and sounds. This because the combination of Image Steganography and Audio Steganography.

Two main classes of Video Steganography include:

- Embedding data in uncompressed raw video and compressing it later
- Embedding data directly into the compressed data stream

4. Audio

In Audio Steganography to hide the secrete data or information audio is used as the cover. It is also very robust in nature but with limitation of the quantity of knowledge one can hide. In audio steganography, the secret message is stored into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound may be a far more difficult process in comparison to others, like Image Steganography. Various methods of audio steganography include:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding
- Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files

IV. STEGANOGRAPHY TOOLS

Xiao steganography:

Xiao Steganography is free software that can be used to beating confidential files in BMP images or WAV files. Using tool in steganography is so easy, just open software and load any BMP image or WAV file to its interface. Then add a file you want to hide. Steganography also hold up specifics file encryption code. We can choose the file from various algorithms like, DES, RC2, RC4, Triple DES 112, and hashing MD5, MD2, MD4 and SHA. We just need to select the one from the list and then need to save at file. To read the private message from this file, we have to use this software again. Steganography software will read the file and will decode the hidden file from it. But we cannot extract the hidden file with any other software instead of steganography. CNET is also popular for offering installation of third-party browser extensions. Be assured to know what other software and adware this tool is offering along with the installation of Xiao Steganography.

Steghide:

Steghide is open-source steganography software, it can also hide your secret file in an image or audio file. We won't notice any of the changes in image or audio file. However, secret file will be inside the original image or audio file. This software is command-line software. But we should know the commands to use the tool. Commands are getting to be used to embed files within the image or audio file. In addition, to extract file from the image or audio file, we need to use another command. Steghide tool was developed many years ago but still it works well. We need Windows 32-bit version to run Steghide software.

Stools:

Stools is the software that helps to hide files & folders using steganography, It hides information or data in graphics files like BMP,GIF, and WAV files(sound/music) in such manner that files are no different from those not containing any of hidden data i.e. picture can be viewed and music can listen to.

The files like .BMP, or .WAV at some extent modified so that the changes will not affect quality of that images or music means changes made will not be virtually noticed.

This software not only hides information or data within a seemly usual files but it also enables to encrypt the hidden information as well.

It is somewhat less powerful in that it lacks features such as the ability to hide information or data within HTML or text files, and irrecoverable data detection.

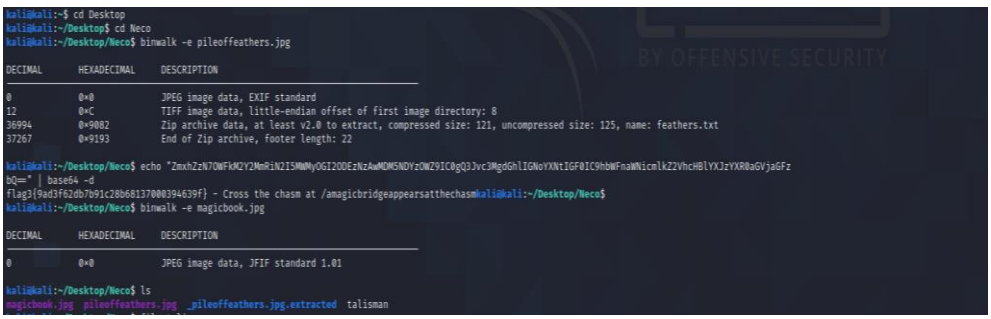
Binwalk:

Binwalk is a tool for explore a given binary image for embedded files and executable code. Specifically, it's designed for identifying files and code embedded inside firmware images. Binwalk uses the libmagic library, so it's compatible with magic signatures created for the Unix file utility. Binwalk also includes a custom magic signature file which contains improved signatures for files that are commonly found in firmware images like compressed/archived files, firmware headers, Linux kernels, bootloaders, filesystems, etc.

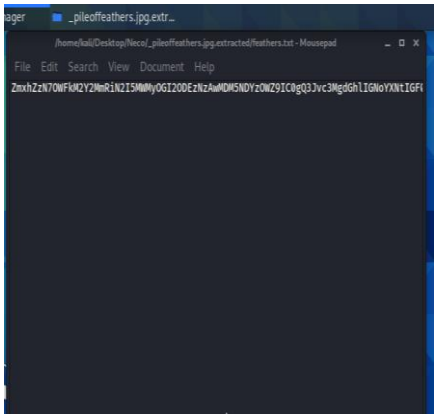
For example,

NOTE: We have done steganography using above image is as follow

- Run the command



The hidden message we get from given image is as below in pileoffeathers.txt file in base64 format after decrypting it we will get information in human readable form.



Exif:

Exif tool is a Kali Linux software that allows a to show and operate the metadata of the image. An image can give lots of data like which device, ISO, date, time, lens type. This data can be extracted and alter using the Exif tool. Exiftool is also very commonly used for producing steganographic and intelligence challenges and also utilized by professionals and students those who take CTF challenges that is Catch The Flag. This tool is very useful to view metadata of the file as it is free and open source.Some of command properties of Exif tool are as follows,

- *exiftool | grep GPS :*

  To Extract GPS coordinates. The photographs we capture using our smartphones or camera have GPS coordinates embedded as metadata within the image files.

- *exiftool -ThumbnailImage:*

  This command is use to extract the thumbnail image

- *exiftool -v – Verbose mode:*

  It generates extended information i.e. when we add [-v] to the exif tool command it will print out the comprehensive data about the process that it is performing.

CONCLUSION

This paper shows the concept that how we used binwalk tool for steganography in necromancer to collect the flag & various other tools used for steganography, different types of steganography, Techniques in order to analyze them & use in proper manner.

Steganography is helpful for concealing messages foe communication, the proper use of steganography proves that it can be the solution for information data hiding.

REFERENCES

[1]. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi6gviG6f3wAhUBzDgGHX98DrIQFjABegQIAhAE&url=https%3A%2F%2Fwww.giac.org%2Fpaper%2Fgsec%2F35%2Fintroduction-steganography%2F101757&usg=AOvVaw3eiJjI6r4dig5fy58rr21c

[2]. https://en.wikipedia.org/wiki/Steganography

[3]. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi6gviG6f3wAhUBzDgGHX98DrIQFjACegQIBBAE&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FSteganography&usg=AOvVaw1IvEK2KetgCEMu2QKFd0Ji

[4]. https://link.springer.com/article/10.1007/s11042-014-1952-z

[5]. https://www.academia.edu/Documents/in/Steganography

[6]. https://www.slideshare.net/saugatapalit/steganography-28604752

[7]. https://www.researchgate.net/publication/309741518_An_Introduction_to_Steganography

