HackTheBox – Davinci Write Up

Tools:
- Steganographic Decoder (https://futureboy.us/stegano/decinput.html)
- MD5 Decoder (https://hashtoolkit.com/decrypt-md5-hash/020e60c6a84db8c5d4c2d56a4e4fe082)
- Hex file viewer (https://hex-works.com/eng)
- Binwalk tool (Kali Linux)
- Steghide tool (Have to install manually in Kali Linux)
- Base64 decoder (https://www.base64encode.org/)

Walkthrough:

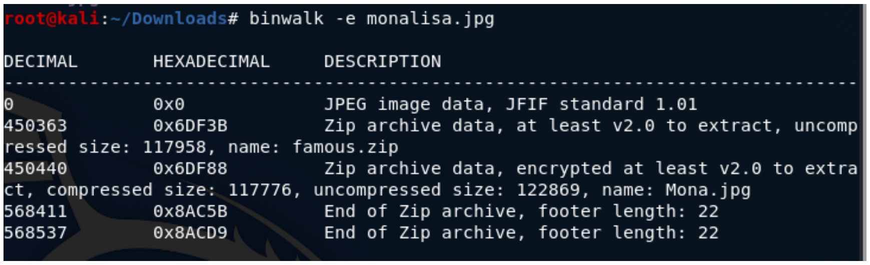
Step	Description
1	Unzip the files from the zip file. 3 files were found. - Thepassword_is_the_small_name_of_the_actor_named_Hanks.jpg - monalisa.jpg - Plans.jpg
2	Based on the name of the file, upload the file to "https://futureboy.us/stegano/decinput.html" and use the password "TOM". The contents hidden in the image is displayed below: === == Content within the image === == Hey Filippos, This is my secret key for our folder.... (key: Please decrypt yourself ☺) I used an encryption with 32 characters. hehehehehe! No one will find it! ;) Decrypt it... It's easy for you right? Don't share it with anyone...plz! if you are reading that, call me! I need your advice for my new CTF challenge! Kisses, -Luc1f3r

3 Decrypt the "key" in https://hashtoolkit.com/decrypt-md5-hash/020e60c6a84db8c5d4c2d56a4e4fe082 as it seems to be a md5 hash.

The answer obtained is "Please decrypt yourself ☺"

4 Next, open the "Plans.jpg" in https://hex-works.com/eng to view the hex values. Upon inspecting the file, there was a Youtube video link (Please investigate yourself☺).

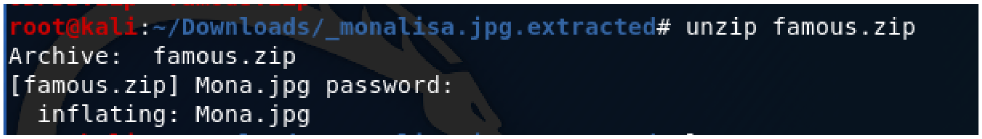
5 Inside Kali Linux, use the "binwalk" tool to perform the command "binwalk –e monalisa.jpg". After that, a zip file "famous.zip" was found to be extracted.



```
root@kali:~/Downloads# binwalk -e monalisa.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
450363        0x6DF3B         Zip archive data, at least v2.0 to extract, uncomp
ressed size: 117958, name: famous.zip
450440        0x6DF88         Zip archive data, encrypted at least v2.0 to extra
ct, compressed size: 117776, uncompressed size: 122869, name: Mona.jpg
568411        0x8AC5B         End of Zip archive, footer length: 22
568537        0x8ACD9         End of Zip archive, footer length: 22
```

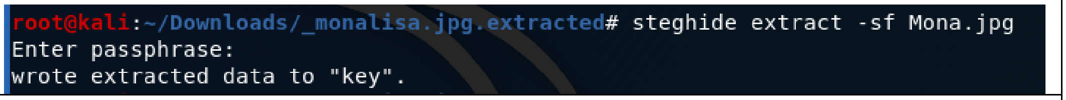
6 Based on the hint "famous.zip", the password refers to the "key" decrypted earlier. The content extracted from the zip file is "Mona.jpg".



```
root@kali:~/Downloads/_monalisa.jpg.extracted# unzip famous.zip
Archive:  famous.zip
[famous.zip] Mona.jpg password:
  inflating: Mona.jpg
```

7 Use the Steghide tool with the command "steghide extract –sf Mona.jpg" to extract the contents hidden within "Mona.jpg". The password for the file is "Guernica" based on the Youtube Video link discovered.

The extracted content was a file named "key".



```
root@kali:~/Downloads/_monalisa.jpg.extracted# steghide extract -sf Mona.jpg
Enter passphrase:
wrote extracted data to "key".
```

8 The "key" file contained a ciphertext which seems to be encrypted in Based64 and had to be decrypted 3 times to get the flag.

Another alternative to this step is to use Cyber Chef (https://gchq.github.io/CyberChef) and use the "Magic" recipe.

Flag is HTB{ Please decrypt yourself ☺}