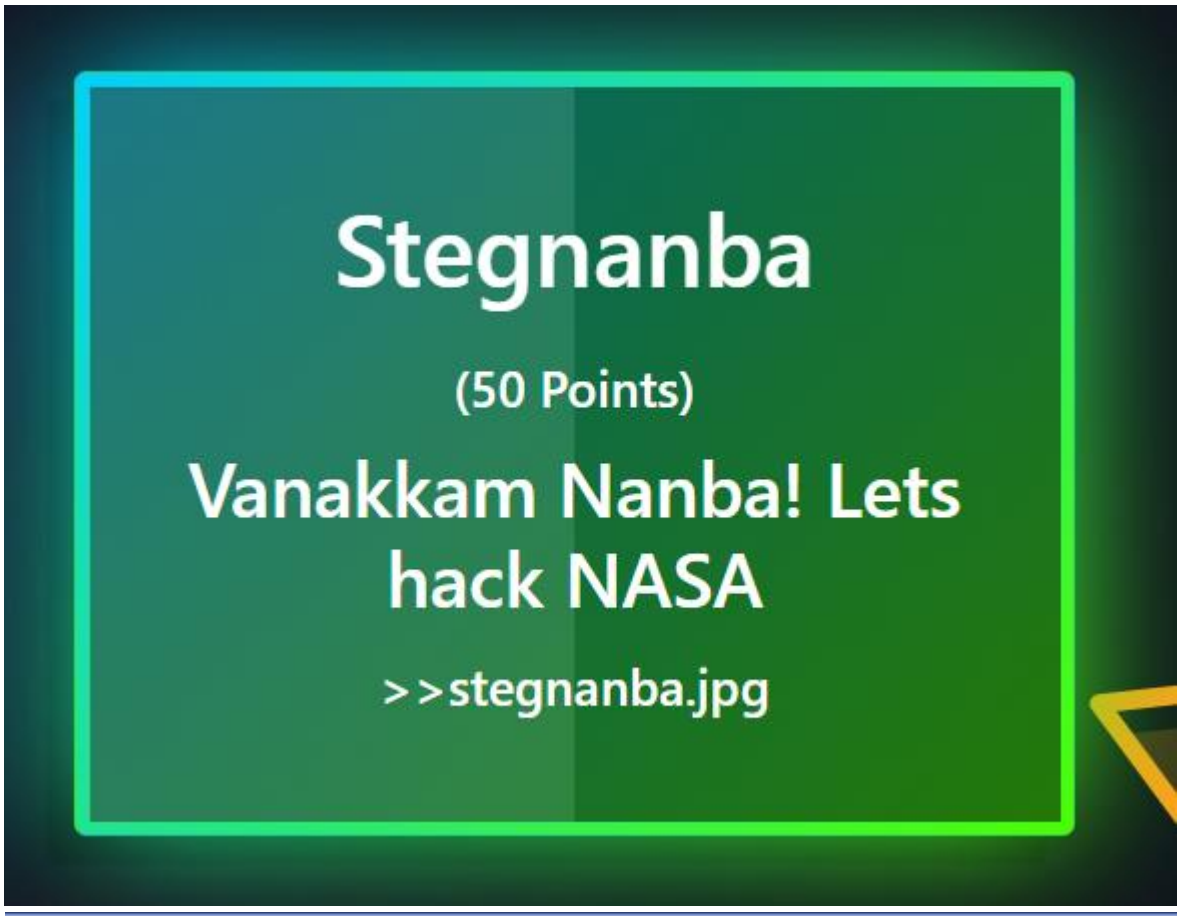
CTF Walkthrough

STEGNO Challenge

Stegnanba

50 Points



First click on the stegnanba.jpg and then a **.zip** will be downloaded then unzip the files and a .jpg will be extracted from it.

```
┌──(kali㉿kali)-[~/Desktop/steg]
└─$ ls
stegnanba.zip

┌──(kali㉿kali)-[~/Desktop/steg]
└─$ unzip stegnanba.zip
Archive:  stegnanba.zip
  inflating: stegnanba.jpg
```

let's use **exiftool** to view the metadata of "**stegnanba.jpg**" image.

```
┌──(kali㉿kali)-[~/Desktop/steg]
└─$ exiftool stegnanba.jpg
ExifTool Version Number         : 12.16
File Name                       : stegnanba.jpg
Directory                       : .
File Size                       : 396 KiB
File Modification Date/Time     : 2021:05:17 22:04:42-04:00
File Access Date/Time           : 2021:05:24 13:21:44-04:00
File Inode Change Date/Time     : 2021:05:24 13:21:44-04:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 236
Y Resolution                    : 236
Resolution Unit                 : cm
Artist                          : dDRtMWw0bmQ0Cg==
Y Cb Cr Positioning             : Centered
Comment                         : vanakam nanba iam p4ul
Image Width                     : 3840
Image Height                    : 2160
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 3840x2160
Megapixels                      : 8.3
```

The base64 encoded string is found in the **Artist**. Let's decode it.

```
┌──(kali㉿kali)-[~]
└─$ echo "dDRtMWw0bmQ0Cg==" |base64 -d
t4m1l4nd4
```

By decoding it I found a string. Next just try to extract the hidden data from **stegnanba.jpg** using the below command.

steghide extract -sf stegnanba.jpg

And the passphrase for extraction is : **t4m1l4nd4**

```
┌──(kali㉿kali)-[~/Desktop/steg]
└─$ steghide extract -sf stegnanba.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
```

The flag.txt file is extracted. Let's view the file using "**cat**" command and it contains a base64 encoded text.

```
┌──(kali㉿kali)-[~/Desktop/steg]
└─$ cat flag.txt
VkdGdGFXeERWRVo3Y3pjeloxOXRNMTl3TVRNME5UTmZNekUxTTE5Y1NURXhYMk0wYkd4ZmRtNTlD
Zz09Cg==
```

Decode it and again we got a base64 encoded text and again decode it and finally we got the flag.!!

```
┌──(kali㉿kali)-[~/Desktop/steg]
└─$ echo "VkdGdGFXeERWRVo3Y3pjeloxOXRNMTl3TVRNME5UTmZNekUxTTE5Y1NURXhYMk0wYkd4ZmRtNTlDZz09Cg==" | base64 -d
VGFtaWxDVEZ7czczZ19tM19wMTM0NTNfMzE1M19cSTExX2M0bGxfdm59Cg==

┌──(kali㉿kali)-[~/Desktop/steg]
└─$ echo "VGFtaWxDVEZ7czczZ19tM19wMTM0NTNfMzE1M19cSTExX2M0bGxfdm59Cg==" |base64 -d
TamilCTF{s73g_m3_p13453_3153_\I11_c4ll_vn}
```

THE END