NeverLAN CTF

Crypto : It is like an onion secrets

Value : 300 pts

Difficulty : Hard

Description : This one has layes like an onion. Just don’t let it make you cry...

Your flag won’t be in the normal flag{flagGoesHere} syntax.

Attachment : Much_Confused.png

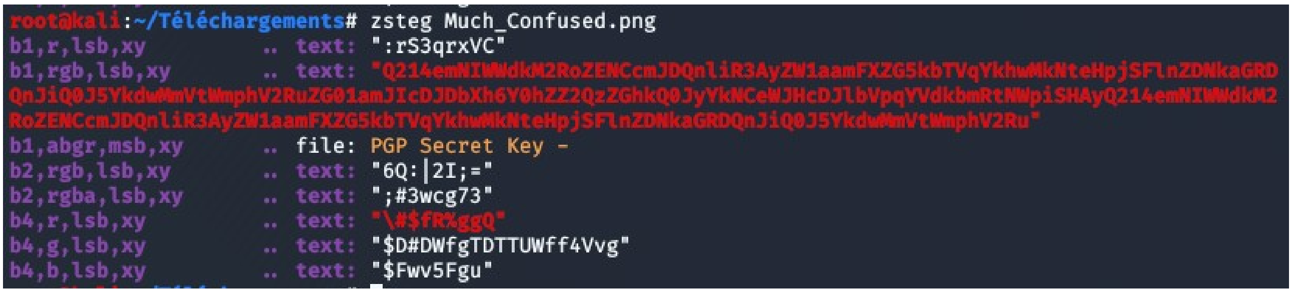
Solution :

Downloading and opening the attachment «Much_Confused.png» and we see this picture.

First we need to install zsteg tool, with the command bellow :

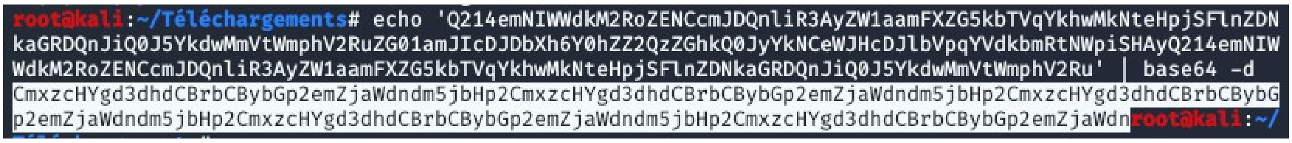
```
gem install zsteg
```

Running the tools agains the picture and we got this result.



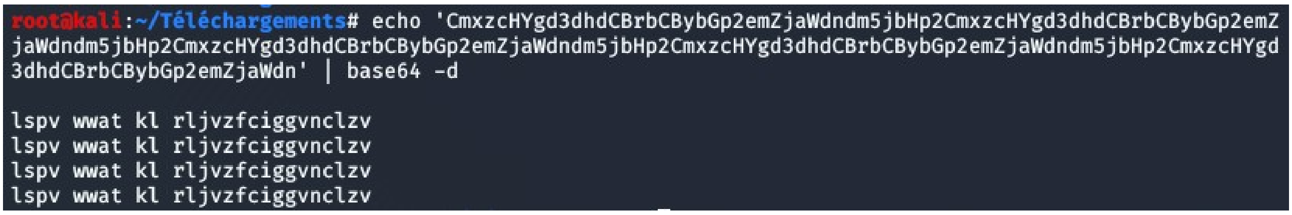
```
root@kali:~/Téléchargements# zsteg Much_Confused.png
b1,r,lsb,xy         .. text: ":rS3qrxVC"
b1,rgb,lsb,xy       .. text: "Q214emNIWWdkM2RoZENCcmJDQnliR3AyZW1aamFXZG5kbTVqYkhwMkNteHpjSFlnZDNkaGRD
QnJiQ0J5YkdwMmVtWmphV2RuZG01amJIcDJDbXh6Y0hZZ2QzZGhkQ0JyYkNCeWJHcDJlbVpqYVdkbmRtNWpiSHAyQ214emNIWWdkM2
RoZENCcmJDQnliR3AyZW1aamFXZG5kbTVqYkhwMkNteHpjSFlnZDNkaGRDQnJiQ0J5YkdwMmVtWmphV2Ru"
b1,abgr,msb,xy      .. file: PGP Secret Key -
b2,rgb,lsb,xy       .. text: "6Q:|2I;="
b2,rgba,lsb,xy      .. text: ";#3wcg73"
b4,r,lsb,xy         .. text: "\#$fR%ggQ"
b4,g,lsb,xy         .. text: "$D#DWfgTDTTUWff4Vvg"
b4,b,lsb,xy         .. text: "$Fwv5Fgu"
```

It look like a base64.



```
root@kali:~/Téléchargements# echo 'Q214emNIWWdkM2RoZENCcmJDQnliR3AyZW1aamFXZG5kbTVqYkhwMkNteHpjSFlnZDN
kaGRDQnJiQ0J5YkdwMmVtWmphV2RuZG01amJIcDJDbXh6Y0hZZ2QzZGhkQ0JyYkNCeWJHcDJlbVpqYVdkbmRtNWpiSHAyQ214emNIW
WdkM2RoZENCcmJDQnliR3AyZW1aamFXZG5kbTVqYkhwMkNteHpjSFlnZDNkaGRDQnJiQ0J5YkdwMmVtWmphV2Ru' | base64 -d
CmxzcHYgd3dhdCBrbCBybGp2emZjaWdndm5jbHp2CmxzcHYgd3dhdCBrbCBybGp2emZjaWdndm5jbHp2CmxzcHYgd3dhdCBrbCBybG
p2emZjaWdndm5jbHp2CmxzcHYgd3dhdCBrbCBybGp2emZjaWdndm5jbHp2CmxzcHYgd3dhdCBrbCBybGp2emZjaWdnroot@kali:~/
```

Decoding it, we got another cipher who look like base64 let’s try to decode again.



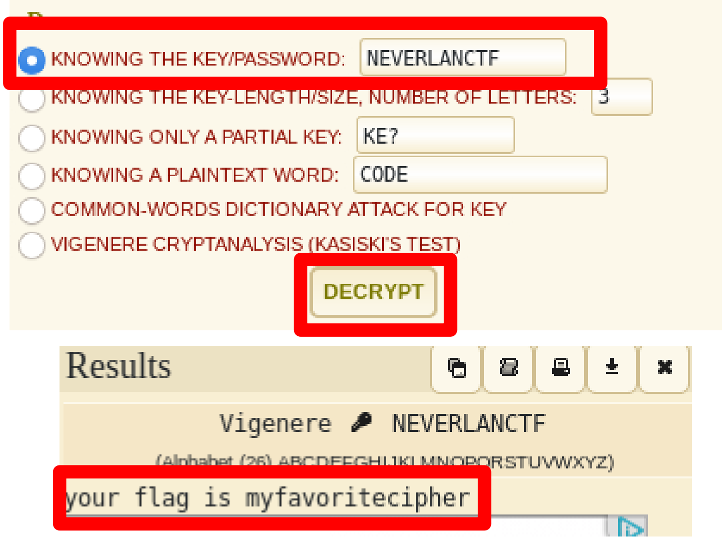
```
root@kali:~/Téléchargements# echo 'CmxzcHYgd3dhdCBrbCBybGp2emZjaWdndm5jbHp2CmxzcHYgd3dhdCBrbCBybGp2emZ
jaWdndm5jbHp2CmxzcHYgd3dhdCBrbCBybGp2emZjaWdndm5jbHp2CmxzcHYgd3dhdCBrbCBybGp2emZjaWdndm5jbHp2CmxzcHYgd
3dhdCBrbCBybGp2emZjaWdn' | base64 -d

lspv wwat kl rljvzfciggvnclzv
lspv wwat kl rljvzfciggvnclzv
lspv wwat kl rljvzfciggvnclzv
lspv wwat kl rljvzfciggvnclzv
```

And another cipher, it look like Vigenere cipher.

Source : https://www.dcode.fr/vigenere-cipher

Trying to decode it didnt worked so far, so i tried to guess a key/password and chose the name of the ctf «NEVERLANCTF» and press on decrypt.



● KNOWING THE KEY/PASSWORD: NEVERLANCTF

○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

○ KNOWING ONLY A PARTIAL KEY: KE?

○ KNOWING A PLAINTEXT WORD: CODE

○ COMMON-WORDS DICTIONARY ATTACK FOR KEY

○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

Vigenere 🔑 NEVERLANCTF

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

your flag is myfavoritecipher

Flag : myfavoritecipher