MENU

# THE EMBEDDED WORLD

*Embedded system and hacking tutorial*

WRITTEN BY KELCY66

AUGUST 14, 2019

# [HACKING WALKTHROUGH] ANOTHER CTF CHALLENGE

CTF

This is yet another CTF challenge from tryhackme. This is my first blog post after the holiday and the challenge covers the very basic codes and hashes cracking. Hope you enjoy the write-up.

## TASK 1: TRANSLATION AND SHIFTING

This task required the challenger to perform a translation or shifting certain ciphers such as ROT13, ROT47, Morse code, etc.

## TASK 1-1: LEET A.K.A L33T

Leet is a form of font which is used mostly on the internet. Is a famous font used by numerous hackers.

**Cipher: c4n you c4p7u23 7h3 f149**
**Solution**: This is a straight forward task, you can guess the answer easily. Or, using this converter.
**Answer**: can you capture the flag

## TASK 1-2: BINARY TO ASCII

Binary is a type of machine language.

**Cipher: 01101100 01100101 01110100 01110011 00100000 01110100 01110010 01111001 00100000 01110011 01101111 01101101 01100101 00100000 01100010 01101001 01101110 01100001 01110010 01111001 00100000 01101111 01110101 01110100 00100001**
**Solution**: Copy the cipher code into the converter.
**Answer**: lets try some binary out!

## TASK 1-3: BASE32

Base32 is a common transfer encoding. It consists of 32-char set. These char-sets are usually alphabet in uppercase.

**Cipher:MJQXGZJTGIQGS4ZAON2XAZLSEBRW63LNN5XCA2LOEBBVIRRHOM======**

**Solution**: Put the cipher code into the converter

**Answer**: base32 is super common in CTF’s

## TASK 1-4: BASE64

Base64 is another common transfer encoding. It consists of 64-char set. These char-sets are usually alphabet in uppercase and lowercase.

**Cipher:RWFjaCBCYXNlNjQgZGlnaXQgcmVwcmVzZW50cyBleGFjdGx5IDYgYml0cyBvZiBkYXRhLg==**

**Solution**: Put the cipher code into the converter

**Answer**: Each Base64 digit represents exactly 6 bits of data.

## TASK 1-5: HEX TO ASCII

Hex consists of 16 bits of binary. It also known as base16.

**Cipher: 68 65 78 61 64 65 63 69 6d 61 6c 20 6f 72 20 62 61 73 65 31 36 3f**

**Solution**: Copy the cipher into the converter

**Answer**: hexadecimal or base16?

## TASK 1-6: ROT 13

Rot 13 or known as rotate 13 is a form of Caesar cipher which rotate in 13 times.

**Cipher: Ebgngr zr 13 cynprf!**

**Solution:** Punch in the cipher into the converter

**Answer:** Rotate me 13 places!

## TASK 1-7: ROT 47

Rot 47 or known as rotate 47 is another form of Caesar cipher which rotate in 47 times. It encode almost all visible ASCII character.

**Cipher: *@F DA:? >6 C:89E C@F?5 323J C:89E C@F?5 Wcf E:>6DX**

**Solution:** Copy the cipher into the converter

**Answer:** You spin me right round baby right round (47 times)

## TASK 1-8: MORSE CODE

Morse code is a combination of signal made of short and long impulsion (dot and dash). It was designed for telecommunication.

**Cipher: – . .-.. . -.-. ——— . .- -. .. -.-. .- – .. —-. . -. -.-. —-.. .. -. –.**

**Solution:** Put the cipher into the converter

**Answer:** telecommunication encoding

## TASK 1-9: BCD TO ASCII

Binary-Coded Decimal (BCD) is a base10 encoding technique.

**Cipher: 85 110 112 97 99 107 32 116 104 105 115 32 66 67 68**

**Solution:** Punch in the cipher into the converter

**Answer:** Unpack this BCD

## TASK 1-10: MULTIPLE CIPHER

This task consists of multiple ciphers. Challenger required to decode the cipher from the previous task

**Cipher 1: Base64**

**Cipher 2: Morse code**

**Cipher 3: Binary to ASCII**

**Cipher 4: ROT 47**

**Cipher 5: BCD to ASCII**

**Answer:** Let's make this a bit trickier...

# TASK 2: HASHES

If you refer to my previous post, a hash can be cracked using hashcat either by brute force or dictionary. However, it is not a 100% guarantee that the hash can be cracked using the hashcat. For this task, the author suggested using a brute-forcing. However, it is impossible as the permutation is too large and it will take more than a day. The only way to do that is to decrypt it using online tools such as md5decrypt. This is because the hashed text has been stored in their database.

## TASK 2-1: MD2

This task can be done using this online tool.

**Hash**: **39d4a2ba07e44421c9bedd54dc4e1182**
**Answer**: MDwhat?

## TASK 2-2: MD4

From this task onward, the hashes can be cracked using md5decrypt.

**Hash: e0418e7c6c2f630c71b2acabbcf8a2fb**
**Answer:** digest the message algorithm

## TASK 2-3: MD5

**Hash: efbd448a935421a54dda43da43a701e1**

**Answer:** 128-bit of delicious hash values

## TASK 2-4: NTLM

**Hash: 11FE61CE0639AC2A1E815D62D7DEEC53**

**Answer:** Microsoft has encryption?

## TASK 2-5: SHA512

**Hash:**
**a361f05487b879f25cc4d7d7fae3c7442e7849ed15c94010b389faafaf8763f0dd022e52364027283d55dcb10974b09e7937f901584c092da65a14d1aa8dc4**
**Answer**: 1024 bit blocks!

## TASK 2-6: SHA256

**Hash: d48a2f790f7294a4ecbac10b99a1a4271cdc67fff7246a314297f2bca2aaa71f**

**Answer:** Commonly used in Blockchain

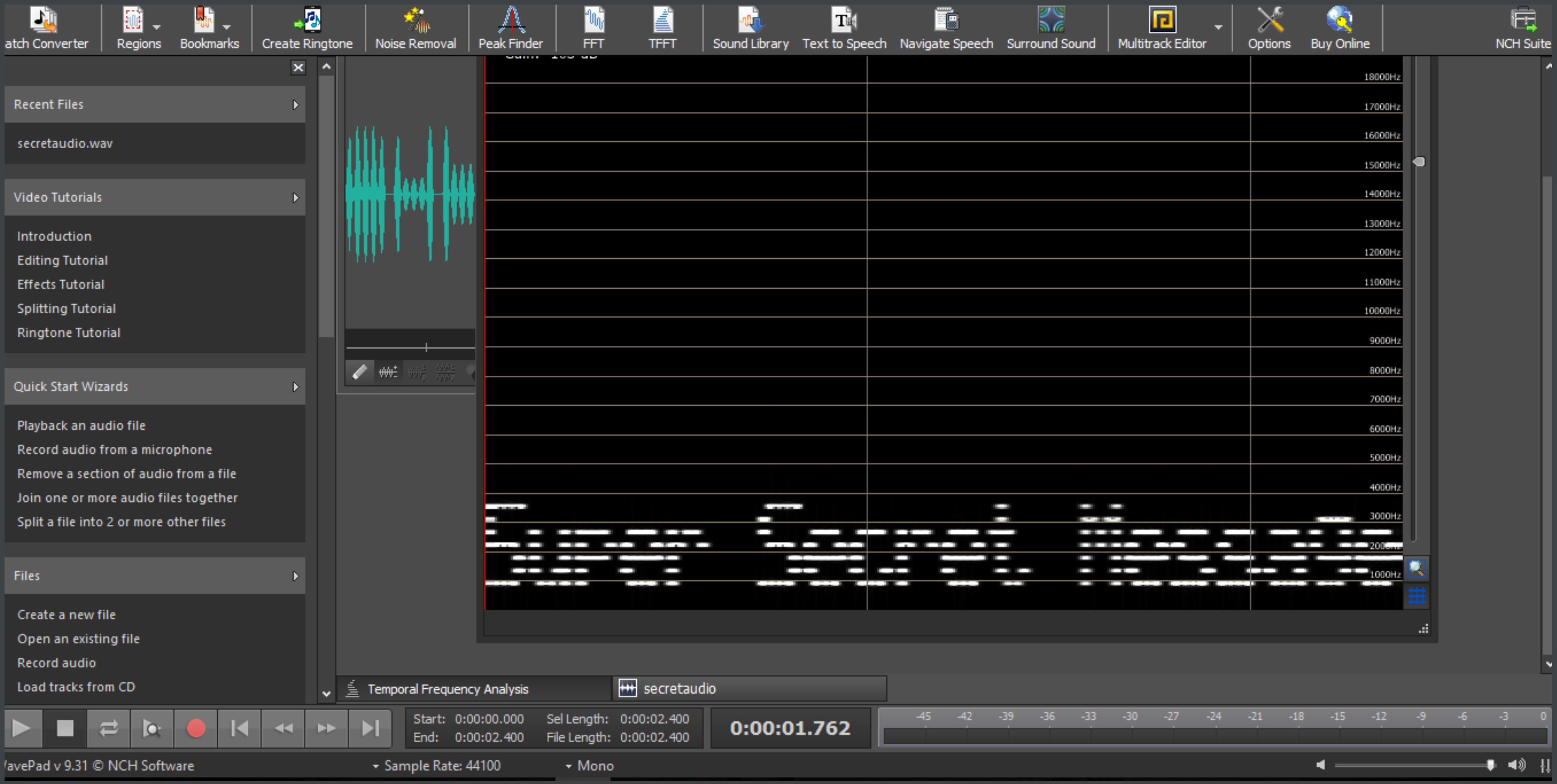
## TASK 2-7: SHA1

**Hash: a34e50c78f67d3ec5d0479cde1406c6f82ff6cd0**

**Answer:** The OG

# TASK 3: SPECTROGRAM

This task is easy. Just download any sound or wave analyzer tool such as aducity. For this task, I going to use wavepad. Simply open the downloaded wave file and open it up in TFFT (Tool > TFFT). A message will be revealed.



The secret message

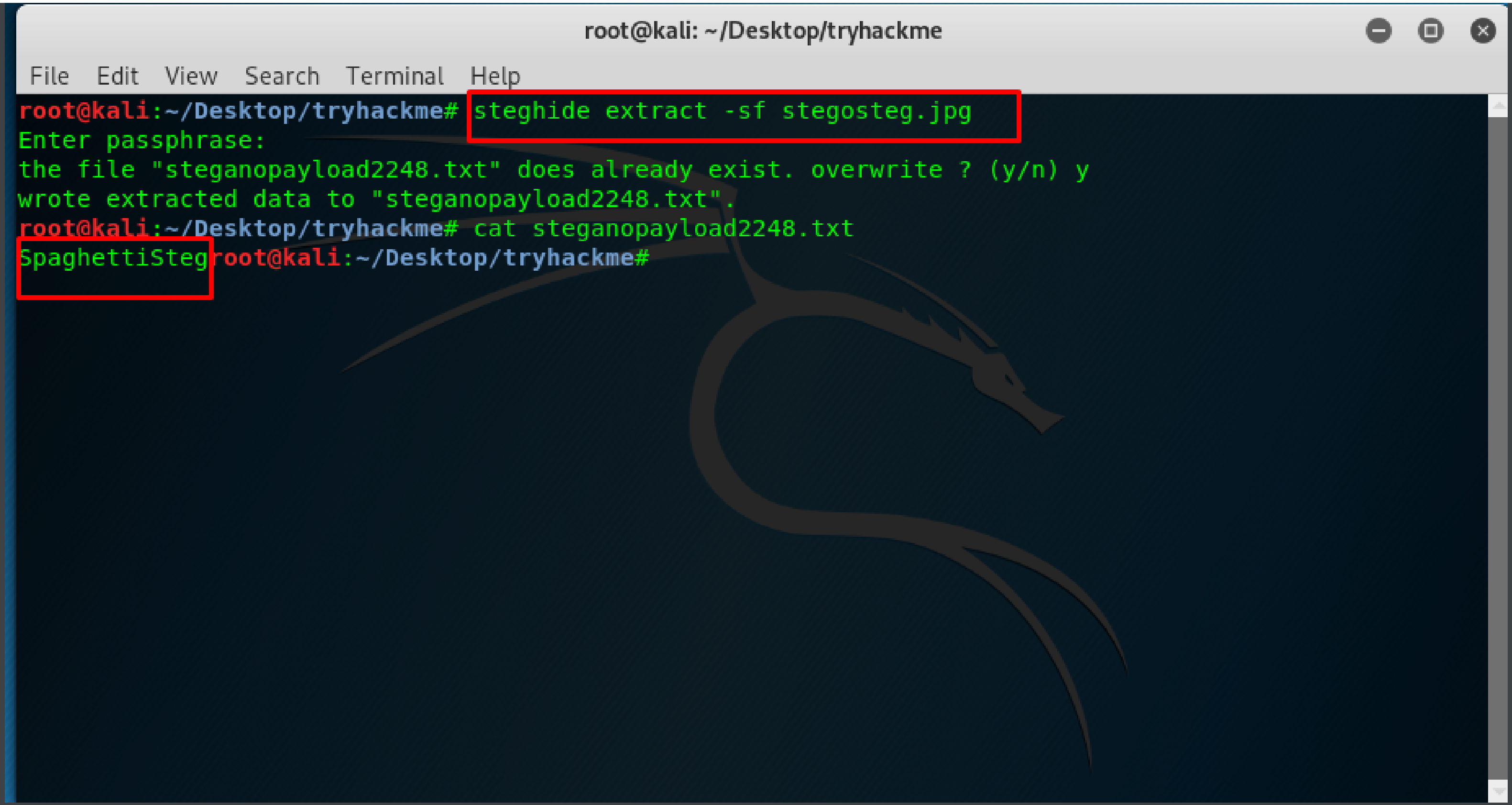
**Answer**: Super Secret Message

# TASK 4: STEGANOGRAPHY

This task can be solved either by an online tool or steghide. I prefer steghide. The hidden file within the image can be extracted using the following command

```
$ steghide extract -sf stegosteg.jpg
```

After that, a file named steganopayload2248.txt will be extracted from the image as shown in the figure below.



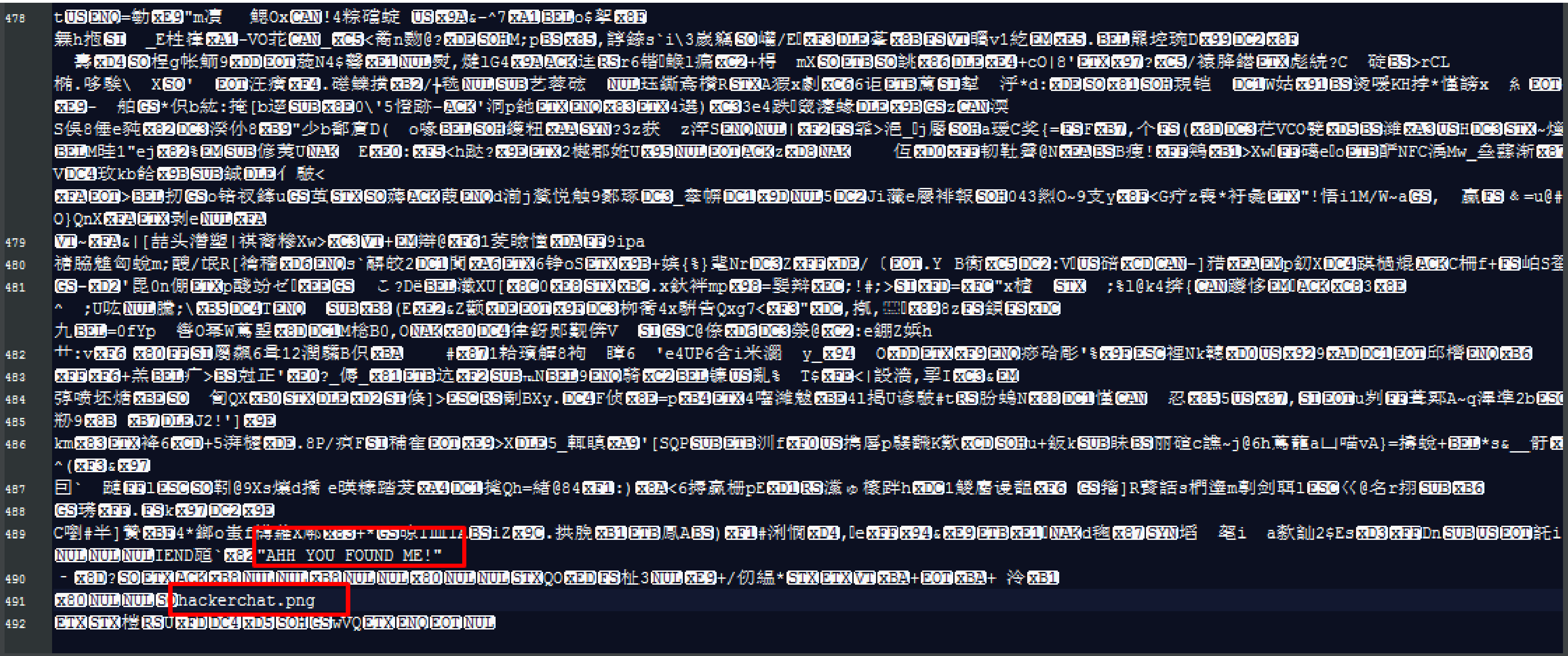
root@kali: ~/Desktop/tryhackme
File Edit View Search Terminal Help

```
root@kali:~/Desktop/tryhackme# steghide extract -sf stegosteg.jpg
Enter passphrase:
the file "steganopayload2248.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "steganopayload2248.txt".
root@kali:~/Desktop/tryhackme# cat steganopayload2248.txt
SpaghettiStegroot@kali:~/Desktop/tryhackme#
```

Steghide output

# TASK 5: WHAT IS INSIDE THE FILE?

This task cannot simply be solved by steghide. There is another dumb way to do it which is open the file as a txt. Both answers for the task is on the last few paragraphs.



1 stone kill 2 birds.

Answer (Task 5-1): hackerchat.png

Answer (Task 5-2): AHH_YOU_FOUND_ME!

# CONCLUSION

This challenge is much easier when compared to the last one. This Task 1 is enlightening me as it covers more on basic of ciphering. However, Task 2 is a little bit of disappointed as the description made some confusion for beginners. Other than that, well done to the creator of the room. That’s all for my second CTF challenge, until next time!

**SHARE THIS:**

Twitter Facebook

★ Like

Be the first to like this.

## RELATED

[Hacking walkthrough] CTF challenge
In "Hacking"

[Hacking walkthrough] Simple CTF
In "Hacking"

[Hacking walkthrough] Cracking the hashes
In "Hacking"

POSTED IN HACKING, TUTORIAL. TAGGED CIPHER, CTF, HASH, HASHCAT, STEGHIDE.

## LEAVE A REPLY

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.

PREVIOUS POST

NEXT POST

*Powered by WordPress.com.*