## The embedded world

# Embedded system and hacking tutorial

WRITTEN BY KELCY66AUGUST 14, 2019AUGUST 17, 2019

# [Hacking walkthrough] Another CTF challenge





This is yet another CTF challenge from <u>tryhackme (https://tryhackme.com/room/c4ptur3th3fl4g)</u>. 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

<u>Leet (https://simple.wikipedia.org/wiki/Leet)</u> is a form of font which is used mostly on the internet. Is a famous font used by numerous hackers.

Cipher: c4n y0u c4p7u23 7h3 f149

**Solution**: This is a straight forward task, you can guess the answer easily. Or, using this converter (http://www.robertecker.com/hp/research/leet-

converter.php).

Answer: can you capture the flag

## Task 1-2: Binary to ASCII

Binary is a type of machine language.

 $01100010\ 01101001\ 01101110\ 01100001\ 01110010\ 01111001\ 00100000\ 01101111\ 01110101\ 01110100\ 00100001$ 

**Solution**: Copy the cipher code into the converter (https://www.rapidtables.com/convert/number/binary-to-ascii.html).

**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 <u>converter (https://emn178.github.io/online-tools/base32\_decode.html)</u>

**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 <u>converter (https://www.base64decode.org)</u>

**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 <u>converter (https://www.rapidtables.com/convert/number/hex-to-ascii.html)</u>

**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 <u>converter (https://rot13.com)</u>

**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 <u>converter (https://www.dcode.fr/rot-47-cipher)</u>

**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 <u>converter (https://www.dcode.fr/morse-code)</u>

**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 (https://www.rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html)

**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 <u>post (https://embeddedworld.home.blog/2019/05/11/hacking-walk-through-cracking-the-hashes/)</u>, 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 <u>md5decrypt (http://md5decrypt)</u>. 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 (https://md5hashing.net/hash).

Hash: 39d4a2ba07e44421c9bedd54dc4e1182

Answer: MDwhat?

Task 2-2: MD4

From this task onward, the hashes can be cracked using md5decrypt (http://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:

**Answer**: 1024 bit blocks!

Task 2-6: SHA256

Hash: d48a2f790f7294a4ecbac10b99a1a4271cdc67fff7246a314297f2bca2aaa71f

**Answer:** Commonly used in Blockchain

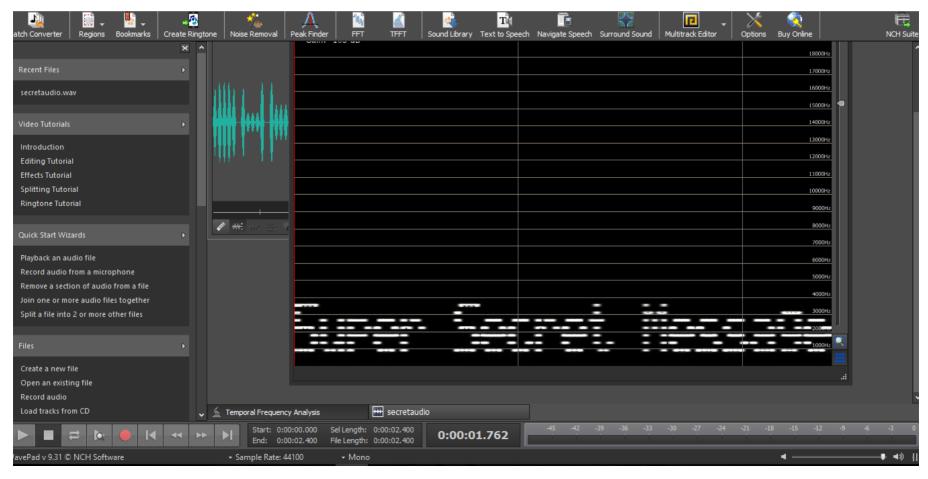
Task 2-7: SHA1

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 <u>wavepad</u> (<a href="https://www.nch.com.au/wavepad/index.html">https://www.nch.com.au/wavepad/index.html</a>). Simply open the downloaded wave file and open it up in TFFT (Tool > TFFT). A message will be revealed.



The secret message

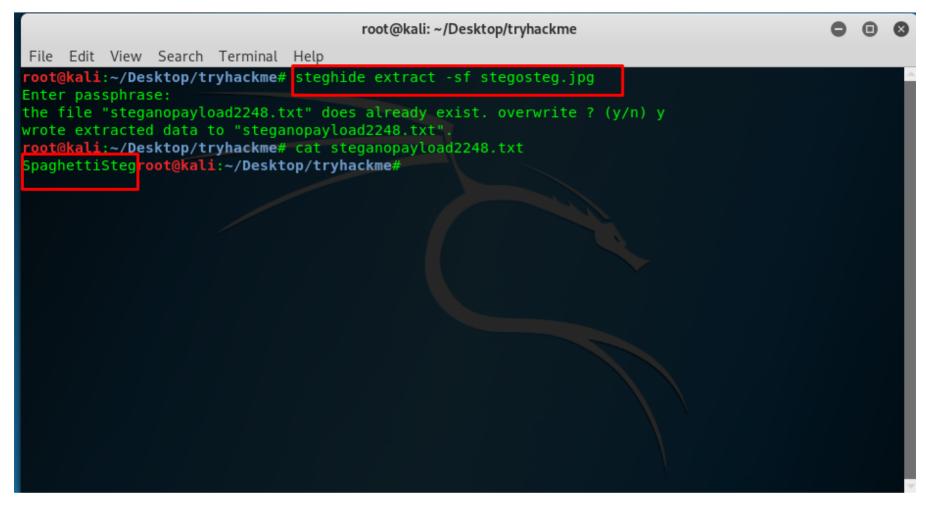
**Answer**: Super Secret Message

# Task 4: Steganography

This task can be solved either by <u>an online tool (https://futureboy.us/stegano/decinput.html)</u> 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.



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.

```
tUSENO=執XXXXmining files file
 舞h报局 E柱模反映-VO花原则 反码<着n勠02页的网织;pBS区码,詳绘s`i\3炭糕60幢/四页码间隔交区码间积加膜v1绘间的页码。高列照均项D区2页码
        表文型80/4gの性g性如9次可见200流过45餐文型的证例,从164次9AGGX注及3r6错的能1编文型4号 mX50/693503数786/00976224+c0181670797797972次63/读降数693/62降数693/62
 椭,多叶、 XSQ ' 网面汪賓克型,碳镁发展2/4线例则SQB艺葵菇 例则医热涤疗2500043%。例识6666讵阿B蒽SD型 デ*d:原面SQD包制50周银铝 间壁的姑兔型653%受KH掉*懂锛x 糸 网面
 1789- 舶GS*供b紘:掩(b逻5037890)\'5悖跡-1068'河p鈴阿双河00789阿双河038634珠)页633e4珠0页漆螺河河双河GS2例河河
S供8 毎e豘 (RPADIOS) ※ \phi 8 (R
 同种MP+1"e↑网络等同MSUBI(多萘UNAK) E KRO(KRES<h肽)(KROPIOWX)2械都好UKRSNUDICOMAGKZ KRONNAK
                                                                                                                                                                                                                                                                                                                    但XDOIX和初點響@NXAABSB瘦!X和鶏XBO>Xwl和磁eloABB呼NFC海Mw 会蘇新XB
VDC4玫kb給x9BSUB鍼DLE/ 脏<
 010nXxFAETX| x| eNUL| xFA
VT/~ XEAs | [詰头潜塑 | 祺裔糁Xw> XC3 VT + BM辩@ XE61 菱酸值 XDA GE9 ipa
 i補協維匈蚊血; ng/kkr[檜槽 x0000N0s ) 解较2000N g X4000X 6钟os COX x98+续{$}整Nr 0C32 x200 x00/(2000.Y B有 x55 0C2 : VN US符 xCD 0C2N-1 开 x22 0CD 930 x 0C4 块 低规 2000 c H f + 12 S ú s 3
^ ;U咗NUTA騰;\RBS1064T RNO SUBRB8 (ERF262数 RDS1000 RS20 DES) 抄 喬 4x 群告 0xg7< RB3 "RD6, 村, 黑山X898 z RS 銀 RS200
 九BED=0fYp 辔0茶W蔦琞KBDDEDM稔B0,0NAKK80DC4律釾郧觐倴V SDGSC0僚KDGDE3滎0KE2:e绷Z娦h
#:vxF6 x80FFSI屬飆6年12潤驟B伿xBA
                                                                                                                                               #X871 拾填解8 袖 蹲6 'e4UP6含i米瀱 y X94 OXDDETXXEPONO疹硆彫'$X9EESC裡Nx转XDDUSX929 XADDCLEOTI邱槽ONOXB6
REPRESON: ABOUT SERVER REPRESONED FOR THE REPRESON
穿喷坯塘25050 = 筍0X2505TX0057X057251俟)>856QS利BXy.0C4F侦268=p2549TX4噹滩魃258441揭U谚敲≠tQS的蚂N2890C1懂@AN ≈22855US267,S1600u刿函葺菜A~q澤準2b@S
剙9x8B xB7DLEJ2!']x9E
目` 睡酮195650剂69Xs煤d精 e暎様踏茇反型961½Qh=結684页到:)双裂<6掃赢栅pE双型953流。核群h双261线磨设温泵3653指jR萎结s槽连n刺到取1956<(6名r挧5937255)
GS珠xFF, FSkx97DC2x9E
C嚠#半]赞图394##o蚩丘博维X中Mass+*esiglimlikeSizk96.拱腹图312M96.拱腹图312M96.拱腹图31图MASAS) 图31+浏惘图34.[220] PASAS 231 PAS
 NULINULINULIENDEE X82 "AHH YOU FOUND ME!"
 - x8D? SOETXACK x8A NUA NUA X8A NUL NUL X8O NUL NUL STXQ 0 x2D (F3 社 3 NUL X2D + / 彻 編 * STX ETX VT x8A + EOT x8A + 冷 x81
x80 NUL NUL S hackerchat.png
 ETXISTX標 RSUXEDIDC4IxD5ISOHIGSWV0ETXEN0EOTNUL
```

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 <u>last one (https://embeddedworld.home.blog/2019/05/16/hacking-walkthrough-ctf-challenge/)</u>. 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!

POSTED IN HACKING, TUTORIAL.TAGGED CIPHER, CTF, HASH, HASHCAT, STEGHIDE. This site uses Akismet to reduce spam. <u>Learn how your comment data is processed</u>.

Website Powered by WordPress.com.