

NeverLAN CTF

Crypto : Crypto Hole

Value : 250 pts

Difficulty : Unknown

Description : Here's a lot of crypto challenges all packed into one. To start, unzip the starting zip file and enter **NeverLANCTF** as the password.

Each correct decryption, besides two, will be prefixed with **password :**

Your flag will be in the flag{flagGoesHere} syntax

You'll know when you're done

Attachment : A_ffine_Cipher_here_3.zip

Solution :

First as said the description, we need to download the attachment zip file and extract it with the password «NeverLANCTF».

```
root@kali:~/Téléchargements# unzip A_ffine_Cipher_here_3.zip
Archive:  A_ffine_Cipher_here_3.zip
  creating:  A ffine Cipher here 3/
[A_ffine_Cipher_here_3.zip] A ffine Cipher here 3/.DS_Store password:
  inflating: A ffine Cipher here 3/.DS_Store
  extracting: A ffine Cipher here 3/chal.txt
  extracting: A ffine Cipher here 3/Two is better than one.zip
```

Once extracted, we get a directory named «A ffine Cipher here 3» with the next encrypted zip, and our chal.txt file with the cipher.

Part 1 - A fine Cipher here 3 :

Chal.txt content :

whzzdvyk: HmcxWGD0iKTI&OAmgv

After seeing the directory name, I looked for a basic cipher and discovered it was Caesar-cipher with the shift 7 a → h.

Decoder : <https://cryptii.com/pipes/caesar-cipher>

Cipher decoded :

password: AfvqPZW0bDMB&HTfzo

Now we can unzip our next zip file «Two is better than one.zip» with the password **AfvqPZW0bDMB&HTfzo**

Part 2 - Two is better than one :

Chal.txt content :

PASTNRQXX78DRDVI6KBD3SDFXXXXXXSWO

Once again the directory name gives a hint about the cipher type. So I looked for «Double Transposition Cipher» with these parameters

Decoder : <https://www.dcode.fr/double-transposition-cipher>

DOUBLE TRANSPOSITION DECODER

★ DOUBLE TRANSPOSITION CIPHERTEXT

PASTNRQXX78DRDVI6KBD3SDFXXXXXXSWO

★ PERMUTATION KEY 1

NEVERLANCTF

→ (7,9,2,4,11,6,1,8,5,10,3) ⇔ (7,3,11,4,9,6,1,8,2,10,5)⁻¹

★ APPLY ON Lines

★ PERMUTATION KEY 2

NEVERLANCTF

→ (7,9,2,4,11,6,1,8,5,10,3) ⇔ (7,3,11,4,9,6,1,8,2,10,5)⁻¹

★ APPLY ON Lines

DECRYPT

Cipher decoded :

PASSWORDV78DTNRI6KBD3SDFQXXXXXXXXXX

Now we can unzip our next zip file «I'm on the fence with this one.zip» with the password **V78DTNRI6KBD3SDFQ**

Part 3 - I'm on the fence with this one :

Chal.txt content :

pw:Ea8oasod SA5egBlvsrVSvwr

Again and again, looking of the directory name, so i thinking of rail fence cipher.

Decoder : <https://www.dcode.fr/rail-fence-cipher>

RAIL FENCE DECODER

★ ZIGZAG CIPHERTEXT

pw:Ea8oasod SA5egBlvsrVSvwr

★ START ZIGZAG FROM BOTTOM (UPWARDS) ☐

KNOWING THE NUMBER OF LINES (LEVELS) 10

● TEST ALL LEVELS AND ZIGZAGS (BRUTE-FORCE ATTACK)

★ KEEP PUNCTUATION AND SPACES ☒

DECRYPT RAIL FENCE

Cipher decoded :

password: VSEAS5aevg8Bwlovr

Now we can unzip our next zip file «Salad Time.zip» with the password **VSEAS5aevg8Bwlovr**

Part 4 - Salad Time :

Chal.txt content :

knppwjor: cQGuVCd\$TyOUPppXUnPX

Again, look at the directory name, i thinking about Caesar Salad, so tried some caesar cipher and found the right one.

Decoder : <http://rumkin.com/tools/cipher/caesar-keyed.php>

Decrypt ▾

Shift: 0 ▾

The key: - [Show Keymaker](#)

Alphabet Used: NEVRLACTFBDGHIJKMOPQSUNXYZ

This is your encoded or decoded text:

Cipher decoded :

password: gTLvCGk\$HyRVsSsXVaSX

Now we can unzip our next zip file «ROTten.zip» with the password **gTLvCGk\$HyRVsSsXVaSX**

Part 5 - ROTten

Chal.txt content :

cnffjbeq: r1Lqe*mkkBBloS6EE%u5s

For this one i used a multi rot decoder, as the name of the directory is ROTten.

Decoder : <https://multidec.web-lab.at/rot.php>

And the result is ROT 13 or ROT18, after tried both the correct password was the ROT13.

```
ROT13
password: e1Ydr*zx0OybF6RR%h5f

ROT5
cnffjbeq: r6Lqe*mkBBloS1EE%u0s

ROT18
password: e6Ydr*zx0OybF1RR%h0f
```

Cipher decoded :

password: e1Ydr*zx0OybF6RR%h5f

Now we can unzip our next zip file «Viginere Equivalent E.zip» with the password **e1Ydr*zx0OybF6RR%h5f**

Part 6 – Viginere Equivalent E

Chal.txt content :

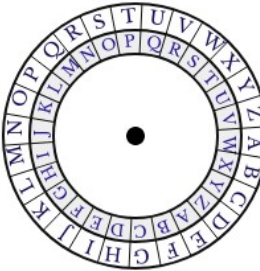
tewwasvh: jM7FTDP#DR5TM!&tfXBg

After some research i found it was Caesar cipher with the key 22

Source : <https://www.xarg.org/tools/caesar-cipher/>

tewwasvh: jM7FTDP#DR5TM!&tfXBg

Use key: 22



Encrypt / Decrypt

Output:

password: fi7BPZL#ZN5PI!&pbTXc

Cipher decoded :

password: fi7BPZL#ZN5PI!&pbTXc

Now we can unzip our next zip file «Easy One.zip» with the password **fI7BPZL#ZN5PI!&pbTXc**

Part 7 – Easy One

Chal.txt content :

cGFzc3dvcmQ6IHZ4d0BadGV0I1pmQm5ZVnhKMUIN

It look like a base64 decode it.

```
root@kali:~# echo 'cGFzc3dvcmQ6IHZ4d0BadGV0I1pmQm5ZVnhKMUIN' | base64 -d
password: vxw@Ztet#ZfBnYVxJ1IMroot@kali:~#
```

Cipher decoded :

password: **vxw@Ztet#ZfBnYVxJ1IM**

Now we can unzip our next zip file «Message indigestion.zip» with this password **vxw@Ztet#ZfBnYVxJ1IM**

Part 8 – Message Indigestion

Chal.txt content :

1f82cdf9195b31244721c6026587fb78

It look like md5, let's decode it.

Decoder : <https://crackstation.net/>

Hash	Type	Result
1f82cdf9195b31244721c6026587fb78	md5	password23

Cipher decoded :

password23

Now we can unzip our next zip file «for SHA dude.zip» with the password **password23**

Part 9 – for SHA dude

Chal.txt content :

57fc022fb8dbf1640e732c40e835f74e637526d8

As said the directory name, its encoded with a SHA encoder. Let's crack it under crackstation.

Decoder : <https://crackstation.net/>

Hash	Type	Result
57fc022fb8dbf1640e732c40e835f74e637526d8	sha1	applez14

It was «SHA1».

Cipher decoded :

applez14

Now we can unzip our next zip file «ONE more TIME.zip» with the password **applez14**

Part 10 – ONE more TIME

Chal.txt content :

This is our world now...

**Vvvyzshm fj tzylfvegn ehz ksh qwrwxsnlcecsagrv ubmdp qgvv momt sny lsdjk
osmy grhc xoxk zgprjr... Ks pzij, lecv'w yrsv ctsz nbx w rhi kyea dmvr
lqox{yyyiv0gLakvr}**

With the directory name «ONE more TIME» i fastly thinking of ONE TIME PAD (OTP). I used the decoder bellow and used as key «This is our world now...»

Decoder : <https://www.geocachingtoolbox.com/index.php?lang=en&page=oneTimePad>

Method: Decrypt ▾

Key:
This is our world now..|

Text:
Vvvyzshm fj tzylfvegn ehz ksh qwrwxs nlcecsagrv ubmdp qgvv momt sny lsdjk osmy grhc xoxk zgprjr... Ks pzij, lecv'w yrsv ctsz nbx
w rhi kyea dmvr lqox{yyyiv0gLakvr}

Reset fields

Result:
Congrats on finishign ehz ksh qwrwxs nlcecsagrv ubmdp qgvv momt sny lsdjk osmy grhc xoxk zgprjr... Ks pzij, lecv'w yrsv ctsz nbx
w rhi kyea dmvr lqox{yyyiv0gLakvr}

Please note: The key is shorter than the text, not everything might be substituted.

As we can see, we didn't have the full key, just a part. And we only decoded «Congrats on finishign» and note that the «finishing» word is wrongly decoded. So i started some research on google about the wording «This is our wolrd now...». But i dont find anything, so i started to guess some words. And i decoded with success «Congrats on finishing all the crypt....» by guessing the key «This is our world now... The world of the»

Method: Decrypt ▾

Key:
This is our world now... The world of the

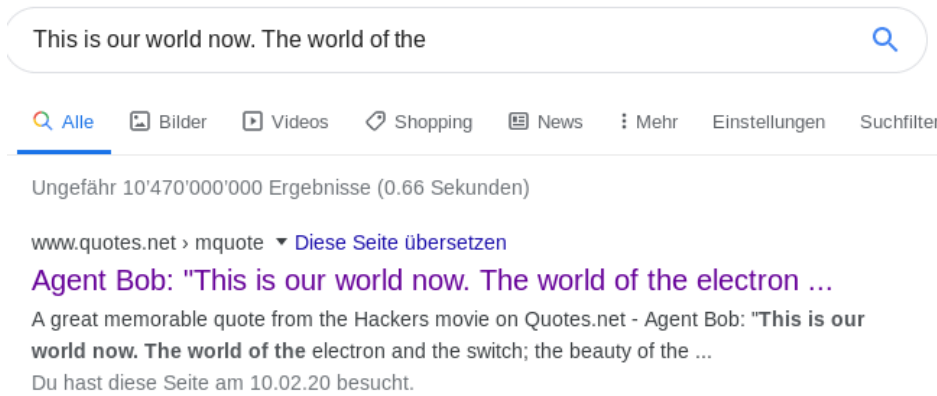
Text:
Vvvyzshm fj tzylfvegn ehz ksh qwrwxs nlcecsagrv ubmdp qgvv momt sny lsdjk osmy grhc xoxk zgprjr... Ks pzij, lecv'w yrsv ctsz nbx
w rhi kyea dmvr lqox{yyyiv0gLakvr}

Reset fields

Result:
Congrats on finishing all the crypts nlcecsagrv ubmdp qgvv momt sny lsdjk osmy grhc xoxk zgprjr... Ks pzij, lecv'w yrsv ctsz nbx
w rhi kyea dmvr lqox{yyyiv0gLakvr}

Please note: The key is shorter than the text, not everything might be substituted.

Doing a google research now with «This is our world now... The world of the» and i get those result.



Source : <https://www.quotes.net/mquote/39955>

On this blog, i found a text starting by the same phrase.

Agent Bob:

"This is our world now. The world of the electron and the switch; the beauty of the baud. We exist without nationality, skin color, or religious bias. You wage wars, murder, cheat, lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. I am a hacker, and this is my manifesto." Huh? Right? Manifesto? "You may stop me, but you can't stop us all."

Rate this quote: ☆☆☆☆☆ (0.00 / 0 votes)

1,390 Views

Trying to use this text as key for decode our cipher didnt worked really well.

Method: Decrypt ▾

Key:
This is our world now. The world of the electron and the switch; the beauty of the baud. We exist without nationality, skin color, or religious bias. You wage wars, murder, cheat, lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. I am a hacker, and this is my manifesto." Huh? Right? Manifesto? "You may stop me, but you can't stop us all."

Text:
Vvyzshmfjtzylfvegn ehz ksh qwrwxsnlcecsagr ubmdp qgvv momt sny lsdik osmy grhc xoxk zgprj... Ks pzij, lecv'w yrsv ctsz nbx w rhi kyea dmvr lqox{yyyiv0gLakvr}

Reset fields

Result:
Congrats on finishing all the crypto challenges built into this one super holy moly trps gkhycd... Qz czpb, xrck'o ftal ugql cng i aqe zqys psdq dqwz{kecip0cPatdf}

As we can see it decoded a little more, than before, but then it's corrupted. Seem we dont get the right text. So i removed the part of the key who dont work for get only the working part.

Method: Decrypt ▾

Key:
This is our world now. The world of the electron and the switch; the beauty of the baud. |

Text:
Vvyvzshm fj tzylfvegn ehz ksh qwrwxsnlcecsagr ubmdp aggv momt sny lsdjk osmy grhc xoxk zgprjr... Ks pzij, lecv'w yrsv ctsz nbx w rhi kyea dmvrlqox{yyyiv0gLakvr}

Reset fields

Result:
Congrats on finishing all the crypto challenges built into this one super holy mohc xoxk zgprjr... Ks pzij, lecv'w yrsv ctsz nbx w rhi kyea dmvrlqox{yyyiv0gLakvr}

Please note: The key is shorter than the text, not everything might be substituted.

So i was able to decrypt «Congrats on finishing all the crypto challenges built into this one super holy...» with the key «This is our world now. The world of the electron and the switch ; the beauty of the baud.» Searching this key part on google once again and i found a different result.

This is our world now. The world of the electron and the switch; the beauty of the | 🔍

🔍 Alle 📺 Videos 🖼 Bilder 📰 News 🛒 Shopping ⋮ Mehr ⚙ Einstellungen 🔍 Suchfilter

Ungefähr 171'000 Ergebnisse (0.46 Sekunden)

Tipp: [Begrenze die Suche auf deutschsprachige Ergebnisse](#). Du kannst deine Suchsprache in den [Einstellungen](#) ändern.

phrack.org > issues ▾ [Diese Seite übersetzen](#)

Hacker's Manifesto - Phrack Magazine

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could ...

Du hast diese Seite am 10.02.20 besucht.

Hacker's Manifesto blog, on phrack.org, it seem we hit our goal.

Source : <http://phrack.org/issues/7/3.html>

And we found a text starting by the same part of our key.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Trying to use this text as key worked !

Method: Decrypt ▾

Key:
for what could be dirt-cheap if it wasn't run by profiteering gluttons, and
you call us criminals. We explore... and you call us criminals. We seek
after knowledge... and you call us criminals. We exist without skin color,
without nationality, without religious bias... and you call us criminals.
You build atomic bombs, you wage wars, you murder, cheat, and lie to us
and try to make us believe it's for our own good, yet we're the criminals.

Text:
Vvvyzshm fj tzylfvegn ehz ksh qwrwxsnlcecsagr ubmdp qgvv momt sny lsdjk osmy grhc xoxk zgprjr... Ks pzij, lecv'w yrsv ctsz nbx
w rhi kyea dmvrlqox{yyiv0gLakvr}

Reset fields

Result:
Congrats on finishing all the crypto challenges built into this one super holy moly long folder... So yeah, here's your flag for a job
well done flag{crypt0sRphun}

We decrypted with success the bellow text :

Congrats on finishing all the crypto challenges built into this one super holy moly long folder... So yeah, here's your flag for a job well done **flag{crypt0sRphun}**

Flag : flag{crypt0sRphun}