

Ctf collection vol 1

Ctf collection vol 1

Estos retos son un compilado de muchos retos relacionados con reversing , sternografia y codificación don de lo que se debe conseguir es la flag

la tarea 1 es ingresar a la sala.

la segunda dice si puedes decodificar el mensaje:

VEhNe2p1NTdfZDNjMGQzXzdoM19iNDUzfQ==

claramente esto es un cifrado en Base64

The screenshot shows the CyberChef interface. In the 'Input' field, the string 'VEhNe2p1NTdfZDNjMGQzXzdoM19iNDUzfQ==' is pasted. The 'Recipe' dropdown is set to 'From Base64' with the 'Alphabet' set to 'A-Za-z0-9%2B%3D'. The 'Remove non-alphabet chars' checkbox is checked. The 'Output' section shows the decoded result: 'THM{ju57_d3c0d3_7h3_b453}'.

otra forma de decodificarlo es usando la terminal.

```
comando= echo -n "VEhNe2p1NTdfZDNjMGQzXzdoM19iNDUzfQ==" | base64 -d  
echo -n "textocodificadoenbase64" | base64 -d
```

```
$ echo -n "VEhNe2p1NTdfZDNjMGQzXzdoM19iNDUzfQ==" | base64 -d  
THM{ju57_d3c0d3_7h3_b453}
```

Flag:

THM{ju57_d3c0d3_7h3_b453}

Tarea 3 : Meta! meta! meta! meta.....
y adjunta una imagen



se llama findme , la pista que da es meta . meta , deben ser metadatos, haré un prueba con exiftool

```
(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
$ exiftool Findme.jpg
ExifTool Version Number      : 12.70
File Name                   : Findme.jpg
Directory                  : .
File Size                   : 35 kB
File Modification Date/Time : 2024:02:12 19:27:29-03:00
File Access Date/Time       : 2024:02:12 19:28:20-03:00
File Inode Change Date/Time: 2024:02:12 19:28:20-03:00
File Permissions            : -rw-r--r--
File Type                  : JPEG
File Type Extension         : jpg
MIME Type                  : image/jpeg
JFIF Version               : 1.01
X Resolution                «Findme.jpg: 96x42 Kib (34.985 bytes) | imagen JPEG
Y Resolution                : 96
Exif Byte Order             : Big-endian, (Motorola, MM)
Resolution Unit              : inches
Y Cb Cr Positioning        : Centered
Exif Version                : 0231
Components Configuration    : Y, Cb, Cr, ....Magick
Flashpix Version            : 0100
Owner Name                  : THM{3x1f_Or_3x17}
Comment                     : CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 60.
Image Width                 : 800
Image Height                : 480
Encoding Process             : Progressive DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                  : 800x480
Megapixels                  : 0.384
```

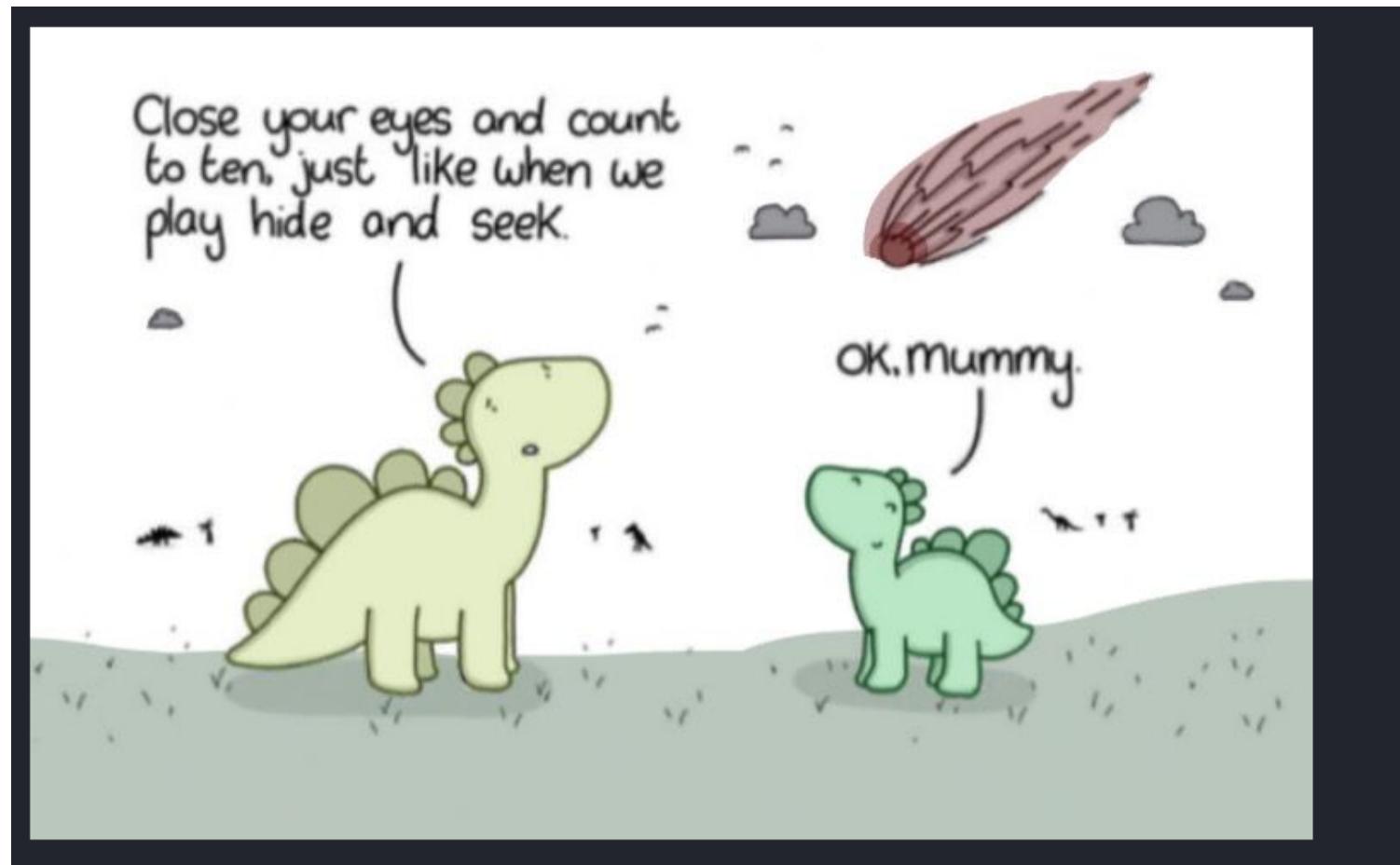
justamente era eso , flag : THM{3x1f_Or_3x17}

Tarea 4 ,

Something is hiding. That's all you need to know.

It is sad. Feed me the flag.

revisando hay una imagen para bajar :



```
[viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
$ exiftool Extinction.jpg
ExifTool Version Number      : 12.70
File Name                   : Extinction.jpg
Directory                   : .
File Size                   : 28 KB
File Modification Date/Time : 2024:02:12 19:31:42-03:00
File Access Date/Time       : 2024:02:12 19:33:14-03:00
File Inode Change Date/Time: 2024:02:12 19:32:07-03:00
File Permissions            : -rw-r--r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit              : None
X Resolution                 : 1
Y Resolution                 : 1
Image Width                  : 750
Image Height                 : 475
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                   : 750×475
Megapixels                   : 0.356
```

probaremos con steghide ,

```
[viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
$ steghide info Extinction.jpg
"Extinction.jpg":
  formato: jpeg
  capacidad: 1,3 KB
*Intenta informarse sobre los datos adjuntos? (s/n) s
Anotar salvoconducto:
  archivo adjunto "Final_message.txt":
    tamaño: 79,0 Byte
    encriptado: rijndael-128, cbc
    compactado: si
```

tenemos un archivo para extraer... usaremos el siguiente comando.

```
(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
$ steghide extract -sf Extinction.jpg
Anotar salvoconducto:
anot• los datos extra•dos e/"Final_message.txt".

(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
$ ls
Extinction.jpg  Final_message.txt  Findme.jpg

(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
$ cat Final_message.txt
It going to be over soon. Sleep my child.

THM{500n3r_0r_l473r_17_15_0ur_7urn}

(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
$
```

flag:THM{500n3r_0r_l473r_17_15_0ur_7urn}
tarea5

Task 5 ○ Erm.....Magick

Huh, where is the flag?

Answer the questions below

Did you find the flag?

[Join this room](#) [Join this room](#) [Hint](#)

WTF no hay donde buscar , no hay datos a descargar ¿habrá que inspeccionar la página?

Task 5 ○ Erm.....Magick

Huh, where is the flag?

Did you find the flag?

Answer format: ***{*****}

 Submit

 Hint

Console Debugger Style Editor Performance Memory Network Storage >

THM{wh173_fl46}

Flag: THM{wh173_fl46}

Tarea 6

Such technology is quite reliable.

hay un qr para revisar , lo abri con cyberchef y lo tradujo en un instante.

The screenshot shows the CyberChef interface with the following details:

- Operations:** Parse QR Code
- Recipe:** Parse QR Code
- Input:** A large base64 string representing a PNG image of a QR code. The string starts with "iVBORw0KGgoAAAANSUhEUgAAADICAYAACtWK6eAAAHmUIEQV".
- Output:** THM{qr_m4k3_l1f3_345y}
- File details:** Name: QR.png, Size: 2,002 bytes, Type: Image/png
- Buttons:** STEP, BAKE!, Auto Bake

Flag: THM{qr_m4k3_l1f3_345y}

Tarea7 :

Both works, it's all up to you.

bajamos un archivo llamado hello.hello

la vamos a desamblar con R2

```
(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]$ r2 hello.hello
Warning: run r2 with -e bin.cache=true to fix relocations in disassembly
[0x000001060]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar) Findme.jpg
[x] Finding and parsing C++ vtables (avrr)
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information (aanr)
[x] Use p=AA or aaaa to perform additional experimental analysis.
```

usamos el comando afl

```
[0x00001060]> afl
0x00001060 1 43 entry0
0x00001090 4 41 → 34 sym.deregister_tm_clones
0x000010c0 4 57 → 51 sym.register_tm_clones
0x00001100 5 57 → 50 sym._do_global_dtors_aux
0x00001050 1 6 sym.imp._cxa_finalize
0x00001140 1 5 entry.init0
0x00001000 3 23 sym._init
0x000011e0 1 1 sym._libc_csu_fini
0x00001145 1 24 sym.skip
0x00001040 1 6 sym.imp.printf
0x000011e4 1 9 sym._fini
0x00001180 4 93 sym._libc_csu_init
0x0000115d 1 23 main
0x00001030 1 6 sym.imp.puts
[0x00001060]>
```

4 archivos: 78,0 KiB (79.857 bytes) | Espacio libre: 52,3 GiB

pdf @sym.skip

```
[0x00001060]> pdf @sym.skip
24; sym.skip ();
Ayuda:ctb 0x00001145 55 push rbp
          0x00001146 4889e5 mov rbp, rsp
          0x00001149 488d3db80e00 lea rdi, str.THM345y_f1nd_345y_60 ; 0x2008 ; "THM{345y_f1nd_345y_60}" ; const char *format
          0x00001150 b800000000 mov eax, 0
          0x00001155 e8e6feffff call sym.imp.printf ; int printf(const char *format)
          0x0000115a 90 nop
          0x0000115b 5d pop rbp
          0x0000115c c3 ret
[0x00001060]>
```

Flag : THM{345y_f1nd_345y_60}

Tarea 8:

Can you decode it?

3agrSy1CewF9v8ukcSkPSYm3oKUoByUpKG4L

es base58

CyberChef interface showing the conversion of the string '3agrSy1CewF9v8ukcSkPSYm3oKUoByUpKG4L' from Base58 to ASCII.

Operations:

- base58
- To Base58
- From Base58
- Favourites
- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic
- From Base58
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking

Recipe: From Base58

Input: 3agrSy1CewF9v8ukcSkPSYm3oKUoByUpKG4L

Output: THM{17_h45_13553r_13773r5}

flag : THM{17_h45_l3553r_l3773r5}

Tarea 9:

Left, right, left, right... Rot 13 is too mainstream. Solve this

MAF{atbe_max_vtxltk}

en un principio es rot 13 pero hay que bajarle las posiciones a 7

The screenshot shows the CyberChef interface. On the left, the 'Operations' sidebar lists various encoding and decoding functions. In the center, the 'Recipe' section is set to 'ROT13'. Under 'ROT13', the 'Amount' field is set to 7. The 'Input' field contains the string 'MAF{atbe_max_vtxltk}'. The 'Output' field shows the result: 'THM{hail_the_caesar}'. At the bottom, there is a green button labeled 'BAKE!' with a chef icon.

Flag: THM{hail_the_caesar}

Tarea 10

No downloadable file, no ciphered or encoded text. Huh

nos da indicios de que hay algo en el código manos a la obra...

kali-linux-2023.4-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

File Edit View History Bookmarks Tools Help

TryHackMe | CTF collection Parse QR Code - CyberChef que es R2 - Buscar con Go

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Task 7 Reverse it or read it?

Task 8 Another decoding stuff

Task 9 Left or right

Task 10 Make a comment

No downloadable file, no ciphered or encoded text. Huh

Answer the questions below

I'm hungry now... I need the flag

Join this room Hint

Inspector Console Debugger Network Style Editor Memory Storage Accessibility Application

Search HTML

div#task-10 class="card" data-bbox="154 304 561 368">div#collapse10 class="collapse show" data-parent="#taskContent" style="display: flex; align-items: center;">div#collapse10 .card-header task-header data-toggle="collapse" href="#collapse10" aria-expanded="true">div#collapse10 .card-body task-incomplete p

element :: { display: none; } p { margin-top: 0; margin-bottom: 1em; } *, ::after, ::before { box-sizing: border-box; }

Layout Computed Changes Compatibility

Flexbox Select a Flex container or item to continue.

Grid Overlay Grid

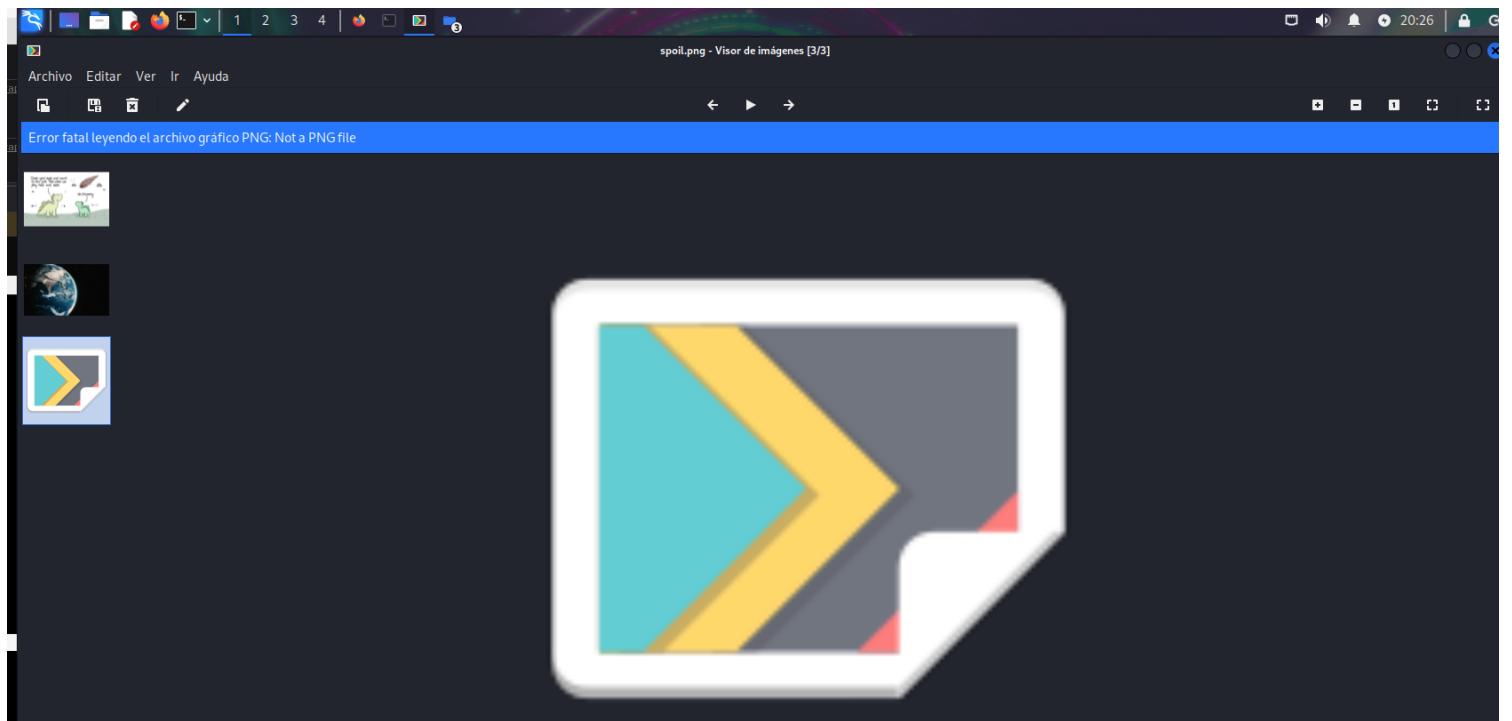
div.room-header div.room-task-input

Errors Warnings Logs Info Debug CSS XHR Requests

Flag: THM{4lw4y5_ch3ck_7h3_c0m3mn7}

Tarea 11

accidentally messed up with this PNG file. Can you help me fix it? Thanks, ^^



Dumpeamos en hexa el archivo spoil.png

```
(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]$ xxd -p spoil.png > spoil_hex_data
```

leemos la cabecera

```
$ head spoil_hex_data
2333445f0d0a1a0a0000000d4948445200000320000003200806000000db
700668000000017352474200aece1ce900000097048597300000ec40000
0ec401952b0e1b0000200049444154789cecdd799c9c559deff1cf799e5a
bb7a5f927477f640480209201150c420bba288a8805c19067c5d64c079e9
752e03ce38e30e8e2f75e63a23ea8c0ce8308e036470c191cd80880c4b20
0909184c42b64ed2e9f4bed7f23ce7fe51559dea4e27a4bbaaf7effbf5ea
57d2d5554f9daa7abafa7ceb9cf33bc65a6b111111111111907ce443740
4444444444660e051011111111119370a20222222222326e1440444444
444464dc2880888888888c8b85100111111119171a300222222222222
e346014444444444444c68d02888888888888c1b051011111111119370a
```

2333445f
89504E47

Segun lo revisado , esos numeros no corresponden a PNG

The screenshot shows a web browser window with the URL <https://asecuritysite.com/forensics/magic>. The page title is "Digital Investigation". The main content is a table titled "[Network Forensics Home][Home]" which lists file extensions and their corresponding magic numbers. The table includes columns for Description, Extension, and Magic Number. A sidebar on the right contains the text "Digital Forensics FFD8 47 49 46 39 PK @asecuritysite.com".

Description	Extension	Magic Number
Adobe Illustrator	.ai	25 50 44 46 [%PDF]
Bitmap graphic	.bmp	42 4D [BM]
Class File	.class	CA FE BA BE
JPEG graphic file	.jpg	FFD8
JPEG 2000 graphic file	.jp2	0000000C6A5020200D0A [...JP..]
GIF graphic file	.gif	47 49 46 38 [GIF89]
TIF graphic file	.tif	49 49 [II]
PNG graphic file	.png	89 50 4E 47 .PNG
WAV audio file	.wav	52 49 46 46 RIFF
ELF Linux EXE	.	7F 45 4C 46 .ELF
Photoshop Graphics	.psd	38 42 50 53 [8BPS]
Windows Meta File	.wmf	D7 CD C6 9A
MIDI file	.mid	4D 54 68 64 [MThd]
Icon file	.ico	00 00 01 00
MP3 file with ID3 identity tag	.mp3	49 44 33 [ID3]
AVI video file	.avi	52 49 46 46 [RIFF]

uhmmm sospechoso llevaremos el dump a cyberchef y cambiaremos los numeros mágicos a PNG

Operations

- render
- Render Image
- Render Markdown
- HTML To Text
- Hex Density chart
- To Table
- Favourites
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking
- Language
- Utils
- Date / Time
- Extractors
- Compression

Recipe

- From Hex
- Delimiter
- Auto
- Render Image
- Input format
- Raw

Last build: 3 days ago - Version 10 is here! Read about the new features [here](#)

File details



Name: spoil_hex_data
Size: 143,877 bytes
Type: unknown
Loaded: 100%

Output

Try Hack Me

STEP **BAKE!** Auto Bake

lo que obtuvimos es la flag :



THM{y35_w3_c4n}

Tarea 12

Some hidden flag inside Tryhackme social account.

la pista dice que es en reddit por lo cual ya podemos aplicar google dorking.

inurl:"reddit.com" &intext:"THM" & intitle:"tryhackme"

Google inurl:"reddit.com" &intext:"THM" & intitle:"tryhackme" X | 🔍

Imágenes Vídeos Shopping Maps Noticias Libros Vuelos Finance Todos los filtros ▾ Herramientas

Cerca de 2 resultados (0.17 segundos)

Reddit https://www.reddit.com › eizxaq · Traducir esta página

New room Coming soon! : r/tryhackme

2 ene 2020 — Share your method how you easily found this flag in reddit.

ingresamos.

encontramos este comentario,

Amok42 • 4mo ago

By using google dorking :
site:reddit.com/r/tryhackme intext:THM{*}

It's the first result.

Modificamos el dork , sacando el asterisco al medio de los corchetes y lo aplicamos.

site:reddit.com/r/tryhackme intext:THM{}

TryHackMe | CTF collective × From Hex, Render Image × Digital Forensics Magic N × site:reddit.com/r/tryhackme ×

Google Imágenes

Hi! I recently made account on... · Reddit

WTF is wrong with THM serve... · Reddit

Answered correctly but thm ... · Reddit

6 imágenes más

New room Coming soon! : r/tryhackme

2 ene 2020 — New room Coming soon! r/tryhackme - THM{50c14l_4cc0un7_15_p4r7_0f_051n7}

Is THM pro really worth it?? : r/tryhackme

21 nov 2021 — The difference is that THM currently offers the best beginner content and doesn't have an intense amount of Advanced content compared to HTB.

Flag: THM{50c14l_4cc0un7_15_p4r7_0f_051n7}

Tarea 13

What is this?

```
+++++[>+>++++>++++++>++++++><<<-]>>>++++++  
+-.-.++++.>+++++++.<<+++++++.<<+++++++.  
.>>>-----.>-----.>-----.<<+++++++.<<+++++++.  
++++++.<<+++++++.<+++,.>---->++++.
```

en otras entregas de write ups , les expliqué sobre el cifrado brainfuck , parece ser este , intentaremos descifrarlo con la página dcode.fr

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Brainfuck" and contains a Brainfuck interpreter and a memory dump. The URL in the address bar is <https://www.dcode.fr/langage-brainfuck>.

Brainfuck Interpreter:

- Input:** `>+++++[>+<]`
- Arg:** `THM{0h_my_h34d}` (highlighted with a red box)
- Output:** `THM{0h_my_h34d}`

Memory Dump:

[0] = (0)
[1] = (10)
[2] = 4 (52)
[3] = d (108)
[4] = } (125)
pointer = 4

Similar Pages:

- ReverseFuck
- Langage JSFuck \square (\square + \square)
- Langage LOLCODE
- Binaryfuck
- Alphuck
- Ook!
- Pikalang
- LISTE DES OUTILS DCODE

Flag: THM{0h my h34d}

tarea 14

Exclusive strings for everyone!

S1: 44585d6b2368737c65252166234f20626d

En esta tarea, obtuvimos 2 cadenas pero no sabíamos qué hacer con estas cadenas, el hint muestra XOR estas cadenas.

← → ⌛ ⌂ https://www.google.com/search?client=firefox-b-e&q=calcular+xor+de+dos+cadenas+online

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Google calcular xor de dos cadenas online

Imágenes Vídeos Shopping Libros Noticias Maps Vuelos Finance

Todos los filtros ▾ | Herramientas

Cerca de 74,700 resultados (0.28 segundos)

XOR Calculator https://xor.pw · Traducir esta página

XOR Calculator Online

Calculate the exclusive or (**XOR**) with a simple web-based calculator. Input and output in binary, decimal, hexadecimal or ASCII.

Falta(n): [cadenas](#) | Realizar una búsqueda con lo siguiente: [cadenas](#)

Khan Academy https://es.khanacademy.org › xor-bitwise-operation

Operación XOR bit a bit (artículo)

Para entender por qué, primero necesitamos introducir las operaciones bit a bit AND, OR y XOR. Específicamente por qué **XOR** debe usarse cuando se realiza el ...

Falta(n): [online](#) | Realizar una búsqueda con lo siguiente: [online](#)

MiniWebtool https://miniwebtool.com › bitwise-calculator

Calculadora bit a bit

La **Calculadora Bitwise** se utiliza para realizar operaciones Bitwise AND, Bitwise OR, Bitwise XOR (exclusivas de Bitwise o) en **dos** números enteros. También ...

Un día una canción https://www.undiaunacancion.es › como-calcular-el-x...

Cómo calcular el XOR: Guía paso a paso

Para calcular el **XOR** necesitas tener **dos** valores binarios de igual longitud ... Una vez que

ambos valores son base 16 y lo queremos es que sea un ascii de base 256 ponemos las dos cadenas y ya está.

Flag : THM{3xclu51v3_Or}

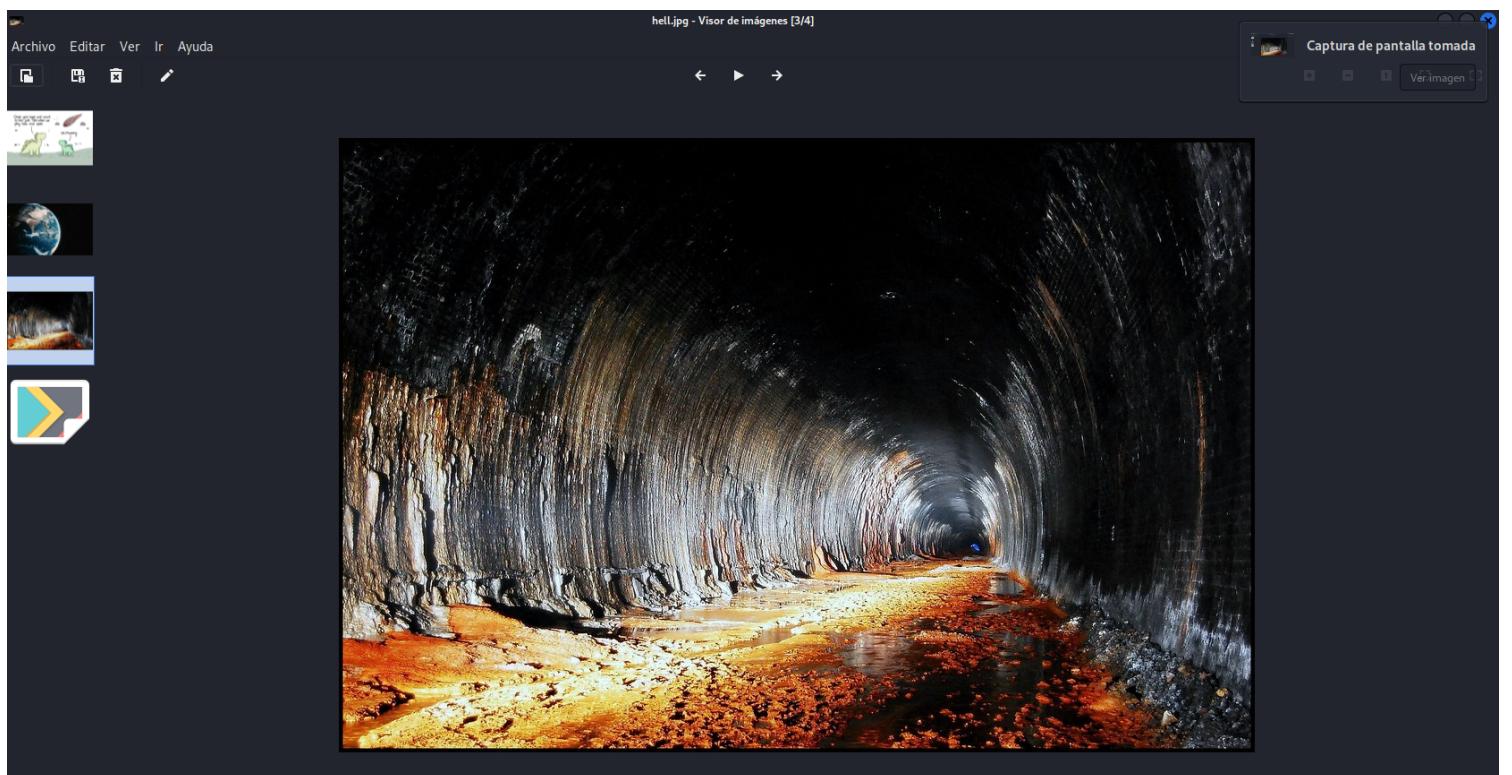
tarea 15

Please exfiltrate my file :)

Answer the questions below

Flag! Flag! Flag!

tiene una imagen adjunta :



el titulo es binary walk , creo que hay una herramienta llamada binwalk

```
(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
└─$ cd _hell.jpg.extracted

(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1/_hell.jpg.extracted]
└─$ ls
40E75.zip  hello_there.txt

(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1/_hell.jpg.extracted]
└─$ cat hello_there.txt
Thank you for extracting me, you are the best!

THM{y0u_w4lk_m3_0u7}
```

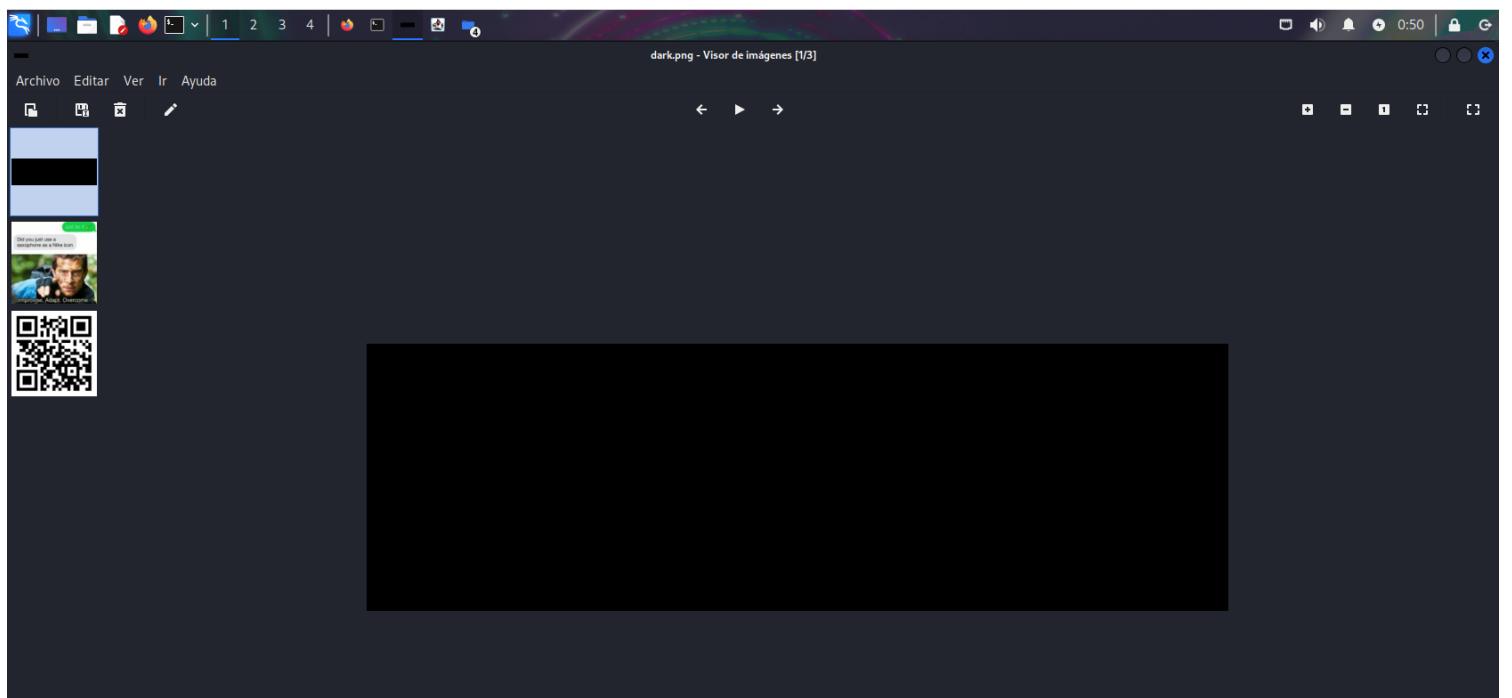
```
cat
hello_there.txt
```

Thank you for extracting me, you are the best!

THM{y0u_w4lk_m3_0u7}

Flag : THM{y0u_w4lk_m3_0u7}

tarea 16 : There is something lurking in the dark.



usaré para este reto stegsolve

Installation

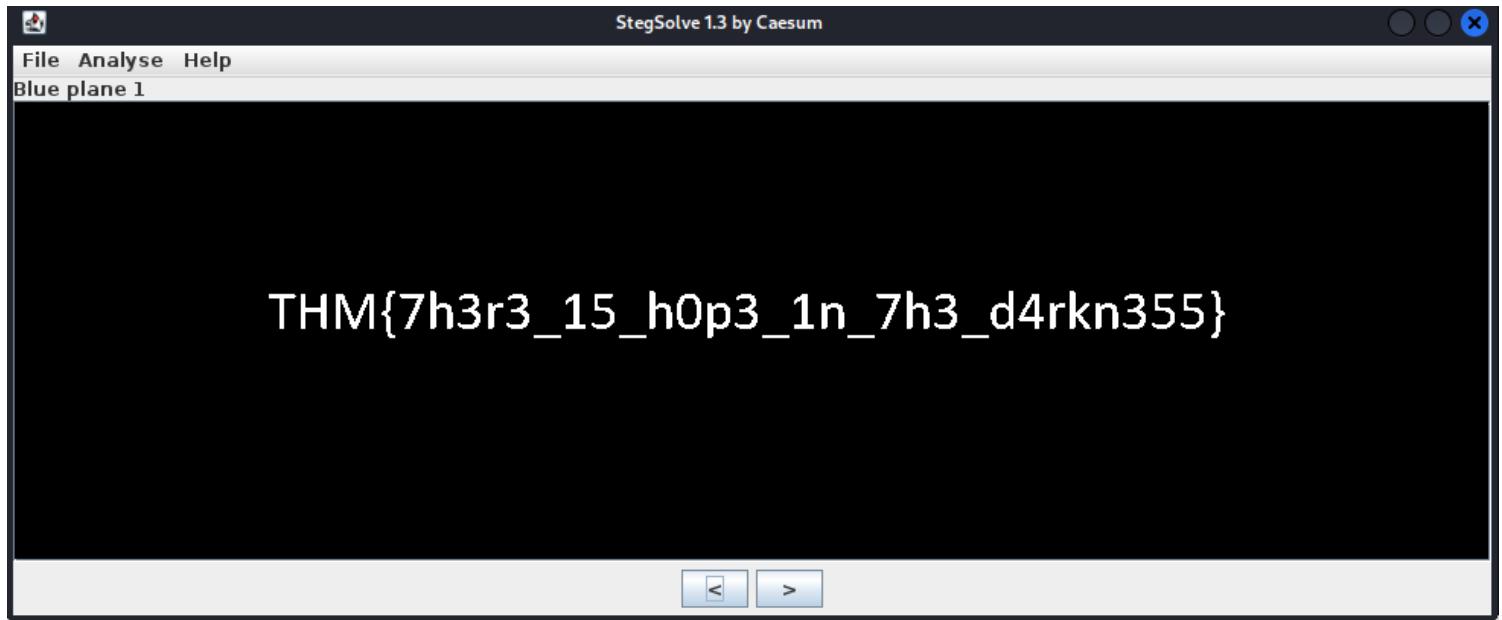
```
$ wget http://www.caesum.com/handbook/Stegsolve.jar -O stegsolve.jar  
$ chmod +x stegsolve.jar  
$ mkdir bin  
$ mv stegsolve.jar bin/
```

Usage

Stegsolve can be invoked by placing the image in the /bin folder and running stegsolve.

```
$ java -jar stegsolve.jar
```

una vez instalada abrir el archivo e ir aplicando filtros con las flechas , hasta llegar una que delate el mensaje oculto.



THM{7h3r3_15_h0p3_1n_7h3_d4rkn355}

Tarea 17 :

Operations

- QR
- Parse QR Code
- Generate QR Code
- To Quoted Printable
- From Quoted Printable
- Chi Square
- Frequency distribution
- Expand alphabet range
- From Base45
- LS47 Decrypt
- LS47 Encrypt
- To Base45

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Recipe

Parse QR Code

Normalise image

Input

File details

Name: QRCTF.png
Size: 1,933 bytes
Type: image/png

Output

<https://soundcloud.com/user-86667759/thm-ctf-vol1>

<https://soundcloud.com/user-86667759/thm-ctf-vol1>

THM{soundinqqr}

tarea18

Sometimes we need a 'machine' to dig the past

Targetted website: <https://www.embeddedhacker.com/>

Targetted time: 2 January 2020

ocuparemos waybackmachine.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

INTERNET ARCHIVE https://www.embeddedhacker.com/ Go JUN JAN MAY 02 2014 2020 2021 About this capture

66 captures 4 Aug 2016 - 9 Feb 2024

previously published on the embeddedworld and now the site is renamed to embeddedhacker. All the latest tutorial, news, and tech review...

0 COMMENTS AUGUST 22, 2019

UNCATEGORIZED

THM flag

What did you just say? flag? THM{ch3ck_th3_h4ckb4ck}

0 COMMENTS JANUARY 2, 2020

CTFLearn / HACKING / MEDIUM

[Hacking walkthrough]

CTFLearn: Crypto (Medium)

[Hacking walkthrough] CTFLearn: Crypto (Medium)

Greetings and good ay, welcome to another ctlearn walkthrough. Today, we are going to complete the medium level crypto challenge. Let's get started. 1) RSA Noob Link:

Privacy & Cookies Policy

Flag :: THM{ch3ck_th3_h4ckb4ck}

TArea19

Can you solve the following? By the way, I lost the key. Sorry >.<

MYKAHODTQ{RVG_YVGGK_FAL_WXF}

Flag format: TRYHACKME{FLAG IN ALL CAP}

parece ser cifrado vignere,

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Last build: 3 days ago - Version 10 is here! Read about the new features [here](#)

Download CyberChef

Operations

vigne

Vigenère Encode

Vigenère Decode

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

Code tidy

Forensics

Recipe

Vigenère Decode

Input

TRYHACKME

Output

THMTHMTHM{YEI_RVEWY_BHU_YQF}

STEP BAKE! Auto Bake

44ms Raw Bytes LF

THMTHMTHM{YEI_RVEWY_BHU_YQF}

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like 'Operations', 'Vigenère Encode', 'Vigenère Decode', etc. The main area has tabs for 'Recipe' (set to 'Vigenère Decode') and 'Input' (containing 'MYKAHODTQ{RVG_YVGGK_FAL_WXF}'). Below that is a 'Key' field containing 'THMTHMTHM'. The 'Output' section shows the result: 'TRYHACKME{YOU_FOUND_THE_KEY}'. There are also sections for 'Raw Bytes' and 'LF' at the bottom.

TRYHACKME{YOU_FOUND_THE_KEY}

lo convertimos primero a hexa .

The screenshot shows a 'Conversor de base' (Base Converter) tool. It has fields for 'Introduce tu número' (Enter your number) with the value '581695969015253365094191591547859387620042736036246486373595515576333693', 'escrito en base' (Written in base) set to '10 (decimal)', and 'para convertir este número a base' (Convert this number to base) set to '16 (hexadecimal)'. Below these are dropdowns for 'Precisión de cálculo (decimales)' (Calculation precision (decimals)) set to '30' and a 'Pulsa' (Press) button. A note at the bottom provides tips for using the calculator.

y luego de hexa a ascii

tarea 20

Decode the following text.

581695969015253365094191591547859387620042736036246486373595515576333693

Screenshot of a browser window showing the conversion of hex bytes to ASCII text using the [RapidTables Hex to ASCII Text String Converter](https://www.rapidtables.com/convert/number/hex-to-ascii.html).

The URL in the address bar is <https://www.rapidtables.com/convert/number/hex-to-ascii.html>.

The page title is "RapidTables".

The main heading is "Hex to ASCII Text String Converter".

Instructions: Enter hex bytes with any prefix / postfix / delimiter and press the *Convert* button (e.g. 45 78 61 6d 70 6C 65 21):

The "From" dropdown is set to "Hexadecimal" and the "To" dropdown is set to "Text".

The input field contains the hex bytes: 54484D7B31375F6A7535375F346E5F307264316E3472795F623435333
57D.

The "Character encoding" dropdown is set to "ASCII".

The "Convert" button is highlighted in green.

The output field shows the converted ASCII text: THM{17_ju57_4n_0rd1n4ry_b4535}.

flag=THM{17_ju57_4n_0rd1n4ry_b4535}

tarea 21 y final

I just hacked my neighbor's WiFi and try to capture some packet. He must be up to no good. Help me find it.

es un archivo PCAP lo abrimos con wireshark

Time	Source	Destination	Type	Length	Raw
1825 52.508233774	192.168.247.130	192.168.247.140	HTTP	596	GET /Tiao.txt HTTP/1.1
1822 52.507503635	192.168.247.130	192.168.247.140	TCP	74	36654 → 80 [SYN] Seq:0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=367886693 TSecr=0 WS=128
1824 52.507971168	192.168.247.130	192.168.247.140	TCP	66	36654 → 80 [ACK] Seq:1 Ack=1 Win=64256 Len=0 TStamp=367886694 TSecr=103044 TSecr=367886693
1822 52.5088615591	192.168.247.140	192.168.247.130	TCP	66	80 → 36654 [ACK] Seq:1 Ack=441 Win=30080 Len=0 TStamp=103045 TSecr=367886694
1822 52.510008803	192.168.247.130	192.168.247.140	TCP	66	36654 → 80 [ACK] Seq:441 Ack=390 Win=64128 Len=0 TStamp=367886694 TSecr=103045
1849 57.513011694	192.168.247.140	192.168.247.130	TCP	66	80 → 36654 [FIN, ACK] Seq:390 Ack=441 Win=30080 Len=0 TStamp=104296 TSecr=367886696
1850 57.513219578	192.168.247.130	192.168.247.140	TCP	66	36654 → 80 [FIN, ACK] Seq:441 Ack=391 Win=64128 Len=0 TStamp=367891699 TSecr=104296
1851 57.513611802	192.168.247.140	192.168.247.130	TCP	66	80 → 36654 [ACK] Seq:391 Ack=442 Win=30080 Len=0 TStamp=104296 TSecr=367891699

kali-linux-2023.4-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

flag.picapng

tcp.stream eq 42

No.	Time	Source	Destinat	Paquete	Nombre de equipo	Tipo de contenido	Tamaño	Nombre de archivo
1824	52.507971168	192.168.247.130	192.168.247.140	1164	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1828	52.510008803	192.168.247.130	192.168.247.140	1182	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1850	57.513219578	192.168.247.130	192.168.247.140	1186	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1822	52.507503635	192.168.247.130	192.168.247.140	1188	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1826	52.508615591	192.168.247.140	192.168.247.140	1190	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1851	57.513611802	192.168.247.140	192.168.247.140	1194	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1849	57.513611694	192.168.247.140	192.168.247.140	1526	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1823	52.507946451	192.168.247.140	192.168.247.140	1554	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1825	52.508233774	192.168.247.130	192.168.247.140	1557	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1827	52.509987109	192.168.247.140	192.168.247.140					

//tmp/flag.txt - Mousepad

Fichero Editar Buscar Ver Documento Ayuda

Aviso: está usando la cuenta de superusuario. Puede dañar su sistema.

```
1 THM{d0_n07_574lk_m3}
2
3 Found me!
4
```

Wireshark - Exportar - Listado de objetos HTTP

Tipo de contenido: Todos los tipos de contenido

Paquete	Nombre de equipo	Tipo de contenido	Tamaño	Nombre de archivo
1164	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1182	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1186	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1188	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1190	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1194	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1526	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1554	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1557	ocsp.digicert.com	application/ocsp-response	471 bytes	/

40 text/plain 32 bytes flag.txt

11 08 00 45 00 .) - . . .) 0 . . E
18 f7 8c c0 a8 . R:@ @ . v . . .
78 09 e6 80 18 . P . . . >X . . .
31 92 85 15 ed . 5
32 30 30 20 4f fHTTP/1.1 200 0
39 2c 20 30 33 K-Date: Fri, 03 Jan 202 0 04:43:
34 3a 34 33 3a 14 GMT- Server:
76 65 72 3a 20 32 32 20 4a Apache/2.2.22 (Ubuntu) . Last-Mod
74 2d 4d 6f 64 ified: Fri, 03 J
30 30 33 20 4a an 2020 04:42:12
0000 61 6e 20 32 30 32 30 20 30 34 3a 34 32 3a 31 32 GMT- ET ag: "e1b
0000 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 65 31 62 b7-20-59 b34eee33
0000 62 37 2d 32 30 2d 35 39 62 33 34 65 65 33 33 e0c"- Ac cept-Ran
0000 65 30 63 22 0d 0a 41 63 63 65 78 74 2d 52 61 6e ges: byt es_Vary
0000 67 65 73 3a 20 62 79 74 65 73 0d 0a 56 61 72 79 : Accept_Encodin
0100 3a 20 41 63 63 65 70 74 2d 45 66 63 6f 64 69 6e g_Content-Encod
0110 67 6d 0a 43 6f 6e 74 65 6e 74 2d 45 66 63 6f 64 ing: gzip p Conte
0120 69 6e 67 3a 20 67 7a 69 70 0d 0a 43 6f 6e 74 65 nt-Lengt h: 52 -K
0130 6e 74 2d 4c 65 6e 67 74 68 3a 20 35 32 0d 0a 4b

Paquetes: 2209 - Mostrado: 10 (0.5%)

Guardar Guardar todo Preview Cerrar Ayuda

Perfil: Default

vimos que era un txt obtenido por http , por lo cual lo exportamos y aparece la flag.

kali-linux-2023.4-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

flag.picapng

tcp.stream eq 42

No.	Time	Source	Destinat	Paquete	Nombre de equipo	Tipo de contenido	Tamaño	Nombre de archivo
1824	52.507971168	192.168.247.130	192.168.247.140	1164	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1828	52.510008803	192.168.247.130	192.168.247.140	1182	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1850	57.513219578	192.168.247.130	192.168.247.140	1186	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1822	52.507503635	192.168.247.130	192.168.247.140	1188	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1826	52.508615591	192.168.247.140	192.168.247.140	1190	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1851	57.513611802	192.168.247.140	192.168.247.140	1194	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1849	57.513611694	192.168.247.140	192.168.247.140	1526	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1823	52.507946451	192.168.247.140	192.168.247.140	1554	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1825	52.508233774	192.168.247.130	192.168.247.140	1557	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1827	52.509987109	192.168.247.140	192.168.247.140					

//tmp/flag.txt - Mousepad

Fichero Editar Buscar Ver Documento Ayuda

Aviso: está usando la cuenta de superusuario. Puede dañar su sistema.

```
1 THM{d0_n07_574lk_m3}
2
3 Found me!
4
```

Wireshark - Exportar - Listado de objetos HTTP

Tipo de contenido: Todos los tipos de contenido

Paquete	Nombre de equipo	Tipo de contenido	Tamaño	Nombre de archivo
1164	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1182	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1186	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1188	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1190	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1194	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1526	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1554	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1557	ocsp.digicert.com	application/ocsp-response	471 bytes	/

40 text/plain 32 bytes flag.txt

11 08 00 45 00 .) - . . .) 0 . . E
18 f7 8c c0 a8 . R:@ @ . v . . .
78 09 e6 80 18 . P . . . >X . . .
31 92 85 15 ed . 5
32 30 30 20 4f fHTTP/1.1 200 0
39 2c 20 30 33 K-Date: Fri, 03 Jan 202 0 04:43:
34 3a 34 33 3a 14 GMT- Server:
76 65 72 3a 20 32 32 20 4a Apache/2.2.22 (Ubuntu) . Last-Mod
74 2d 4d 6f 64 ified: Fri, 03 J
30 30 33 20 4a an 2020 04:42:12
0000 61 6e 20 32 30 32 30 20 30 34 3a 34 32 3a 31 32 GMT- ET ag: "e1b
0000 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 65 31 62 b7-20-59 b34eee33
0000 62 37 2d 32 30 2d 35 39 62 33 34 65 65 33 33 e0c"- Ac cept-Ran
0000 65 30 63 22 0d 0a 41 63 63 65 78 74 2d 52 61 6e ges: byt es_Vary
0000 67 65 73 3a 20 62 79 74 65 73 0d 0a 56 61 72 79 : Accept_Encodin
0100 3a 20 41 63 63 65 70 74 2d 45 66 63 6f 64 69 6e g_Content-Encod
0110 67 6d 0a 43 6f 6e 74 65 6e 74 2d 45 66 63 6f 64 ing: gzip p Conte
0120 69 6e 67 3a 20 67 7a 69 70 0d 0a 43 6f 6e 74 65 nt-Lengt h: 52 -K
0130 6e 74 2d 4c 65 6e 67 74 68 3a 20 35 32 0d 0a 4b

Paquetes: 2209 - Mostrado: 10 (0.5%)

Guardar Guardar todo Preview Cerrar Ayuda

Perfil: Default

Flag= THM{d0_n07_574lk_m3}