

PRACTICAL CHALLENGE + REPORT TEMPLATE MATA LOMBA CTF

Metadata

Tanggal	24 april (24 april 2024) 2024
Nama Sekolah	SMK TARUNA BANGSA
Disusun Oleh	Abdurrohman Al Fathi

CYBERSECURITY

Overview

PERATURAN PRACTICAL CHALLENGE

Disclaimer

Peraturan Pengerajan

Kategori Challenge

Durasi Pengerajan

Cara Dokumentasi

Cara duplikasi dokumen pada google docs:

Link Submit Laporan

Index Penilaian

THE CHALLENGES

WEB EXPLOITATION

1. Task 1 - Kue Admin
2. Task 2 - Konsolog
3. Task 3 - Mr.Robot

DIGITAL FORENSICS

1. Task 1 - Manipulasi Kepala
2. Task 2 - OpenMe!
2. Task 3 - Garmbar Bagus

REVERSE ENGINEERING

1. Task 1 - Perbandingan

KRIPTOGRAFI

1. Task 1 - Kode CIP Vigenere
2. Task 2 - Eks OR

STEGANOGRAPHY

1. Task 1 - Exifme
2. Task 2 - Awas Jebakan
3. Task 3 - Kiu AR

CYBERSECURITY

Overview

Dokumen ini berisi seluruh challenge dari mata lomba CTF Cybersecurity. Dalam challenge ini akan disediakan sejumlah 12 Challenge yang akan diselesaikan dalam waktu yang ditentukan untuk seluruh peserta secara individu. Dokumen ini menjadi laporan untuk menjawab seluruh challenge yang diberikan kepada seluruh peserta.



CYBERSECURITY

PERATURAN PRACTICAL CHALLENGE

Disclaimer

Peserta akan menemukan bentuk flag dengan format **LKS_CTF{}** yang nantinya akan juri mention untuk format menjawabnya.

Silahkan dikerjakan se bisa mungkin karena durasi penggeraan **4 Jam** dengan berbagai macam tipe **mind-blowing** challenge untuk problem solving skills.

Peraturan Penggeraan

1. Peserta mengerjakan challenge secara fleksibel.
2. Penggeraan dan lampiran jawaban wajib pada dokumen ini.
3. Dilarang mencontek dari dokumentasi orang lain.
4. Tidak ada bantuan hint dari panitia atau juri, diharapkan peserta dapat memecahkan masalah pada exam secara mandiri.

Kategori Challenge

1. Web Exploitation
2. Digital Forensics
3. Reverse Engineering
4. Cryptography
5. Steganography

Durasi Penggeraan

Penggeraan challenge ini memiliki durasi **4 Jam** dari mulai lomba Cybersecurity dimulai hingga selesai.

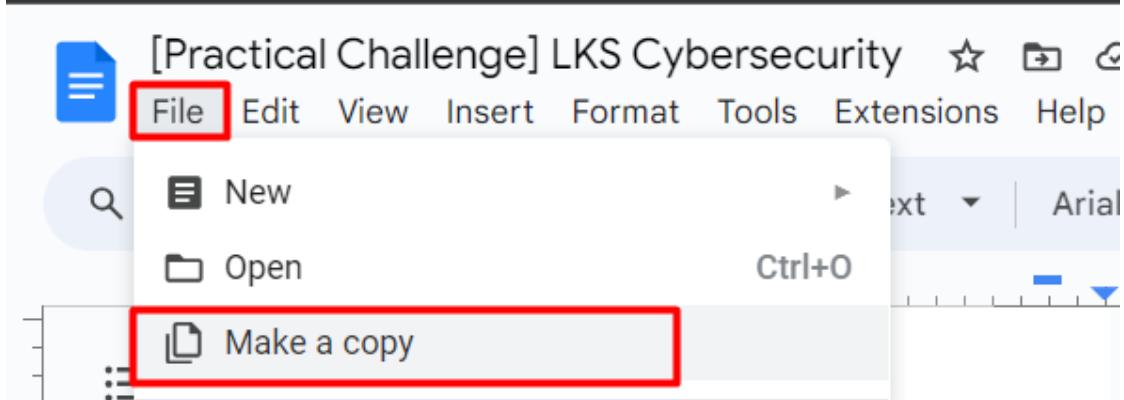
Cara Dokumentasi

Silahkan untuk melakukan copy pada dokumen challenge ini dan dikerjakan pada **Google Docs** peserta masing-masing.

Cara duplikasi dokumen pada google docs:

1. Buka pada bagian **File** kemudian pilih **Make a copy**.

CYBERSECURITY

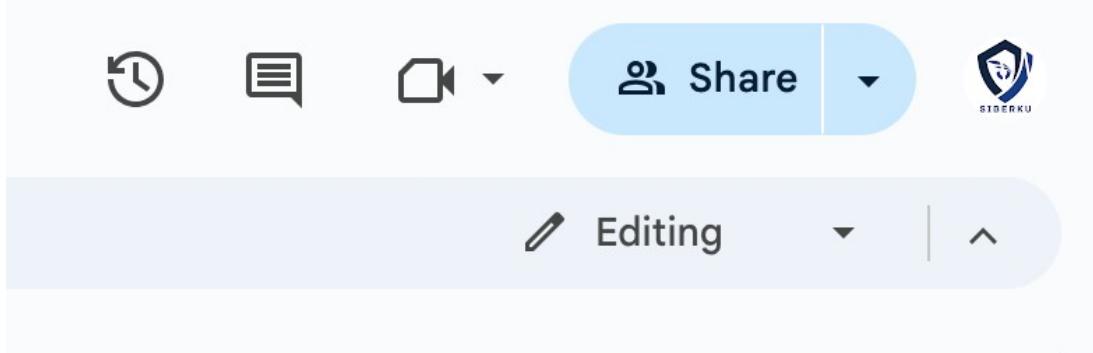


2. Dokumen akan ter-duplikasi pada **google docs** peserta, dan peserta dapat langsung mengerjakannya.
3. Format nama file untuk dokumen masing-masing peserta adalah berikut:

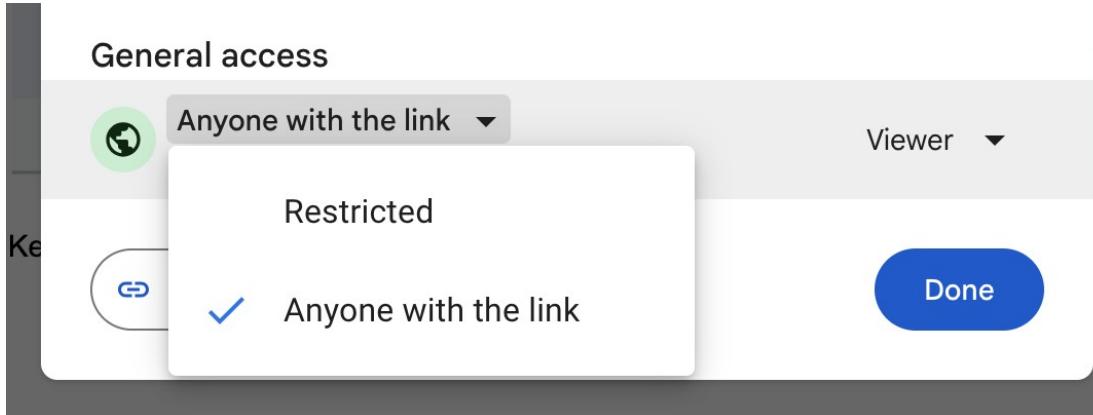
Nama Sekolah _ CYBERSECURITY _ CTF

Example: SMK 1 BEKASI_CYBERSECURITY_CTF

4. Diharapkan peserta memastikan bahwa dokumen dapat diakses secara public. Pilih pada bagian **Share**.



5. Kemudian, pada **General Access**, pilih opsi **Anyone With The Link**.





Link Submit Laporan

Silahkan submit URL Google Docs laporan kamu apabila sudah selesai mengerjakan seluruh challenge pada link berikut: <https://forms.gle/Zauoa8oAV5Yqg9mW9> (tanggal 24 April 2024)

Index Penilaian

1. Akumulasi persentase dari setiap kategori challenge.
2. Kecepatan penggerjaan dan ketepatan submit challenge pertama kali.
3. Kejelasan pada dokumentasi.

WEB EXPLOITATION

TASK-1 > pada halaman awal web hanya terdapat “ harus sebagai admin”

The screenshot shows the browser's developer tools with the Application tab selected. In the Storage section under Cookies, there is a cookie named "admin" with a value of "1". The cookie has a domain of "103.174.114.130", a path of "/", an expiration date of "2024-0...", a size of 6 bytes, and is marked as HttpOnly and SameSite. The cookie value is also displayed below the table.

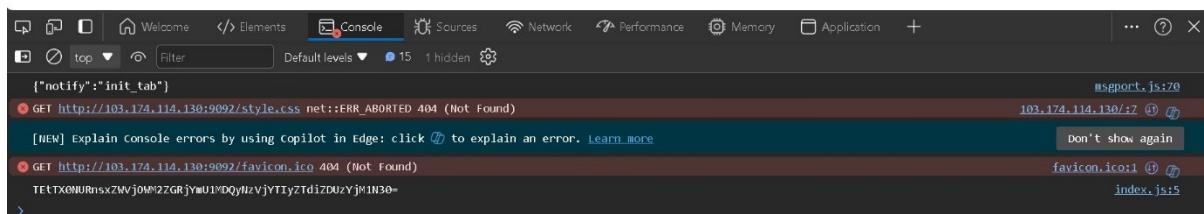
Setelah di edit pada cookiesnya dan direfresh terdapat flagnya pada TASK-1

The screenshot shows the browser's developer tools with the Application tab selected. In the Storage section under Cookies, there is a cookie named "admin" with a value of "1". The cookie has a domain of "103.174.114.130", a path of "/", an expiration date of "2024-0...", a size of 6 bytes, and is marked as HttpOnly and SameSite. A message "Select a cookie to preview its value" is displayed in the center of the application tab area.

TASK-2 > Pada halaman awal web terdapat tombol klik "CLICK ME" setelah diklik dan dicek pada bagian console terdapat text ter enkripsi

First code

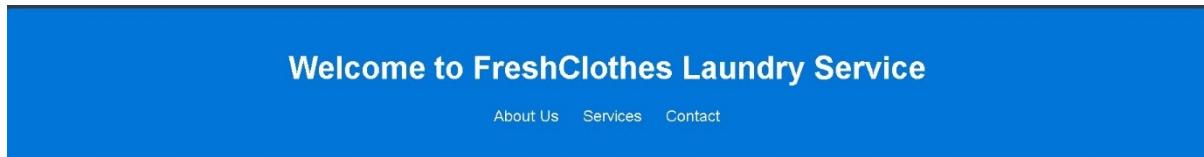
Click Me!



Dan setelah didecrypt dengan decoder tipe enkripsi base64 terdapat flag pada TASK-2

```
(root㉿PC-Abdurrohman)-[/home/silent_majority]
# echo "TEtTX0NURnsxZWVj0WM2ZGRjYmU1MDQyNzVjYTIyZTdiZDUzYjM1N30=" | base64 -d
LKS_CTF{1eec9c6ddcbe504275ca22e7bd53b357}
(root㉿PC-Abdurrohman)-[/home/silent_majority]
#
```

TASK-3 > pada halaman awal web hanya terdapat index.html



About Us

We are your friendly neighborhood laundry service, ensuring your clothes are fresh and clean.

Our Services

- Dry Cleaning
- Washing & Folding
- Ironing

© 2024 FreshClothes Laundry. All rights reserved.

Setelah diubah pada belakang urlnya/path terdapat flag pada TASK-3



DIGITAL FORENSIC

Pada tampilan awal file ketika dibuka menggunakan binaryninja/hxd pada headernya masih tertera “www”

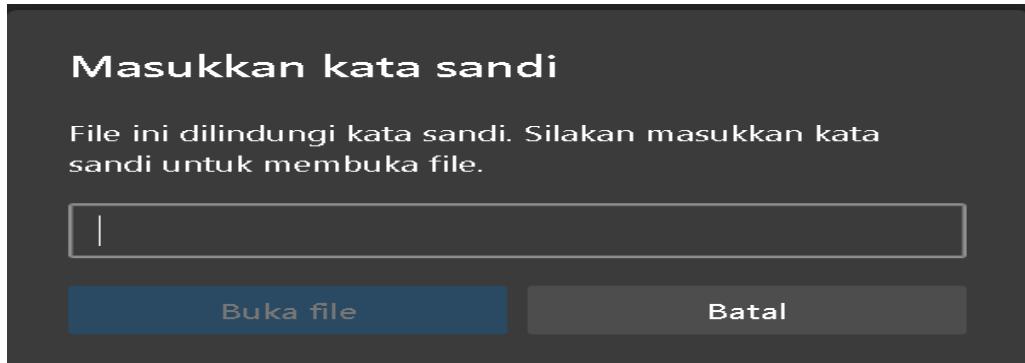
Address	Value	Content
00000000	77 77 77 77 0d 0a 1a 0a-00 00 00 0d 49 48 44 52	www.....IHDR
00000010	00 00 03 88 00 00 03 89-08 02 00 00 00 d0 8e 9b
00000020	3c 00 00 00 01 73 52 47-42 01 d9 c9 2c 7f 00 00	<....sRGB.....
00000030	00 09 70 48 59 73 00 00-0e c4 00 00 0e c4 01 95	.pHYs.....
00000040	2b 0e 1b 00 1a 04 01 49-44 41 54 78 9c 4c bb 67	+.....IDATx.L.g
00000050	af eb 78 b6 e6 d7 80 fd-e2 8e dd 98 e9 50 75 d2	.x.....Pu.
00000060	8e ca 99 54 ce 89 ca 12-45 25 92 92 28 4a 54 ce	..T....E%.(JT.
00000070	39 6b 4b 3b e7 bd cf 3e-39 54 9d aa ea ba 75 bb	9kK;...>9T....u.
00000080	a7 7b fa de eb b1 e1 31-c6 98 17 06 0c fb 0b f8	.{.....1.....
00000090	2b 79 ed 53 83 c1 00 0b-c4 9f 14 93 c8 b5 d6 f3	+y.S.....
000000a0	7b 48 e9 37 d6 80 59 61-92 4b 75 62 d4 8a 68 ec	{H.7..Ya.Kub..h.
000000b0	a8 ca a2 54 9a 14 2a b3-02 16 f2 55 fb 2f 44 cf	...T..*....U./D.
000000c0	04 28 9f 87 ec 4b 0c 42-85 5d 2a 30 ec 0b 4d 3c	.(...K.B.]*0..M<

Setelah kita samakan headernya dengan foto mekar.png dari www jadi %PNG dan diubah format filenya dengan menambahkan .png pada belakang file lalu kita open dan kita gabungkan flag yang terdapat pada kedua foto tersebut terdapat flag pada TASK-1



CYBERSECURITY

TASK-2 > pada tampilan awal disaat mencoba membuka file ternyata terkunci



Setelah diubah format filenya menjadi .txt dan dibuka terdapat password yang dapat kita masukan untuk membuka file openme.pdf

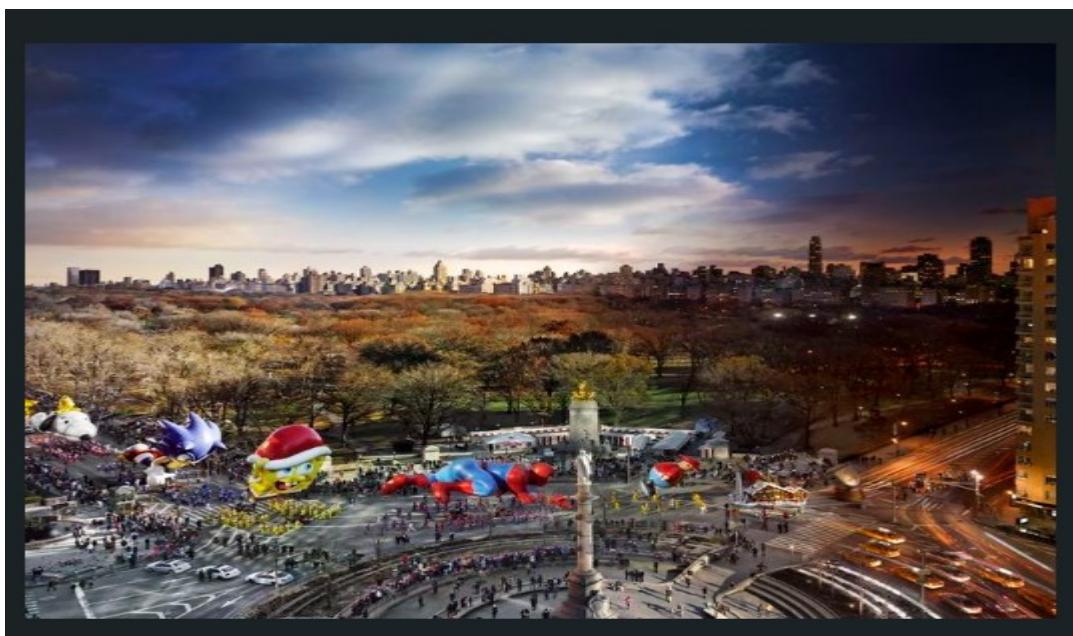
```
|Passwordnya: rainbow
%PDF-1.7
%μμμμ
1 0 obj
<</Type/Catalog/Pages 2 0 R/Lang(Z\u01011|36æO%úmi\u00d1:
endobj
2 0 obj
<</Type/Pages/Count 1/Kids[ 3 0 R] >>
endobj
3 0 obj
```

Setelah dibuka terdapat flag pada TASK-2

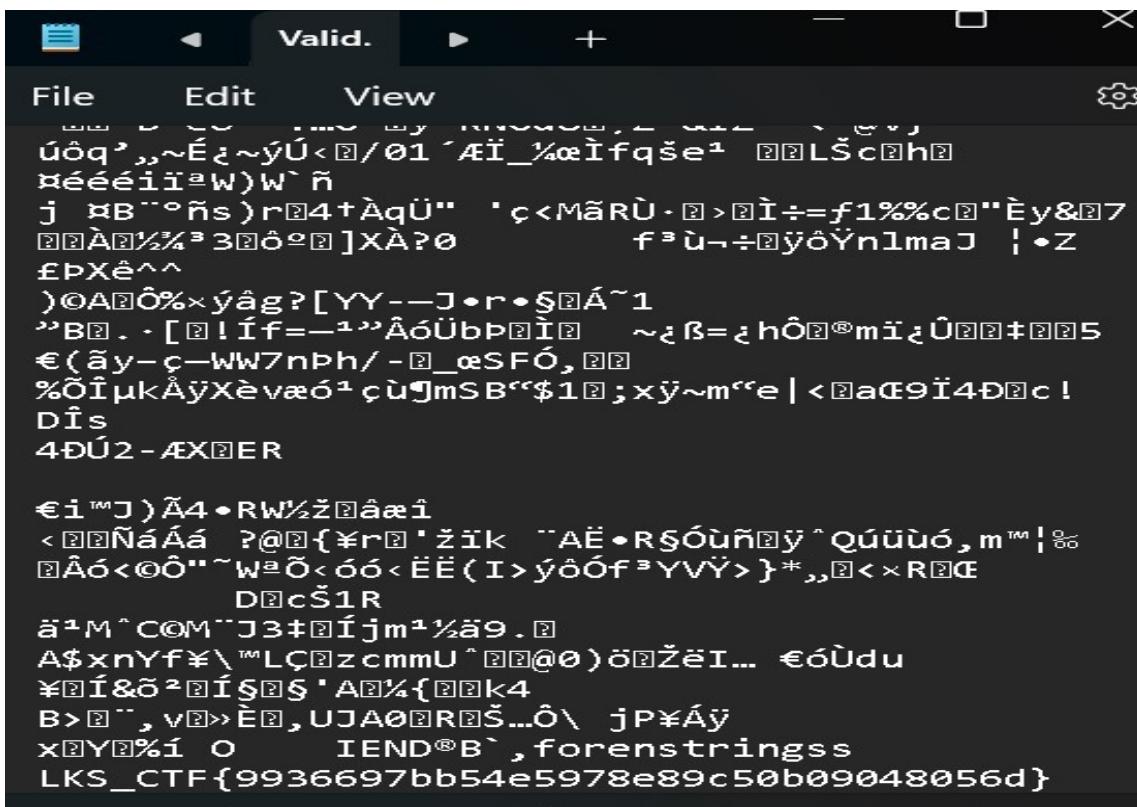


CYBERSECURITY

TASK-3 > pada tampilan awal file Valid.png hanya berisi gambar berikut



Setelah dibuka menggunakan notepad/binaryninja/hxd terdapat flag pada TASK-3



REVERSE ENGINEERING

TASK-1 > Pada tampilan awal file berisi kode string berikut

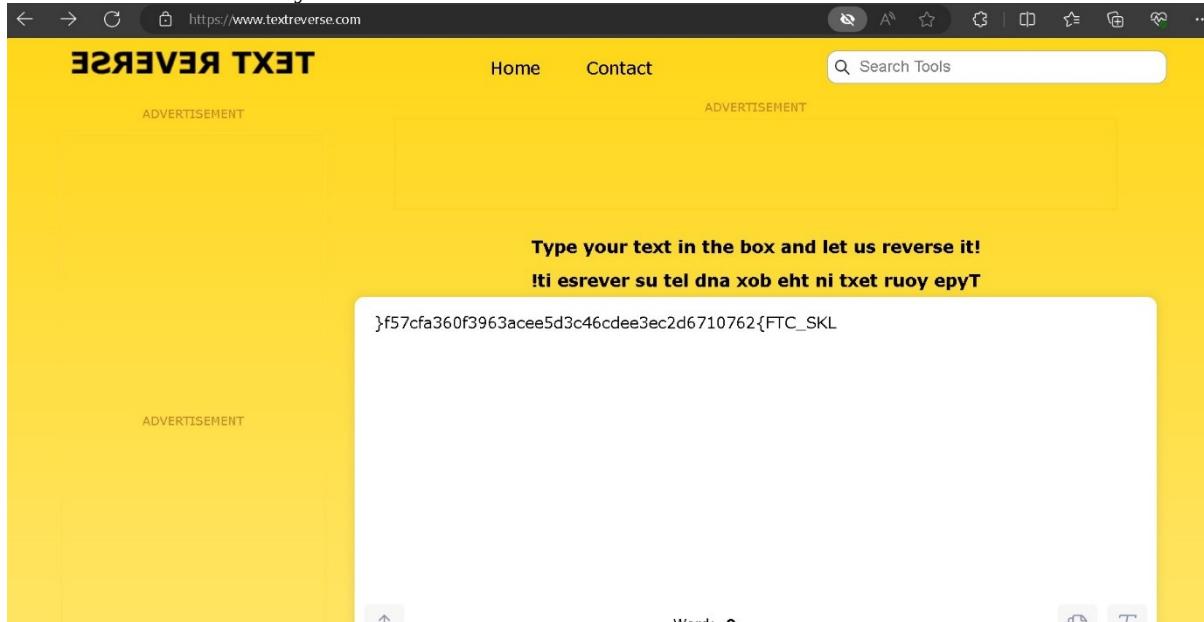
Setelah dibuka file /perbandingan dibuka dengan binaryninja dan discroll terdapat flag yang masih ke reverse textnya

```
void frame_dummy()
14 |     return register_tm_clones() __tailcall

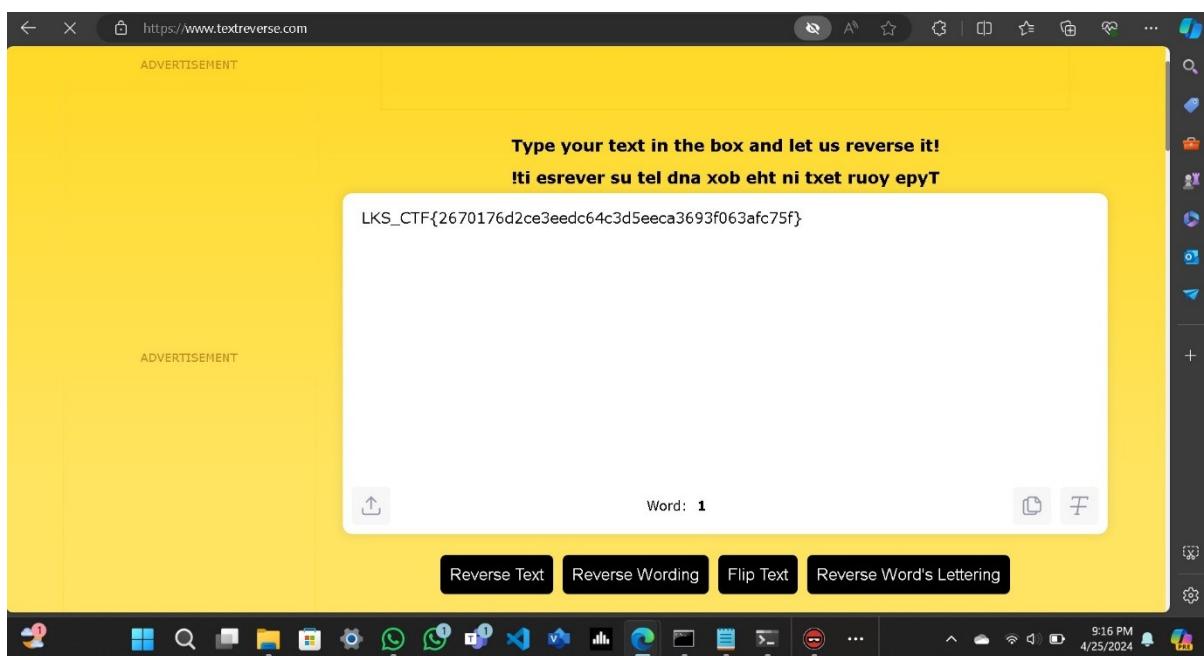
19 int32_t main(int32_t argc, char** argv, char** envp)
8     void* fsbase
8     int64_t rax = *(fsbase + 0x28)
7     int32_t var_1af
7     __builtin_strncpy(dest: &var_1af, src: "StrCMp", n: 7)
5     int64_t __s
5     __builtin_strncpy(dest: &__s, src: "\f57cfaf360f3963acee5d3c46cdee3ec2d6710762{FTC_SKL", n: 0x
5     std::operator<<(std::char_traits<char> )(&__out: &std::cout, __s: "*****CHECK PASSWORD*****")
5     std::operator<<(std::char_traits<char> )(&__out: &std::cout, __s: "First Password: \n")
5     std::operator<<(std::char_traits<char> )(&__out: &std::cout, __s: "Second Password :")
1 void var_1a8
1 std::operator>>(char>(&std::cin, &var_1a8)
```

CYBERSECURITY

Lalu kita reverse textnya



Setelah direverse textnya terdapat flag pada TASK-1



CRYPTOGRAPHY

TASK-1 > pada tampilan awal file terdapat text terenkripsi kode cip vignere dengan key:bekasi

```
MOC_CLN{c067j1723pc4098vic5i33n65660cs0nc67i9606}
KEY: bekasi
```

Setelah di decrypt dengan decryptor terdapat flag pada TASK-1

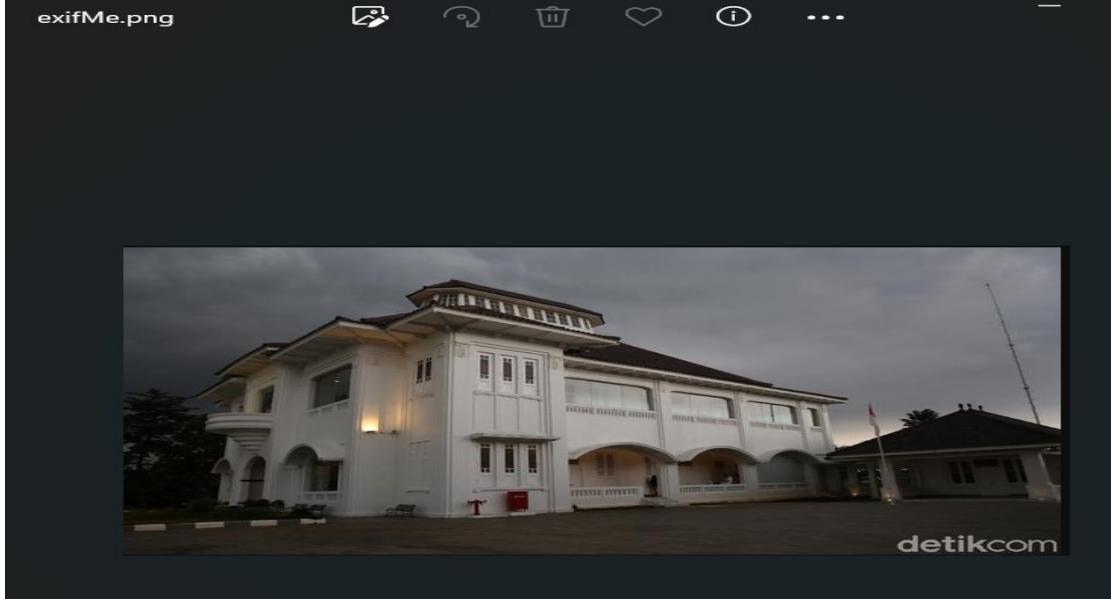
The screenshot shows a decryption interface for the Vigenère cipher. The ciphertext input field contains "MOC_CLN{c067j1723pc4098vic5i33n65660cs0nc67i9606}". The key input field is set to "bekasi". The decrypted plaintext output field shows the flag: "LKS_CTF{b067f1723fc4098dab5e33d65660ca0fb67e9606}".

TASK-2 > terdapat text ternkripsi pada tampilan awal setelah didecrypt menggunakan decryptor xor terdapat flag pada TASK-2

The screenshot shows an XOR Decoder interface. On the left, the "Results" section displays several rows of decrypted data, with row 15 highlighted in blue. Row 15 contains the flag: "LKS_CTF{8376a787eb65de01daf03825a4426cff0146e5bf}♦♦". On the right, the "XOR DECODER" section shows the original ciphertext: "YAFJVASH-&"#t"="pw# qp%\$qts%&-` t!! '#vss%\$!#p ws". Below it, the "ENCRYPTION/DECRIPTION METHOD" section has "AUTOMATIC (BRUTEFORCE 1 TO 16 BYTES)" selected. The "RESULTS FORMAT" section has "ASCII (PRINTABLE) CHARACTERS" selected. At the bottom right is a large yellow button labeled "► ENCRYPT / DECRYPT".

STEGANOGRAPHY

TASK-1 > pada tampilan awal hanya terdapat gambar berikut

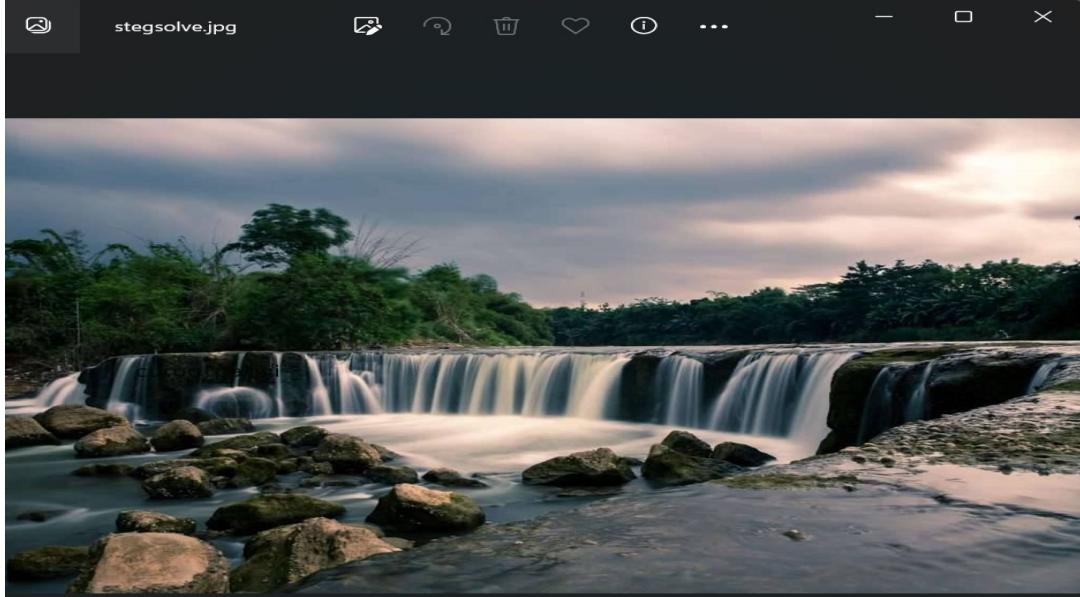


Setelah di cek menggunakan exiftool terdapat flag pada TASK-1

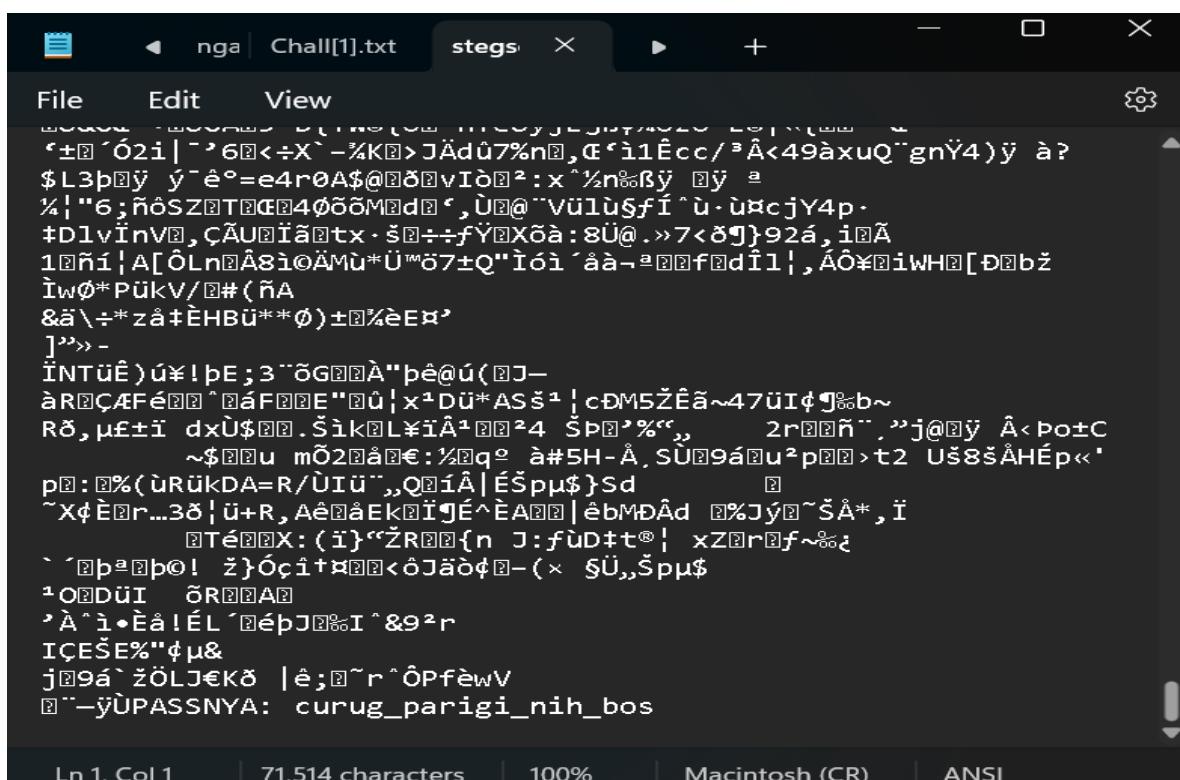
```
└─(root㉿kali)-[~/home/abdurrohman/Downloads] 24 Mar 2024
  └─# ls
    Chall                               Maltego.v4.6.0.deb   'Open Me.pdf'   'Pantai(1)'      QR.png
    Chall-20240425T014609Z-001.zip     Mekar.png        Pantai          Perbandingan  Untitled.jpeg
    Downloads
└─(root㉿kali)-[~/home/abdurrohman/Downloads] 24 Mar 2024
  └─# exiftool exifMe.png
ExifTool Version Number : 12.76
File Name               : exifMe.png
Directory              :
File Size               : 193 kB
File Modification Date/Time : 2024:04:24 23:01:06+07:00
File Access Date/Time   : 2024:04:24 23:01:35+07:00
File Inode Change Date/Time : 2024:04:24 23:01:06+07:00
File Permissions        : -rw-r--r--
File Type               : PNG
File Type Extension    : png
MIME Type               : image/png
Image Width             : 624
Image Height            : 352
Bit Depth               : 8
Color Type              : RGB
Compression             : Deflate/Inflate
Filter                  : Adaptive
Interlace                : Noninterlaced
Pixels Per Unit X       : 3780
Pixels Per Unit Y       : 3780
Pixel Units              : meters
Comment                 : LKS_CTF{099a6037dc55d9c49037073721c73bc4965e32d4}
Image Size              : 624x352
Megapixels              : 0.220
└─#
```

CYBERSECURITY

TASK-2 > pada tampilan awal file stegsolve.png hanya terdapat gambar Berikut



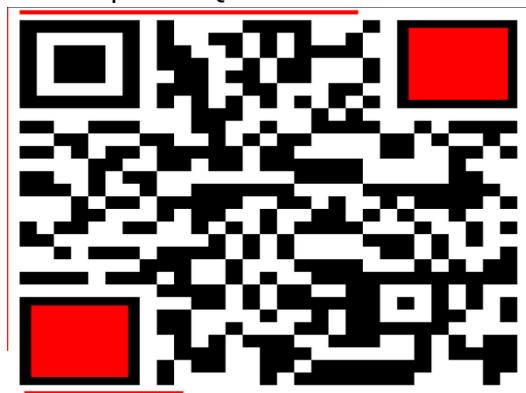
Setelah format file stegsolve.png diubah menjadi stegsolve.txt kita scroll terdapat kunci untuk membuka file qatcha.zip



CYBERSECURITY

Sekarang kita buka file terdapat gatcha.png setelah kita ubah format filenya /metode cat pada bagian paling bawah terdapat flag

TASK-3 > terdapat file QR dalam keadaan sudah teredit



Setelah kita edit menggunakan photoeditor



Dan kita scan dengan search engine terdapat flag pada TASK-3

A large QR code is displayed on the left side of the interface. To its right, there is a search bar with the placeholder text "Cari sumber gambar" (Search image source). Below the QR code, the text "LKS_CTF(836e39330b42c3503734c46c61fcc0)" is shown, which is the flag for the challenge.

TASK 1 - KUE ADMIN

Tugas Anda adalah untuk memotong kue yang disediakan menggunakan "pisau admin". Kue ini merupakan sebuah analogi untuk sebuah website yang rentan terhadap serangan yang memanfaatkan kelemahan sistem administrasi. Anda diminta untuk menemukan celah keamanan di dalam website tersebut dan menggunakan "pisau admin" untuk memanfaatkannya.

Endpoint: <http://103.174.114.130:9091/>

Dokumentasi, Jawaban dan Pembahasan:

TASK 2 - KONSOLOG

Tantangan "Konsolog" mengharuskan peserta untuk menemukan sebuah flag yang tersembunyi di dalam suatu pesan atau respon yang diberikan oleh website target. Peserta perlu melakukan eksplorasi dan analisis menyeluruh terhadap website tersebut untuk menemukan tempat di mana flag disembunyikan.

Endpoint: <http://103.174.114.130:9092/>

Dokumentasi, Jawaban dan Pembahasan:

TASK 3 - MR.ROBOT

Tantangan "Mr.Robot" mengajak peserta untuk menemukan sebuah kunci yang tersembunyi di dalam website target. Peserta perlu melakukan eksplorasi menyeluruh terhadap halaman web dan mengidentifikasi cara untuk menemukan kunci tersebut tanpa adanya petunjuk yang spesifik.

Endpoint: <http://103.174.114.130:9093/index.html>

Dokumentasi, Jawaban dan Pembahasan:

TASK 1 - MANIPULASI KEPALA

Tantangan "Manipulasi Kepala" menantang peserta untuk membantu tim forensik dalam memperbaiki sebuah file yang mencurigakan. Peserta diminta untuk melakukan analisis dan manipulasi terhadap bagian-bagian tertentu dari file tersebut.

Challenge: https://drive.google.com/drive/folders/1TfO24HEmoaqZ-GNN7b5kLXv_z_ISp4rj?usp=sharing

Dokumentasi, Jawaban dan Pembahasan:

TASK 2 - OPENME!

Tantangan "OpenMe!" meminta Anda untuk menemukan password yang mengunci sebuah file PDF. Anda harus mencari dan menemukan password tersebut untuk membuka file PDF tersebut dan mengungkap isinya.

Challenge: https://drive.google.com/drive/folders/1DnluBiiz8VYD_OrqHRX6EPmr70IT0laS?usp=sharing

Dokumentasi, Jawaban dan Pembahasan:

TASK 3 - GAMBAR BAGUS

Temukan flag yang tersembunyi di dalam sebuah gambar yang diberikan. Anda perlu memeriksa setiap detail gambar dengan cermat dan mencari tahu di mana flag tersebut disembunyikan.

Challenge:

https://drive.google.com/drive/folders/1h17GGtekwDjPvoBEzF2T_9PrlqHN2ARK?usp=sharing

Dokumentasi, Jawaban dan Pembahasan:



TASK 1 - PERBANDINGAN

Tantangan "Perbandingan" meminta Anda untuk menemukan password utama yang akan memberikan akses ke flag yang tersembunyi. Anda perlu melakukan pencarian teliti dan analisis yang mendalam untuk mengungkap password tersebut.

Challenge: <https://drive.google.com/drive/folders/1VRqlXr00ayhsdBzAv6yOFHbzZF1ID7i?usp=sharing>

Dokumentasi, Jawaban dan Penjelasan

CRYPTOGRAPHY

TASK 1 - KODE CIP VIGENERE

Bantu intelijen dalam memecahkan sebuah kode chiper yang menggunakan metode Vigenere. Anda akan diberikan teks terenkripsi yang perlu diuraikan menggunakan pengetahuan tentang teknik chiper Vigenere. Dengan menggunakan kecerdasan dan ketelitian Anda, Anda akan memecahkan teka-teki ini dan mengungkap pesan yang tersembunyi di dalamnya.

Challenge: <https://drive.google.com/drive/folders/1J4YTqe10iMho79nKyljoKqxtQRC8HuHn?usp=sharing>

Dokumentasi, Jawaban dan Penjelasan

TASK 2 - EKS OR

Bantu intelijen dalam memecahkan sebuah enkripsi yang tidak diketahui. Anda akan diberikan teks terenkripsi yang perlu diuraikan menggunakan pengetahuan dan keterampilan kriptografi Anda. Dengan analisis yang teliti dan pemecahan teka-teki yang cerdas, Anda akan mencoba mengungkap pesan yang tersembunyi di dalamnya.

XOR
Y^FJVASn-&"#t"- "pw# qp%\$qts%&- ' t ! ! '#vss%\$!#p wsh

Dokumentasi, Jawaban dan Penjelasan

STEGANOGRAPHY

TASK 1 - EXIFME!

Temukan flag yang tersembunyi dalam sebuah file yang diberikan. Lakukan pencarian dan analisis pada metadata file tersebut menggunakan pengetahuan dan keterampilan Anda. Dengan teliti mengeksplorasi setiap detail yang tersedia, Anda akan berusaha untuk menemukan flag yang disembunyikan di dalamnya.

Challenge: <https://drive.google.com/drive/folders/10jbDqoqi1F8wgdJLlxM0y-lBez7dUaTe?usp=sharing>

Dokumentasi, Jawaban dan Penjelasan:

TASK 2 - AWAS JEBAKAN

Temukan teka-teki yang tersembunyi dalam sebuah gambar. Dalam gambar tersebut, terdapat petunjuk atau kode yang akan membawa Anda menuju gacha atau hadiah spesial. Dengan cermat memeriksa setiap detail gambar, Anda akan mencoba untuk mengungkap teka-teki yang tersembunyi di dalamnya.

Challenge:

https://drive.google.com/drive/folders/1OjlqW8uOZ516j7r9qs-pJTDJGHa_fSnE?usp=sharing

Dokumentasi, Jawaban dan Penjelasan:

TASK 3 - KIU AR

Baca sebuah teks atau pesan yang tersembunyi di dalam gambar yang diberikan.

Challenge: <https://drive.google.com/drive/folders/1Wb7IIIBjZyGAafZOatJoiXYvkdyCbQWy?usp=sharing>

Dokumentasi, Jawaban dan Penjelasan: