

# 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          |



#### Overview

#### PERATURAN PRACTICAL CHALLENGE

Disclaimer

Peraturan Pengerjaan

Kategori Challenge

Durasi Pengerjaan

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

# 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.

# PERATURAN PRACTICAL CHALLENGE

### Disclaimer

Peserta akan menemukan bentuk flag dengan format LKS\_CTF{} yang nantinya akan juri mention untuk format menjawabnya.

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

### Peraturan Pengerjaan

- 1. Peserta mengerjakan challenge secara fleksibel.
- 2. Pengerjaan 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 Pengerjaan

Pengerjaan challenge ini memiliki durasi **4 Jam** dari mulai lomba Cybersecurity dimulai higga 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**.

| BERSECURITY  |  |
|--|--|
| [Practical Challenge] LKS Cy<br>File Edit View Insert Format | /bersecurity ☆ 🗈 🖉<br>Tools Extensions Help  |
| New  | ► ext 💌 Arial  |
| 🖿 Open   | Ctrl+O   |
| 🗋 Make a copy  |  |
|  | BERSECURITY         [Practical Challenge] LKS Cy         File       Edit       View       Insert       Format         Image: Second system       Image: Second system       Image: Second system       Image: Second system         Image: Second system |

- 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:



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: <u>https://forms.gle/Zauoa8oAV5Yqg9mW9</u> (tanggal 24 April 2024)

## **Index Penilaian**

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



## WEB EXPLOITATION

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

| $\leftarrow$ $	ext{C}$ $	heta$ Tidak an | nan   103.174.11 | <b>4.130</b> :9091 |               |                     |   |        |      |         | Aŋ      |          | (3   0 | ₽ ₹      | Ē        | <del>8</del> 9 |            |
|---|------------------|--------------------|---------------|---------------------|---|--------|------|---------|---------|----------|--------|----------|----------|----------------|------------|
| Harus sebagai admin                     |                  |                    |               |                     |   |        |      |         |         |          |        |          |          |                |            |
|   |                  |                    |               |                     |   |        |      |         |         |          |        |          |          |                |            |
|   |                  |                    |               |                     |   |        |      |         |         |          |        |          |          |                |            |
|   |                  |                    |               |                     |   |        |      |         |         |          |        |          |          |                |            |
|   |                  |                    | conference -  |                     | 8410-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1- |        |      |         |         |          |        |          | ľ        |                |            |
| P P Welcome                             |                  | 도 Console          | 똱 Sources     | 🛜 Network           | 🌮 Performance                             | Ö      |      |         | ication |          |        |          |          | ?              | $) \times$ |
| Service workers                         | C Filter         | =                  | 🗙 🔲 Only show | w cookies with an i | ssue                                      |        |      |         |         |          |        |          |          |                |            |
| Storage                                 | Name             | •                  | Value         |                     |   | Domain | Path | Expires | Size    | HttpOnly | Secure | SameSite | Partitio | . Prior        | ity 🛕      |
| Storage                                 | admin            |                    | 1             |                     |   | 103.17 | 1    | 2024-0  |         | 6        |        |          |          | Med            | ium 🚽      |
| Local storage                           | Cookie Value     | Show URL-decod     | bed           |                     |   |        |      |         |         |          |        |          |          |                |            |
| Gession storage                         |                  |                    |               |                     |   |        |      |         |         |          |        |          |          |                |            |
| ▼ (☆) Cookies                           |                  |                    |               |                     |   |        |      |         |         |          |        |          |          |                |            |
| http://103.174.114.13                   | _                |                    |               |                     |   |        |      |         |         |          |        |          |          |                |            |
| Private state tokens                    |                  |                    |               |                     |   |        |      |         |         |          |        |          |          |                |            |
| Console Issues 🕂                        |                  |                    |               |                     |   |        |      |         |         |          |        |          |          | ŝ              | ÷          |
| 🗈 🖉 top 🔻 🔿 Filter                      | Def              | fault levels 🔻 🔎   | 11 😥          |                     |   |        |      |         |         |          |        |          |          |                |            |
| {"notify":"init tab"}                   |                  |                    |               |                     |   |        |      |         |         |          |        |          | IISEDO   |                | 70         |

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

| LKS_CTF{17b38903f8cc8e6 | 5ebf9ce3210960af | ac}            |               |                     |                       |        |         |          |        |          |        |          |          |            |
|-------------------------|------------------|----------------|---------------|---------------------|-----------------------|--------|---------|----------|--------|----------|--------|----------|----------|------------|
|                         |                  |                |               |                     |                       |        |         |          |        |          |        |          |          |            |
| G G Welcome             | Elements         | 反 Console      | 똱 Sources     | 奈 Network           | <b>∽≫</b> Performance | 0      | Vemory  | 🗖 Appli  | cation | +        |        |          |          | (?) ×      |
| Service workers         | C Filter         |                | 🗶 🔲 Only show | cookies with an is: |                       |        |         |          |        |          |        |          |          |            |
| ☐ Storage               | Name             | <b></b>        | Value         |                     |                       | Domain | Path    | Expires  | Size   | HttpOnly | Secure | SameSite | Partitio | Priority 🔺 |
| Storage                 | admin            |                |               |                     |                       |        |         | 2024-0   |        |          |        |          |          | Medium     |
| Local storage           |                  |                |               |                     |                       |        |         |          |        |          |        |          |          |            |
| Session storage         |                  |                |               |                     |                       |        |         |          |        |          |        |          |          |            |
| IndexedDB     Cookies   |                  |                |               | Sele                | ct a cookie           | to pre | eview i | ts value |        |          |        |          |          |            |
| http://103.174.114.13   |                  |                |               |                     |                       |        |         |          |        |          |        |          |          |            |
| Private state tokens    |                  |                |               |                     |                       |        |         |          |        |          |        |          |          |            |
| Console Issues +        |                  |                |               |                     |                       |        |         |          |        |          |        |          |          | 48 E       |
| 🗉 🖉 top 🔻 🔿 Filter      | Defau            | ult levels 🔻 🧔 | 8 tội         |                     |                       |        |         |          |        |          |        |          |          |            |
| {"notify":"init_tab"}   |                  |                |               |                     |                       |        |         |          |        |          |        |          | msgport  |            |

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!   |                               |
|   |                               |
| 🖵 🗗 🗋 🕼 Welcome 🌾 Elements 📴 Console 💥 Sources 🛜 Network 🛷 Performance 🧔 Memory 🗖 Application 🕂 | ··· ⑦ ×                       |
| 🖻 🖉 top ▼ 👁 Filter Default levels ▼ 🏚 15 1 hidden 🐯   |                               |
| {"notify":"init_tab"}   | ∎sgport.js:70                 |
| © GET http://103.174.114.130:9092/style.css net::ERR_ABORTED 404 (Not Found)                    | <u>103.174.114.130/:7</u> 🕕 🍙 |
| [HEW] Explain Console errors by using Copilot in Edge: click 🕼 to explain an error. Learn more  | Don't show again              |
| S GET <u>http://103.174.114.130:9092/favicon.ico</u> 404 (Hot Found)                            | favicon.ico:1 🕕 🍈             |
| TEŁTXCMURnsxZMVjOMM2ZGRjYmU1MDQVU2VjYTTyZTdiZDU2YjM1N30*  | <u>index.js:5</u>             |

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





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

| Welcome to FreshClothes Laundry Service   |
|---|
| About Us Services Contact   |
|   |
| 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                            |
|   |
|   |
|   |
| - 「「「「「「」」 「「」 「」 JUNGLE DUCT X ULAR V4 × 「」 103.174.114.130:9093/robots.txt ×                |
| ← C Iidak aman   103.174.114.130:9093/robots.txt  |
|   |
| Oser-agent: *<br>Allow:<br>Dissalow:  |
|   |
| LKS_CTF{ab9ef71f7d32b806d7186d947ae6a964}   |





## DIGITAL FORENSIC

Pada tampilan awal file ketika dibuka menggunakan binaryninja/hxd pada headernya masih tertera "wwww"

| Debugger Plugins W | 'indow Help |       |    |    |    |    |    |       |    |    |    |    |    |    |    |                         |
|--------------------|-------------|-------|----|----|----|----|----|-------|----|----|----|----|----|----|----|-------------------------|
| Pantai X +         |             |       |    |    |    |    |    |       |    |    |    |    |    |    |    |                         |
| ch symbols 🛛 🚍     | Mapped 🔻 🖡  | lex ▼ |    |    |    |    |    |       |    |    |    |    |    |    |    |                         |
| ss 🔶 Section       | 00000000    | 77 77 | 77 | 77 | 0d | 0a | 1a | 0a-00 | 00 | 00 | Ød | 49 | 48 | 44 | 52 | wwwwIHDR                |
|                    | 00000010    | 00 00 | 03 | 88 | 00 | 00 | 03 | 89-08 | 02 | 00 | 00 | 00 | d0 | 8e | 9b |                         |
|                    | 00000020 3  | 3c 00 | 00 | 00 | 01 | 73 | 52 | 47-42 | 01 | d9 | c9 | 2c | 7f | 00 | 00 | <srgb,< td=""></srgb,<> |
|                    | 00000030    | 00 09 | 70 | 48 | 59 | 73 | 00 | 00-0e | c4 | 00 | 00 | 0e | c4 | 01 | 95 | pHYs                    |
|                    | 00000040 2  | 2b 0e | 1b | 00 | 1a | 04 | 01 | 49-44 | 41 | 54 | 78 | 9c | 4c | bb | 67 | +IDATx.L.g              |
|                    | 00000050 a  | af eb | 78 | b6 | e6 | d7 | 80 | fd-e2 | 8e | dd | 98 | e9 | 50 | 75 | d2 | xPu.                    |
|                    | 00000060 8  | Be ca | 99 | 54 | ce | 89 | са | 12-45 | 25 | 92 | 92 | 28 | 4a | 54 | ce | TE%(JT.                 |
|                    | 00000070 3  | 39 6b | 4b | 3b | e7 | bd | cf | 3e-39 | 54 | 9d | aa | ea | ba | 75 | bb | 9kK;>9Tu.               |
|                    | 00000080 a  | a7 7b | fa | de | eb | b1 | e1 | 31-c6 | 98 | 17 | 06 | 0c | fb | 0b | f8 | . { 1                   |
|                    | 00000090 2  | 2b 79 | ed | 53 | 83 | c1 | 00 | 0b-c4 | 9f | 14 | 93 | c8 | b5 | d6 | f3 | +y.S                    |
|                    | 000000a0 7  | 7b 48 | e9 | 37 | d6 | 80 | 59 | 61-92 | 4b | 75 | 62 | d4 | 8a | 68 | ec | {H.7Ya.Kubh.            |
|                    | 000000b0 a  | a8 ca | a2 | 54 | 9a | 14 | 2a | b3-02 | 16 | f2 | 55 | fb | 2f | 44 | cf | T*U./D.                 |
|                    | 000000000   | 94 28 | 9f | 87 | ec | 4b | 0c | 42-85 | 5d | 2a | 30 | ec | Øb | 4d | 3c | .(K.B.]*0M<             |

Setelah kita samakan headernya dengan foto mekar.png dari wwww 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



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

| Masukkan kata san  | Masukkan kata sandi |  |  |  |  |  |  |  |
|--|---------------------|--|--|--|--|--|--|--|
| File ini dilindungi kata sandi. Silakan masukkan kata<br>sandi untuk membuka file. |                     |  |  |  |  |  |  |  |
|  |                     |  |  |  |  |  |  |  |
| Buka file  | Batal               |  |  |  |  |  |  |  |
|  |                     |  |  |  |  |  |  |  |

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



Setelah dibuka terdapat flag pada TASK-2





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



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

|   | •   | Valid.  | •  | +  |  |                                 |                                | $\times$        |
|---|---|---|--|--|--|---------------------------------|--------------------------------|-----------------|
| File  | Edit  | Vie   | w  |  |  |                                 |                                | <b>5</b> 3      |
| úôq',,<br>¤éééi<br>j ¤B"<br>≌¤À⊡½<br>£ÞXê^<br>)©A⊡Ô<br>"B⊡<br>€(ãy-<br>%Õεk,<br>DÎs<br>4ĐÚ2-,                     | ~É¿~<br>ĩª₩)<br>°ñs)<br>¼³30<br>^<br>ýâ<br>[0!Í<br>¢−₩₩<br>ÅÿXè<br>ÆX0E | ýÚ<∑/e<br>W`ñ<br>r⊇4†Àq<br>ô≌∑]XÀ<br>g?[YY-<br>f=— <sup>1</sup> "Â<br>7nÞh/-<br>væó¹çù<br>R | jÜ" 'Ç<br>,?Ø<br>,   | ∑œÌfqš<br><mãrù<br>f³<br/>§⊡Á~1<br/>IÌ⊡ ~a<br/>S∫,⊡⊡<br/>\$1⊡;xy</mãrù<br> | ē <sup>1</sup> ⊡⊡L5<br>□>⊇Ì÷=j<br>ù-÷⊡ÿô`<br>ß=¿hÔ⊡°<br>⊽~m~e <⊡ | šc⊡hi<br>f1%%<br>řnlma<br>®mï¿l | ם<br>aJ ¦∙2<br>Ûפפ≠פת<br>Ï4Đפc | 8127<br>Z<br>25 |
| <pre>€i™J),<br/>&lt; DDÑá,<br/>DÂó&lt;@<br/>ä¹M^C<br/>A\$xnY<br/>¥DÍ&amp;õ<br/>B&gt;D",<br/>xDYD%<br/>LKS_C</pre> | Ã4•R<br>Áá?¦<br>Ô"~W<br>D<br>@M"J<br>f¥\™<br>²⊇ͧ<br>v2≫È<br>í O<br>TF{9 | ₩%ž≌âæ<br>@2{¥r<br>2cš1R<br>3‡2Íjm<br>LÇ2zcm<br>2§'A2%<br>2,UJA0<br>IEN<br>936697           | 21<br>ËË(I><br>1 <sup>1</sup> %ä9.<br>1 <sup>1</sup> %ä9.<br>10 <sup>1</sup> 20<br>4{00R05.<br>10®B`,<br>76546 | <sup>~</sup> AË•R§<br>ýôÓf³∖<br>₪0)ö₪Ž<br>.Ô\ jP¥<br>forens<br>5978e8      | óùñ⊡ÿ^(<br>'VŸ>}*,,<br>'ëI €óù<br>:Áÿ<br>:tringss<br>:9c50b09    | Qúüù∢<br>I<×R<br>Ìdu<br>90480   | ó,m™¦៖<br>⊡Œ<br>056d}          | 50              |
|   |   |   |  |  |  |                                 |                                |                 |

## **REVERSE ENGINEERING**

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

| PELFPPP                 | 2 > 2       |         | 0                   | ð9      | (                 | @ 8                 |             |              |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
|-------------------------|-------------|---------|---------------------|---------|-------------------|---------------------|-------------|--------------|---------------------|--------------|------------------|-----------------------|--------------|----------------|--------|---|------------------|------------|---------|---------|
| @ 2 2 2 2<br>?          | 0           | 0       | 0                   | Ø₽      | ØÐ                | 2                   | 2           | 8 86         | ) (                 | 3(2)         | 55               | 8                     | 2            | 2              | 2      | 2   |                  |            |         | 8       |
| 2                       |             |         |                     |         | 12                | 10                  |             |              |                     |              |                  |                       | -0           | -12            |        |   |                  |            |         |         |
| •0 0                    | 1           | 12 12   | x-                  | x=      | x=                | Ð                   | 2           | ß            | ]                   | 8 8          | 80               | 80                    | 82           | 0              | 0      | l   | a c              |            | hD      | h⊠      |
| h D D                   | D           | Di la   | Såtd⊠               | 80      | 80                | 80                  | 0           | 6            |                     | 0            | PātdD            | T                     | <u>т</u>     | T<br>Nuur àr   | L      |   | L G              | 1          | QåtdD   |         |
|                         | -           | =       | =                   |         |                   |                     | /11         | b64/10       | I-linux             | -x86-64      | .so.2            | 10<br>                | [] [] (<br>] | 5NU⊵I A⊡<br>∵~ |        |   | BI€ ADI G        | 1          | 8 8     |         |
| GNU _a@abij¥bbbis       | 310W%5\$E A |         | 3 ⊠ GN              | U D     |                   |                     |             | 8 8          | <b>۱</b> ۱          | 202 12 12 12 |                  | Đeims-                | - ຟ%   uµl   | 1              |        |   |                  |            |         |         |
| د<br>۲۰۰۰ ۳             |             |         | au                  |         |                   | VU U                |             |              | 1977                |              |                  | ļ                     | N LL         |                |        | А   |                  |            |         |         |
| -10                     |             |         |                     |         |                   |                     |             |              |                     | 3            | 00               |                       |              |                |        | · · · · · · · ·   | (01 <b>T</b> - I |            |         |         |
| gu                      | we1         | Y 8     |                     | UU<br>  | 12<br>            | ° 2 a2<br>⊳-] ⊼o+4- |             | C + 4 4 - 1  |                     | 00           |                  | gmo                   | on_star      |                | dereg  | 1stern  | Cione lat        | ote        | -04     |         |
| _IIM_registeri          | mcionera    | DIE _25 | sti/istr            | eam_ext | +12600            | PCI _2St4e          | nalic       | STILC        | ar_tra:             | ITSICEE      | KST13Das         | 1C_OSTR               | eamil_l      | 2_ES62         | 51301  | n _2N5  | celos_bas        | e4init     | T TO F  |         |
| _ZNSOISEPFRSOS          | _E _25t1    | SISTIIC | nar_trait           | SICEERS | tisbasi           | c_ostreami          | CI_ES       | 5_PKC        | _2NST8:             | los_bas      | e4InitCI         | EV _ZST               | SICSTI.      | cnar_tra       | 10110  | TROVY   | SDASIC_1         | treami     |         | 56_P53_ |
| _ZST4COUTCX             | a<br>เล เล  | .ze     | LDC_Start_          | main st | rcmp              | cxa_atexit          | st          | ack_cr       | ик_таці             |              | C++.50.6         |                       |              | SCXX_3.4.      | 29 GL  | IRCYY   | 5.4 GLIBU        | _2.4 6     | PLIRC_2 | . 34    |
|                         |             |         |                     |         |                   | <br>                | y y w       | – u u<br>• – | ALLI LLI<br>171     | <u>د)</u> ه  | 111 ULI<br>1 011 | עם שיים<br>היים שייים | 400 D        | រចា ខេររ       | 0      |   | m A              | ÈD         | 171     |         |
| שים שים<br>היות כת      | -a a ea     | പ്പ     | נס נט בנטג<br>רס רס |         | = ,<br>62         | ມ ແ<br>ກ            |             | n=           |                     | Eu           | i h=             |                       |              | ALCI LI        | 6      |   | шe               | <b>C</b> 1 | L       |         |
| دة 10                   |             | φ:      |                     |         | a:                |                     |             |              |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
| e:<br>مک                | 5           |         |                     |         |                   |                     |             |              |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
| d2                      | E<br>R      |         |                     |         |                   |                     |             |              |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
| 69                      | <u>ت</u>    |         | ۰`                  |         |                   | <b>C</b> II         |             |              |                     | ~>           |                  |                       |              |                |        |   | >                |            |         |         |
| • <u>&gt;</u>           |             | ຶ >     | ติ                  |         | ۵۶                |                     |             |              |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
|                         |             |         |                     |         |                   |                     |             |              |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
| ດ໌ຫຼາຍມໍHfງຫຼາ⊦ເຫບໍ່/   | HÀt®ÿF      | HFÄDÃ   | ÿ57/                | کت%[/ ۱ | මම රමමර           | h òéáÿÿ             | Via 6 ia 10 | úh®          | òéÑÿÿÿI             | aóiaidíúhia  | òéÁÿÿ            | Veóselúh              | a òé+        |                | ര്ത    | é:vvv   | ว์ติติน์หติ      | òé vừ v    | /BóBBÚh | 2       |
| òéBŸŸŸBÓBBúòŸ%          | (a) (a)     | ÓBBÚÒS  | 7%õ. 00D            | ÓBBÚÒV  | %í. 00            | D ÓBBÚÒŸ%           | Â. D        | D ór         | ı⊡úòÿ%%             | . 88D        | ó@@úòv%          | u. DDD                | ÓDDÚÒ        | 7%. DDD        | ÓRRÚ   | òÿ%¥.   | DOD ÓDD          | ]ú1íI‰Ñ    | í^H‰    |         |
| âHfäðPTE1À1ÉH⊠          | ]=Ê ÿ⊠^     | . ôf.0  | 10., HO             | =1. H0  | 2°. H9            | øt⊡H<⊡v.            | HÀt         | i.           | ànn€                | Ãnn€         | H0=%.            | H05                   | H)bH%        | SHÁi?HÁøD      | HELÆHÑ | btDH <d< td=""><td>E. H.At</td><td>İVàfeed</td><td>) ä⊡€</td><td></td></d<> | E. H.At          | İVàfeed    | ) ä⊡€   |         |
| ó⊠⊡ú€=0 u+UH            | lf=ò- ́⊦    | ‰ât     |                     |         |                   |                     |             | Ĩ            |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
| H<=&. è¹bÿÿèd           | VVVA⊡0      | 0 1Ã00  | Ã⊡⊡€ ć              | ⊠⊡úéwÿÿ | ÿó⊠⊡úUH           | kåH⊡ì°⊡ d           | H< 🛛 % (    | H‰E          | ø1ÀCYI              | oÿÿStrC      | fC1bööM          | pÆ bÿÿ                | H }f57       | fa3H≌60f       | 3963a  | H‰0ÿÿ'  | ÿH‰              |            |         |         |
| •8ÿÿÿH cee5d3c          | 4Hº6cdee    | 3ecH‱6  | ₩ŸŸŸH‰•HŸ           | VH 2d67 | ,<br>1076Hº2      | {FTC SKH8.          | PŸŸŸĤ       | ‰•XŸŸŸ       | HC` ŸŸ              | L HC         | hÿÿÿ             | HCDVV                 | Ü НС.        | .xÿÿÿ          | HCE€   | HCE   | HCE              | i HG       | CE~     |         |
| HÇE HÇE"                | HÇE°        | HÇE.    | HÇEÀ                | HÇEÈ    | HÇEÐ              | HÇEØ                | HÇE         | à⊦           | IÇEè                | HÇEð         | HEE 2            |                       |              |                |        |   |                  |            |         |         |
| H&ÆHDDä, H&             | çè∖ýÿÿH⊵    | B•      |                     |         |                   |                     |             |              |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
| H‰ÆHDDË, H‰             | ÇèCýÿÿH     | 0±      |                     |         |                   |                     |             |              |                     |              |                  |                       |              |                |        |   |                  |            |         |         |
| H‰ÆH⊉⊉², H‰             | Çè*ýÿÿH⊵    | l`þÿÿH≋ | 6ÆH⊡⊇¹- ⊦           | ‰Çè5⊡ I | H <b>⊡•`</b> þÿÿl | Н⊡YþÿÿН‰Ö           | H䂏(         | ýÿÿ‰…⊺       | þÿÿ <sub>f%</sub> t | oÿÿ uXH      | 22 <b>i</b>      |                       |              |                |        |   |                  |            |         |         |
| ประ <i>ก</i> บกกรุง ประ | CADIIIIII.  | ໜ້າ ບະ  | -öus-còfiiiii       |         | ประศุมภาพ         | UP-CAX00            | 00, na      | , usio       | ue-cheili           | 102 105      | la la            |                       |              |                |        |   |                  |            |         |         |

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

| -  |  |
|----|--|
| G  | <pre>void frame_dummy()</pre>  |
| 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)   |
| i5 | int64_ts   |
| 5  | builtin_strncpy(dest: &s, src: "}f57cfa360f3963acee5d3c46cdee3ec2d6710762{FTC_SKL", n: 0xc                             |
| if | std::operator<< <std::char_traits<char> &gt;(out: &amp;std::cout,s: "*****CHECK PASSWORD******</std::char_traits<char> |
| 8' | std::operator<< <std::char_traits<char> &gt;(out: &amp;std::cout,s: "First Password: \n")</std::char_traits<char>      |
| 11 | std::operator<< <std::char_traits<char> &gt;(out: &amp;std::cout,s: "Second Password :")</std::char_traits<char>       |
| ia | void var_1a8   |
| a  | std::operator>> <char>(&amp;std::cin, &amp;var_1a8)</char>   |





#### Lalu kita reverse textnya



Setelah direverse textny terdapat flag pada TASK-1





## CRYPTOGRAPHY

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





Setelah di decrypt dengan decryptor terdapat flag pada TASK-1



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

| Results   | [@ 2 2 ± ∓ ×]   | XOR DECODER   |
|---|---|---|
| Bruteforce attempt. C<br>dis<br>[ Hexadecimal I<br>ASCII output limited to printa<br>ASCII characters replaced by 4 | only relevant results are<br>played.<br><ey ]<br="" plain="" text=""  ="">ble characters (control chars and non-<br/>∳)</ey>                            | * TEXT TO BE XORED (MULTIPLIED BY XOR)<br>ASCII Printable Characters (Autome<br>YAFJVASn-&"#t"-"pw# qp%\$qts%&-' til'#vss%\$1#p wsh   |
| t1  | †↓  | ENCRYPTION/DECRYPTION METHOD  |
| 11  | HOW[GPB�<732e3<3af21<br>`a45`eb47<61e0062gbb4<br>502a1fby��<br>KLTXDSA 7401f0?<br>0be12cb76cfa74?<br>52f3351daa7631b2eaz�<br>�<br>LKS_CTF{8376a787eb65d | <ul> <li>AUTOMATIC (BRUTEFORCE 1 TO 16 BYTES)?</li> <li>USE THE BINARY KEY 10110111</li> <li>USE THE HEXADECIMAL KEY 7F</li> <li>USE THE ASCII KEY XOR</li> <li>KNOWING THE KEY SIZE (IN BYTES) 1</li> <li>* RESULTS FORMAT A ASCII (PRINTABLE) CHARACTERS</li> <li>HEXADECIMAL 00-7F-FF</li> </ul> |
| 15  | e01daf03825a4426cff01<br>46e5bf}��<br>OHP\@wEx;045b4;4fa56g   | <ul> <li>DECIMAL 0-127-255</li> <li>OCTAL 000-177-377</li> <li>BINARY 00000000-11111111</li> </ul>  |
| 16  | f32gbe30;16b7715`ee32<br>75f6ae~��  | Integer NUMBER File to DOWNLOAD   |
| 18  | AF^RNYKV5>:;l:5:ho;81<br>h= <ilk=>5?8199?;nkk=<br/>&lt;9;h8okp��</ilk=>   | ENCRYPT / DECRYPT   |



## **STEGANOGRAPHY**



#### Setelah di cek menggunakan exiftool terdapat flag pada TASK-1

| <b>root@kali</b> )-[/home/abdurrohm                  | an/Downloads |           |                 |                 | 4 Mar 2024       |  |  |  |  |  |  |
|--|--------------|-----------|-----------------|-----------------|------------------|--|--|--|--|--|--|
| Chall  |              |           | 'Onen Me.ndf'   | 'Pantai(1)'     | OR nng           |  |  |  |  |  |  |
| Chall-20240425T0146097-001.zip                       | Mekar, png   |           | Pantai          | Perbandingan    | Untitled.ineg    |  |  |  |  |  |  |
|  |              |           |                 | . croandingan   | - Merzoza - Ares |  |  |  |  |  |  |
| <pre>(root@kali)-[/home/abdurrohman/Downloads]</pre> |              |           |                 |                 |                  |  |  |  |  |  |  |
| 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-rr     |           |                 |                 |                  |  |  |  |  |  |  |
| 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/In | flate     |                 |                 |                  |  |  |  |  |  |  |
| Filter   | : Adaptive   |           |                 |                 |                  |  |  |  |  |  |  |
| Interlace  | : Noninterla | ced       |                 |                 |                  |  |  |  |  |  |  |
| Pixels Per Unit X                                    | : 3780       |           |                 |                 |                  |  |  |  |  |  |  |
| Pixels Per Unit Y                                    | : 3780       |           |                 |                 |                  |  |  |  |  |  |  |
| Pixel Units  | : meters     |           |                 |                 |                  |  |  |  |  |  |  |
| Comment  | : LKS_CTF{09 | 9a6037dc5 | 5d9c49037073721 | c73bc4965e32d4} |                  |  |  |  |  |  |  |
| Image Size   | : 624×352    |           |                 |                 |                  |  |  |  |  |  |  |
| Megapixels   | : 0.220      |           |                 |                 |                  |  |  |  |  |  |  |
| (root@kali)-[/home/abdurrohman/Downloads]            |              |           |                 |                 |                  |  |  |  |  |  |  |





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 gatcha.zip

|  | <b>∢</b> n      | iga C         | .hall[1].txt         | stegs            | ×     | ►   | +        |      |      |  | $\times$ |
|--|-----------------|---------------|----------------------|------------------|-------|-----|----------|------|------|--|----------|
| File   | Edit            | V             | iew                  |                  |       |     |          |      |      |  | <b>1</b> |
| <pre>'tE' Ó2i ''6E&lt;+X`-%KE&gt;JÄdû7%nE,C'ì1Êcc/³Â&lt;49àxuQ"gnŸ4)ÿ à? \$L3þEÿ ý<sup>2</sup>ê°=e4r0A\$@EðEvIòE²:x^%n‰ßÿ Eÿ ª %¦"6;ñôSZETECE4ØõõMEdE',ÙE@"VÜlù§fÍ^ù·ù¤cjY4p· ‡DlvÏnVE,ÇÃUEÏãEtx·šE++fŸEXõà:8Ü@.»7&lt;ð¶}92á,iEÃ 1Eñí¦A[ÔLnEÂ&amp;ì@ÄMù*Ü™ö7±Q"Ìóì´âପEEfEdÎ1¦,ÁÔ¥EiWHE[ĐEbž<br/>ÌwØ*PÜkV/E#(ñA &amp;ä\+*zâ‡ÈHBÜ**Ø)±E%ÈE¤' ]'»- ÏNTÜÊ)ú¥!þE;3"õGEEÀ"pê@ú(EJ-</pre> |                 |               |                      |                  |       |     |          |      |      |  |          |
| aR@ÇÆFe⊡@ @aF@@E*`@u;x*Du*ASs*;cÐM5ZEa~47uI¢¶‰b~<br>Rð,µ£±ï dxÙ\$@@.Šìk@L¥ï¹@@²4 ŠÞ@'%"", 2r@@ñ¨,"j@@ÿ Â<Þo±C  |                 |               |                      |                  |       |     |          |      |      |  |          |
| ~\$⊡u mÕ2⊡å⊡€:%⊡q≏ à#5H-Å,SÙ⊡9á⊡u²p⊡⊇>t2 Uš8šÅHÉp«'<br>p⊡:⊡%(ùRükDA=R/ÙIü",,Q⊡íÂ ÉŠpµ\$}Sd ⊡<br>~X¢È⊡r3ð¦ü+R,Aê⊡åEk⊡϶É^ÈA⊡⊡ êbMĐÂd ⊡%Jý⊡~ŠÅ*,Ï<br>⊡TÉ⊡⊡X:(ï}"ŽR⊡E{n J:fùD‡t®¦ xZ⊡r⊡f~‰¿<br>`Í⊵þª⊇þ©! ž}óç⊡⊇<ôJäò¢⊡-(× §Ü,,Špµ\$<br><sup>°</sup> O⊡DüI õR⊡EA⊡<br>'À^ì•Èå!ÉL´⊡éþJ⊡‰I^&9²r   |                 |               |                      |                  |       |     |          |      |      |  |          |
| j⊡9á`<br>⊡‴—ÿÙ   | ŽÖLJ4<br>IPASSI | EKð  <br>NYA: | ê;⊡~r^ÔF<br>curug_pa | PfèwV<br>arigi_ι | nih_t | oos |          |      |      |  | Î        |
| Ln 1, C  | ol 1            | 71            | ,514 charact         | ers .            | 100%  | Ma  | acintosh | (CR) | ANSI |  |          |



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

🔞 Cari sumber gambar



Ġ Cari

📋 Salin teks 🤄 Terjemahkan

LKS\_CTF{836e39330b42c3503734c46c61fcc05a23e0bfa5}

# WEB EXPLOITATION

#### 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:

# DIGITAL FORENSICS

#### **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:** <u>https://drive.google.com/drive/folders/1TfO24HEmoaqZ-</u> 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:** <u>https://drive.google.com/drive/folders/1DnluBiiz8VYD\_OrqHRX6EPmr70IT0IaS?</u> <u>usp=sharing</u>

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\_9PrlgHN2ARK? usp=sharing

Dokumentasi, Jawaban dan Pembahasan:

# REVERSE ENGINEERING

#### **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:** <u>https://drive.google.com/drive/folders/1VRqIXr00ayhsdBzAv6yOFHbzZF1ID7i\_?</u> <u>usp=sharing</u>

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:** <u>https://drive.google.com/drive/folders/1J4YTqe10iMho79nKyIjoKqxtQRC8HuHn?</u> <u>usp=sharing</u>

#### 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:** <u>https://drive.google.com/drive/folders/10jbDqoqi1F8wgdJLlxM0y-lBez7dUaTe?</u> 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/10jIqW8uOZ516j7r9qs-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:** <u>https://drive.google.com/drive/folders/1Wb7IllBjZyGAafZOatJoiXYvkdyCbQWy?</u> <u>usp=sharing</u>

Dokumentasi, Jawaban dan Penjelasan: