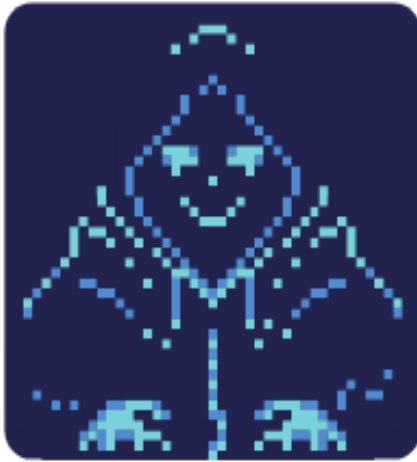


TED CTF WRITEUP



AVERAGE INTEL
ENJOYERS

exzettabyte (Paska Parahita)
banua (Muhammad Ichwan)
clonewriter (Ananda Fikri Ijlal Akbar)

UNIVERSITAS AMIKOM YOGYAKARTA

[Network Analyze]

Baby Shark

Challenge


11 Solves

×

Baby Shark

5

Author : fajr

 hiu.pcapng

Flag

Submit

Deskripsi Soal

Tidak diberikan deskripsi pada soal, hanya disertakan file hiu.pcapng saja

Solusi

Diberikan sebuah file hiu.pcapng, lalu kami melakukan analisa paket data yang ada di file tersebut menggunakan wireshark, terlihat banyak capture paket HTTP, kemudian kami melakukan filter `http.response.code == 200`, pada tcp.stream eq 5 nampak seperti format flag yang terenkripsi rot13, copy text tersebut kemudian coba decrypt menggunakan rot13 maka didapatkan flagnya

```
HTTP/1.1 200 OK
Date: Mon, 10 Aug 2020 01:51:45 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Fri, 07 Aug 2020 00:45:02 GMT
ETag: "2f-5ac3eea4fcf01"
Accept-Ranges: bytes
Content-Length: 47
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Vav nqnynu syntaln PGSGRQ2021{g4y1 U1hhhhhhh}.
```

Results



Ini adalah flagnya CTFTED2021{t4l1
H1uuuuuuuuu}.

ROT-13 Cipher - [dCode](#)

Flag : CTFTED2021{t4l1 H1uuuuuuuuu}

[Stegano]

Dear Friend

Dear Friend

5

Dear my friend...

Author : Vibonacci#5281

 message.txt

Flag

Submit

Deskripsi soal

Dear my friend...

Solusi

Diberikan sebuah file message.txt yang berisi pesan sebagai berikut :

Dear Friend , We know you are interested in receiving cutting-edge intelligence . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail !

This mail is being sent in compliance with Senate bill 2416 ; Title 5 , Section 302 ! This is not a get rich scheme ! Why work for somebody else when you can become rich as few as 43 MONTHS ! Have you ever noticed how long the line-ups are at bank machines plus people will do almost anything to avoid mailing their bills . Well, now is your chance to capitalize on this ! We will help you decrease perceived waiting time by 200% & decrease perceived waiting time by 150% . You can begin at absolutely no cost to you ! But don't believe us . Ms Anderson who resides in Rhode Island tried us and says "I was skeptical but it worked for me" ! We are licensed to operate in all states ! If not for you then for your loved ones - act now . Sign up a friend and you get half off ! Thanks . Dear Friend ; Your email address has been submitted to us indicating your interest in our publication ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 2616 , Title 6 ; Section 309 ! This is not multi-level marketing . Why work for somebody else when you can become rich in 69 weeks ! Have you ever noticed how long the line-ups are at bank machines and nobody is getting any younger ! Well, now is your chance to capitalize on this ! WE will help YOU deliver goods right to the customer's doorstep & increase customer response by 160% ! You can begin at absolutely no cost to you ! But don't believe us . Ms Simpson who resides in Wisconsin tried us and says "Now I'm rich, Rich, RICH" ! We assure you that we operate within all applicable laws ! We implore you - act now ! Sign up a friend and your friend will be rich too ! Cheers . Dear Salaryman , Especially for you - this red-hot announcement . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1623 , Title 5 ; Section 306 ! This is a legitimate business proposal ! Why work for somebody else when you can become rich in 50 WEEKS . Have you ever noticed more people than ever are surfing the web and the baby boomers are more demanding than their parents . Well, now is your chance to capitalize on this . We will help you use credit cards on your website & deliver goods right to the customer's doorstep . You can begin at absolutely no cost to you . But don't believe us ! Mrs Anderson who resides in Tennessee tried us and says "I was skeptical but it worked for me" ! This offer is 100% legal . Because the Internet operates on "Internet time" you must hurry ! Sign up a friend

and you get half off ! Cheers . Dear Business person
; We know you are interested in receiving red-hot announcement
. This is a one time mailing there is no need to request
removal if you won't want any more ! This mail is being
sent in compliance with Senate bill 1618 , Title 4
; Section 302 ! This is NOT unsolicited bulk mail .
Why work for somebody else when you can become rich
in 54 WEEKS ! Have you ever noticed nobody is getting
any younger and more people than ever are surfing the
web ! Well, now is your chance to capitalize on this
. We will help you process your orders within seconds
& process your orders within seconds ! The best thing
about our system is that it is absolutely risk free
for you . But don't believe us . Mrs Simpson of Ohio
tried us and says "I was skeptical but it worked for
me" ! We are a BBB member in good standing . If not
for you then for your LOVED ONES - act now . Sign up
a friend and your friend will be rich too ! God Bless
! Dear Salaryman , Your email address has been submitted
to us indicating your interest in our newsletter .
If you are not interested in our publications and wish
to be removed from our lists, simply do NOT respond
and ignore this mail ! This mail is being sent in compliance
with Senate bill 1626 ; Title 8 ; Section 304 ! This
is not a get rich scheme ! Why work for somebody else
when you can become rich as few as 72 weeks ! Have
you ever noticed nearly every commercial on television
has a .com on in it and more people than ever are surfing
the web ! Well, now is your chance to capitalize on
this . We will help you process your orders within
seconds plus turn your business into an E-BUSINESS
! You can begin at absolutely no cost to you ! But
don't believe us ! Mr Ames of Georgia tried us and
says "I was skeptical but it worked for me" ! We assure
you that we operate within all applicable laws . You
will blame yourself forever if you don't order now
. Sign up a friend and your friend will be rich too
! Thanks !

Hal yang dapat kita amati adalah bahwa pada text tersebut mengandung metode pertama pada dunia steganografi, yaitu text steganografi. Hal yang dilakukan adalah kita mencari decoder untuk text steganografi. Kami menemukan online tool yaitu :
<https://www.spammimic.com/>

[Encode](#)[Decode](#)[Explanation](#)[Credits](#)[FAQ & Feedback](#)[Terms](#)[Français](#)

Decode

Paste in a spam-encoded message:

a friend and your friend will be rich too ! God Bless
! Dear Salaryman , Your email address has been submitted
to us indicating your interest in our newsletter .
If you are not interested in our publications and wish
to be removed from our lists, simply do NOT respond
and ignore this mail ! This mail is being sent in compliance
with Senate bill 1626 ; Title 8 ; Section 304 ! This
is not a get rich scheme ! Why work for somebody else
when you can become rich as few as 72 weeks ! Have
you ever noticed nearly every commercial on television
has a .com on in it and more people than ever are surfing
the web ! Well, now is your chance to capitalize on
this . We will help you process your orders within
seconds plus turn your business into an E-BUSINESS
! You can begin at absolutely no cost to you ! But
don't believe us ! Mr Ames of Georgia tried us and
says "I was skeptical but it worked for me" ! We assure
you that we operate within all applicable laws . You
will blame yourself forever if you don't order now
. Sign up a friend and your friend will be rich too
! Thanks !

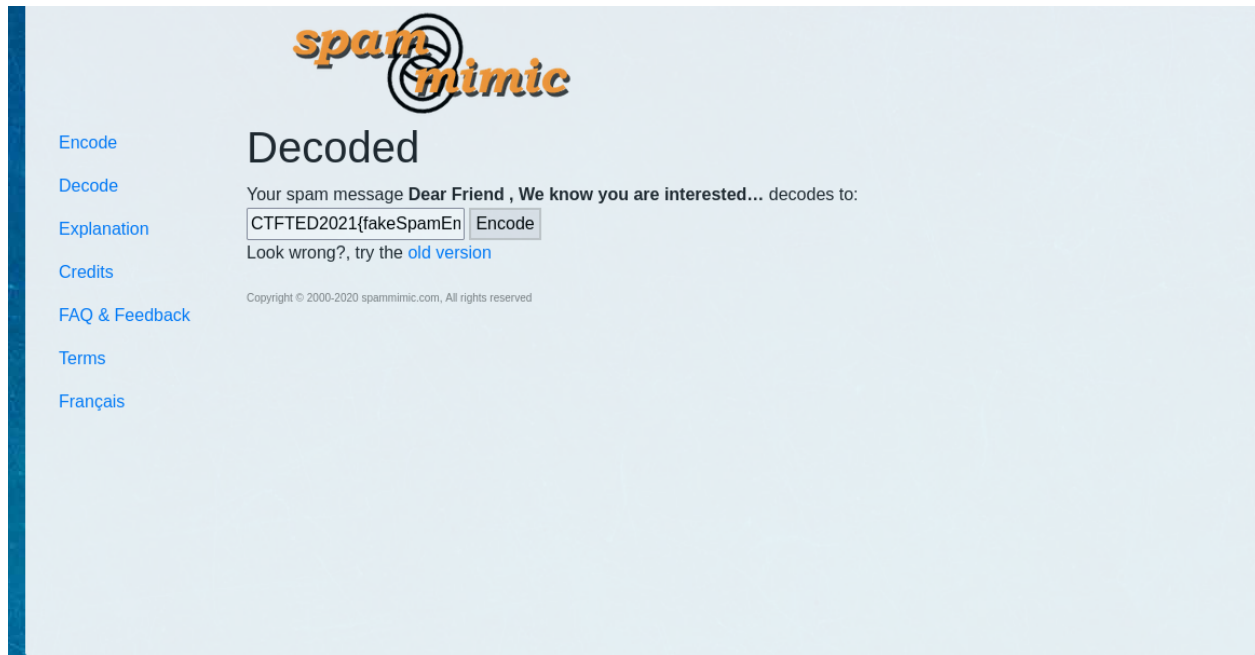
Decode

Alternate decodings:

- [Decode spam with a password](#)
- [Decode fake spreadsheet](#) new
- [Decode fake PGP](#)
- [Decode fake Russian](#)
- [Decode space](#)

Copyright © 2000-2020 spammimic.com, All rights reserved

Kemudian kami copas text pada spammimic dan muncul hasil decode dari text steganography



Flag : CTFTED2021{fakeSpamEmail_turn_out_to_be_important_message}

The Sound is Waving Toward You

Challenge 2 Solves ×

The sound is Waving
toward you
30

The sound that you cant hear, the flag that you cant see. That's
our beloved LaSBchool's media.

Author : Vibonacci#5281

Deskripsi Soal

The sound that you cant hear, the flag that you cant see. That's our beloved LaSBchool's media.

**Update : Terdapat pembaharuan untuk soal The sound is Waving toward you dan hint2 , silahkan download ulang filenya. Silahkan ulangi langkah yang sama (tidak ada perubahan pada cara solve). Perbedaan terdapat pada hasil yg diberikan file baru, jika langkah sudah benar, pada file yg baru akan menyediakan link untuk download file pada hasil.*

Solusi

Diberikan sebuah file wav dengan clue LSB terdapat pada deskripsi soal, kemudian kami mencoba melakukan pencarian tools stegolsb untuk file wav didapatkan sebuah tools dari

(<https://github.com/ragibson/Steganography>). Untuk penggunaannya cukup mudah dimana kami menambahkan options recover dan juga lsb-count, karena lsb-count nya tidak diketahui berapa jadi kami melakukan bruteforce manual didapatkan pada count 7 script python subst_cipher dan terdapat link gdrive. Buka gdrive tersebut terdapat file Ringtoned.wav, download file tersebut. Karena pada hint kedua disebutkan bahwa "Different files, use different amount of LSBs." kami menduga lsb count berada di nilai yang berbeda, coba bruteforce manual lagi file yang didapat dari drive tadi didapatkan flag pada count 13 namun masih ada beberapa huruf yang salah, karena di file pertama terdapat output script subst python, gunakan script tersebut, mapping nya kami tukar antara key dan value dan flag asli berhasil di recover.

```
Shell-$ stegolsb wavsteg -r -i file.wav -o output1.py -n 7 -b 1000
Files read                               in 0.00s
Recovered 1000 bytes                     in 0.00s
Written output file                       in 0.00s
```

```
open("Ringtoned.wav", "wb+").write(new_file)
#Ringtoned.wav = https://drive.google.com/file/d/1gJVqN97nZ8429aRGtLnubkcz8FZVo3Ec/view?usp=sharing
```

```
Shell-$ stegolsb wavsteg -r -i Ringtoned.wav -o output2.txt -n 13 -b 1000
Files read                               in 0.00s
Recovered 1000 bytes                     in 0.00s
Written output file                       in 0.00s
```

```
[16:21:15]-banua@basiber:~/Downloads/TED/stegano/thesound
```

```
Shell-$ cat output2.txt
```

```
CTFTED2021{significant_bit_on_wav_file_plus_little_mapping_char_encryption}
```

```
[16:25:55]-banua@basiber:~/Downloads/TED/stegano/thesound
```

```
Shell-$ stegolsb wavsteg -r -i Ringtoned-fixed.wav -o flag.txt -n 13 -b 1000
Files read                               in 0.00s
Recovered 1000 bytes                     in 0.00s
Written output file                       in 0.00s
```

```
[16:25:58]-banua@basiber:~/Downloads/TED/stegano/thesound
```

```
Shell-$ cat flag.txt
```

```
CTFTED2021{significant_bit_on_wav_file_plus_little_mapping_char_encryption}
```

Script Solver :

Dict mapping nya masih default tetapi kami tukar key dan value nya dengan cara code seperti dibawah ini

```
new_dict = {}
for k, v in letter_map.items():
    new_dict[v] = k

def subst_cipher(letter_map, text):
    return "".join(letter_map.get(c, c) for c in text)

file = open('Ringtoned.wav', 'rb').read()
new_file = file[:100] + subst_cipher(new_dict, file[100:])
open("Ringtoned-fixed.wav", "wb+").write(new_file)
```

Flag : CTFTED2021{significant_bit_on_wav_file_plus_little_mapping_char_encryption}

Congratulations

Challenge

8 Solves



Congratulations

5

Thanks for participating in this challenge, we got you a certificate.

Author : Vibonacci#5281

 Congratulati...

Flag

Submit

Deskripsi Soal

Thanks for participating in this challenge, we got you a certificate. Dan juga sebuah file zip

Solusi

Diberikan sebuah file Congratulations.zip, lakukan ekstrak file zip tersebut kemudian didapatkan output 2 file pdf. Kami melakukan pengecekan file tersebut dengan command "file" nampak file "anotherCertificate.pdf" itu adalah file png. Ganti format file another tersebut dari pdf menjadi png kemudian coba buka terlihat pada bagian atas kalimat "Certificate" namun dengan transparansi yang minim, langsung saja kami coba buka menggunakan stegsolve didapatkan potongan flag pertama pada Red Plane 1 yaitu "CTFTED2021{embed_dat", karena potongan flag pertama terdapat kata "embed_dat" langsung terlintas untuk mencoba cek file png tersebut menggunakan binwalk, terlihat file pdf dan png, langsung saja ekstrak dan cek informasi semua file dengan "file" terdapat sebuah file png, tambahkan ekstensi png dan buka didapatkan flag terakhir.

CTFTED2021{embed_dat



```
[15:23:35]-banua@basiber:~/Downloads/TED/stegano/congrats
Shell-$ binwalk -e anotherCertificate.pdf.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 1366 x 768, 8-bit/color RGBA, non-interlaced
57	0x39	Zlib compressed data, compressed
862428	0xD28DC	PDF document, version: "1.1"
863271	0xD2C27	Zlib compressed data, default compression
863278	0xD2C2E	PNG image, 496 x 496, 8-bit/color RGB, non-interlaced
863334	0xD2C66	Zlib compressed data, default compression

D2C27: PNG image data, 496 x 496, 8-bit/color RGB, non-interlaced



Flag : CTFTED2021{embed_data_in_pdf}

[Web]

Ladu Singh

Deskripsi soal:

link : <http://104.43.91.41:10026/>

Solusi:

Diberikan sebuah website inspektur ladu singh, kita diminta untuk membantunya , potongan flag pertama berada di index

```
➥ curl http://104.43.91.41:10026/
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, ini
<link rel="stylesheet" href="/static/style.css">
<script src="/static/script.js"></script>
</head>
<body>
  
</body>
</html>
```

Potongan Flag kedua ada di style.css

```
/* part 2 _p4ngg1l_4ku_4n */
```

Potongan flag terakhir ada di script.js

```
➥ curl http://104.43.91.41:10026/static/script.js
(async()=>{await new Promise((e=>window.addEventLis
ocument.querySelector("form").addEventListener("sub
Default();const r={u:"input[name=username]",p:"inpu
t={};for(const e in r)t[e]=btoa(document.querySelec
place(/=/g,"");return"YWRtaW4"!==t.u?alert("Incorre
VEVEMjAyMXtMMGcxbiBING55NGw0aCBUMVBVNG59"!==t.p?ale
ord"):void alert(`Correct Password! Your flag is ${
});
// part 3 4k_k3c1l_p4m4n}
```

Flag : CTFTED2021{j4ng4_p4ngg1l_4ku_4n4k_k3c1l_p4m4n}

[Web]

Login Bang

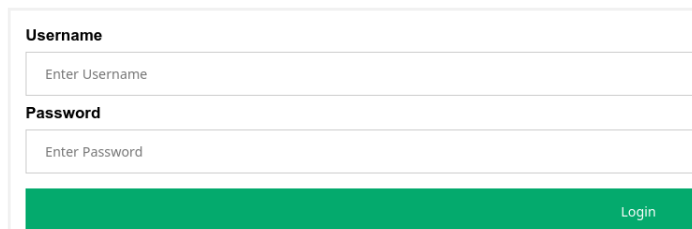
Deskripsi soal:

Bantu saya login di web ini bang,, Link : <http://104.43.91.41:10025/>

Solusi:

Diberikan sebuah website berupa halaman login

Login Form



The image shows a simple login form. It has two input fields: one labeled 'Username' with the placeholder text 'Enter Username', and another labeled 'Password' with the placeholder text 'Enter Password'. Below these fields is a green button labeled 'Login'.

Ketika dilakukan pengecekan pada js didapat password yang diencode ke dalam base64. Decode lalu didapatkan flagnya.

```
⇒ curl http://104.43.91.41:10025/static/script.js
(async()=>{await new Promise((e=>window.addEventListener("load",e)),document.querySelector("form").addEventListener("submit",(e=>{e.preventDefault();const r={u:"input[name=username]",p:"input[name=password]"},t={};for(const e in r)t[e]=btoa(document.querySelector(r[e]).value).replace(/=/g,"");return"YWRtaW4"!==t.u?alert("Incorrect Username"):"Q1RGVEVEMjAyMXtMMGcxbiBING55NGw0aCBUMVBVNG59"!==t.p?alert("Incorrect Password"):void alert(`Correct Password! Your flag is ${atob(t.p)}.`)}})});
exzettabyte@Avadra_Kedavra:~/Documents/ted|
⇒ echo Q1RGVEVEMjAyMXtMMGcxbiBING55NGw0aCBUMVBVNG59|base64 -d
CTFTED2021{L0g1n H4ny4l4h T1PU4n}
```

Flag : CTFTED2021{L0g1n H4ny4l4h T1PU4n}

[Forensic]

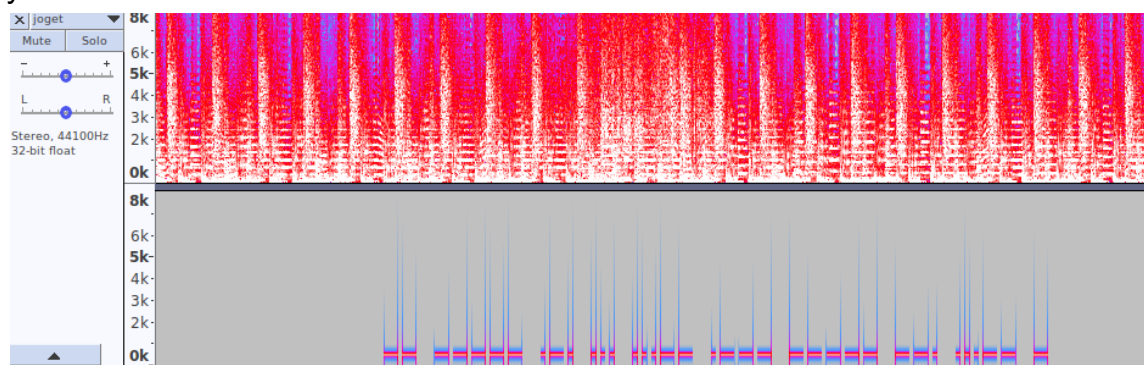
Dance

Deskripsi Soal:

Masukkan nilai yang ditemukan pada template flag `CTFTED2021{}`

Solusi:

Diberikan sebuah file wav. Ketika dilakukan pengecekan pada spectogramnya, audio berupa stereo dengan channel yang satunya tampak seperti representasi dari morse yaitu . dan - .



Morsenya seperti ini -- ----- .- -- .- ----- --. ...- - . Decode maka akan didapat flagnya.

↑ ↓	↑ ↓
{ . - } ↔ { - . }	TN0NTT&T
{ . - } ↔ { - . }	EA0AEE0E
{ - . } ↔ { - . }	M0RS3J0G3T
{ . - } ↔ { - . }	I5K08B5U8E
{ - . } ↔ { - . }	0ETTU0TF
{ - . } ↔ { - . }	0TEEG0EQ

Flag : `CTFTED2021{M0RS3J0G3T}`

[Forensic]

Crash

Deskripsi Soal:

Laptop teman saya, pak @dhipz mengalami crash. Doi lagi sibuk skripsian jadi tidak sempat benerin sendiri. Katanya yang bantu benerin dan balikin file file nya ntar dapet flag gan.

<https://drive.google.com/file/d/15D3zp7oHRqyZY2rkU1LQqS8ee9ty88Ap/view?usp=sharing>

Solusi:

Diberikan memory dump, dilakukan identifikasi os profile secara manual karena dengan plugin imageinfo tidak mendapat hasil, diduga os profile merupakan linux, dengan strings didapat informasi bahwa memory dump dari os ubuntu 20.04.1 LTS

```
exzettabyte@Avadra_Kedavra:~/Documents/ted|  
⇒ strings mem.raw|grep "VERSION=" -A4
```

```
VERSION="20.04.1 LTS (Focal Fossa)"  
ID=ubuntu  
ID_LIKE=debian  
PRETTY_NAME="Ubuntu 20.04.1 LTS"  
VERSION_ID="20.04"  
--
```

Untuk versi kernelnya 5.4.0-42-generic

```
⇒ strings mem.raw|grep "BOOT_IMAGE" -m1  
BOOT_IMAGE=/boot/vmlinuz-5.4.0-42-generic root=UUID=af569b8a-eebe-4145-892d-0fcdd9fce88b ro
```

Sebelumnya saya memiliki os profile Ubuntu 20.0.4

```
⇒ volatility --info|grep Ubuntu20  
Volatility Foundation Volatility Framework 2.6.1  
LinuxUbuntu20_04x64 - A Profile for Linux Ubuntu20.04  
x64
```

Ketika dicoba dengan os profile ubuntu 20.0.4 ternyata bisa, jadi tidak perlu repot untuk membuat os profile ubuntu 20.0.4.1. Pertama dilakukan recover bash history, didapat hasil command wget dengan file flag.zip.

```
⇒ volatility -f mem.raw --profile=LinuxUbuntu20_04x64 linux_bash  
Volatility Foundation Volatility Framework 2.6.1  
Pid      Name      Command Time                               Command  
-----  
898 bash  2021-11-10 08:18:12 UTC+0000    ls  
898 bash  2021-11-10 08:19:19 UTC+0000    ls -lah  
898 bash  2021-11-10 08:19:19 UTC+0000    ls  
898 bash  2021-11-10 08:19:56 UTC+0000    ls  
898 bash  2021-11-10 08:20:28 UTC+0000    wget 192.168.100.55:8000/flag.zip
```

Mencari tau path dari user dengan strings dan grep sebaris root dari passwd maka akan mendapatkan informasi pathnya.

```
exzettabyte@Avadra_Kedavra:~/Documents/ted|  
⇒ strings mem.raw|grep "root:x:0:0:root:/root:/bin/bash" -A30 -m1|tail -1  
user:x:1000:1000:,,,:/home/user:/bin/bash
```

Kami menduga flag.zip berada pada home. Menggunakan plugin linux_find_file untuk mendapatkan inode dari flag.zip yang nantinya digunakan untuk dump.

```
exzettabyte@Avadra_Kedavra:~/Documents/ted|  
⇒ volatility -f mem.raw --profile=LinuxUbuntu20_04x64 linux_find_file  
-F "/home/user/flag.zip"  
Volatility Foundation Volatility Framework 2.6.1  
Inode Number          Inode File Path  
-----  
393231 0xffff9612c47dcdf8 /home/user/flag.zip
```

Dump flag.zip dengan inode yang sudah didapat

```
exzettabyte@Avadra_Kedavra:~/Documents/ted|  
⇒ volatility -f mem.raw --profile=LinuxUbuntu20_04x64 linux_find_file  
-i 0xffff9612c47dcdf8 -o ~/Documents/ted/flag.zip  
Volatility Foundation Volatility Framework 2.6.1
```

Extract dengan 7z, terlihat extract error namun sebenarnya berhasil. Didapat flag.png yang berisi flag.

```
Extracting archive: flag.zip  
ERRORS:  
Headers Error  
--  
Path = flag.zip  
Type = zip  
ERRORS:  
Headers Error  
Physical Size = 44504  
  
Archives with Errors: 1
```

CTFTED2021{simple_profile_creation_and_fake_password}

Flag : CTFTED2021{simple_profile_creation_and_fake_password}

[Reverse]

Simple Login

Deskripsi Soal:

Didi lupa dengan password program yang telah dibuatnya, mau kah kamu membantu didi

Solusi:

Diberikan sebuah file executable simple_login, coba execute file tersebut disuruh memasukkan password tetapi tidak diketahui passwordnya, kami mencoba menjalankan dengan ltrace didapatkan password comparison nya dengan "thecorrectpassword", jalankan kembali file simple_login kemudian masukkan password yang didapat tadi terdapat output base64, decode base64 didapatkan flag nya.

```
[16:46:26]-banua@basiber:~/Downloads
Shell-$ ltrace ./simple_login
puts("\n Masukkan password : "
  Masukkan password :
)
      = 23
gets(0x7ffc5fc4ed10, 0x11f62a0, 0, 0x7fdf36f191e7password
) = 0x7ffc5fc4ed10
strcmp("password", "thecorrectpassword")      = -4
puts("\n password salah "
  password salah
)
      = 18
+++ exited (status 0) +++
```

```
[16:45:40]-banua@basiber:~/Downloads
Shell-$ ./simple_login

  Masukkan password :
thecorrectpassword

  password benar

  Q1RGVEVEMjAyMXswdjNyZjEwdzNkfQ==
[16:45:47]-banua@basiber:~/Downloads
Shell-$ echo Q1RGVEVEMjAyMXswdjNyZjEwdzNkfQ== | base64 -d && echo
CTFTED2021{0v3rf10w3d}
```

Flag : CTFTED2021{0v3rf10w3d}