

## LATIHAN CYBER SECURITY 2020

REJA REVALDY F.

### COMPLETED

- Bongkar
- Crackme
- Reverse 1
- Reverse 2
- Pass
- File.exe

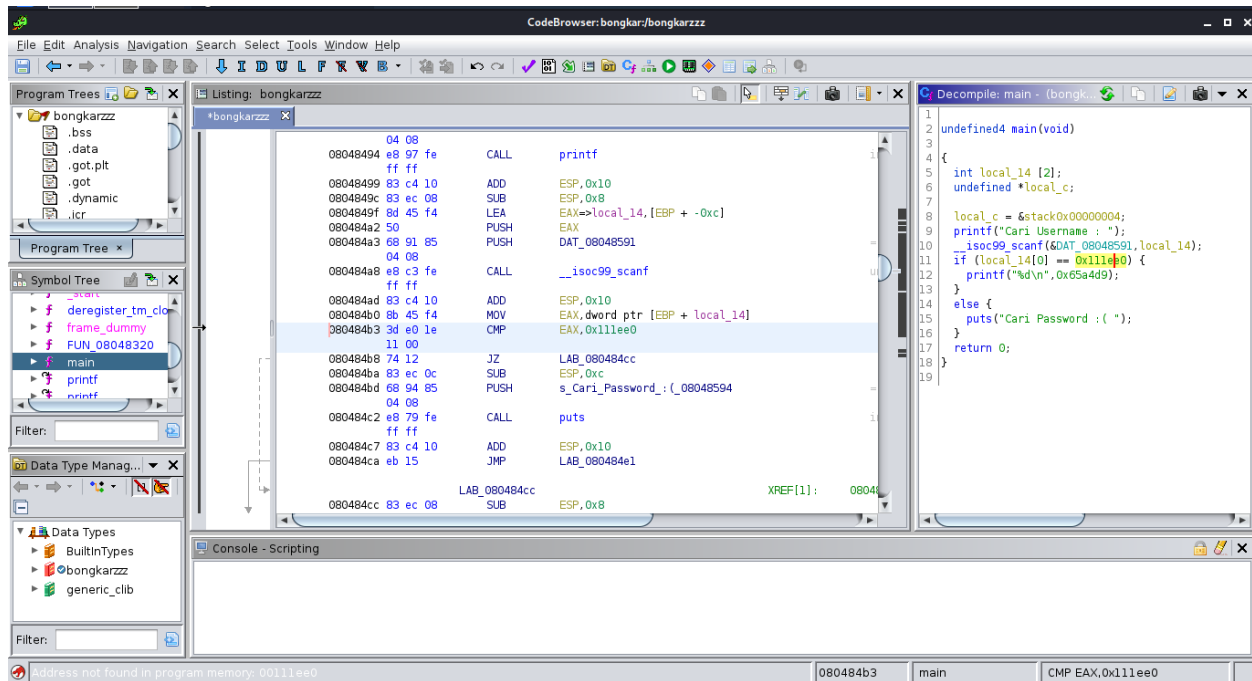
### UNFINISHED

- flag.jpeg.exe.doc.rar

## PENYELESAIAN

### Bongkarzzz

1. diberikan file program bongkarzzz, lalu saya menggunakan perintah `chmod +x` agar program bisa saya jalankan, setelah saya jalankan program ini memerlukan username lalu akan memunculkan password, jadi dari sini saya tau apa yang dicari yaitu username



2. Lalu saya menggunakan tool ghidra untuk melihat jalannya program dan membuka function main lalu saya melihat perkondisian dimana "`local14[0] == 0x111ee0`" disini saya asumsikan jika username yang harus diinput adalah `0x111ee0`, lalu setelah saya coba inputkan ternyata gagal, lalu saya mencoba untuk mengubah "`0x111ee0`" yang ternyata bilangan hexadecimal lalu saya ubah ke decimal dan muncul decimal 1122616

Hexadecimal	BASE64	Decimal
0x111ee0	ARHuAA==	1122616
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Convert"/> <input type="button" value="Highlight Text"/>	<input type="button" value="Convert"/> <input type="button" value="Highlight Text"/>	<input type="button" value="Convert"/> <input type="button" value="Highlight Text"/>

3. Lalu saya inputkan decimal tsb ke program dan muncul lah passwordnya

```
(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/bongkar]
$ ./bongkarzzz
Cari Username : 0x111ee0
Cari Password :(

(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/bongkar]
$ ./bongkarzzz
Cari Username : 1122016
6661337

(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/bongkar]
$
```

## CRACKME

1. diberikan program dan saya menggunakan perintah chmod +x agar program bisa dieksekusi, lalu saya mencoba menggunakan ltrace untuk melihat jalannya program lalu saya lihat kita harus memasukan password, setelah itu saya melihat text disamping password inputan saya, maka saya mencoba untuk memasukan text tersebut sebagai password, dan berhasil

```
kali@kali: ~/lks-cs/Latih...
kali@kali: ~/lks-cs/Latihan/Latihan 2020/crackme

File Actions Edit View Help

(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/crackme]
$ ltrace ./crackme
puts("Hi!\nInput Your Password!Hi!
Input Your Password
)
= 24
malloc(16)
memset(0x564e0c8bf6b0, '\0', 16)
= 0x564e0c8bf6b0
fgets(sdasdsdasdsad
= 0x564e0c8bf6b0
"sdsasdsdasdsad\n", 16, 0x7fa6982ff980)
= 0x564e0c8bf6b0
strcmp("sdasdsdasdsad\n", "JJJJJJJJJJJJJBxs")
= 41
puts("Password Salah!"Password Salah!
)
= 16
free(0x564e0c8bf6b0)
+++ exited (status 0) +++
= <void>

(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/crackme]
$ ./crackme
Hi!
Input Your Password
JJJJJJJJJJJJJBxs
MANTUL, flag is LKSSMK28{JJJJJJJJJJJJJBxs}
```

## REVERSE 1

1. diberikan file program lalu saya menggunakan chmod +x agar bisa program nya bisa dijalankan, lalu program berisi inputan untuk memasukan password, lalu saya menggunakan ltrace untuk melihat alur program dan saya mencoba untuk memasukan password di sana, dan saya melihat string compare "k0opi\_hitam\_pht" dan saya mencoba menjalankan program dan memasukan passwordnya maka muncullah flagnya

```
_ZNSt8ios_base4InitC1Ev(0x562ee9ab82b9, 0xffff, 0x7ffdaea2c188, 224) = 0
__cxa_atexit(0x7fef334d9a40, 0x562ee9ab82b9, 0x562ee9ab8060, 6) = 0
strcpy(0x7ffdaea2bf33, "k0o") = 0x7ffdaea2bf33
strcat("k0o", "pi_h") = "k0opi_h"
_ZNSt8ios_base4InitC1Ev(0x562ee9ab8080, 0x7fef335486d0, 4, 0x685f69) = 0
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x562ee9ab8080, 0x562ee9ab6010, 0, 3072) = 0x562ee9ab8080
_ZNSolsEPFRSo5_E(0x562ee9ab8080, 0x7fef335486d0, 0x562ee9ab8080, 3072) = 0x562ee9ab8080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x562ee9ab8080, 0x562ee9ab6039, 0, 3072) = 0x562ee9ab8080
_ZNSolsEPFRSo5_E(0x562ee9ab8080, 0x7fef335486d0, 0x562ee9ab8080, 3072) = 0x562ee9ab8080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x562ee9ab8080, 0x562ee9ab6058, 0, 3072) = 0x562ee9ab8080
_ZNSolsEPFRSo5_E(0x562ee9ab8080, 0x7fef335486d0, 0x562ee9ab8080, 3072) = 0x562ee9ab8080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x562ee9ab8080, 0x562ee9ab6077, 0, 3072) = 0x562ee9ab8080
_ZNSolsEPFRSo5_E(0x562ee9ab8080, 0x7fef335486d0, 0x562ee9ab8080, 3072) = 0x562ee9ab8080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x562ee9ab8080, 0x562ee9ab6085, 0, 3072) = 0x562ee9ab8080
_ZNSolsEPFRSo5_E(0x562ee9ab8080, 0x7fef335486d0, 0x562ee9ab8080, 3072) = 0x562ee9ab8080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x562ee9ab8080, 0x562ee9ab609f, 111, 0xffffffff) = 0x562ee9ab8080
_ZNSolsEPFRSo5_E(0x562ee9ab8080, 0x7fef335486d0, 0x562ee9ab8080, 3072) = 0x562ee9ab8080
+++ exited (status 0) +++

(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/reverse2_complete]
$ ltrace ./reverse2
puts("||-----|| ... ||-----||") = 73
puts("||-----|| ... ||-----||") = 73
puts("||-----|| CTF ... ||-----|| CTF") = 66
puts("||-----|| LKS SMK ... ||-----|| LKS SMK 28") = 66
puts("||-----|| ... ||-----||") = 73
puts("||-----|| ... ||-----||") = 73
puts("Password:Password:") = 10
__isoc99_scanf(0x5a3cc3cc13c, 0x7ffe9e9945e0, 0, 0x7f66b85cff33asdf) = 1
strcmp(0x00007fff, "asdf") = -49
puts("You Failed>You Failed") = 11
+++ exited (status 0) +++
```

## REVERSE 2

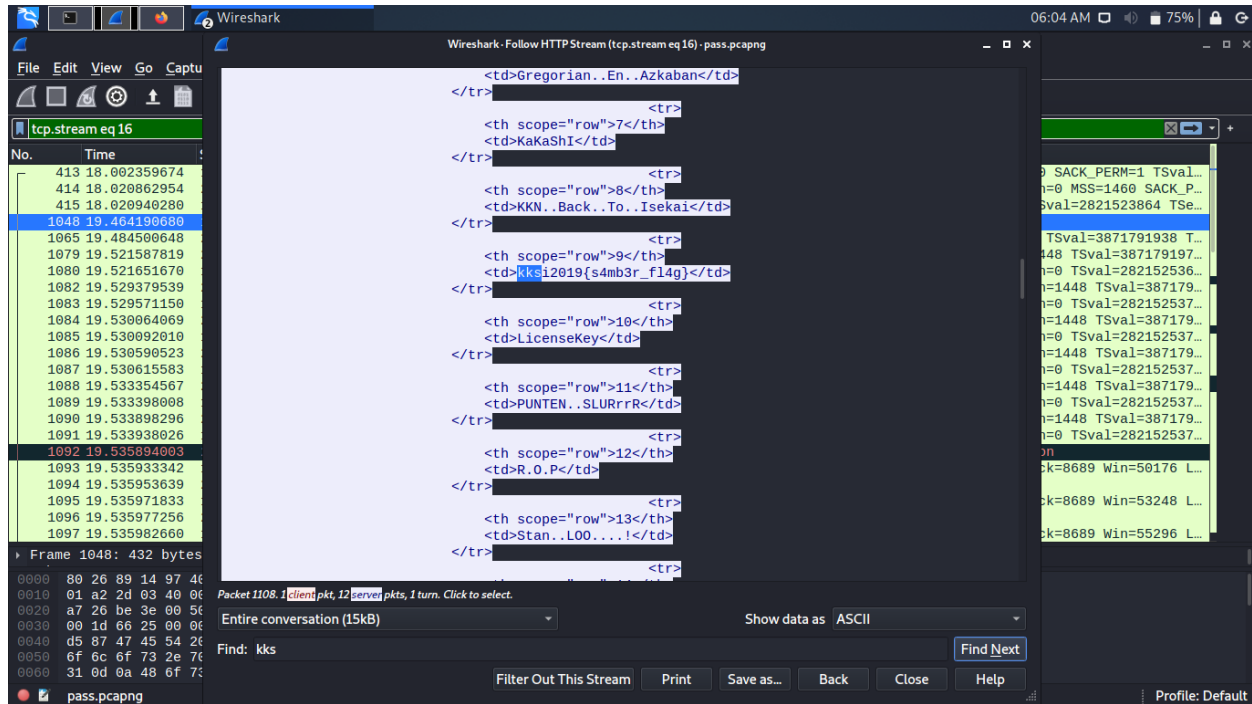
1. saya menggunakan teknik yang sama dengan reverse 1 lalu menemukan string compare "0x00007fff" dan saya coba memasukan nya di program maka muncul flagnya

```
puts("Password:Password:") = 10
__isoc99_scanf(0x5a3cc3cc13c, 0x7ffe9e9945e0, 0, 0x7f66b85cff33asdf) = 1
strcmp(0x00007fff, "asdf") = -49
puts("You Failed>You Failed") = 11
+++ exited (status 0) +++

(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/reverse2_complete]
$ ./reverse2
||-----|| | | | |
||-----|| CTF ||-----||
||-----|| LKS SMK 28 ||-----||
||-----||
Password:
0x00007fff
You Win
LKSSMK28{LKSSMK28_486619254b9c9f6e6800cfae77}
```

## PASS

1. saya membuka file menggunakan wireshark lalu saya melakukan http stream di 1108 dan saya menemukan kksi2019{s4mb3r\_fl4g} di html tersebut



## FILE EXE

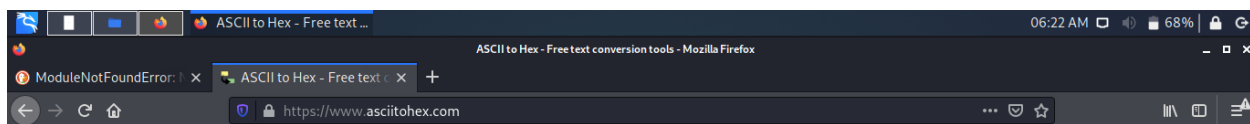
1. diberikan file ber extensi .exe, lalu setelah saya menggunakan program dari linux yaitu "file" maka saya menemukan bahwa file adalah rar
2. setelah saya extract rar tsb maka muncul file pdf dan file txt "rockyou-20.txt" yang saya asumsikan kita harus melakukan bruteforce kepada file pdf
3. lalu saya membuat script python sederhana untuk melakukan bruteforce lalu ditemukan password yang dipakai adalah "hellokitty"
4. lalu setelah saya buka dan masuka password tsb maka muncul text berisikan base64 yaitu "TEtTU01LMjh7Y3JhY2sxbjlfZG9jdW0zb1R9==" lalu setelah saya konversikan maka muncul flag

```
kali@kali: ~/lks-cs/Latih... 06:07 AM 73%
File Actions Edit View Help
(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/file.exe]
$ file file.exe
file.exe: Zip archive data, at least v2.0 to extract
(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/file.exe]
$ cp file.exe file.zip
(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/file.exe]
$ ls
file.exe  file.zip
(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/file.exe]
$ unzip file.zip
Archive:  file.zip
  inflating: rockyou-20.txt
   creating: __MACOSX/
  inflating: __MACOSX/._rockyou-20.txt
  inflating: file_secret.pdf
  inflating: __MACOSX/._file_secret.pdf
(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/file.exe]
$ ls
file.exe  file_secret.pdf  file.zip  __MACOSX  rockyou-20.txt

kali@kali: ~/lks-cs/Latih... 06:19 AM 69%
File Actions Edit View Help
(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/file.exe/file]
$ ls
file_secret.pdf  __MACOSX/  rockyou-20.txt  script.py
(kali@kali)-[~/lks-cs/Latihan/Latihan 2020/file.exe/file]
$ python3 script.py
Decrypting PDF: 37% | 188/512 [00:00<00:00, 373.78it/s]
[+] Password found: hellokitty
Decrypting PDF: 42% | 215/512 [00:00<00:00, 364.75it/s]

kali@kali: ~/lks-cs/Latih... 06:21 AM 68%
File Actions Edit View Help
GNU nano 5.4 script.py
import pikepdf
from tqdm import tqdm

passwords = [ line.strip() for line in open("rockyou-20.txt") ]
for password in tqdm(passwords, "Decrypting PDF"):
    try:
        with pikepdf.open("file_secret.pdf", password=password) as pdf:
            print("[+] Password found:", password)
            break
    except pikepdf._qpdf.PasswordError as e:
        continue
```



# ASCII to Hex

...and other free text conversion tools

## Text (ASCII / ANSI)

LKSSMK28{crack1n9\_docum3n1}

Convert

Highlight Text

## Binary

01001100 01001011 01010011 01010011 01001101  
01001011 00110010 00111000 01111011 01100011  
01110010 01100001 01100011 01101011 00110001  
01101110 00111001 01011111 01100100 01101111  
01100011 01110101 01101101 00110011 01101110  
01010100 01111101

Convert

Highlight Text

## Hexadecimal

4c 4b 53 53 4d 4b 32 38 7b 63 72 61 63 6b 31 6e 39  
5f 64 6f 63 75 6d 33 6e 54 7d

## BASE64

TETU01LMjh7Y3JhY2sxbjlfZG9jdW0zblR9==

## Decimal

76 75 83 83 77 75 50 56 123 99 114 97 99 107 49 110  
57 95 100 111 99 117 109 51 110 84 125