LATIHAN CYBER SECURITY 2020

REJA REVALDY F.

COMPLETED

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

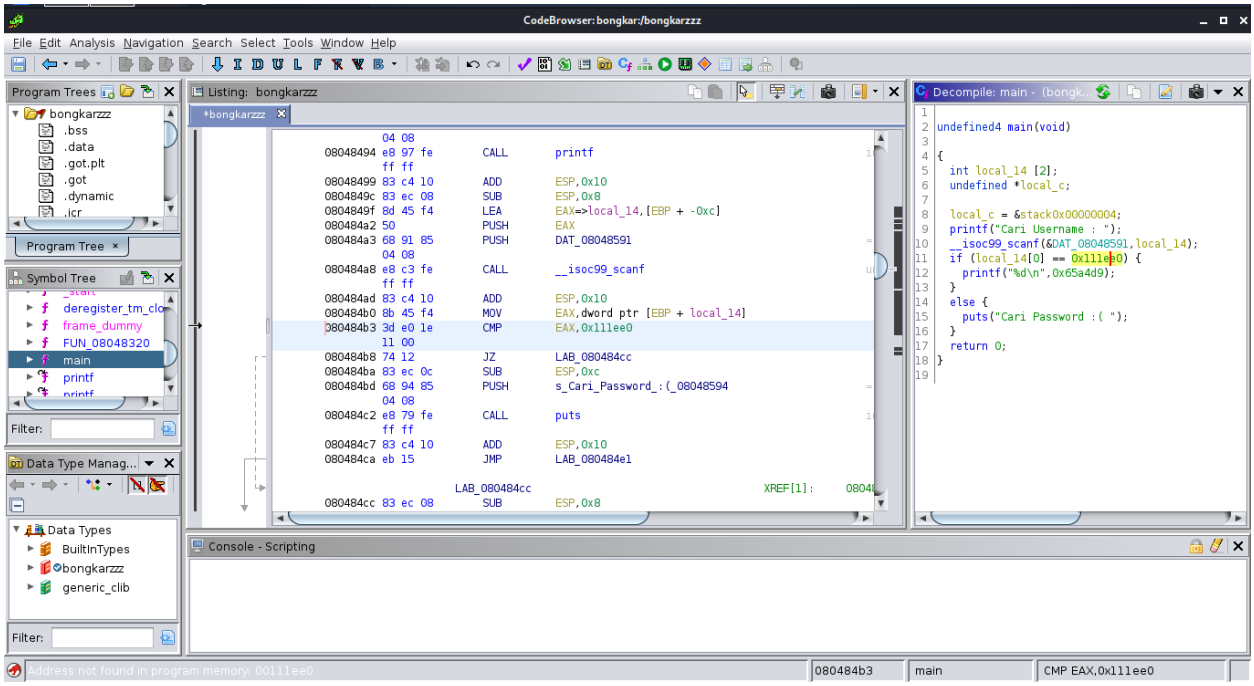
UNFINISHED

- 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

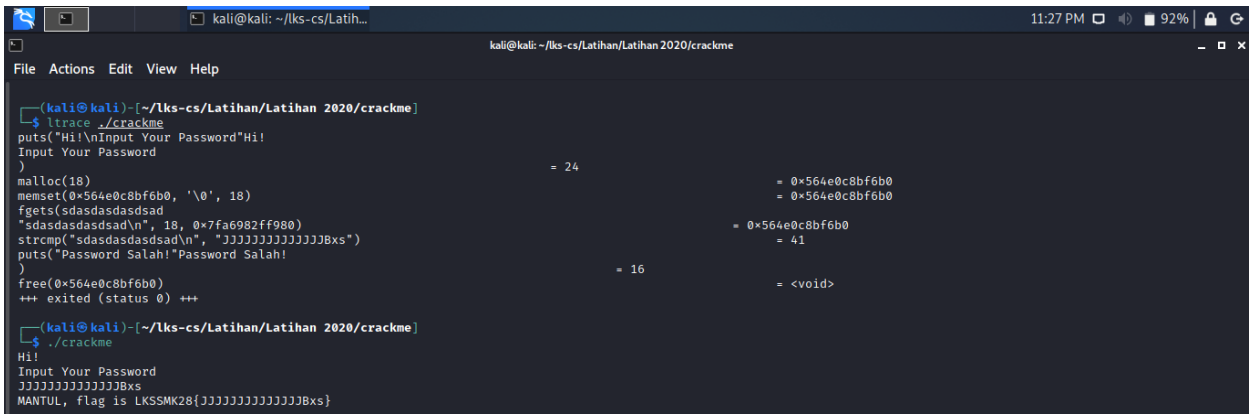


2. Lalu saya menggunakan tool ghidra untuk melihat jalannya program dan membuka function main lalu saya melihat perkondisian dimana “local14[0] == 0x111ee0” disini saya asumsikan jika username yang harus diinput adalah 0x111ee0, lalu setelah saya coba inputkan ternyata gagal, lalu saya mencoba untuk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

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

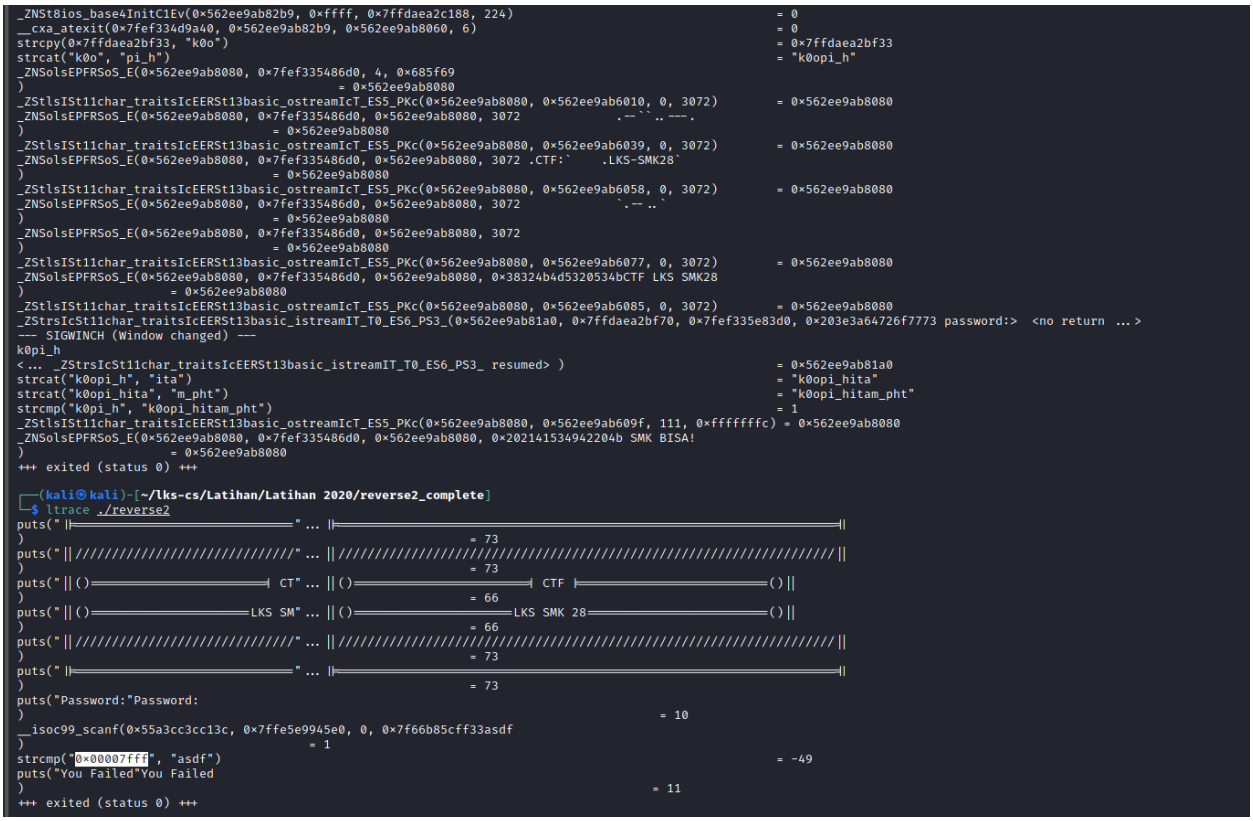
CRACKME

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



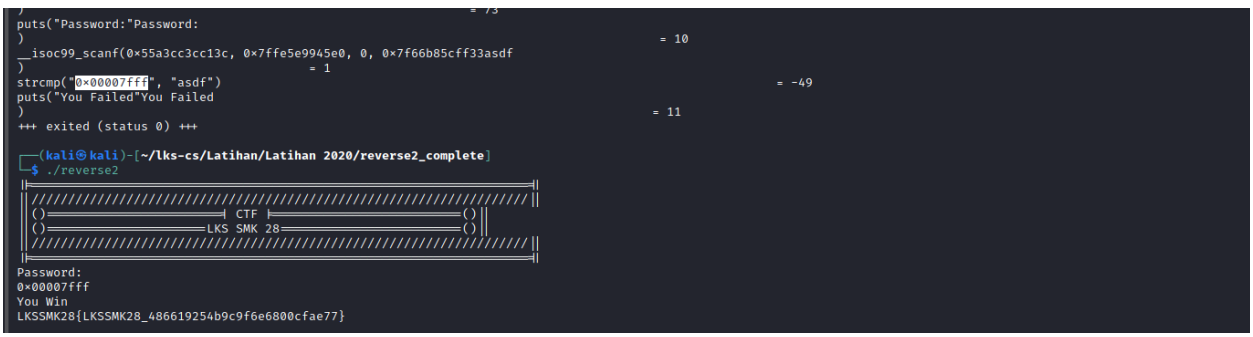
REVERSE 1

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



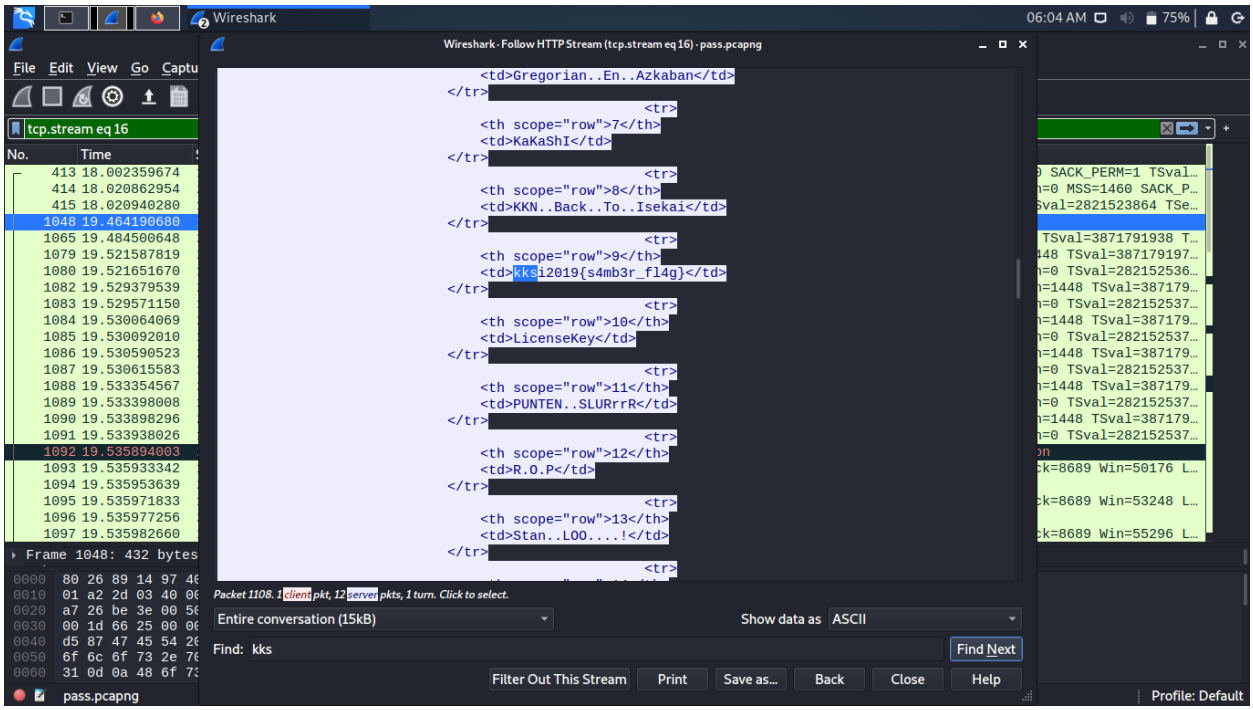
REVERSE 2

1. saya menggunakan teknik yang sama dengan reverse 1 lalu menemukan string compare “0x00007ff” dan saya coba memasukan nya di program maka muncul flagnya



PASS

1. saya membuka file menggunakan wireshark lalu saya melakukan http stream di 1108 dan saya menemukan kksi2019{s4mb3r_fl4g} di html tersebut



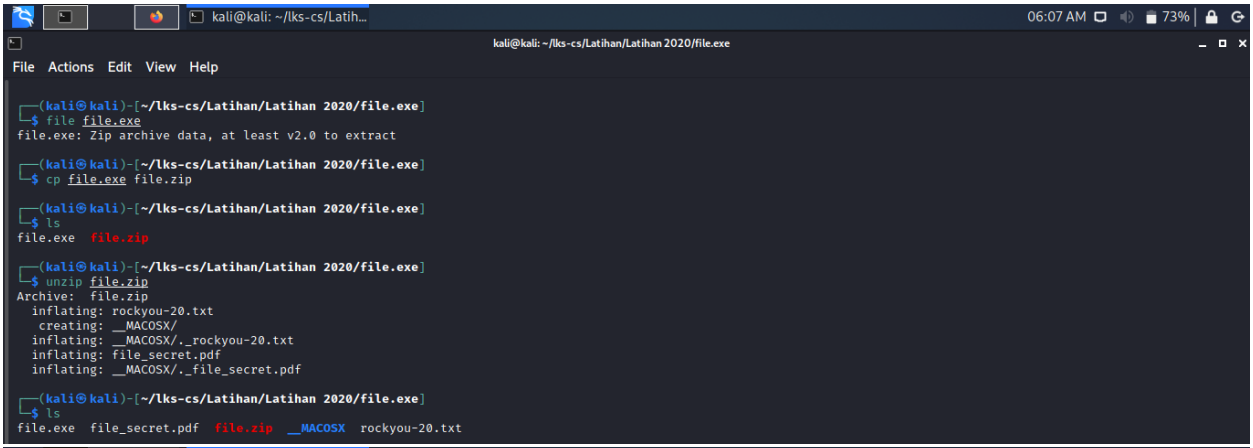
FILE EXE

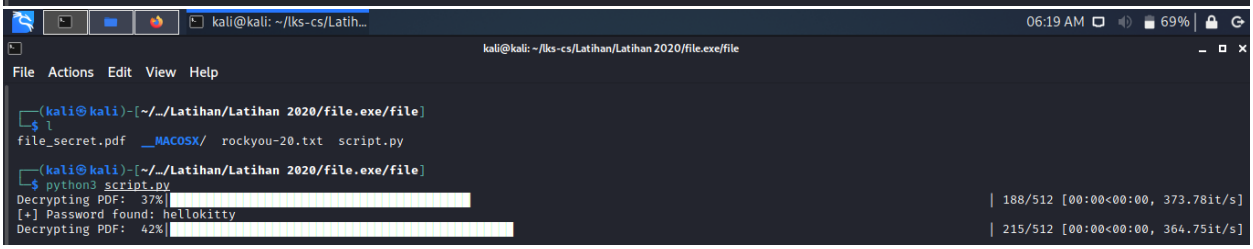
1. diberikan file ber extensi .exe, lalu setelah saya menggunakan program dari linux yaitu "file" maka saya menemukan bahwa file adalah rar

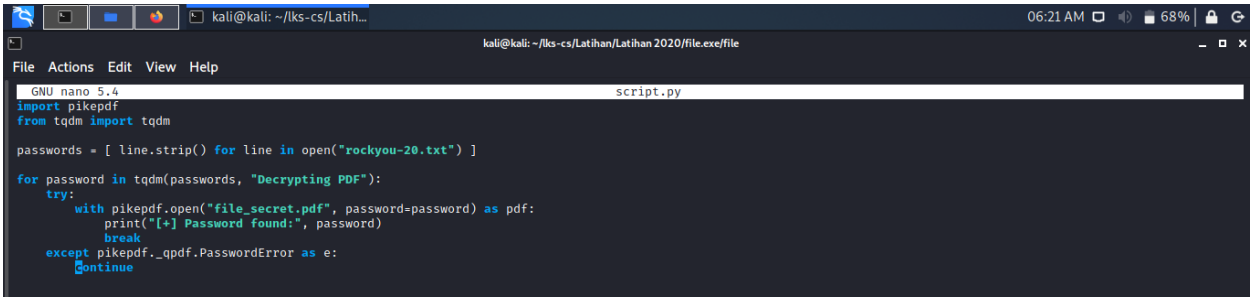
2. setelah saya extract rar tsb maka muncul file pdf dan file txt "rockyou-20.txt" yang saya asumsikan kita harus melakukan brtueforce kepada file pdf

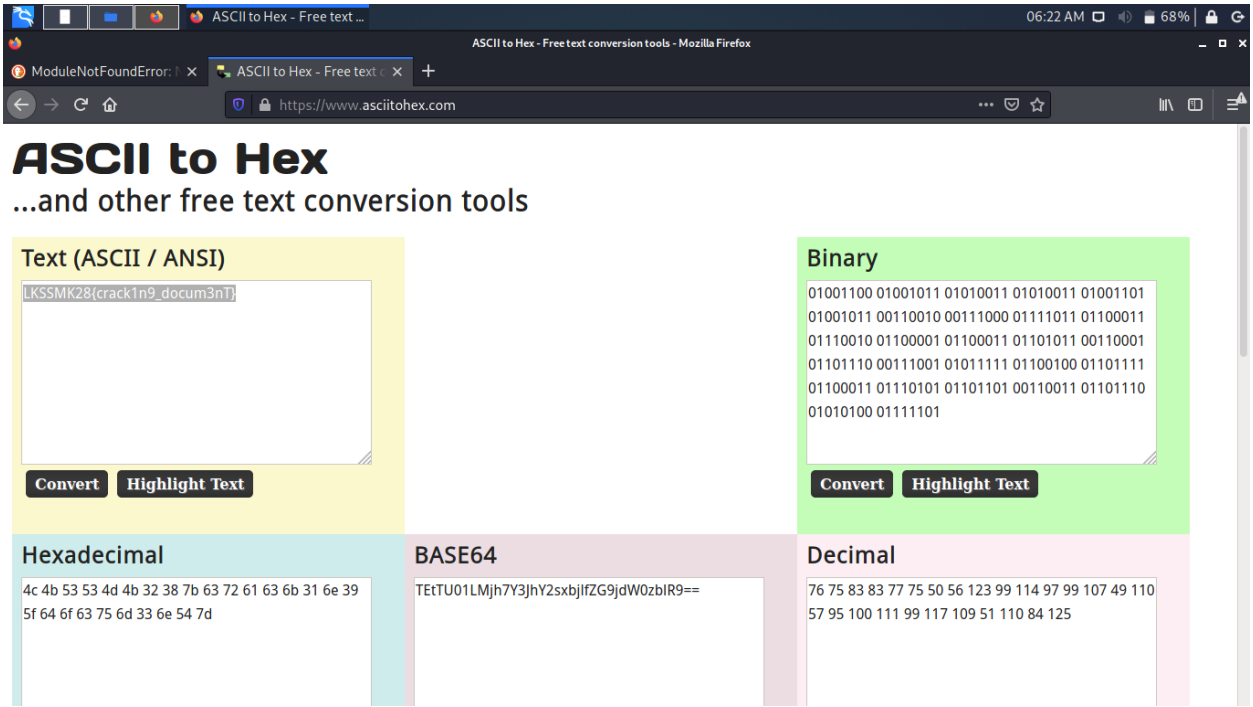
3. lalu saya membuat script python sederhana untuk melakukan bruteforce lalu ditemukan password yang dipakai adalah "hellokitty"

4. lalu setelah saya buka dan masuka password tsb maka muncul text berisikan base64 yaitu "TEtTU01LMjh7Y3JhY2sxbjlfZG9jdW0zblR9==" lalu setelah saya konversikan maka muncul flag


kali@kali: ~/lks-cs/Latih...
06:07 AM
73%
kali@kali: ~/lks-cs/Latihan/Latihan 2020/file.exe
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%
kali@kali: ~/lks-cs/Latihan/Latihan 2020/file.exe/file
File Actions Edit View Help
┌──(kali㉿kali)-[~/…/Latihan/Latihan 2020/file.exe/file]
└─$ l
file_secret.pdf __MACOSX/ rockyou-20.txt script.py
┌──(kali㉿kali)-[~/…/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%
kali@kali: ~/lks-cs/Latihan/Latihan 2020/file.exe/file
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 - Free text ...
06:22 AM
68%
ASCII to Hex - Free text conversion tools - Mozilla Firefox
ModuleNotFoundError:
ASCII to Hex - Free text
https://www.asciitohex.com
ASCII to Hex
...and other free text conversion tools
Text (ASCII / ANSI)
LKSSMK28{crack1n9_docum3nT}
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
TEtTU01LMjh7Y3JhY2sxbjlfZG9jdW0zblR9==
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