WRITEUP

THE LAST COMPETITION

Kategori CTF

Oleh:

Muhammad Ichwan a.K.a banua

TEKNIK KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

[PROGRAMMING]

VERSE

Diberikan sebuah deskripsi dimana jika kekuatan FAA = 52k Power, maka berapa kekuatan 198x azatoth dari faa? Dan hasilnya tersebut akan dibagi menjadi 3. Dari deskripsi yang diberikan dapat disimpulkan bahwa terdapat perhitungan matematika tetapi saya lupa nama materinya.

Solusi :

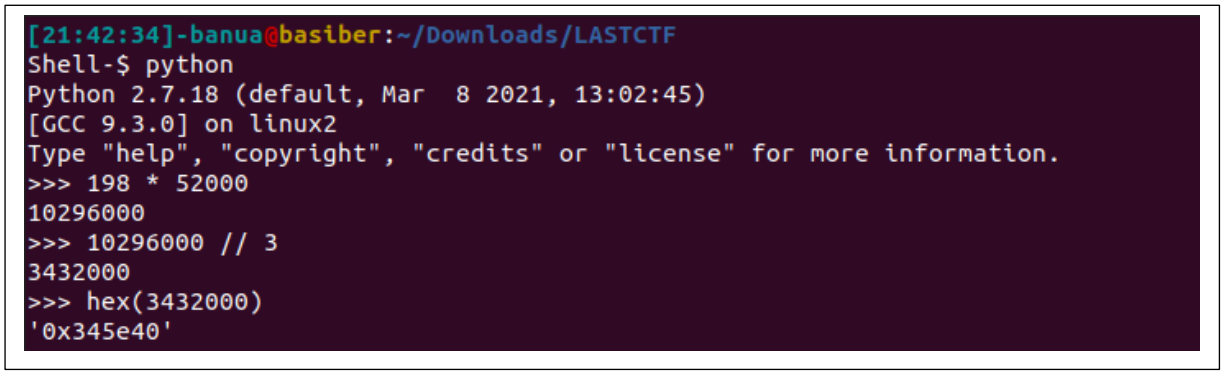
Diketahui FAA = 52k Power == 52.000 Power

Dicari :

Kekuatan azatoth 198x dari FAA kemudian hasilnya dibagi menjadi 3

(198 x 52.000) : 3 = 10296000 : 3 = 3432000

Format flag : LASTCTF{0x[hexadecimal]}



Flag : LASTCTF{0x345e40}

KOPID

Diberikan sebuah file dimana isinya hanya sebuah variabel berisi pesan yang terenkripsi. Pada deskripsi soal terdapat hint yaitu 19 + 7. Sebelumnya saya menduga ini adalah operasi xor ataupun shift cipher namun setelah dicoba ternyata gagal.

Solusi :

Dari hint tersebut 19 + 7 = 26, maka saya mencari bagaimana jika operasi nya ditukar tapi nilai nya tetap sama, dapat diselesaikan dengan modulus. Jadi 26 mod 19 = 7. Dan soal ini hasil sama seperti soal Covid 19 yang ada di rasyidmf.com (Kebetulan saya dulu sering main disitu). Tinggal bikin solver nya dengan python dimana ord tiap huruf itu ditambah dengan range dari panjang ciphertext.

```
xor = """l`qq_o`t['l^XR_$b"a!TVKWe"""
key = 19+7

flag = ''
for x in range(len(xor)):
    flag += chr(ord(xor[x]) + (x % key))

print(flag)
```

```
[22:17:46]-banua@basiber:~/Downloads/LASTCTF/programming
Shell-$ python3 solvercovid.py
lastctf{c0vid_m3r3s4hkan}
```

Flag : LASTCTF{c0vid_m3r3s4hkan}

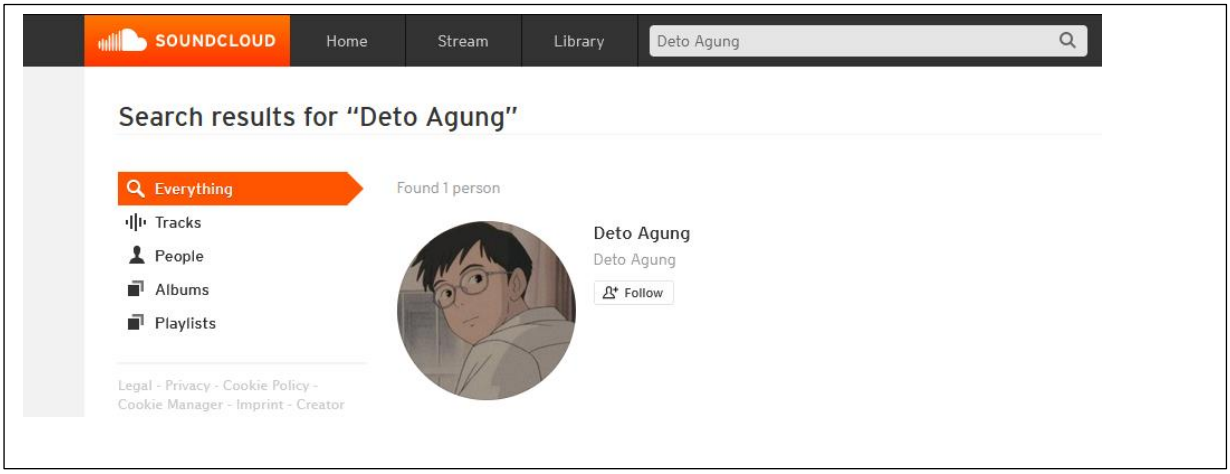
[OSINT]

PARA PENGGILA MUSIK

Diberikan sebuah deskripsi dimana seorang bernama Deto Agung tergila gila dengan music buatan Clean Bandit, dan kita disuruh untuk mencari tau apa yang dia komen, mungkin itu adalah flag nya.

Solusi :

Diketahui nama nya adalah Deto Agung, kemudian dia tergila gila dengan musik, dan musik nya itu buatan Clean Bandit. Disini saya sudah mempunya 3 kata kunci, yaitu nama, musik, dan Clean Bandit, berdasarkan musik tersebut terdapat platform musik yang terkenal dari dulu yaitu soundcloud, saya mencoba cari lewat soundcloud terlebih dahulu dengan mencari nama Deto Agung, kemudian didapatkan 1 person Deto Agung, langsung saja buka dan terdapat Recent musik dari Clean Bandit, cek pada samping kanan terdapat komentar dan flagnya.



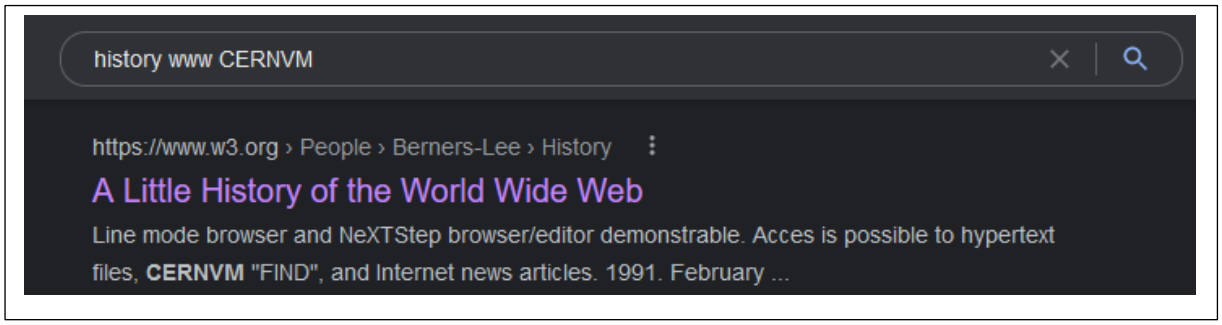
Flag : LASTCTF{e425095f149d9aa9e6d62460ea866066}

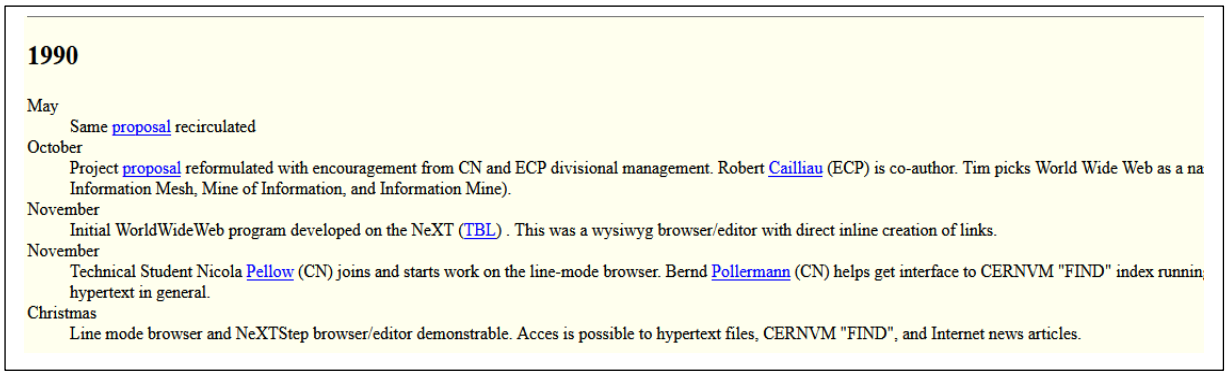
SEJARAH WWW

Diberikan sebuah deskripsi soal yaitu Pengembangan WWW dimulai pada 1989 oleh Tim Berners-Lee dan rekan-rekannya yang berbasis di Jenewa, Swiss, pada bulan November 1990 Nicola Pellow bergabung dan mengerjakan line-mode Browser, cari tau nama rekan yang membuat interface CERNVM “FIND”.

Solusi :

Dengan keyword pencarian google “history www CERNVM” didapatkan sebuah artikel “A Little History of the World Wide Web” dari website www.w3.org. Kemudian pada tahun 1990 bulan November tertera bahwa Bernd Pollermann membantu membuat interface CERNVM “FIND” dan nama Bernd Pollermann itulah flagnya.





1990

May
Same proposal recirculated
October
Project proposal reformulated with encouragement from CN and ECP divisional management. Robert Cailliau (ECP) is co-author. Tim picks World Wide Web as a na
Information Mesh, Mine of Information, and Information Mine).
November
Initial WorldWideWeb program developed on the NeXT (TBL) . This was a wysiwyg browser/editor with direct inline creation of links.
November
Technical Student Nicola Pellow (CN) joins and starts work on the line-mode browser. Bernd Pollermann (CN) helps get interface to CERNVM "FIND" index runnin
hypertext in general.
Christmas
Line mode browser and NeXTStep browser/editor demonstrable. Acces is possible to hypertext files, CERNVM "FIND", and Internet news articles.

Flag : LASTCTF{Bernd Pollermann}

[FORENSIC]

MINECRAFT

Diberikan sebuah link berisi gambar dimana gambar tersebut merupakan salah satu item dari minecraft tapi saya lupa namanya.

Solusi :

Pertama saya melakukan pengecekan terhadap metadata dari gambar tersebut terdapat Warning yaitu Trailer data after PNG IEND chunk. Diduga terdapat stegano pada gambar tersebut, lakukan pengecekan menggunakan command strings ataupun zsteg didapatkan flagnya.

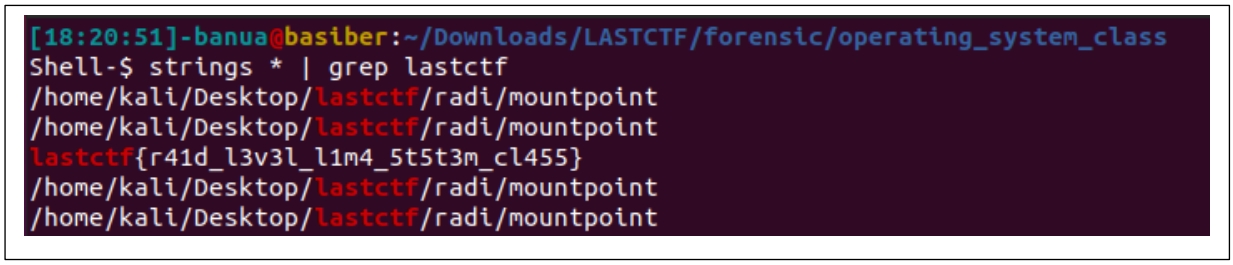
Flag : LASTCTF{mAb4rkuy}

OPERATING SYSTEM

Diberikan sebuah file zip yang ketika di ekstrak terdapat 5 file disk img.

Solusi :

Lakukan strings terhadap semua file hasil ekstrak an tadi, karena flag dengan format lastctf maka saya melakukan grep lastctf dengan strings, sepertinya unintended solution.



Flag : LASTCTF{r41d_l3v3l_l1m4_5t5t3m_cl455}

TRANSMISI APRS

Solusi : **TIDAK SEMPAT BIKIN WRITEUP (TERKENDALA FILE SOAL) KARENA CHALLENGE DIHAPUS TIDAK DI FREEZE**

Flag :

[CRYPTO]

DATABASE

Diberikan sebuah file dimana isinya adalah sebuah encoding base64 yang diimplementasikan kedalam ascii art

Solusi :

Karena ascii art nya masih dapat dibaca huruf dan angka nya maka tinggal ambil huruf dan angkanya kedalam alphabet dan juga angka kemudian lakukan decode base64, ada sedikit guessing untuk menentukan apakah itu 0 atau O.

Flag : TIDAK SEMPAT BIKIN WRITEUP (TERKENDALA FILE SOAL) KARENA CHALLENGE DIHAPUS TIDAK DI FREEZE

RSA LAGI

Diberikan sebuah file dimana terdapat modulus n, public exponent dan juga ciphertext. Namun disini public exponent nya bernilai 431136

Solusi :

Sama seperti soal RARCTF 2021 yaitu sRSA, tinggal ambil solvernya dan dapat flagnya.

```
#https://ctf.rip/write-ups/crypto/rsa/reversing/rarctf-2021/
from libnum import *

n = 549627337745419906524266924858342366692273465272497792325651966169209781
e = 431136
ct = 407047902924659333182370556657656943312013912156 8

for i in range(e):
    pt = ct // e
    pts = n2s(pt)
    if b"lastctf{" in pts:
        print(pts)
        break
    ct += n
```

```
[18:34:54]-banua@basiber:~/Downloads/LASTCTF/crypto
Shell-$ python3 solverlagi.py
b'lastctf{rs4_4g41n}'
```

Flag : LASTCTF{rs4_4g41n}

[BINARY EXPLOITATION]

BREAK ME

Diberikan sebuah deskripsi dimana isinya game seperti itu kalua tidak salah dan juga alamat ip untuk dilakukan nc

Solusi :

Pada nc saat saya memasukan yes maka program akan berjalan dan muncul encoding base64, coba lakukan decoding didapatkan format PNG di awal, maka saya pun mencoba melakukan decode base64 dan menjadikannya file gambar format PNG. Saat dibuka gambar tersebut terdapat angka dimana angka tersebut yang harus saya masukkan sebagai inputan untuk mendapatkan skor dan lanjut terus menerus. Tinggal bikin scripting nya dimana ambil base64 nya kemudian jadikan file gambar dan menggunakan pytesseract ambil text dalam gambar tersebut, adapaun pytesseract yang digunakan dari github untuk mendapatkan akurasi yang baik dalam membaca teks dalam gambar.

```
#https://stackoverflow.com/questions/9480013/image-processing-to-improve-tesseract-ocr-accuracy
#https://github.com/tesseract-ocr/tessdata

from pwn import *
from PIL import Image
import pytesseract
import base64

context.log_level = 'critical'

p = remote('103.147.32.214', 9002)

p.recvuntil(b'[\x1b[33mno\x1b[39m]:\r\n')
p.sendline(b'yes')
p.recvuntil(b'\r\n\r\n\r\n')

while True:
    ctBase = p.recvline().replace(b'\x1b[32m', b'').replace(b'\x1b[39m\r\n', b'').decode('utf8')
    ctBase = base64.b64decode(ctBase)
    with open('tes.png', 'wb') as f:
        f.write(ctBase)

    img = Image.open('tes.png')
    width = img.size[0]
    height = img.size[1]
    for i in range(0,width):# process all pixels
        for j in range(0,height):
            data = img.getpixel((i,j))
            #print(data) #(255, 255, 255)
            if (data[0]!=255 and data[1]!=255 and data[2]!=255):
                img.putpixel((i,j),(0, 0, 0))
    img.save('tes-2.png')
```

```
    code = pytesseract.image_to_string(Image.open('tes-2.png'), config='--psm 6 --oem 0 -l eng -c tessedit_char_whitelist=0123456789')
    code = code.split()
    #print(code)
    codesend = ''
    if len(code) == 2:
        codesend += code[0] + code[1]
    elif len(code) == 3:
        codesend += code[0] + code[1] + code[2]
    elif len(code) == 4:
        codesend += code[0] + code[1] + code[2] + code[3]
    else:
        codesend += code[0]

    print('[+]', codesend)
    p.recvuntil(b'> ')
    p.sendline(bytes(codesend, 'utf8'))
    p.recvline()
    p.recvline()
    res = p.recvline().replace(b'\x1b[32m', b'').replace(b'\x1b[39m\r\n', b'').decode('utf8')
    print('[+]', res)
    if 'flag' in res:
        print('[+] GOT FLAG !!!')
        p.recvline()
        print(p.recvline().replace(b'\x1b[32m', b'').replace(b'\x1b[39m\r\n', b'').decode('utf8'))
        print()
        break
    p.recvline()
```

Flag : LASTCTF{th15_15_h0w_p30pl3_b34t_th3_c4ptch4_0ut_th3r3}

[VM]

Hack Me

Diberikan sebuah file dimana isi file tersebut adalah sebuah disk berekstensi vhdx dengan size kurang lebih 8 GB

Solusi :

Seharusnya ini adalah vm yang harus di exploitasi kerentanannya, namun karena ada kesalahan dari problem setter tidak melakukan masking terhadap flag maka flag bisa didapatkan dengan strings dan grep lastctf jadinya unintended solutions deh.

```
[18:49:41]-banua@basiber:~/Downloads/LASTCTF/vm
Shell-$ strings Ubuntu\ Server.vhdx | grep lastctf
Jan  2 15:28:06 localhost sm-mta[11271]: 2lastctf{th15_15_l1nux_pr3v1l3935_35c4l
at10n}
lastctf{th15_15_l1nux_3l3v4t3d_pr1v1l3935_fr0m_0v3rl4yf5_f1l3_5y5t3m}
```

Flag : LASTCTF{th15_15_l1nux_3l3v4t3d_pr1v1l3935_fr0m_0v3rl4yf5_f1l3_5y5t3m}

MUNGKIN HANYA ITU WRITEUP YANG BISA SAYA BIKIN KARENA TERKENDALA CHALLENGE YANG TIDAK BISA DI AKSES LAGI UNTUK PEMBUATAN WRITEUP