TENESYS

IAM9ROOT

AKINARI X ZHEEK

TEKNOKRAT AND SYSTEM SECURITY TENESYS 2019

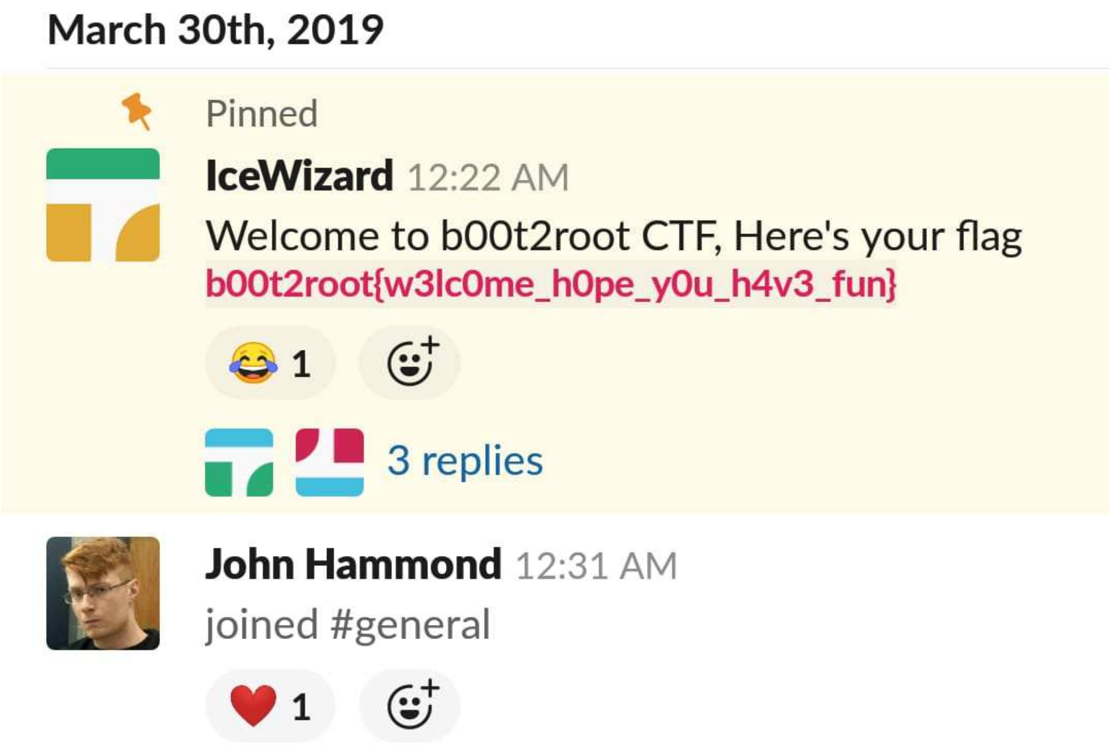
1. Welcome – 50 point – Misc –

Welcome to b00t2root CTF. Join the slack channel to get your flag.

slack

Author: NULLKrypt3rs :)

- Didapatkan sebuah web slack
- Lalu gabung dengan slack tersebut



March 30th, 2019

Pinned

IceWizard 12:22 AM

Welcome to b00t2root CTF, Here's your flag b00t2root{w3lc0me_h0pe_y0u_h4v3_fun}

😂 1

3 replies

John Hammond 12:31 AM

joined #general

❤️ 1

- Dan didapatkan flag : **b00t2root{w3lc0me_h0pe_y0u_h4v3_fun}**

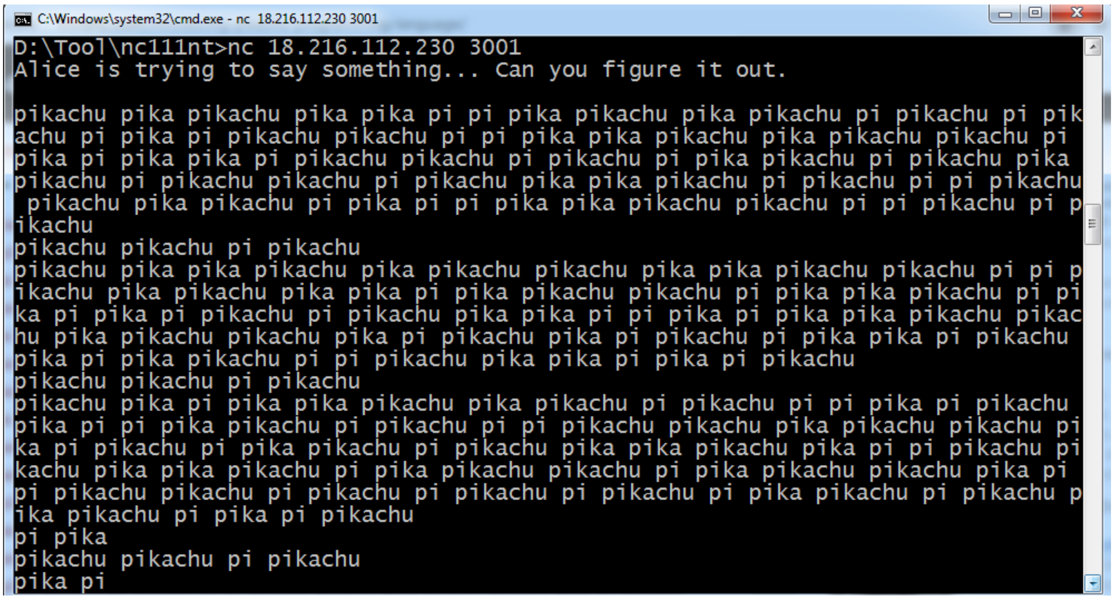
2. Can You Read Me – 233 point – Misc –

Find What I'm trying to say.

nc 18.216.112.230 3001

Author: GYeyosi

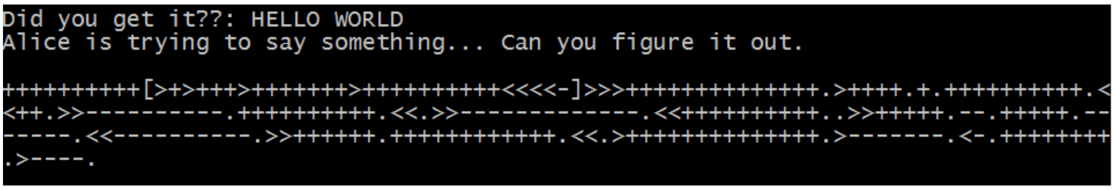
- Jalankan nc 18.216.112.230 3001
- Lalu di dapatkan sebuah pikalang https://esolangs.org/wiki/pikalang



```
D:\Tool\nc111nt>nc 18.216.112.230 3001
Alice is trying to say something... Can you figure it out.

pikachu pika pikachu pika pika pi pi pika pikachu pika pikachu pi pikachu pi pik
achu pi pika pi pikachu pikachu pi pi pika pika pikachu pika pikachu pikachu pi
pika pi pika pika pi pikachu pikachu pi pikachu pi pika pikachu pi pikachu pika
pikachu pi pikachu pikachu pi pikachu pika pika pikachu pi pikachu pi pi pikachu
 pikachu pika pikachu pi pika pi pi pika pika pikachu pikachu pi pi pikachu pi p
ikachu
pikachu pikachu pi pikachu
pikachu pika pika pikachu pika pikachu pikachu pika pika pikachu pikachu pi pi p
ikachu pika pikachu pika pika pi pika pikachu pikachu pi pika pika pikachu pi pi
ka pi pika pi pikachu pi pikachu pika pika pi pi pika pi pika pika pikachu pikac
hu pika pikachu pikachu pika pi pikachu pika pi pikachu pi pika pika pi pikachu
pika pi pika pikachu pi pi pikachu pika pika pi pika pi pikachu
pikachu pikachu pi pikachu
pikachu pika pi pika pika pikachu pika pikachu pi pikachu pi pi pika pi pikachu
pika pi pi pika pikachu pi pikachu pi pi pikachu pikachu pika pikachu pikachu pi
ka pi pikachu pi pika pikachu pi pikachu pika pika pikachu pika pi pi pikachu pi
kachu pika pika pikachu pi pika pikachu pikachu pi pika pikachu pikachu pika pi
pi pikachu pikachu pi pikachu pi pikachu pi pikachu pi pika pikachu pi pikachu p
ika pikachu pi pika pi pikachu
pi pika
pikachu pikachu pi pikachu
pika pi
```

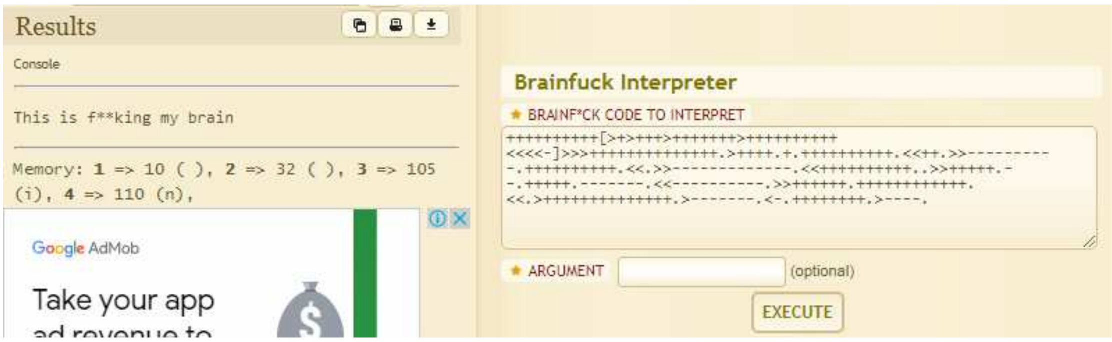
- Lalu decode dengan Pikachu-interpreter https://github.com/joelsmithjohnson/pikachu-interpreter
- Dan didapatkan HELLO WORLD
- Lalu masukkan HELLO WORLD



```
Did you get it??: HELLO WORLD
Alice is trying to say something... Can you figure it out.

++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>++++++++++++++.>++++.+.++++++++++.<
<++.>>----------.++++++++++.<<.>>-------------.<<++++++++++..>>+++++.--.+++++.--
-----.<<----------.>>++++++.++++++++++++.<<.>++++++++++++++.>-------.<-.++++++++
.>----.
```

- Didapatkan sebuah Brainfuck https://esolangs.org/wiki/brainfuck
- Lalu decode brainfuck https://www.dcode.fr/brainfuck-language

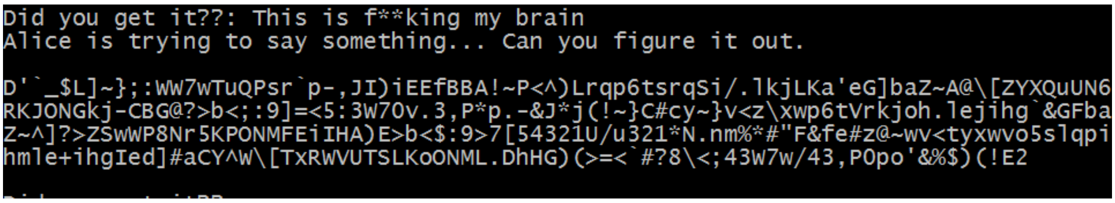


```
This is f**king my brain
```

```
Memory: 1 => 10 ( ), 2 => 32 ( ), 3 => 105
(i), 4 => 110 (n),
```

```
++++++++++[>+>+++>+++++++>++++++++++
<<<<-]>>>++++++++++++++.>++++.+.++++++++++.<<++.>>---------
-.++++++++++.<<.>>-------------.<<++++++++++..>>+++++.-
-.+++++.-------.<<----------.>>++++++.++++++++++++.
<<.>++++++++++++++.>-------.<-.++++++++.>----.
```

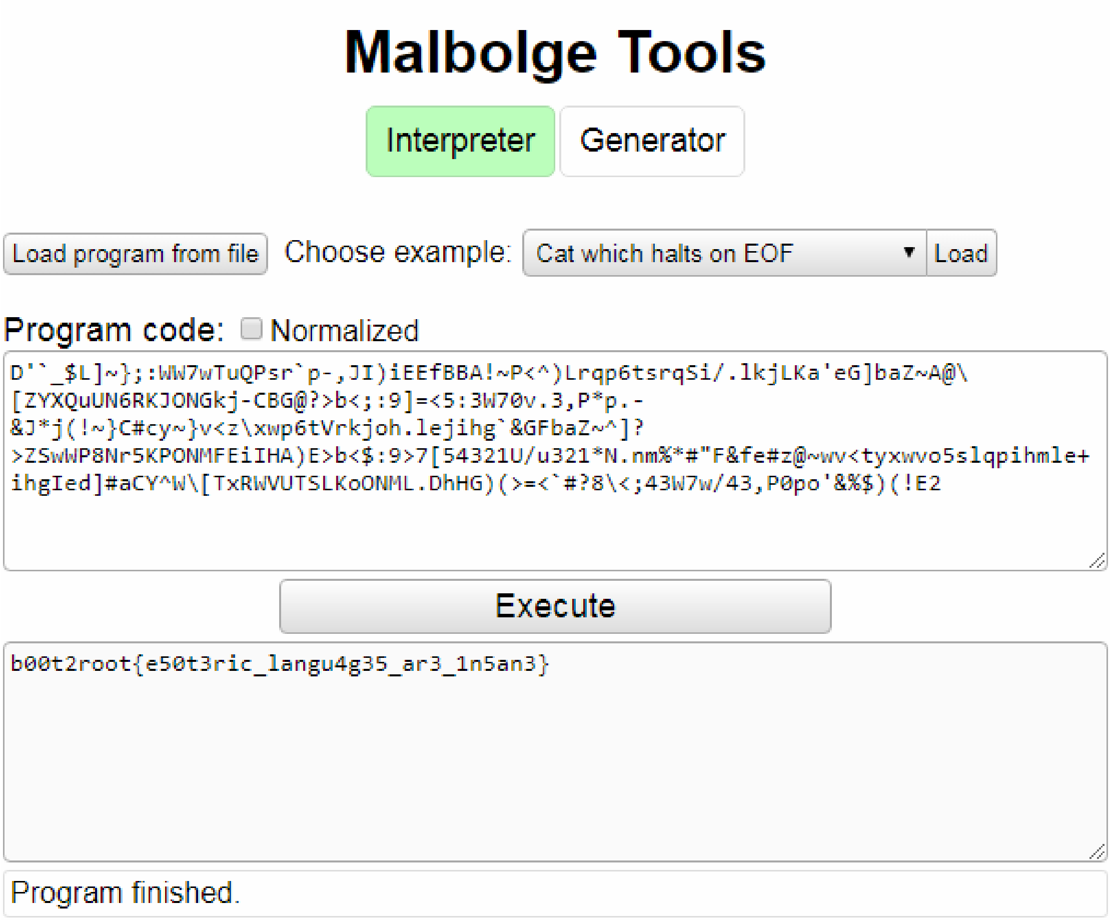
- Didapatkan This is f**king my brain dan lalu dimasukkan
- Didapatkan sebuah Malbolge https://esolangs.org/wiki/malbolge



```
Did you get it??: This is f**king my brain
Alice is trying to say something... Can you figure it out.

D'`_$L]~};:WW7wTuQPsr`p-,JI)iEEfBBA!~P<^)Lrqp6tsrqSi/.lkjLKa'eG]baZ~A@\[ZYXQuUN6
RKJONGkj-CBG@?>b<;:9]=<5:3W70v.3,P*p.-&J*j(!~}C#cy~}v<z\xwp6tVrkjoh.lejihg`&GFba
Z~^]?>ZSwWP8Nr5KPONMFEiIHA)E>b<$:9>7[54321U/u321*N.nm%*#"F&fe#z@~wv<tyxwvo5slqpi
hmle+ihgIed]#aCY^W\[TxRWVUTSLKoONML.DhHG)(>=<`#?8\<;43W7w/43,P0po'&%$)(!E2
```

- Lalu decode dengan https://zb3.me/malbolge-tools/



Choose example: Cat which halts on EOF

```
D'`_$L]~};:WW7wTuQPsr`p-,JI)iEEfBBA!~P<^)Lrqp6tsrqSi/.lkjLKa'eG]baZ~A@\
[ZYXQuUN6RKJONGkj-CBG@?>b<;:9]=<5:3W70v.3,P*p.-
&J*j(!~}C#cy~}v<z\xwp6tVrkjoh.lejihg`&GFbaZ~^]?
>ZSwWP8Nr5KPONMFEiIHA)E>b<$:9>7[54321U/u321*N.nm%*#"F&fe#z@~wv<tyxwvo5slqpihmle+
ihgIed]#aCY^W\[TxRWVUTSLKoONML.DhHG)(>=<`#?8\<;43W7w/43,P0po'&%$)(!E2
```

```
b00t2root{e50t3ric_langu4g35_ar3_1n5an3}
```

Program finished.

- Dan didapatkan flag : **b00t2root{e50t3ric_langu4g35_ar3_1n5an3}**

3. Cuz_rsa_is_lub – 50 point – Crypto –

```
n=
716418315469267193033696452965285464800834259054582
474052790611962144245581006789479962711796597615217
752909737905975336836680811733149403920982567214884
68660504161994357

e = 65537

c =
631270798325004123629501002425497381763181700723314
917508027161386213229745299949144078464489544876850
683315640089368085394205622516614357908554221304435
84773306161128156
```

- Didapatkan n, e dan c
- Lalu running script berikut :

```
import math
import gmpy2


def num_to_str(num):
    res = ""
    while num > 0:
        res = chr(num % 256) + res
        num = num / 256
    return res
```

```
n =
7164183154692671930336964529652854648008342590545
8247405279061196214424558100678947996271179659761
5217752909737905975336836680811733149403920982567
21488468660504161994357

N = gmpy2.mpz(n)

gmpy2.get_context().precision = 2048

a = int(gmpy2.sqrt(N))

a2 = a*a

b2 = gmpy2.sub(a2,N)

while not(gmpy2.is_square(b2)):

    a = a+1

    b2 = a*a-N

b2 = gmpy2.mpz(b2)

gmpy2.get_context().precision = 2048

b = int(gmpy2.sqrt(b2))

p = a+b

q = a-b

print "p: ", p

print "q: ", q



c =
6312707983250041236295010024254973817631817007233
1491750802716138621322974529994914407846448954487
6850683315640089368085394205622516614357908554221
30443584773306161128156
```

```
e = 65537

t = (p-1)*(q-1)

d = gmpy2.invert(e,t)

m = pow(c,d,n)


print "Flag: ", num_to_str(m)
```

- Dan didapatkan flag :
  b00t2root{RSA_c4n_b3_vuln3r4bl3}

4. Genetics – 235 point – Crypto –

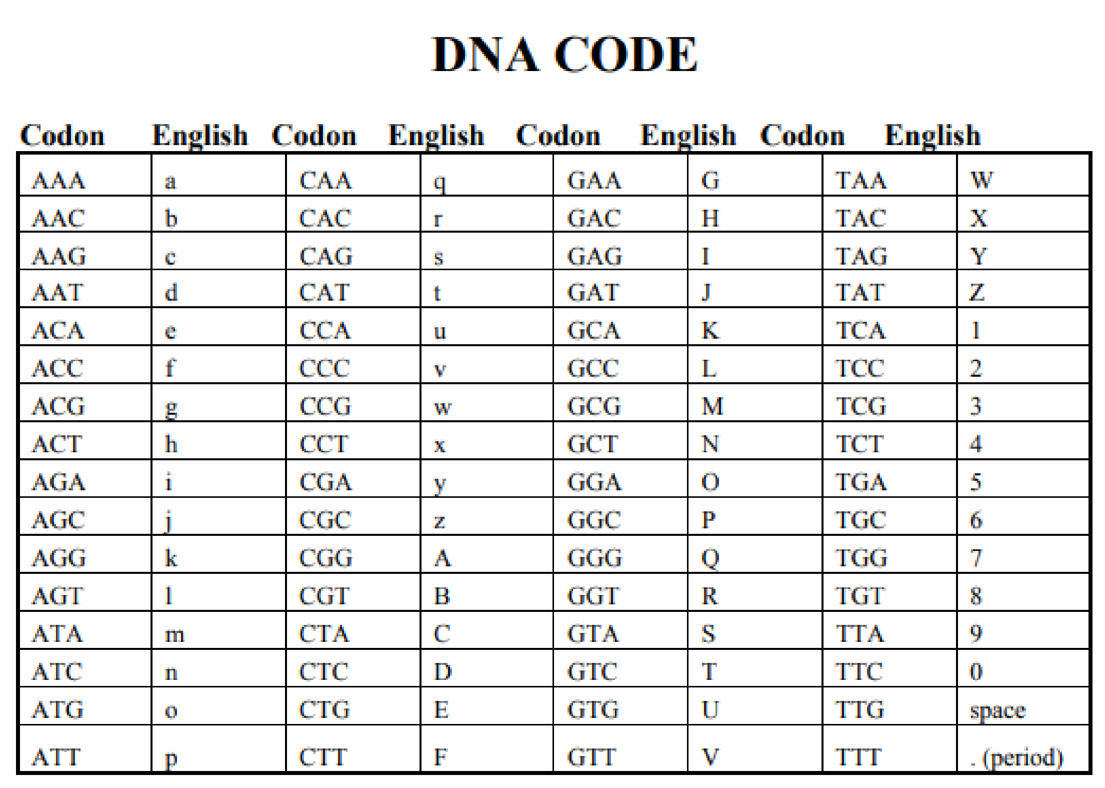
Cipher in my blood. Flag is not in actual format. Wrap it in b00t2root{flag} before you submit.

Author : blackpearl

- Didapatkan sebuah file yang berisikan DNA Code

```
ACCAGTAAAACGTTGAGACAGTTGAATATCAAACTACACCGAATTC
ATATGTCACAGCGGCCGACACAGATGATAACA
```

- Lalu decode dengan table DNA Code dari https://github.com/JohnHammond/ctf-katana



DNA CODE

Codon	English	Codon	English	Codon	English	Codon	English
AAA	a	CAA	q	GAA	G	TAA	W
AAC	b	CAC	r	GAC	H	TAC	X
AAG	c	CAG	s	GAG	I	TAG	Y
AAT	d	CAT	t	GAT	J	TAT	Z
ACA	e	CCA	u	GCA	K	TCA	1
ACC	f	CCC	v	GCC	L	TCC	2
ACG	g	CCG	w	GCG	M	TCG	3
ACT	h	CCT	x	GCT	N	TCT	4
AGA	i	CGA	y	GGA	O	TGA	5
AGC	j	CGC	z	GGC	P	TGC	6
AGG	k	CGG	A	GGG	Q	TGG	7
AGT	l	CGT	B	GGT	R	TGT	8
ATA	m	CTA	C	GTA	S	TTA	9
ATC	n	CTC	D	GTC	T	TTC	0
ATG	o	CTG	E	GTG	U	TTG	space
ATT	p	CTT	F	GTT	V	TTT	. (period)

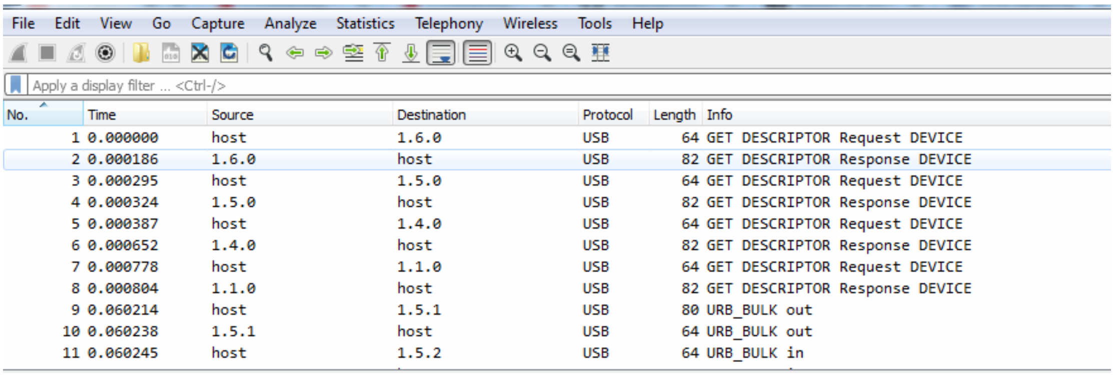
- Dan didapatkan flag : **b00t2root{dnaCrypto1sAwesome}**

5. Key_me_baby – 159 point – Forensic –

https://drive.google.com/file/d/1yO4j-7CEr2lvl3n7kkqGLSBNqsZlhmL_/view

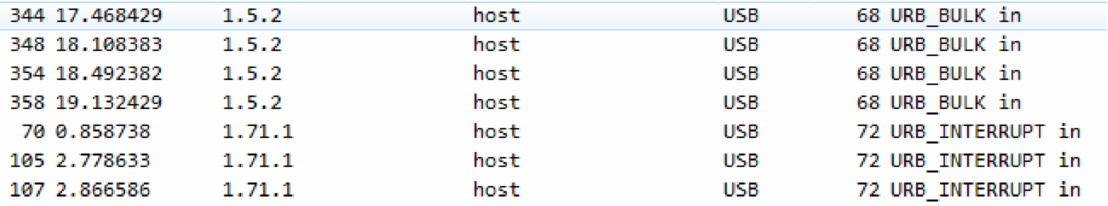
Author : Akir4

- Didapatkan sebuah file pcap dan dijalakan
- Ini merupakan sebuah traffic USB



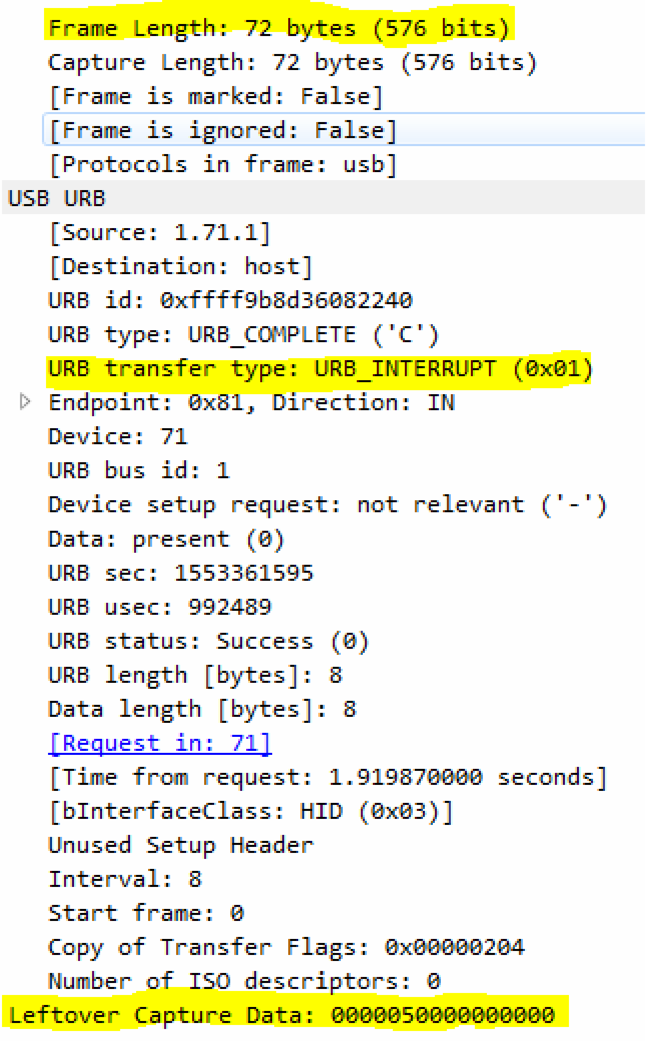
```
No.   Time       Source   Destination   Protocol   Length  Info
    1 0.000000   host     1.6.0         USB        64 GET DESCRIPTOR Request DEVICE
    2 0.000186   1.6.0    host          USB        82 GET DESCRIPTOR Response DEVICE
    3 0.000295   host     1.5.0         USB        64 GET DESCRIPTOR Request DEVICE
    4 0.000324   1.5.0    host          USB        82 GET DESCRIPTOR Response DEVICE
    5 0.000387   host     1.4.0         USB        64 GET DESCRIPTOR Request DEVICE
    6 0.000652   1.4.0    host          USB        82 GET DESCRIPTOR Response DEVICE
    7 0.000778   host     1.1.0         USB        64 GET DESCRIPTOR Request DEVICE
    8 0.000804   1.1.0    host          USB        82 GET DESCRIPTOR Response DEVICE
    9 0.060214   host     1.5.1         USB        80 URB_BULK out
   10 0.060238   1.5.1    host          USB        64 URB_BULK out
   11 0.060245   host     1.5.2         USB        64 URB_BULK in
```

- Ada empat mode dasar transfer untuk USB yaitu isochronous (0), interrupt (1), control (2) atau bulk
- Lalu kita lihat berdasarkan Length disini kita lihat terdapat Interrupt dan bulk



```
344 17.468429    1.5.2         host        USB       68 URB_BULK in
348 18.108383    1.5.2         host        USB       68 URB_BULK in
354 18.492382    1.5.2         host        USB       68 URB_BULK in
358 19.132429    1.5.2         host        USB       68 URB_BULK in
 70 0.858738     1.71.1        host        USB       72 URB_INTERRUPT in
105 2.778633     1.71.1        host        USB       72 URB_INTERRUPT in
107 2.866586     1.71.1        host        USB       72 URB_INTERRUPT in
```

- Lalu kita perhatikan tipe interruptnya , panjang frame dan data yang ditangkap



```
   Frame Length: 72 bytes (576 bits)
   Capture Length: 72 bytes (576 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: usb]
USB URB
   [Source: 1.71.1]
   [Destination: host]
   URB id: 0xffff9b8d36082240
   URB type: URB_COMPLETE ('C')
   URB transfer type: URB_INTERRUPT (0x01)
 ▷ Endpoint: 0x81, Direction: IN
   Device: 71
   URB bus id: 1
   Device setup request: not relevant ('-')
   Data: present (0)
   URB sec: 1553361595
   URB usec: 992489
   URB status: Success (0)
   URB length [bytes]: 8
   Data length [bytes]: 8
   [Request in: 71]
   [Time from request: 1.919870000 seconds]
   [bInterfaceClass: HID (0x03)]
   Unused Setup Header
   Interval: 8
   Start frame: 0
   Copy of Transfer Flags: 0x00000204
   Number of ISO descriptors: 0
Leftover Capture Data: 0000050000000000
```

- Lalu kita membuat filter dengan usb.transfer_type == 0x01

- Lalu kita filter kembali dengan ((usb.transfer_type == 0x01) && (frame.len == 72)) && !(usb.capdata == 00:00:00:00:00:00:00:00)
- Lalu add the capture ke column dan export data ke CSV untuk mendapatkan column
- Lalu filter untuk panggil Leftover Capture Data aja bisa dengan cat file | cut -d “,” -f 7 | cut -d “\”” -f 2 | grep -vE “Leftover Capture Data” > hexoutput.txt atau filter dengan manual monggo.
- Lalu didapatkan Leftover Capture Data

```
0000050000000000
0000270000000000
0000270000000000
0000170000000000
00001f0000000000
0000150000000000
0000120000000000
0000120000000000
0000170000000000
00002f0000000000
0000060000000000
0000040000000000
0000130000000000
0000170000000000
0000180000000000
0000150000000000
0000080000000000
0000170000000000
00000b0000000000
0000080000000000
00000e0000000000
0000080000000000
00001c0000000000
0000300000000000
```

- Lalu running script berikut

```
newmap = {
 2: "PostFail",
 4: "a",
 5: "b",
 6: "c",
 7: "d",
 8: "e",
 9: "f",
 10: "g",
 11: "h",
 12: "i",
 13: "j",
 14: "k",
 15: "l",
 16: "m",
 17: "n",
 18: "o",
 19: "p",
 20: "q",
 21: "r",
 22: "s",
 23: "t",
 24: "u",
 25: "v",
 26: "w",
 27: "x",
 28: "y",
 29: "z",
 30: "1",
 31: "2",
 32: "3",
 33: "4",
 34: "5",
 35: "6",
 36: "7",
 37: "8",
 38: "9",
 39: "0",
 40: "Enter",
 41: "esc",
 42: "del",
 43: "tab",
 44: "space",
 45: "-",
 47: "{",
 48: "}",
 56: "/",
 57: "CapsLock",
 79: "RightArrow",
 80: "LetfArrow"
 }

myKeys = open('hexoutput.txt')
i = 1
aw = ""
for line in myKeys:
     bytesArray = bytearray.fromhex(line.strip())
     #print "Line Number: " + str(i)
     for byte in bytesArray:
          if byte != 0:
               keyVal = int(byte)

     if keyVal in newmap:
          aw+=newmap[keyVal]
     else:
          print "No map found for this value: " +
str(keyVal)
     i+=1
print aw
```

- Dan didapatkan flag : **b00t2root{capturethekey}**