Write Up HACKTODAY 2019

DihKogAku?

Web

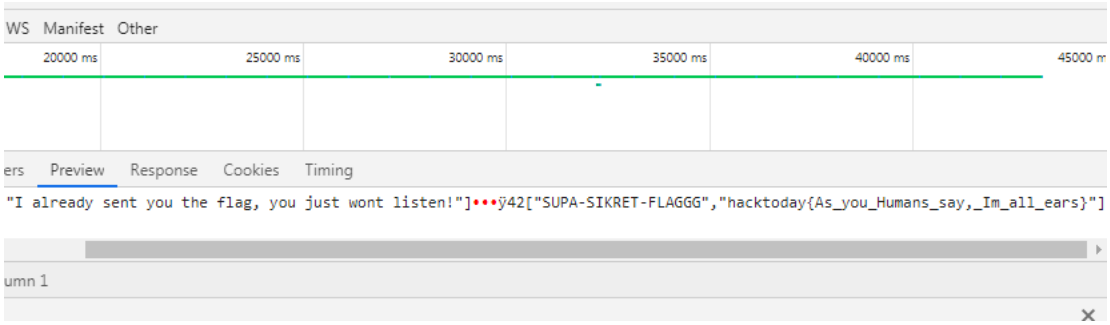
Flag.io

Cara Pengerjaan :

Diberikan sebuah website http://not.codepwnda.id:50001/ dengan sebuah tulisan yang tanpa henti seperti janji manis dia yang tanpa henti :(

I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!
I already sent you the flag, you just wont listen!

Lalu check inspect element di bagian network dan lihat preview nya



Flag :

hacktoday{As_you_Humans_say,_Im_all_ears}

Crypto

Acid (-_-)

Cara Pengerjaan :

Diberikan sebuah file text berupa DNA. Berikut DNA Code :

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)

Kode

Lalu, Jalankan scipt berikut ini :

```
kamus = {
    'AAA': 'a',
    'AAC': 'b',
    'AAG': 'c',
    'AAT': 'd',
    'ACA': 'e',
    'ACC': 'f',
    'ACG': 'g',
    'ACT': 'h',
    'AGA': 'i',
    'AGC': 'j',
```

```
    'AGG': 'k',
    'AGT': 'l',
    'ATA': 'm',
    'ATC': 'n',
    'ATG': 'o',
    'ATT': 'p',
    'CAA': 'q',
    'CAC': 'r',
    'CAG': 's',
    'CAT': 't',
    'CCA': 'u',
    'CCC': 'v',
    'CCG': 'w',
    'CCT': 'x',
    'CGA': 'y',
    'CGC': 'z',
    'CGG': 'A',
    'CGT': 'B',
    'CTA': 'C',
    'CTC': 'D',
    'CTG': 'E',
    'CTT': 'F',
    'GAA': 'G',
    'GAC': 'H',
    'GAG': 'I',
    'GAT': 'J',
    'GCA': 'K',
    'GCC': 'L',
    'GCG': 'M',
    'GCT': 'N',
    'GGA': 'O',
    'GGC': 'P',
    'GGG': 'Q',
    'GGT': 'R',
    'GTA': 'S',
    'GTC': 'T',
    'GTG': 'U',
    'GTT': 'V',
    'TAA': 'W',
    'TAC': 'X',
    'TAG': 'Y',
    'TAT': 'Z',
    'TCA': '1',
```

```
    'TCC': '2',
    'TCG': '3',
    'TCT': '4',
    'TGA': '5',
    'TGC': '6',
    'TGG': '7',
    'TGT': '8',
    'TTA': '9',
    'TTC': '0',
    'TTG': ' ',
    'TTT': '.',
}

c = open('acid.txt').read().strip()

flag = []
for x in range(0,len(c), 3):
    aw = c[x:x+3]
    print aw, kamus[aw]
    flag.append(kamus[aw])

print ''.join(flag)
```

Tambahan : Sebenarnya untuk soal ini mirip dengan salah satu event di ctftime dan sudah pernah saya publish wu nya **https://github.com/Akinarisekigawa/CTF/blob/master/Dna%20Decode.py**

Flag :

hacktoday{DN4ismybl00d}

Forensic

Know-your-flag

Cara Pengerjaan :

Diberikan sebuah gambar meme butterfly

Lalu, check Analyse terdapat passphare untuk extract dengan steghide , passphare : 987123654hohoho

```
End of Image
Additional bytes at end of file = 52
Dump of additional bytes:
Hex:
7061000073730000 7068000072610000
736500003d390000 3837000031320000
3336000035340000 686f0000686f0000
686f0000
Ascii:
pa..ss.. ph..ra..
se..=9.. 87..12..
36..54.. ho..ho..
ho..
```

Lalu, extract dengan steghide dan didapatkan sebuah gambar patrick star

Lalu, Langkah selanjutnya menggunakan exiftool dan didapatkan sebuah base32 dan didecode

```
D:\Tool\exiftool>ex.exe patrick.jpg
ExifTool Version Number         : 10.08
File Name                       : patrick.jpg
Directory                       : .
File Size                       : 5.1 kB
File Modification Date/Time     : 2019:08:10 09:57:16+07:00
File Access Date/Time           : 2019:08:10 10:08:02+07:00
File Creation Date/Time         : 2019:08:10 10:08:00+07:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Comment                         : JJ2XG5BANNUWIZDJNZTS4ICIMVZGKJ3TEB4W65LSEBTGYY
LHHIQGQYLDNN2G6ZDBPF5V6NDMNRPWQNDJNRPV6NLUGM4WQ2LEMVPTCZJSG5RWKM35
Image Width                     : 200
Image Height                    : 148
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
```

```
JJ2XG5BANNUWIZDJNZTS4ICIMVZGKJ3TEB4W65LSEBTGYYLHHIQGQYLDNN2G6ZDBPF5V6NDMN
RPWQNDJNRPV6NLUGM4WQ2LEMVPTCZJSG5RWKM35
```

Decode ☑ Auto Update

```
Just kidding. Here's your flag: hacktoday{_4ll_h4il__5t39hide_1e27ce3}
```

Flag :

hacktoday{_4ll_h4il__5t39hide_1e27ce3}

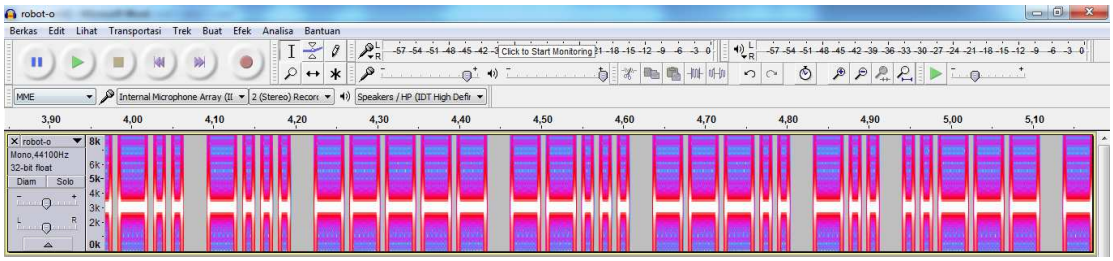
robot-o

Cara Pengerjaan :

Diberikan sebuah file yang awalnya extensionnya .video lalu ketika dicek ternyata merupakan file .wav

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
52 49 46 46 D4 0A 04 00 57 41 56 45 00 00 00 00  RIFFÔ...WAVE....
10 00 00 00 01 00 01 00 40 1F 00 00 40 1F 00 00  ........@...@...
```

Lalu, buka file dengan Audacity dan ternyata ketika dispectogram terdapat morse code. Lalu, decode morse code dengan inputan manual

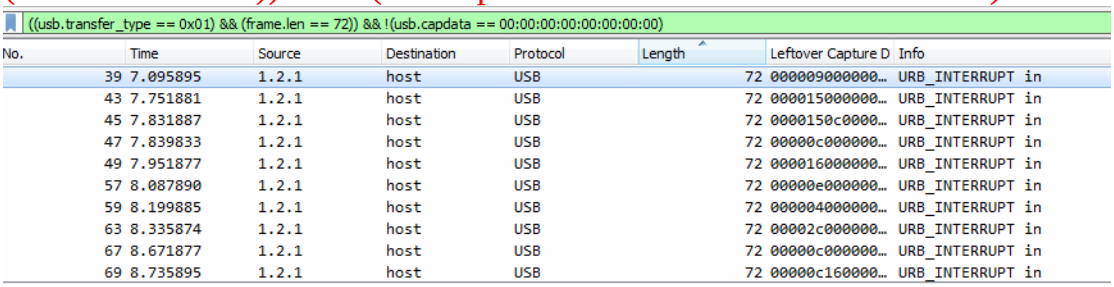


Flag :

hacktoday{8AE8CC93E223D5F957CE8B078D2020E7}

Intro

Cara Pengerjaan :

- Diberikan sebuah file .pcap dan dijalankan terdapat sebuah traffic USB , lalu 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)
- 
((usb.transfer_type == 0x01) && (frame.len == 72)) && !(usb.capdata == 00:00:00:00:00:00:00:00)

No.	Time	Source	Destination	Protocol	Length	Leftover Capture D	Info
39	7.095895	1.2.1	host	USB	72	000009000000…	URB_INTERRUPT in
43	7.751881	1.2.1	host	USB	72	000015000000…	URB_INTERRUPT in
45	7.831887	1.2.1	host	USB	72	0000150c0000…	URB_INTERRUPT in
47	7.839833	1.2.1	host	USB	72	00000c000000…	URB_INTERRUPT in
49	7.951877	1.2.1	host	USB	72	000016000000…	URB_INTERRUPT in
57	8.087890	1.2.1	host	USB	72	00000e000000…	URB_INTERRUPT in
59	8.199885	1.2.1	host	USB	72	000004000000…	URB_INTERRUPT in
63	8.335874	1.2.1	host	USB	72	00002c000000…	URB_INTERRUPT in
67	8.671877	1.2.1	host	USB	72	00000c000000…	URB_INTERRUPT in
69	8.735895	1.2.1	host	USB	72	00000c160000…	URB_INTERRUPT in

- Lalu, add the capture ke column dan export data ke CSV untuk mengambil Leftcover Capture Data
- Didapatkan sebuah leftcover capture data dengan di filter manual
- ```
1 0000090000000000
2 0000150000000000
3 0000150c00000000
4 00000c0000000000
5 0000160000000000
6 00000e0000000000
7 0000040000000000
8 00002c0000000000
9 00000c0000000000
10 00000c1600000000
11 0000160000000000
12 00002c0000000000
13 0000170000000000
14 00000b0000000000
15 00000b0800000000
16 0000080000000000
17 00002c0000000000
18 0000090000000000
19 0000040000000000
20 0000160000000000
21 0000170000000000
22 00002c0000000000
```
```

- Lalu, cek keyboard USB Code
  https://www.win.tue.nl/~aeb/linux/kbd/scancodes-14.html

Kode

Lalu, Jalankan scipt berikut ini :

```
newmap = {
 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",
```

```
 45: "-",
 47: "{",
 48: "}",
 56: "/",
 }

myKeys = open('usb2.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 "Tidak ada: " + str(keyVal)
    i+=1
print aw
```

```
friiskaisstheefastseectionionoffthecsaardasahungarianfolkdaanceeorofmosstofflisz
thunggaariaanrhapsodieswhichtakeetaakeetheirfrormthhisdaanceethefisriskaaisgeene
raallyeitherturbuleentorjubilantintonegriffhollandtogeehterrtherrwithedborownfoo
undeeddthhebusinessin20090909baasseedonapriincipleeioffffdeeliveeringgfeellellg
oodfooddmaasdeefromfreeshqualityanndreesponbilitysiblyyysourceeceedingredientsbo
thfoundeersareeinseedideer422unddeer422alumniithhecompanycyurrentlyyoperaatesflo
urbrraannceeheheessneeaarrhighdiseentyensityofficeebuuildingdiinggswhitthitth70p
eercentoffittsreeveeneuescominggfromlunchhtiimeetraadeeisaawhimwaallkinhhhhgarou
ndthebaackyaardlikeesomethinggstroublingghiimmflaagississi-l3arn-us8-c4ptuptuur3
icaalledhiiminaddnddwhenioiasskedwhatsgoinggonheejustsaaidcaanigoooutfoorrawhile
eikonwnoowheejusstjusttryyinggtoochaanggeethhesubbjectthenagaainmaaybeeheejusstm
eeneeededsoemeefreesairtoocleeaarihiissmdindsooisasiddyeesthheennestxxtdaayisaaw
hiimwaashiinggmyneeighbourscaaranddwhenheecaamehoomeeiasskedhiimwhyheewouldddoot
haatthaatthtahaattheejusstsaaiddheetoldmeetoosoitoldhiimtotaakkeaboaathnandddoth
hissosshiisshoomeeweorkhwheenhewaasdoneeitoldhimthaatheedindnthaavetowaashthheec
aarbeecaauseeitsaaxwwaassnootthissreesponsibiilitieieesshekjjjjusstnood
```

Lalu, karena tulisan flag yang kurang jelas flaagississi-l3arn-us8-c4ptuptuur3 jadi ku menggunakan instingku dan didapatkanlah flagnya karena flagnya uppercase dan ku pakai list lowercase jadi ku uppercase.

Flag :

hacktoday{I-L3ARN-US8-C4PTUR3}

Misc

Sanity Check

Cara Pengerjaan :

Diberikan flag cuman cuma Cuma sahaja copy dan paste

Flag :

hacktoday{sanity_check}