

Write Up HackToday 2019

Siapa ya?

Siapa ya?

M. Nur Hasan Aprilian
M. Hendro Junawarko

Universitas Teknokrat Indonesia

Misc

Sanity Check

Cara Pengerjaan

Udah mantengin <https://hacktoday.codepwnda.id> dari pagi jam 8, eh apa daya disuruh emak belanja kepasar buat besok lebaran, ya udah deh telat, untungnya dikasih flag gratis :v

Flag

hacktoday{sanity_check}

Forensics

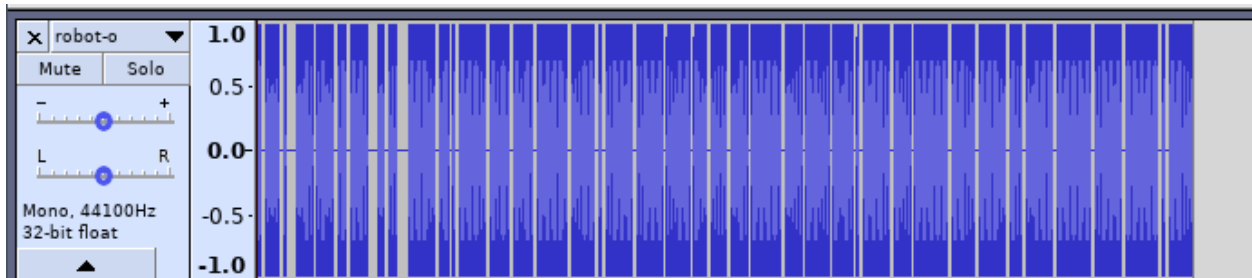
Robot-o

Cara Pengerjaan

Didapat sebuah file audio bertipe wave

```
[flintz@shadow]-(~/Downloads) $file robot-o.voice
robot-o.voice: RIFF (little-endian) data, WAVE audio
```

coba lakukan analisis audio tersebut dengan audacity, diketahui terdapat morse code pada file tersebut.



Lakukan decode di <https://morsecode.scphillips.com/translator.html> dengan inputan manual :v

Input:



Output:

THEFLAGIS8AE8CC93E223D5F957CE8B078D2020E7

Flag

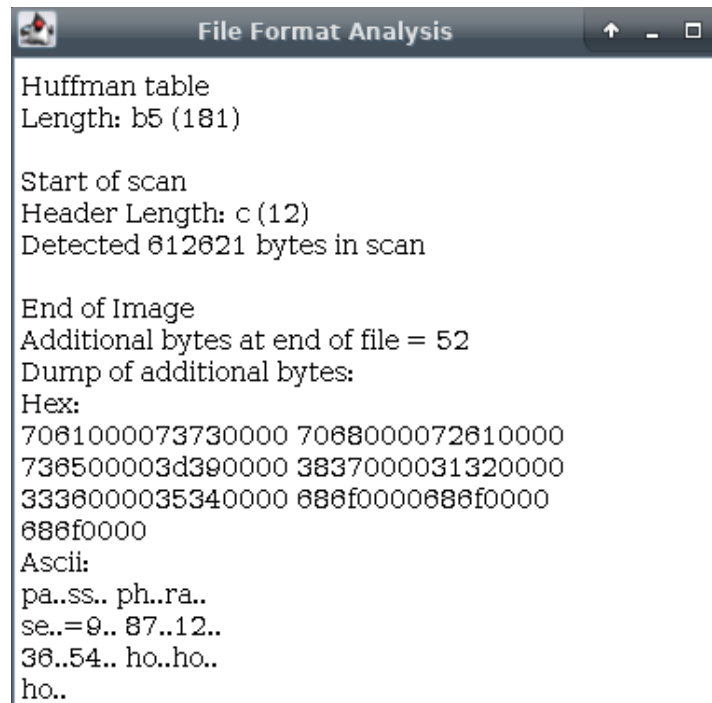
hacktoday{8AE8CC93E223D5F957CE8B078D2020E7}

Know-your-flag

Cara Pengerjaan



Didapat sebuah gambar mim yang terdapat sebuah kotak hitam, saya coba lakukan analisis dengan stegsolve untuk melihat hasil tersebut namun ternyata flag tidak ada disana -_- . masih dengan stegsolve, cek file format analyse dan terdapat hex code disana yang jika didecode terdapat passphrase=987123654hohoho



sudah pasti passphrase tersebut untuk apa, langsung saja lakukan steghide

steghide extract -sf is-this-a-flag.jpg



Didapat file lagi patrick.jpg, dengan exiftool didapat dimana metadata file tersebut terdapat sebuah base32 yang diencode berisi sebuah flag.

```
[x]-[flintz@shadow]~[~/Downloads]
$ echo JJ2XG5BANNUWIZDJNZTS4ICIMVZGKJ3TEB4W65LSEBTGYLHHIQGQYLDNN2G6ZDBPF5V6
NDMNRPWQNDJNRPV6NLUGM4WQ2LEMVPTCZJSG5RWKM35 | base32 -d
Just kidding. Here's your flag: hacktoday{_4ll_h4il__5t39hide_1e27ce3}
```

Flag

hacktoday{_4ll_h4il__5t39hide_1e27ce3}

Intro

Cara Pengerjaan

Diberikan file capture rekaman sebuah USB streams, setelah melakukan analisis dengan wireshark diketahui dengan menggunakan USB keyboard.

```
[x]-[flintz@shadow]-[~/Downloads]
$ tshark -r intro.pcapng -q -z io,phs

=====
Phionify
Protocol Hierarchy Statistics
Filter: morabilia of light glitter ~
usb
  text
  usb.capdata
=====
Berdasarkan frames: 7936 bytes: 530824 ses ekstraksi us
frames: 15 bytes: 1085
frames: 2850 bytes: 205195
=====
```

Lakukan proses ekstraksi usb.capdata dengan bantuan t-shark untuk mendapatkan setiap framenya.

```
tshark -r intro.pcapng -Y usb.capdata -Tfields -e usb.capdata > data
```

```
[flintz@shadow]-[~/Downloads]
$ tshark -r intro.pcapng -Y usb.capdata -Tfields -e usb.capdata | head
00:00:09:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:15:00:00:00:00:00
00:00:15:0c:00:00:00:00
00:00:0c:00:00:00:00:00
00:00:16:00:00:00:00:00
00:00:00:00:00:00:00:00
00:00:0e:00:00:00:00:00
00:00:04:00:00:00:00:00
00:00:00:00:00:00:00:00
tshark: An error occurred while printing packets: Broken pipe.
[flintz@shadow]-[~/Downloads]
$ tshark -r intro.pcapng -Y usb.capdata -Tfields -e usb.capdata > data
```

Saya lakukan pemetaan untuk HID key tersebut juga bantuan dari referensi ini <https://blog.phionify.web.id/post/writeup-bsidessf19-ctf-forensic/>

Kode

solver-usb.py

```
def usbHID(txt):
    dic = {
        'a': '04', 'b': '05', 'c': '06', 'd': '07', 'e': '08',
        'f': '09', 'g': '0a', 'h': '0b', 'i': '0c', 'j': '0d',
        'k': '0e', 'l': '0f', 'm': '10', 'n': '11', 'o': '12',
        'p': '13', 'q': '14', 'r': '15', 's': '16', 't': '17',
        'u': '18', 'v': '19', 'w': '1a', 'x': '1b', 'y': '1c',
        'z': '1d', '=': '2e', '/': '38', '{': '2f', '}': '30',
        '1': '1e', '2': '1f', '3': '20', '4': '21', '5': '22',
        '6': '23', '7': '24', '8': '25', '9': '26', '0': '27',
        '-': '2d', '_': '2c', ':': '33', ';': '36', '/': '38',
        '\n': '58', '.' : '37'
    }
    dic = {dic[i] : i for i in dic}
    plain = "".join(dic.get(i,"") for i in txt.split(':'))
    return plain

def decodeUSBHID():
    cap = open('data').read().rstrip('\r').split('\n')
    cap = [i.split(':')[2] for i in cap if i != ""]
    return "".join(usbHID(i) for i in cap)

print decodeUSBHID().upper()
```

```
[flintz@shadow]~[~/Downloads/into]
$python solver-usb.py
FRRISKA IIS THHE FAST SSECTIONION OOF THE CSSARDAS A HUNGARIAN FOLK DDANCCE OR O
F MOOST OOF LISZT HUNNGGARIAN RHAPSODIES WHICH TAKKETTAKKE THEIR FROM TTHIS DD
ANCE THE FISRISKKA IS GGENERALLY EITHER TURBULLENT OR JUBILANTT INN TONE GRIFF
HOLLAND TOGGEHTHEER WITH ED BOROWN FFOUNDEED TTHE BUSINESSS INN 22090909 B
BAASSED ONN A PRRINCIPLE IOOGFF DDELIVVERINNG FFELL EEL GOOD F000D MMASDDEE FR
OMM FRRESH QUALITY AANDD RRESPONBILITY SIBLUYY SOURCCECCED INGREDIENTS BOTH FOU
NDERS ARRE INSSIDDER 442 UNNDERR 442 ALUMNNI TTHEE COMPANY CYURRENTLY OPERR
ATES FLOUR BBRAANCCEHEHHEES NNEEAARR HIGH DISSENTYENSITY OFFICCE BBUILDINGDDINN
GS WHIITHIITH 70 PPERR CENT OOFF IITS RREVENEUES COMINNG FROM LUNCCHTTIMME TRRA
DDE I SSAW HIM WWA:LLKINNH H G AROUND THEE BBACKYYARD LIKKE SOMETHINNGS TROUBLIN
NG HHIM FLLAGG IIS IIS I-L3ARN-US8-C4PTUPTUUR3 II CCALLED HHIM IN ADDNND WHEN
III AASKED WHATS GOINNGG ON HHEE JUST SSAIDD CCAN I GGO OUT FFOORR A WHILLE I K
ONWNOW HHEE JUUSTT JUST TRYINNG TTOO CHHANNGGE TTHE SUUBJECT THEN AGGAIN MMAYB
BEE HHE JUUSTT MEENNEEDED SOE MME FRRES AIRR TTO CLLEEAR IHHIIS MDIND SSO I SSSI
ID YYES TTHEE ENNEST XTT DDAY I SSAW HHIM WWASHHINNG MY NNEIGHBOURS CCARR ANND
WHENN HHEE CCAME HHOMME I AASKEDD HHIM WHY HHEE WOULD DD THHAATHHATTHAHAAT
T HHEE JUUSTT SSAIDD HHE TOLD MME TTOO SOO I TOLD HHIM TO TTAKE A BOATHN ANND
DO TTHIISOOS HHIIS HHOMMEWEORKK HWHHENN HE WWASS DONNEE I TOLD HIM THHAT HHE DI
NDNT HHAVE TO WWASHH TTH E CCAR BBECCAUSSE IT SSAXWWAASS NN00T HIIS RRESPONBIBI
LITIEIEES HE KKJJJUUSTT NN0D
```

ternyata diawal tadi salah mapping terhadap byte '2d'underscore ternyata sebuah strip _-

dan lakukan sedikit kesalahan pada flagnya.

Flag

hacktoday{I-L3ARN-US8-C4PTUR3}

Web

Flag.io

Cara Pengerjaan

didapat sebuah web <http://not.codepwnda.id:50001>



web tersebut melakukan request dan menampilkan koneksi socket yg berulang untuk menampilkan response tersebut saya coba dengan bantuan burp suite

Response

Raw	Headers	Hex
-----	---------	-----

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Sat, 10 Aug 2019 12:27:05 GMT
Content-Type: application/octet-stream
Connection: close
Access-Control-Allow-Credentials: true
Content-Length: 1136
```

[illegible]

Flag

hacktoday{As_you_Humans_say,_Im_all_ears}

Crypto

Acid (- -)

Cara Pengerjaan

diberikan sebuah file acid.txt


```

[flintz@shadow]--[~/Downloads]
$ cat acid.txt
CGGCAGAAAATATTGAATACAATGAGGCAGAGACACAGAAACATGATCCCAAGGAGTACAAAACATTTGAGTACAAACAG
AACTTTGAATAGAAGGACAATCAAAAGTTTGAATACAATCACGAAAATCTTGACAGAGAATCACGAGGAAACATAAAATCT
TGCTCGCTCGGTTGAAAAATAAAAGTAAACTTTGCAGACAAGCACAATCAGACAGTTGAACAGAATGATAATGAGTACA
AGGCCAAGTTTGCAGAAAATCACGTTGATAACAATCCGAAGAATAATTAATCTTGAATAAAATCTTGATAACAATCCG
AAAAATCAATAGATTGAGAATCCAGCATCACCCAAGGCAGAGATTGAGAATCCAGCATCACCCAAGGCAGAGATTGACGA
CAATCACACATAGAAGGAAATTGCAGACACATAGAAAAATTTTGATGCACACGAAAATCAGACAGATAACATTGAATAAA
ATCTTGAACAAAATCCGAAAAAGGTTGAGCACAATCAGACAGTTGCCAGACACCCACAGTTGAGAATCCAGCATCACCC
AAGGCAGAGATTGAGAATCCAGCATCACCCAAGGCAGAGATTGACGACAATCACACATAGAAGGAAATTGAGAATCAGAT
TGAACACACACATTACACACAAAATCTTGATTACAATCCATAGAATCACGTTGAATAAAAGTAAATATTGATTACACAC
CATCCAATAAACCCAACTAAAATCATTACACACAGGACAATAAACAAAATCACGAAAATCTTGAATAAAATCTTGACCCC
AATCACGCAGAGATTGATGCACACGAAAATCAGACAGATAACATTGAATAAAATCTTGCCAGACACCCACAGTTGCTCG
CTCGGTTGATAACACACCCAATTAAGGAAAATCTTGAACAGAAAATATTGATCCCAAGGAGTACAAAACATTTGAAC
ACACACCAGAAAATAAAAAAATCTTGAATACAATCACGAAAATCTTGATTACATGCATACAAGAATCTTGAATAAAAT

```

diketahui bahwa chipertext tersebut merupakan enkripsi dari DNA code

<https://esolangs.org/wiki/DNA-Sharp>,

lakukan pemetaan dengan memakai script DNA-decode referensi dari

<https://github.com/Akinarisekigawa/CTF/blob/master/Dna%20Decode.py>

Kode

dna-decode.py

```

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)

```

Sebagian besar DNA bersifat non kode yang menyandikan protein Dalam sel DNA tersusun dari 4 flag is DN4ismybl00d kromosom kromosom

Flag

hacktoday{DN4ismybl00d}