CAPTURE THE FLAG
WRITE UP

Dibuat oleh :
PORT80
(Johan Wahyudi)

COMNETS CTF SEASON 2 2015

CHALLENGE : REVERSE ENGINEERING
CASE : REVERSE ENGINEERING01
FLAG :COMNETS{CintailahIndonesia}

Executive Summary

Reversing linux Executable
Tools : Retargetable Decompiler

2. Technical Report

Pada kasus ini kita di beri file dengan nama reverse01, yang mana apabila di cek tipe filenya itu adalah ELF 32-bit LSB executable, apabila di jalankan, program akan menampilan..

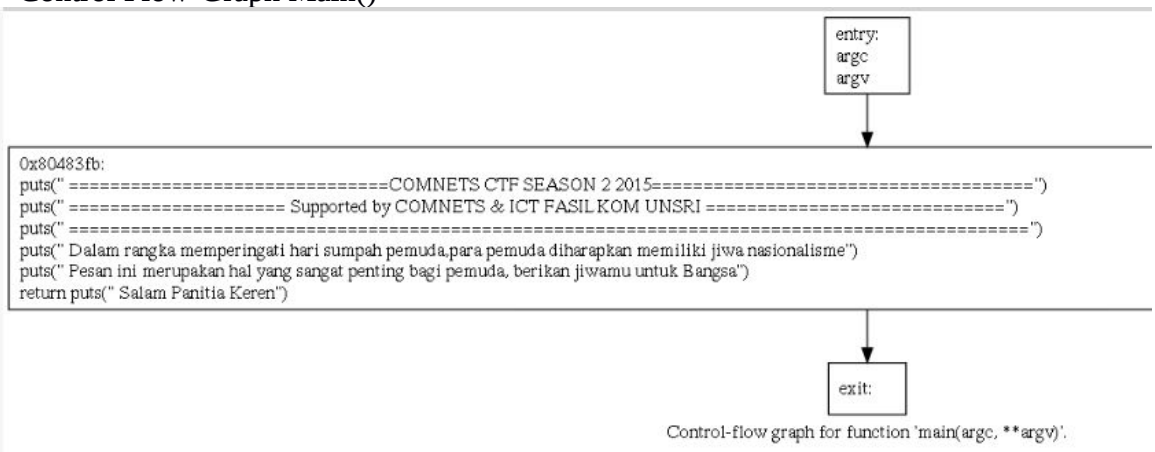
```
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/REVERSE ENGINEERING/reverse01# ./reverse01
 ================================COMNETS CTF SEASON 2 2015====================================
 ==================== Supported by COMNETS & ICT FASILKOM UNSRI ============================
 ================================================================================================
 Dalam rangka memperingati hari sumpah pemuda,para pemuda diharapkan memiliki jiwa nasionalisme
 Pesan ini merupakan hal yang sangat penting bagi pemuda, berikan jiwamu untuk Bangsa
 Salam Panitia Keren
root@kali:/media/root/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/REVERSE ENGINEERING/reverse01#
```

Tidak ada input dari program ini, setelah di decompile menggunakan program RetDec, didapat..

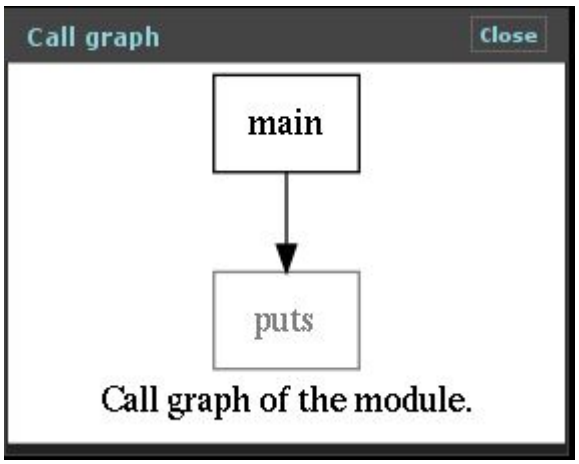
- Program dalam bahasa C

```
#include <stdint.h>
#include <stdio.h>

// ------------------------ Functions ------------------------

// Address range: 0x80483fb - 0x804847f
int main(int argc, char ** argv) {
    // 0x80483fb
    puts(" ================================COMNETS CTF SEASON 2 2015====================================");
    puts(" ==================== Supported by COMNETS & ICT FASILKOM UNSRI ============================");
    puts(" ================================================================================================");
    puts(" Dalam rangka memperingati hari sumpah pemuda,para pemuda diharapkan memiliki jiwa nasionalisme");
    puts(" Pesan ini merupakan hal yang sangat penting bagi pemuda, berikan jiwamu untuk Bangsa");
    return puts(" Salam Panitia Keren");
}

// --------------- Dynamically Linked Functions ---------------

// int puts(const char *);

// --------------------- Meta-Information ---------------------

// Detected compiler/packer: gcc (4.9.2)
// Detected functions: 1
// Decompiler release: v2.1.1.1 (2015-11-18)
// Decompilation date: 2015-11-22 12:42:22
```

- Control Flow-Graph Main()



- Call Graph



Bisa kita lihat disana, tidak ada perintah seperti compare dll, hanya ada perintah put, coba kita lihat hasil decompile dalam bahasa Assembly...

```
;  section: .eh_frame
0x8048728:   14 00 00 00 00 00 00  01 7a 52 00 01 7c 08 01   |.........zR..|..|
0x8048738:   1b 0c 04 04 88 01 00 00  20 00 00 00 1c 00 00 00   |........ .......|
0x8048748:   78 fb ff ff 40 00 00 00  00 0e 08 46 0e 0c 4a 0f   |x...@......F..J.|
0x8048758:   0b 74 04 78 00 3f 1a 3b  2a 32 24 22 43 4f 4d 4e   |.t.x.?.;*2$"COMN|
0x8048768:   45 54 53 7b 43 69 6e 74  61 69 6c 61 68 49 6e 64   |ETS{CintailahInd|
0x8048778:   6f 6e 65 73 69 61 7d 43  0f 03 75 7c 06 02 66 0c   |onesia}C..u|..f.|
0x8048788:   01 00 41 c5 43 0c 04 04  38 00 00 00 6c 00 00 00   |..A.C...8...l...|
0x8048798:   e8 fc ff ff 61 00 00 00  00 41 0e 08 85 02 41 0e   |....a....A....A.|
0x80487a8:   0c 87 03 43 0e 10 86 04  41 0e 14 83 05 4e 0e 30   |...C....A....N.0|
0x80487b8:   02 48 0e 14 41 c3 0e 10  41 c6 0e 0c 41 c7 0e 08   |.H..A...A...A...|
0x80487c8:   41 c5 0e 04 10 00 00 00  a8 00 00 00 1c fd ff ff   |A...............|
0x80487d8:   02 00 00 00 00 00 00 00  00 00 00 00              |............    |
;  section: .init_array
```

Setelah di telusuri, ternyata ada variabel yang tidak pernah di tampilkan,, padahal di sanalah letak flagnya, karena keterbatasan pengetahuan di bidang reverse engineering, saya belum bisa untuk menampilkan variabel tersebut, :/ ... Tapi di sini saya sudah mendapatkan flagnya..

3. Conclusion

Flag : COMNETS{CintailahIndonesia}

4. Reference

https://retdec.com/

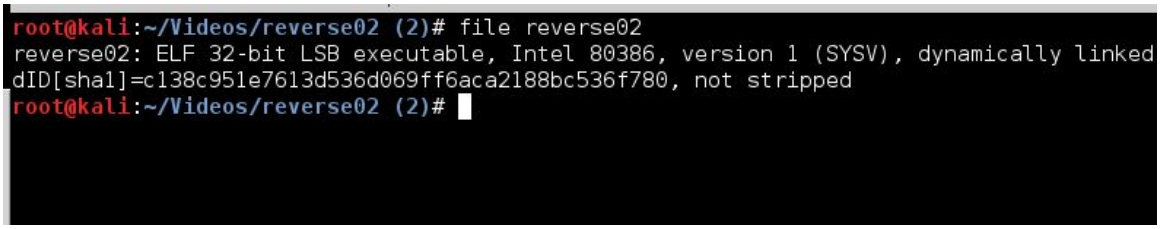
CHALLENGE : REVERSE ENGINEERING
CASE : REVERSE ENGINEERING02
FLAG : COMNETS{mERd3K4KiTa}

1. Executive Summary

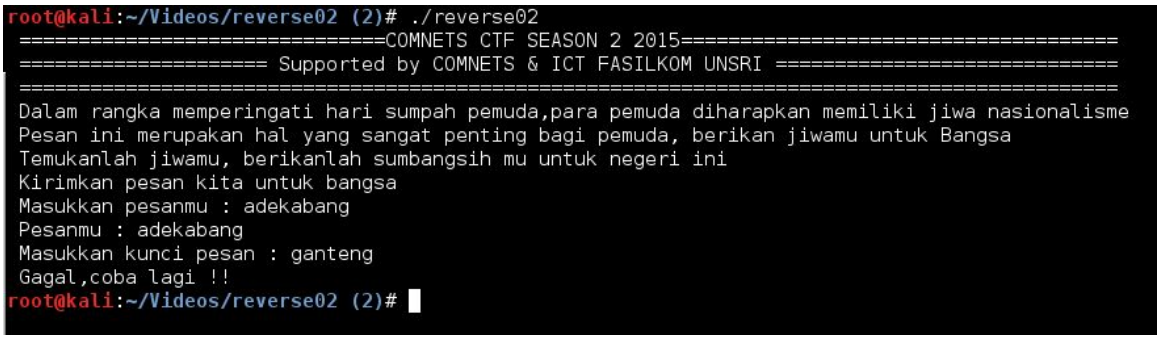
Reversing linux executable
Tools : Ltrace, Retdec

2. Technical Report

Pada kasus kali ini kita di beri file dengan nama reverse02 dengan tipe ELF 32-bit,



Sekarang coba kita jalankan programmnya..



Bisa kita lihat diatas, apabila kunci pesan salah maka pesan gagal dikirim.. Sekarng tugas kita adalah bagaimana cara untuk mendapatkan kata kunci itu..

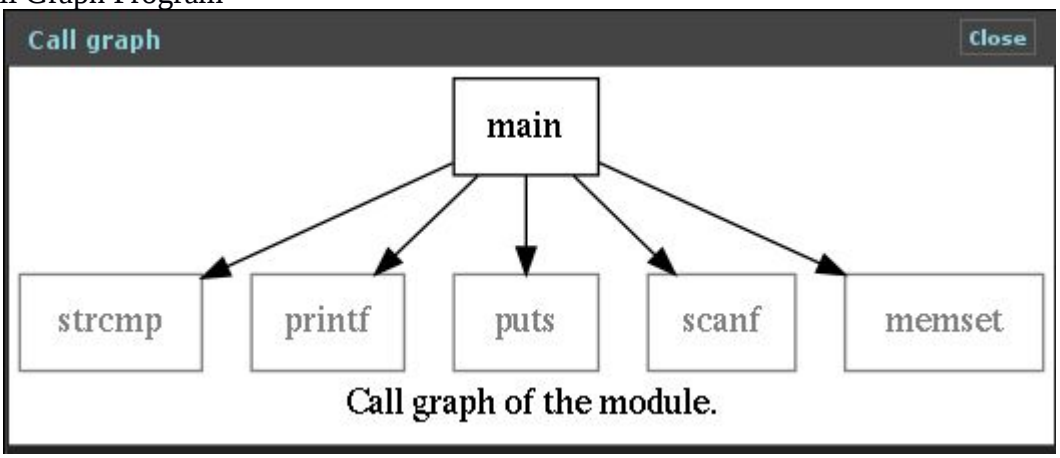
Logikanya adalah kunci pesan yang kita input bakal di sandingkan dengan kata kunci pesan yang sebenarnya, sekarang kita lihat strings pada program di atas,,
Dengan menggunakan perintah : **strings <nama file>**

```
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
strcmp@@GLIBC_2.0
_ITM_deregisterTMCloneTable
__x86.get_pc_thunk.bx
data_start
printf@@GLIBC_2.0
_edata
```

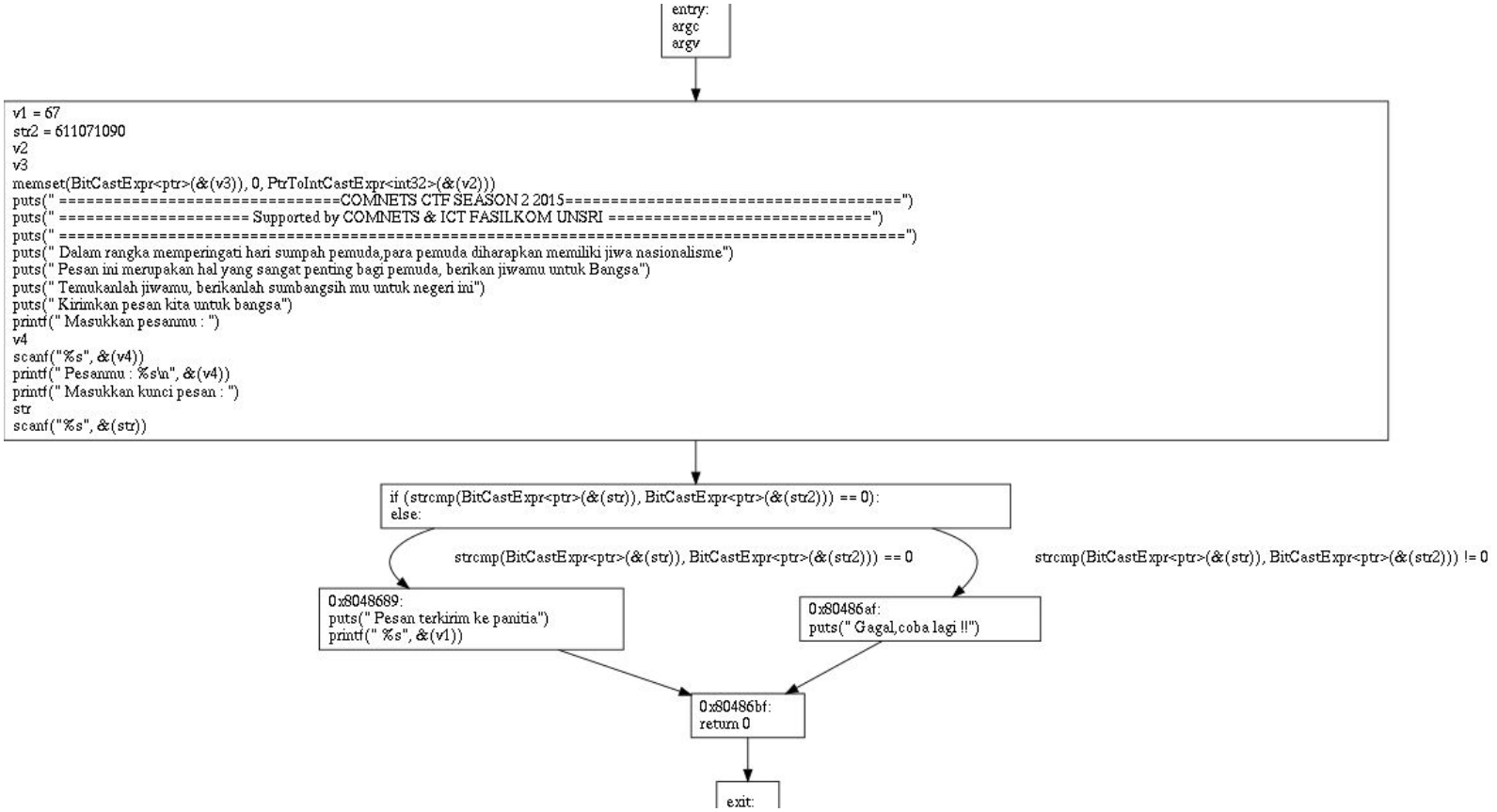
Bisa kita lihat pada gambar diatas, di dalam program ada perintah strcmp, yang mana fungsinya untuk membandingkan nilai string yang kita input dengan string kunci pesan, Biar lebih jelas kita gunakan perintah **grep...**

```
root@kali:~/Videos/reverse02 (2)# strings reverse02 | grep strcmp
strcmp
strcmp@@GLIBC_2.0
root@kali:~/Videos/reverse02 (2)#
```

- call Graph Program



- control flow graph main ()



Kita asumsikan kunci pesan yang dimasukkan berupa string, dan di bandingkan dengan perintah strcmp(), maka cara pertama yang bisa kita lakukan adalah dengan cara mengeceknya dengan tools Ltrace, Ltrace akan melakukan tracing terhadap seluruh pemanggilan fungsi dari library C oleh program, dalam hal ini fungsi yang akan kita “intip” adalah strcmp.. Ok mari kita mulai..
Perintah : **Ltrace ./reverse02**

```
root@kali:~/Videos/reverse02 (2)# ltrace ./reverse02
__libc_start_main(0x80484ab, 1, 0xff918484, 0x80486d0 <unfinished ...>
puts(" ================================"... ================================C
)                                                 = 95
puts(" ===================== Supported"... ===================== Supported b
)                                                 = 95
puts(" ================================"... ================================
)                                                 = 95
puts(" Dalam rangka memperingati hari "... Dalam rangka memperingati hari su
)                                                 = 96
puts(" Pesan ini merupakan hal yang sa"... Pesan ini merupakan hal yang sang
)                                                 = 86
puts(" Temukanlah jiwamu, berikanlah s"... Temukanlah jiwamu, berikanlah sur
)                                                 = 62
puts(" Kirimkan pesan kita untuk bangs"... Kirimkan pesan kita untuk bangsa
)                                                 = 34
printf(" Masukkan pesanmu : ")
__isoc99_scanf(0x80489af, 0xff9182da, 0, 0 Masukkan pesanmu : apaajadeh
)                                                 = 1
printf(" Pesanmu : %s\n", "apaajadeh" Pesanmu : apaajadeh
)                                                      = 21
printf(" Masukkan kunci pesan : ")
__isoc99_scanf(0x80489af, 0xff918370, 0, 0 Masukkan kunci pesan : ganteng
)                                                 = 1
strcmp("ganteng", "r4l$")
puts(" Gagal,coba lagi !!" Gagal,coba lagi !!
)                                                           = 20
+++ exited (status 0) +++
root@kali:~/Videos/reverse02 (2)#
```

Bisa kita lihat, pada fungsi strcmp..

```
__isoc99_scanf(0x80489af, 0xff918370, 0, 0 Masukkan kunci pesan : ganteng
)                                                 = 1
strcmp("ganteng", "r4l$")
puts(" Gagal,coba lagi !!" Gagal,coba lagi !!
)                                                           = 20
+++ exited (status 0) +++
```

String yang kita inputkan akan di bandingkan dengan string “**r4l$”**, dan untuk string pesanmu tidak di bandingkan, itu berarti pesan yang kita inputkan terserah.. Asal kunci pesannya benar maka pesan akan terkirim.. Sekarang kita coba dengan kunci pesan **r4l$** :

```
root@kali:~/Videos/reverse02 (2)# ./reverse02
 ================================COMNETS CTF SEASON 2 2015=================================
 ==================== Supported by COMNETS & ICT FASILKOM UNSRI ============================
 ============================================================================================
 Dalam rangka memperingati hari sumpah pemuda,para pemuda diharapkan memiliki jiwa nasionalisme
 Pesan ini merupakan hal yang sangat penting bagi pemuda, berikan jiwamu untuk Bangsa
 Temukanlah jiwamu, berikanlah sumbangsih mu untuk negeri ini
 Kirimkan pesan kita untuk bangsa
 Masukkan pesanmu : PesanUntukAdekAbang
 Pesanmu : PesanUntukAdekAbang
 Masukkan kunci pesan : r4l$
 Pesan terkirim ke panitia
 C$O$M$N$E$T$S${m%E%R%d%3%K%4%K%i%T%4%}%@!@|v@@/root@kali:~/Videos/reverse02 (2)#
```

Ups... Notif yang kita terima “ pesan terkirim ke panitia” dan di bawahnya adalah flag yang kita cari.. (hilangkan karakter $)

3. Conclusion

Flag : COMNETS{mERd3K4KiTa}

4. Reference

CHALLENGE : REVERSE ENGINEERING
CASE : REVERSE ENGINEERING03
FLAG : COMNETS{Indonesia_R4y4}

1. Executive Summary

REVERSING JAVA
Tools : Strings on linux

2. Technical Report

Pada kasus kali ini, kita di beri program dengan ekstensi .exe , tapi setelah di analisa program tersebut adalah program java, saya mencoba melihat strings di program ini..
Dengan perintah : **strings <nama file>**

```
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
D$$SW
j/j.
T$,RP
h@@@
h8@@
UVh$@@
D$ PQ
D$8E
QRSP
L$$^]_3
2}pUV
hA)@
hX@@
_^]d
hX)@
D$0j
hx)@
  SUVW
_^][
L$ d
L$ UV
```

L$0_^][d
</tY<\tU
L$4Q
u+j h
5j   h
h|@@
D$$R
L$ P
T$ R
D$ P
hX*@
D$PTA@
D$THA@
L$(9l$
D$\@A@
D$`4A@
D$d(A@
L$$9l$
h A@
L$8PQ
D$<RP
T$hj
L$hP
L$@Q
L$hR
L$HPQ
T$$@
h A@
L$PPQ
T$ P
T$(@
L$ h|@@
L$ V
_^][d
hA+@
D$$RhxA@
L$(P
h`A@
hn+@
D$ h
T$(PR
L$0f
L$4QP
T$ j
SUV+
t   HJ

_^][
%X0@
%,0@
%00@
%40@
%80@
%<0@
%@0@
%D0@
%H0@
%L0@
%P0@
%T0@
%\0@
%`0@
%d0@
%h0@
%l0@
%p0@
%t0@
%x0@
%|0@
SVW
MFC42.DLL
wcslen
__CxxFrameHandler
_mbscmp
getenv
printf
MSVCRT.dll
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
FreeLibrary
GetProcAddress
LoadLibraryA

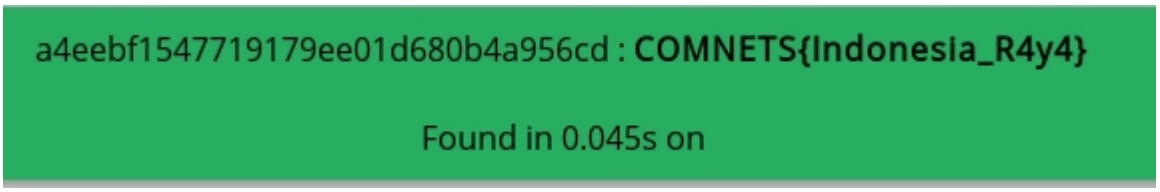
MultiByteToWideChar
GetModuleFileNameA
GetModuleHandleA
KERNEL32.dll
RegCloseKey
RegQueryValueExA
RegOpenKeyExA
ADVAPI32.dll
_strnicmp
JNI_CreateJavaVM
java/lang/String
main
([Ljava/lang/String;)V
-Djava.class.path=
.config
.cfg
classpath
mainclass
jvmdll
RuntimeLib
CurrentVersion
SOFTWARE\JavaSoft\Java Runtime Environment
CLASSPATH
CLASS_PATH
\jvm.dll
jvm.dll
..\jre\bin\
jre\bin\
bin\
JAVA_HOME
JRE_HOME
-Djava.compiler=NONE
-Dj2e.app.path=
MFC failed to initialize!
U33333333333333333333333333333333333333333A37
11111111111111111111111111111111111111
::::::::::::::::::::::::::::::::::::
h|vfffffffffffffffffffffffffv
C]x|||||||||||||||||||||||~
#WjkkkkkkkkkkkkkkkkkkkkkkkkkkrqpkoqqocdO9
PQ_[KIIIIIIIIIIIIIIIIIIIIIIIH`HIG`HGYa`_X6
.....
00000000000000000000000000
/---/

/---/

```
"*************************
!$$$$$$$$$$$$$$$$$$'#)(#)
""""""""""
(&&(
&((&
&((&
(&&(
' """""""""""!!!%
META-INF/
META-INF/MANIFEST.MFManifest-Version: 1.0. Build Series
"a4eebf1547719179ee01d680b4a956cd"
Ant-Version: Apache Ant 1.9.4
Created-By: 1.7.0_79-b14 (Oracle Corporation)
Class-Path:
X-COMMENT: Main-Class will be added automatically by build and Program
   detail youth.Youth COMNETS CTF Season 2 2015
Main-Class: youth.Youth
youth/PK
youth/Youth.class
<init>
Code
LineNumberTable
LocalVariableTable
this
Lyouth/Youth;
main
([Ljava/lang/String;)V
args
[Ljava/lang/String;
SourceFile
Youth.java
~~Jiwa Pemuda~~
0-> Apa yang kamu lihat dan rasakan adalah jiwamu
6-> Jiwa yang menggelora,seperti irama musik bang rhoma
)-> Masa Muda adalah masa yang ber-api-api
E-> Namun Jangan sampai membakar diri,nanti bisa kebakaran sampai mati
By: Panitia Keren
youth/Youth
java/lang/Object
java/lang/System
Ljava/io/PrintStream;
java/io/PrintStream
println
(Ljava/lang/String;)V
META-INF/
META-INF/MANIFEST.MFPK
```

```
youth/PK
youth/Youth.classPK
mainclass youth.Youth
```

Strings pada program, banyak juga ya.. Tapi disini saya tertarik pada strings **Manifest-Version: 1.0. Build Series "a4eebf1547719179ee01d680b4a956cd"** build seriesnya seperti ada yang janggal, sekarang coba kita decrypt strings di atas, sepertinya string di atas di encrypt meggunakan md5, ok kita mulai...



Ups ternyata benar,.. Flag di temukan..

3. Conclusion

Flag : COMNETS{Indonesia_R4y4}

4. Reference

http://md5decrypt.net/en/