KEAMANAN JARINGAN KOMPUTER

Eko Pratama

09011181320004

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

TUGAS 7

ANALISA MALWARE

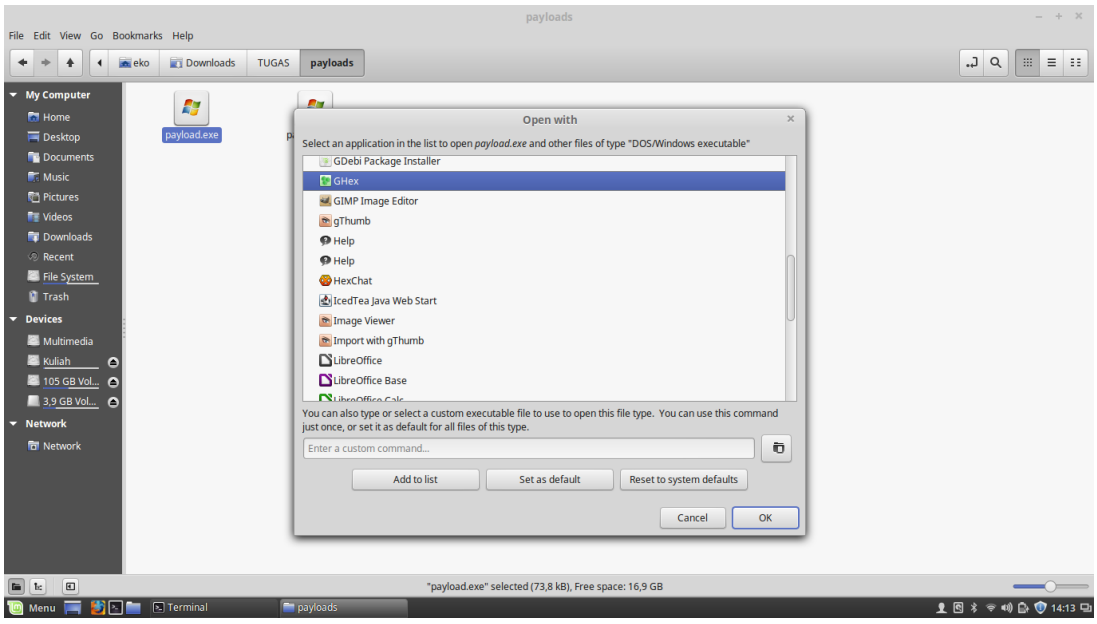
Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen sub-program atau data yang bertujuan jahat dalam sebuah file elektronik.

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:

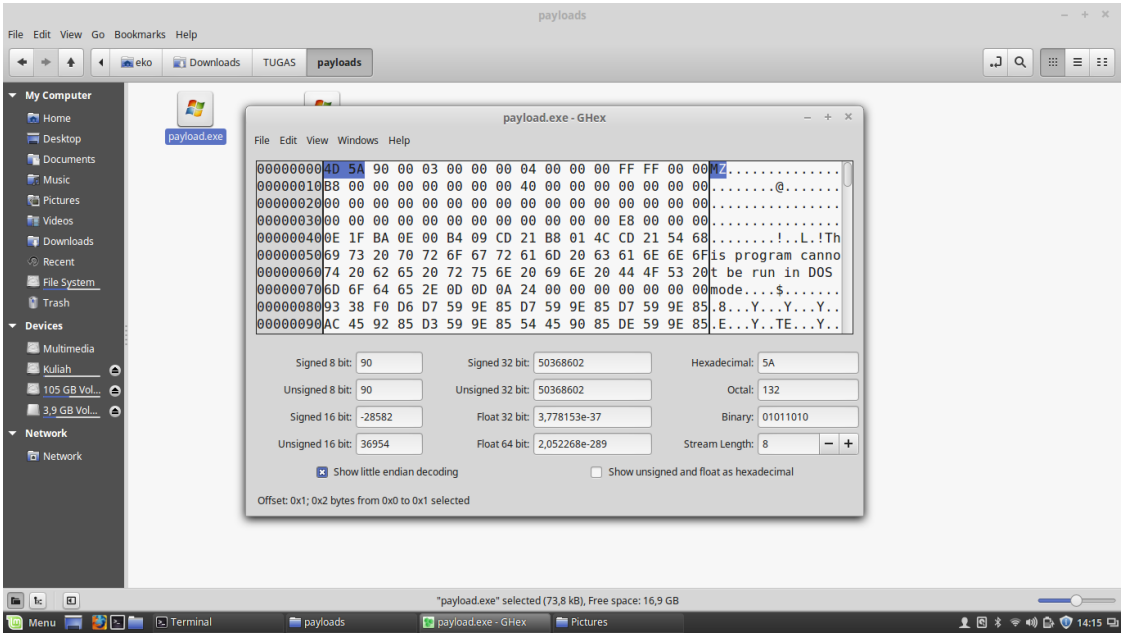
- GHex (linux)
- Hexdump (linux)
- Strings (linux)
- Ollydbg (windows xp)

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



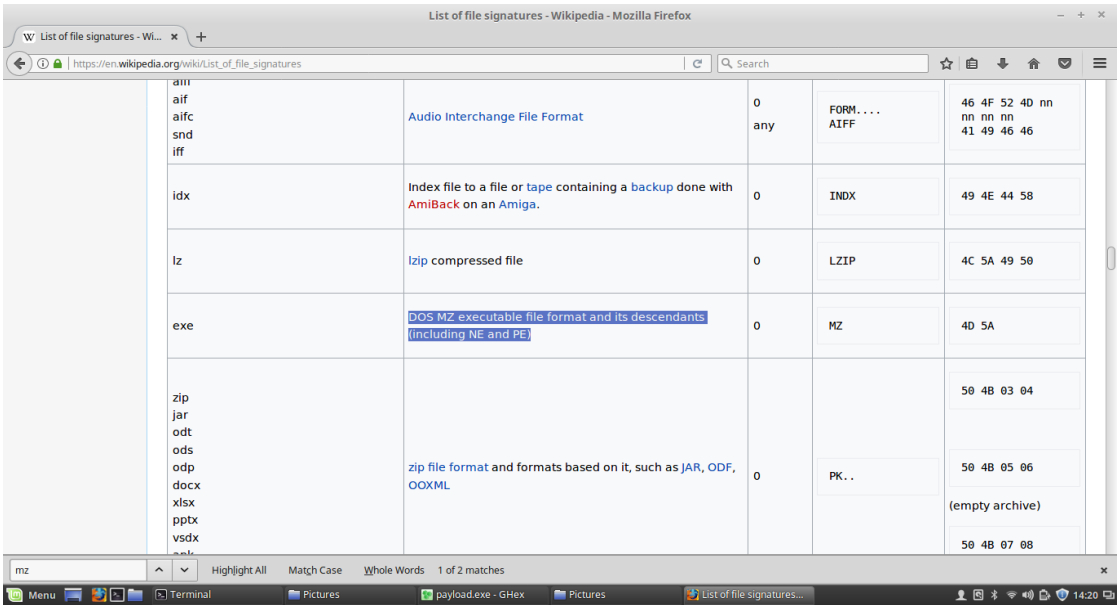
Gambar 1. Tool GHex

Pada Gambar 1 dan 2 merupakan gambar dari saat saya membuka file playload 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.

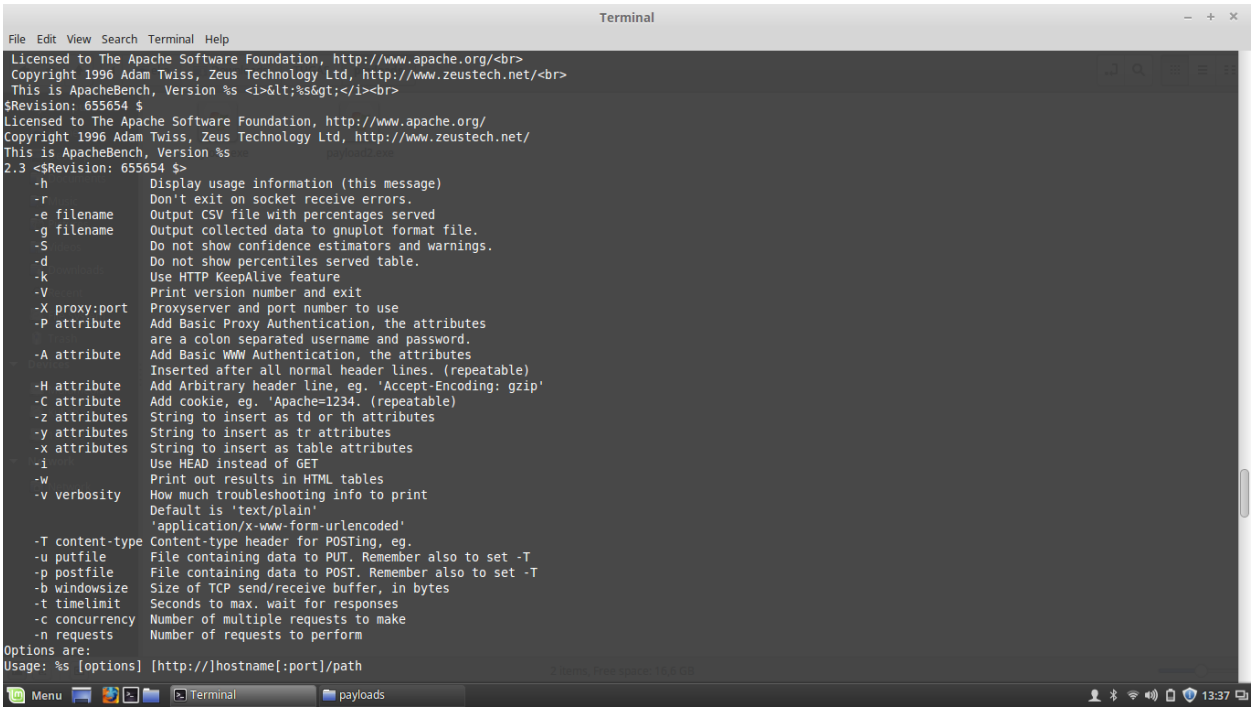


Gambar 2. Tampilan GHex

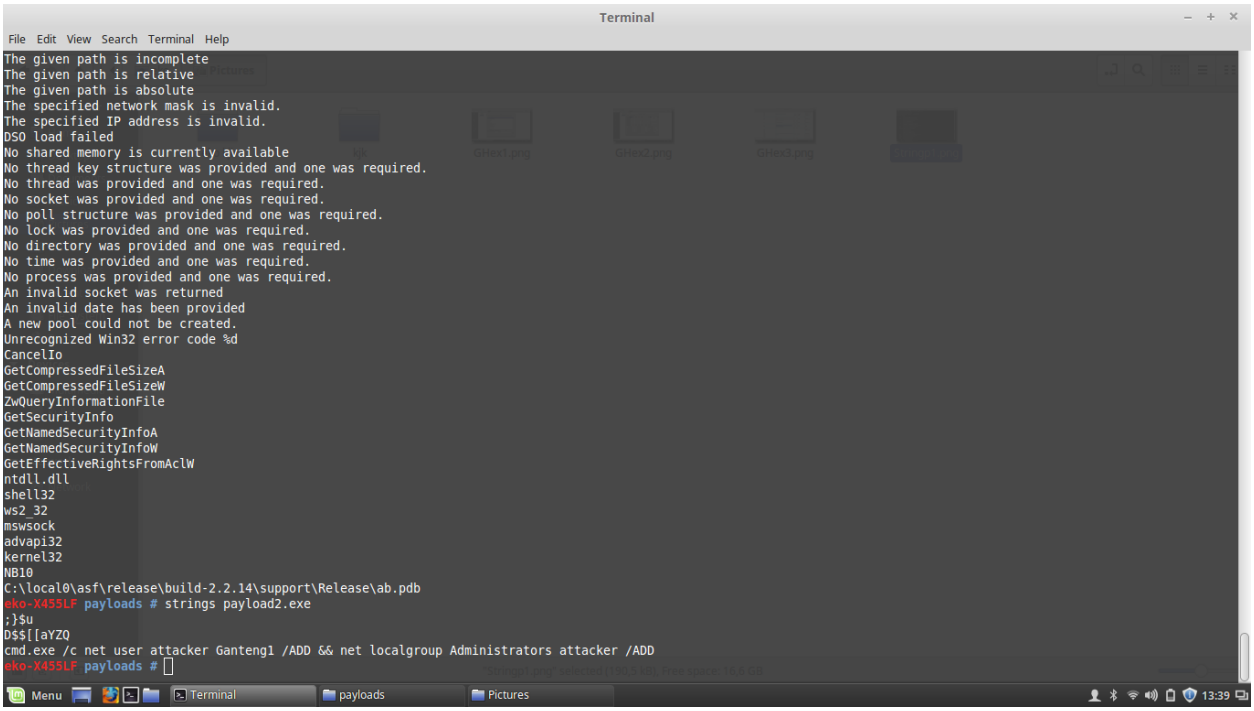
Pada Gambar 3 saya mencoba mencari tahu tentang apa itu MZ dan saya mendapatkan informasi dari Wikipedia bahawa MZ merupakan salah satu format exe.



Gambar 3. Format MZ



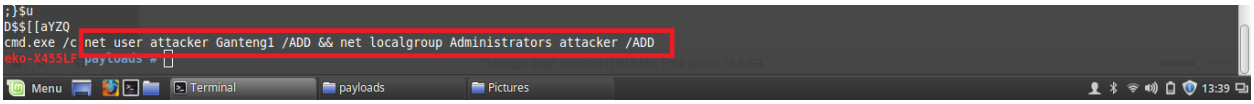
Gambar 4. Strings payload1



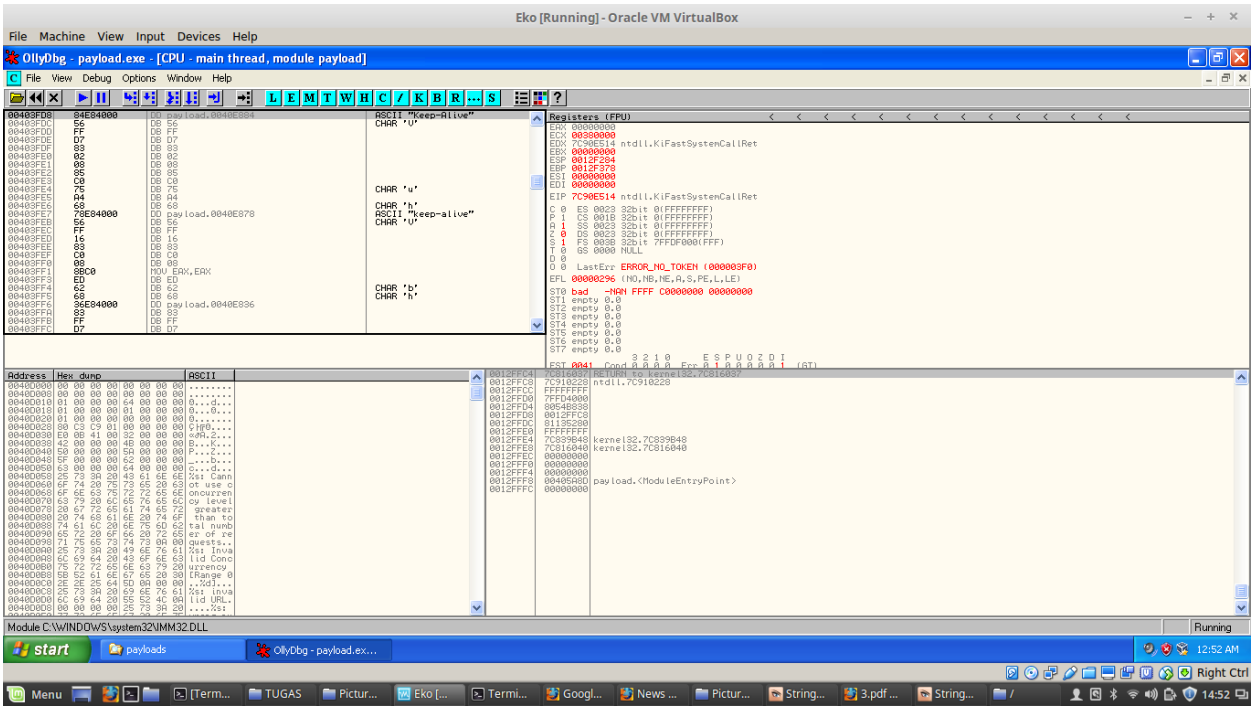
Gambar 5. Strings payload2

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

terhadap payloads 2 bahwa maksud dari ***net user ganteng1*** adalah admin membuat user baru dengan nama ganteng1, kemudian untuk ***net localgroup administrator attacker*** merupakan local group dari admin yang diberi nama attacker. Untuk lebih jelasnya dapat dilihat pada gambar 6.

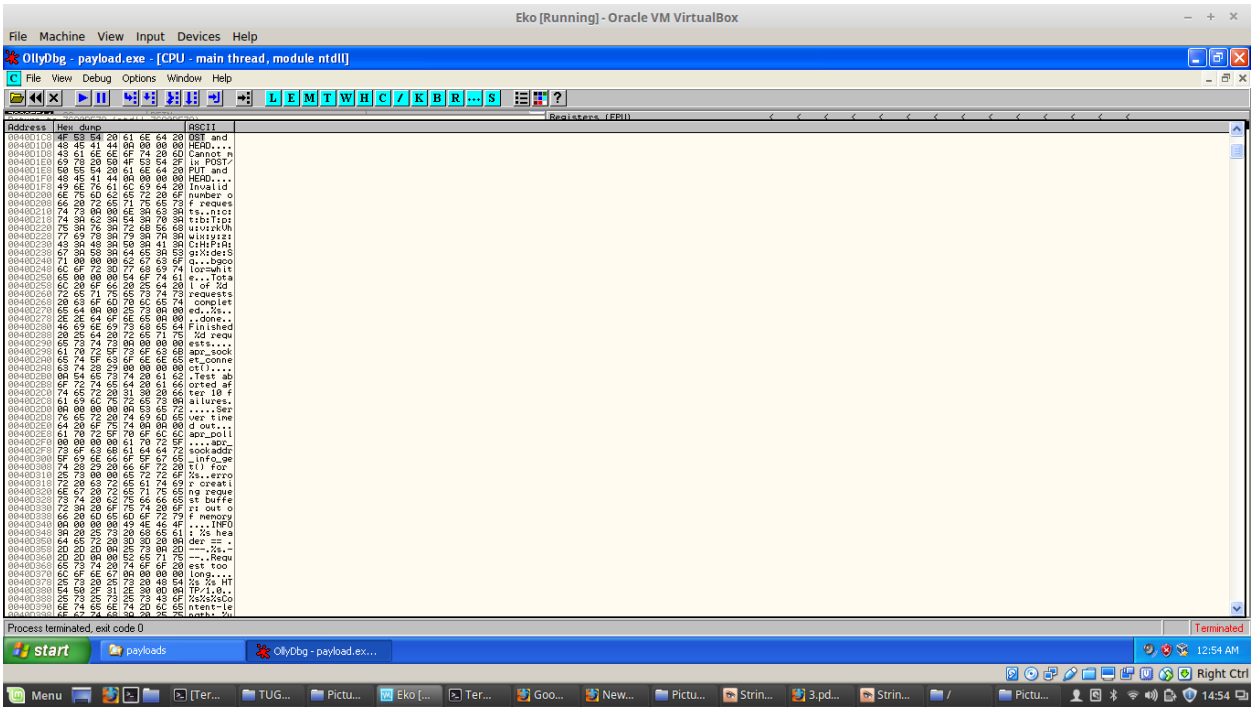


Gambar 6. Detail payload2



Gambar 7. Tools Ollydbg payload2

Untuk Tools Ollydbg saya menggunakan virtualbox dengan system operasinya yaitu windows xp. Hasil dari tampilan payload tersebut dapat dilihat pada gambar 7 diatas. Untuk gambar 8 dibawah merupakan tampilan dari hexdump yang terdapat pada tools Ollydbg dimana pada gambar tersebut sama halnya dengan tools GHex yang ada dilinux yang berfungsi untuk melihat konversi angka biner dari beberapa huruf dari file tersebut



Gambar 8. Tools hexdump payload2

Kesimpulan : Dalam tugas ini saya menggunakan metode analisis secara static dimana pada metode analysis ini saya menganalysis malware tanpa melakukan bedah terhadap program tersebut.