TUGAS KEAMANAN JARINGAN KOMPUTER
ANALISIS MALWARE (FILE PAYLOAD.EXE)

DISUSUN OLEH:

NAMA : Fahrul Rozi

NIM : 09011181320022

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

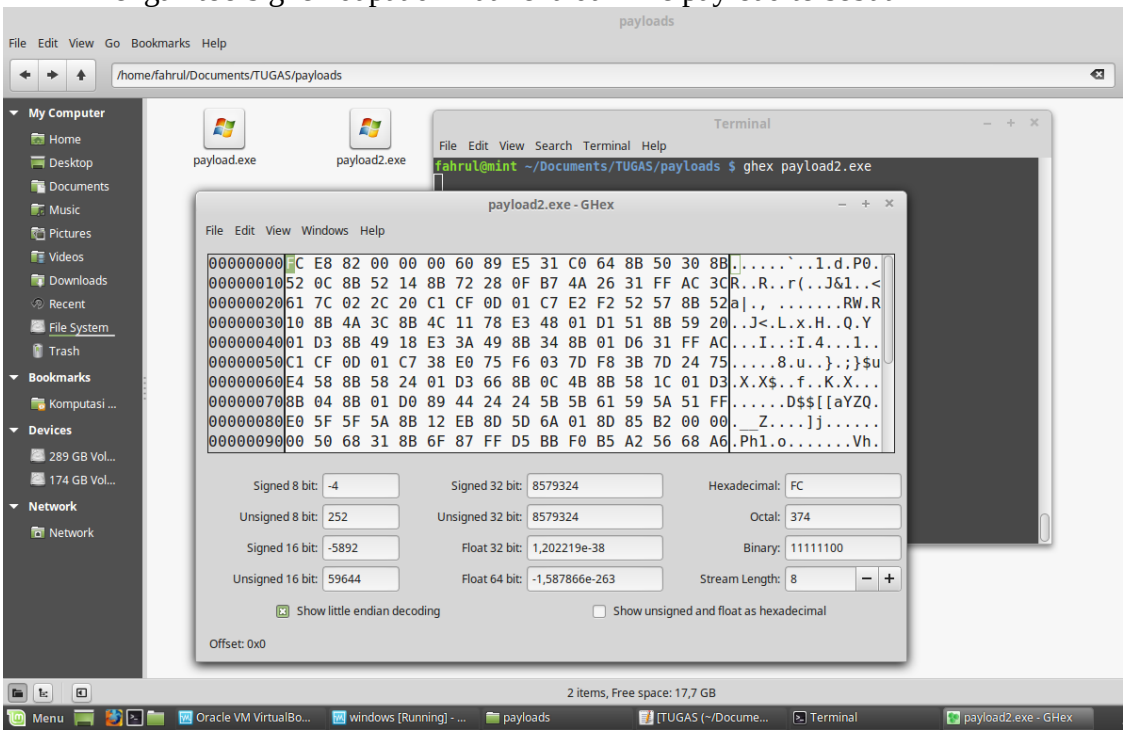
2017

ANALISA MALWARE

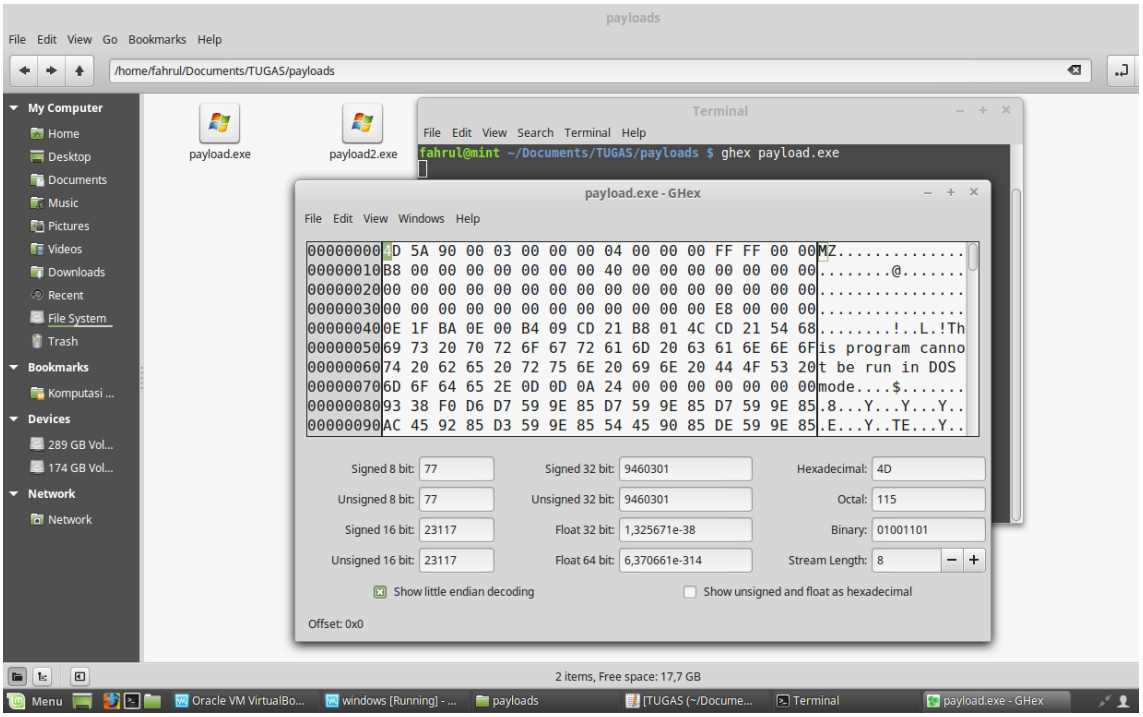
Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Mengapa menganalisa malware dibutuhkan karena malware sering diselundupkan melalui file-file umum dan popular seperti aplikasi (.exe), pengolah kata (.doc), pengolah angka (.xls), gambar (.jpg), dan lain sebagainya – sehingga jika pengguna awam mengakses dan membukanya, akan langsung mejadi korban program jahat seketika dan dapat juga Malware sering diselipkan di dalam kumpulan file yang dibutuhkan untuk menginstalasi sebuah program atau aplikasi tertentu – sehingga jika sang pengguna melakukan instalasi terhadap aplikasi dimaksud, seketika itu juga malware diaktifkan

Pada percobaan ini menganalisa 2 file yaitu payload.exe dan payload2.exe serta skema dari yang digunakan oleh file tersebut.

Dengan tools ghex dapat dilihat hexa dari file payload tersebut

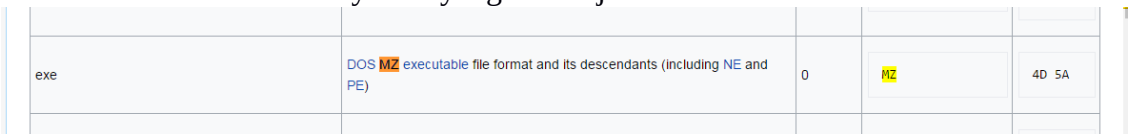


Gambar 1 : hexa file payload.exe



Gambar 2 : hexa file payload2.exe

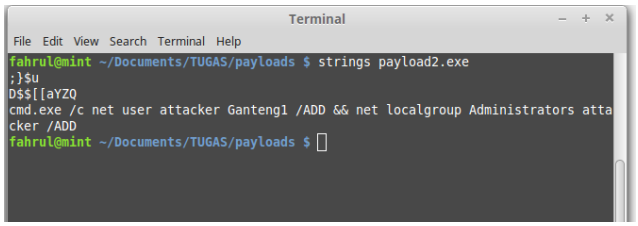
Pada hexa file payload2.exe pada gambar 2 terdapat file pertama yang MZ. MZ merupakan jenis dari file tersebut, jika dilihat pada daftar signature file maka MZ dapat dikatakan benar file tersebut file exe. Untuk file payload.exe tidak dapat dikatakan file exe dikarenakan tidak adanya file yang menunjukan bahwa file tersebut file exe.



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

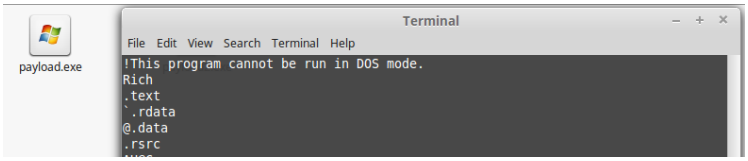
Gambar 3 : list signature file

Jika dengan menggunakan tools strings pada kedua file tersebut maka akan terlihat informasi yang terlihat pada gambar dibawah ini :

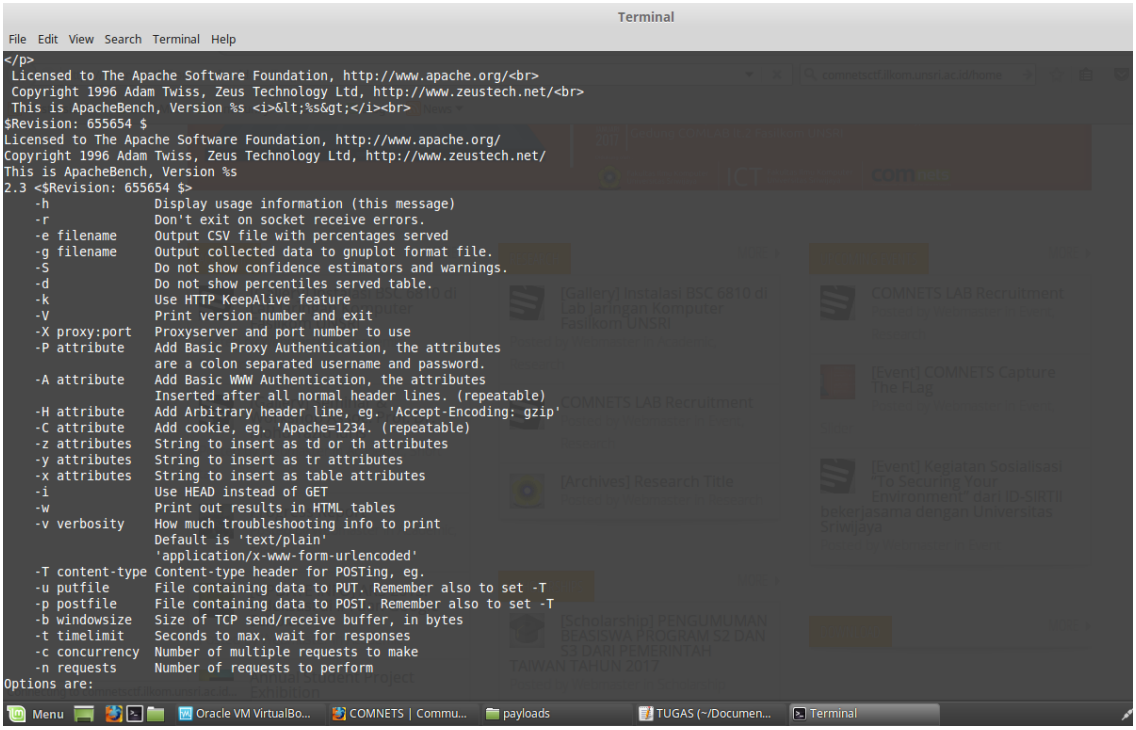


Gambar 4 : strings payload2.exe

Pada informasi payload2.exe jika dieksekusi (running) akan mengesekusi cmd.exe serta secara otomatis akan menambahkan user attacker yang bernama ganteng1 dalam sebuah local group administrator , pembuktian pada saat pengeksekusi dengan menggunakan tools ollydbg dapat dilihat pada gambar 6.



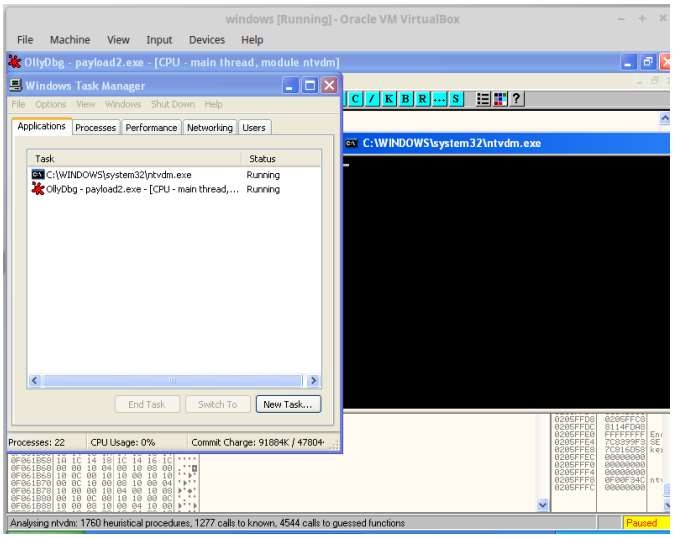
(a)



(b)

Gambar 5 : (a) strings payload.exe , (b) info strings payload.exe

Pada gambar informasi yang di perlihatkan pada gambar 5.b dapat memungkinkan file payload.exe ini merupakan file apachebench.



Gambar 6 : eksekusi file payload2.exe

Pada gambar 6 dapat dilihat saat pengeksekusian file payload2.exe dengan menggunakan ollydbg secara otomatis akan membuka file cmd.exe dan terdapat dalam directory C windows dengan sytem32 dan mengeksekusi ntvdm.exe.

Kesimpulan

Dari percobaan dengan menggunakan beberapa tools maka dapat disimpulkan kedua file tersebut belum bisa menentukan apakah malware atau bukan tetapi pada file payload2.exe sepertinya merupakan file exploitation dikerenakan jika dieksekusi maka akan otomatis akan menjalankan cmd.exe dengan akses menambah user dalam localgroup dalam system32 pada windows. Dan pada file payload.exe ini merupakan sorfware apachebench hanya di rename.