TUGAS

KEAMANAN JARINGAN KOMPUTER

DISUSUN OLEH :

NAMA : INDAH SARI

NIM : 09011181320011

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017 – 2018

ANALISIS MALWARE MENGGUNAKAN PAYLOAD

Kejahatan di dunia siber sangatlah beragam dan bervariasi. Berdasarkan kejadian-kejadian terdahulu, hampir seluruh serangan melibatkan apa yang disebut sebagai *malicious software (malware).* Malicious software (malware) adalah program jahat yang sifatnya yang merusak atau bertujuan negatif. 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.

TUGAS

Lakukan analisis terhadap dua file payload tersebut

1. Payload.exe
2. Payload2.exe

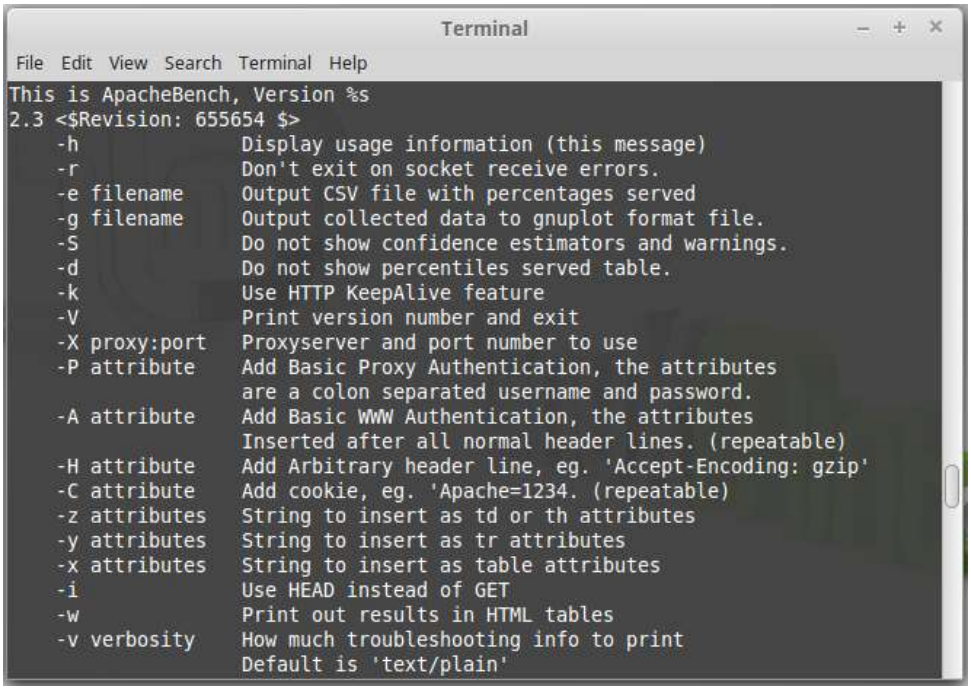
Analisis, proses kerja dan skema dari payload tersebut, menggunakan tools:

1. Ghex, hexdump, strings (linux)
2. Ollydbg (win), ida pro (linux,win)

Berikut Analisis dan Proses Kerja dari Payload Menggunakan Tools Yang Telah Tersedia:

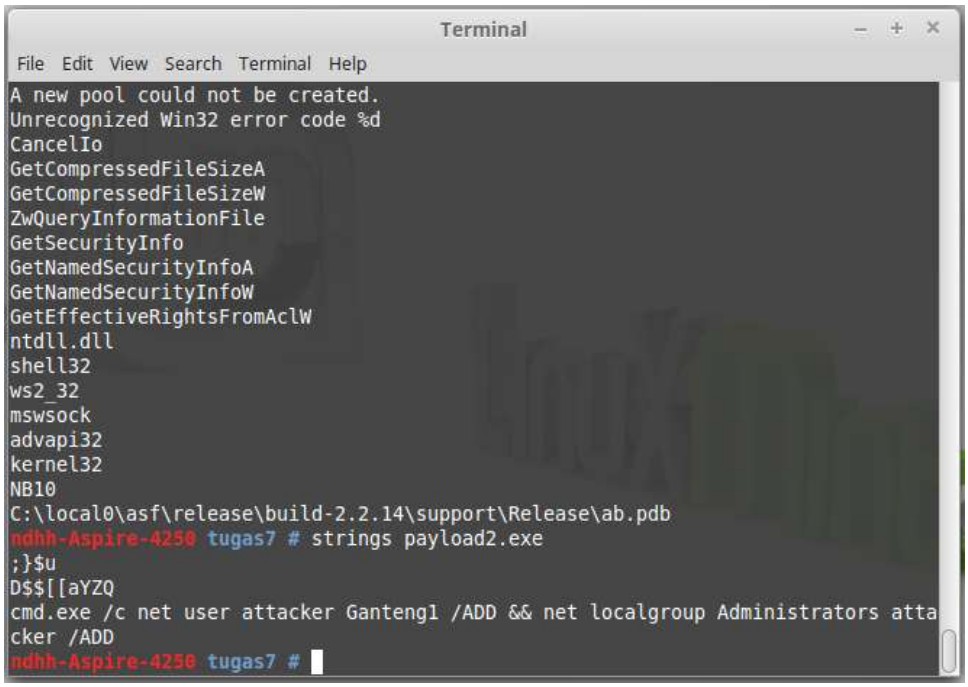
Analisis dua file payload dengan menggunakan tools string (linux)

1. Payload.exe



Dengan menginstall aplikasi payload terlebih dahulu dan melakukan mengkonfig strings payload.exe, pada gambar diatas menampilkan hasil yang menjelaskan bahwa strings payload.exe adalah aplikasi ApacheBench version 2.3 yang menampilkan beberapa fungsi yang memiliki masing – masing kegunaan yang berbeda. ApacheBench (ab) adalah perintah program baris komputer single-threaded untuk mengukur kinerja server web HTTP, yang dirancang untuk menguji Apache HTTP Server.

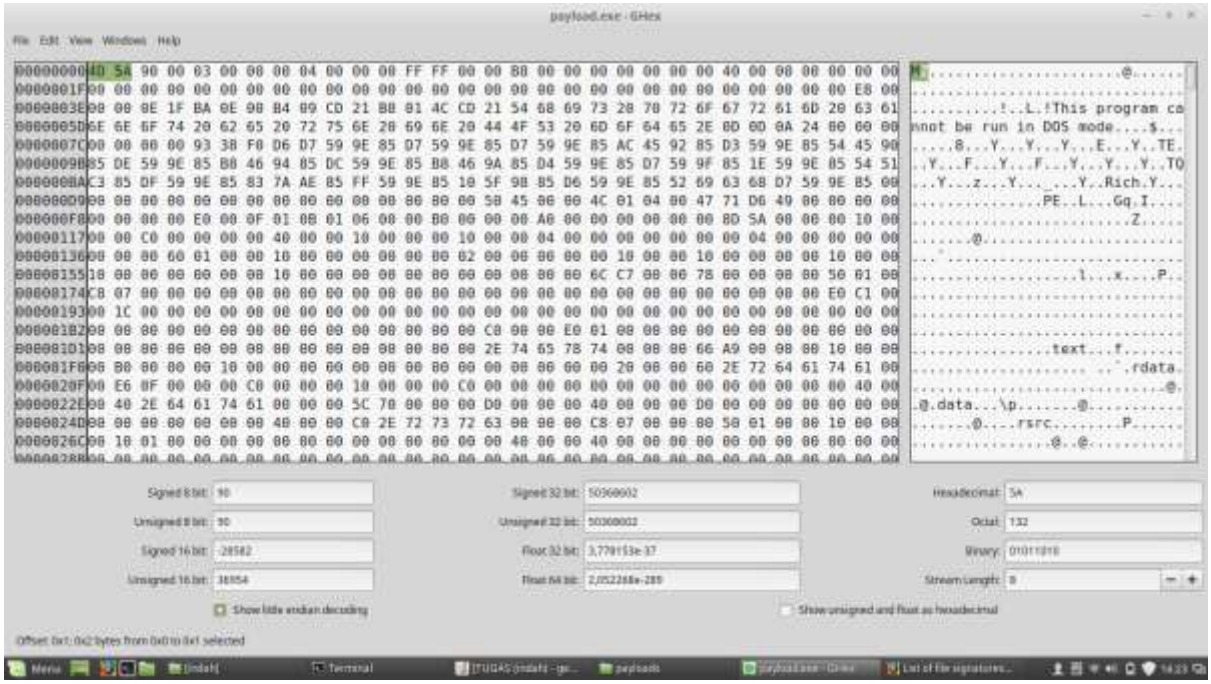
2. Payload2.exe



Dengan mengkonfig strings payload2.exe dapat dilihat pada gambar diatas menampilkan hasil dari konfig, hasil tersebut menjelaskan bahwa strings payload2.exe adalah sejenis exploit. exploit adalah serangan terhadap sistem komputer, terutama yang mengambil keuntungan dari kerentanan tertentu bahwa sistem menawarkan untuk melakukan penyusupan.

strings payload2.exe menghasilkan commant cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD yang artinya cmd.exe merupakan file admin, dimana dari user admin membuat user attacker Ganteng1 dan localgroup kemudian user attacker baru tersebut memiliki hak akses sebagai admin

Analisis file payload dengan menggunakan tools Ghex



Pada hasil gambar ghex diatas, didapat dengan cara mengklik kanan folder dimana payload tersimpan, dan open with ghex. Setelah dibuka file ghex menampilkan simbol – simbol seperti diatas sebelah kanan gambar, dan jika di blok simbol simbol tersebut memiliki nilai masing – masing.

Dari hasil ghex diatas menampilkan simbol – simbil dimana salah satu simbol MZ dilakukan search di **list of signature wikipedia**

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

Gambar diatas menjelaskan bahwa data MZ memiliki nilai 4D 5A, dimana jika dilihat hasil dari searching list of signature wikipedia menampilkan hasil yang sama dari gambar hasil ghex yang dilakukan sebelumnya

ANALISA:

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. 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. Malware sering ditanam di dalam sistem komputer tanpa diketahui oleh sang pengguna – sehingga sewaktu-waktu dapat disalahgunakan oleh pihak yang tidak berwenang untuk melakukan berbagai tindakan kejahatan; dan lain sebagainya.