

**Tugas Mata Kuliah**  
**KEAMANAN JARINGAN KOMPUTER**



Nama : Faris Abdul Aziz

Nim : 09011181320020

**Jurusan Sistem Komputer**  
**Fakultas Ilmu Komputer Universitas Sriwijaya**

**2017**

# MALWARE

Malware adalah adalah program komputer yang diciptakan dengan maksud dan tujuan tertentu dari penciptanya dan merupakan program yang mencari kelemahan dari software.

Tools yang digunakan adalah:

1. Strings
2. GHex
3. Ollydbg
4. Hexdump

Dengan file target:

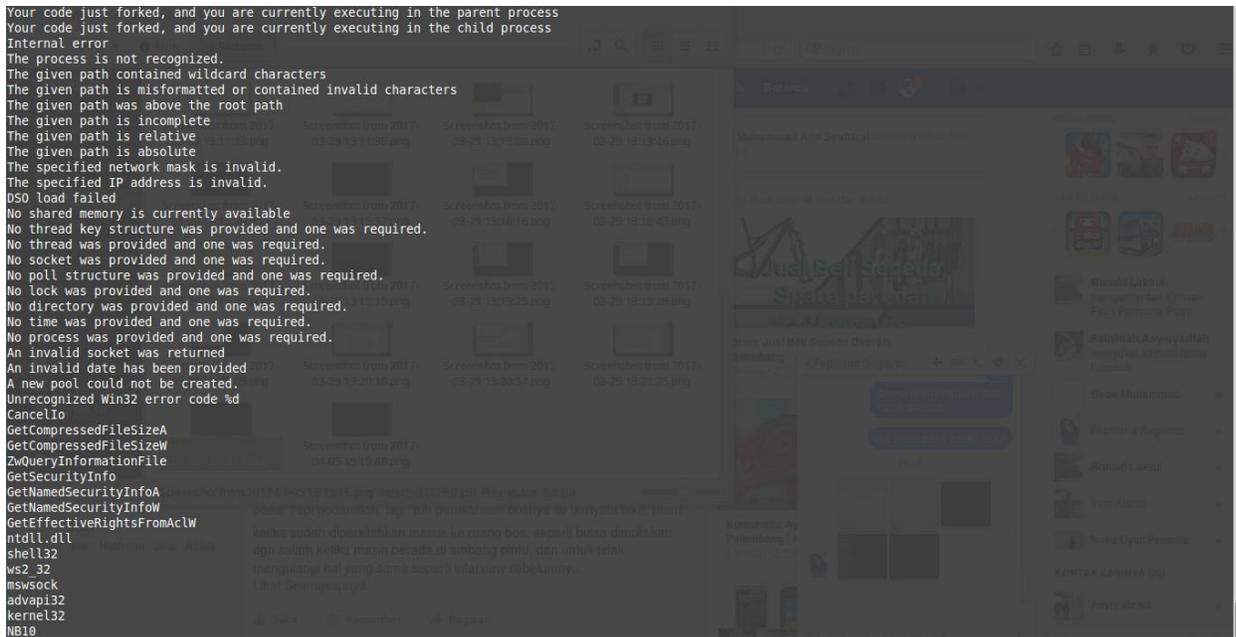
1. Payload
2. Payload2

Pertama menggunakan perintah strings pada payload, string sendiri berguna untuk mengurutkan karakter, mencari karakter, memilih karakter yang ingin ditampilkan. Dan dapat dilihat perintah string pada gambar 1.1 dibawah.

```
faris@farismr ~/Documents/TUGAS/payloads $ strings payload.exe

LOG: header received:
apr_socket_recv
</p>
Licensed to The Apache Software Foundation, http://www.apache.org/<br>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/<br>
This is ApacheBench, Version %s <i><!--></i><br>
$Revision: 655654 $
Licensed to The Apache Software Foundation, http://www.apache.org/
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
This is ApacheBench, Version %s
2.3 <$Revision: 655654 $>
-h          Display usage information (this message)
-r          Don't exit on socket receive errors.
-e filename Output CSV file with percentages served
-g filename Output collected data to gnuplot format file.
-S         Do not show confidence estimators and warnings.
-d         Do not show percentiles served table.
-k         Use HTTP KeepAlive feature
-V         Print version number and exit
-X proxy:port Proxyserver and port number to use
-P attribute Add Basic Proxy Authentication, the attributes
           are a colon separated username and password.
-A attribute Add Basic WWW Authentication, the attributes
           Inserted after all normal header lines. (repeatable)
-H attribute Add Arbitrary header line, eg. 'Accept-Encoding: gzip'
-C attribute Add cookie, eg. 'Apache=1234'. (repeatable)
-z attributes String to insert as td or th attributes
-y attributes String to insert as tr attributes
-x attributes String to insert as table attributes
-i         Use HEAD instead of GET
-w         Print out results in HTML tables
-v verbosity How much troubleshooting info to print
           Default is 'text/plain'
           'application/x-www-form-urlencoded'
-T content-type Content-type header for POSTing, eg.
-u putfile   File containing data to PUT. Remember also to set -T
-p postfile  File containing data to POST. Remember also to set -T
-b window-size Size of TCP send/receive buffer, in bytes
-t timelimit Seconds to max. wait for responses
-c concurrency Number of multiple requests to make
-n requests  Number of requests to perform

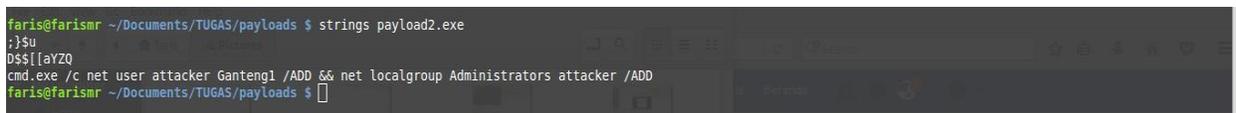
Options are:
```



**Gambar 1.1.** String pada payload

Terlihat pada perintah string pada gambar 1.1, terdapat banyak karakter yang dimiliki oleh file payload, dan kita dapat melihat dan memilih karakter apa saja yang ada di dalam file payload di atas.

Lalu dilanjutkan dengan melakukan perintah string ke file ke dua, yaitu payload2. Dan dapat dilihat pada gambar 1.2 di bawah.



**Gambar 1.2.** Strings pada payload2

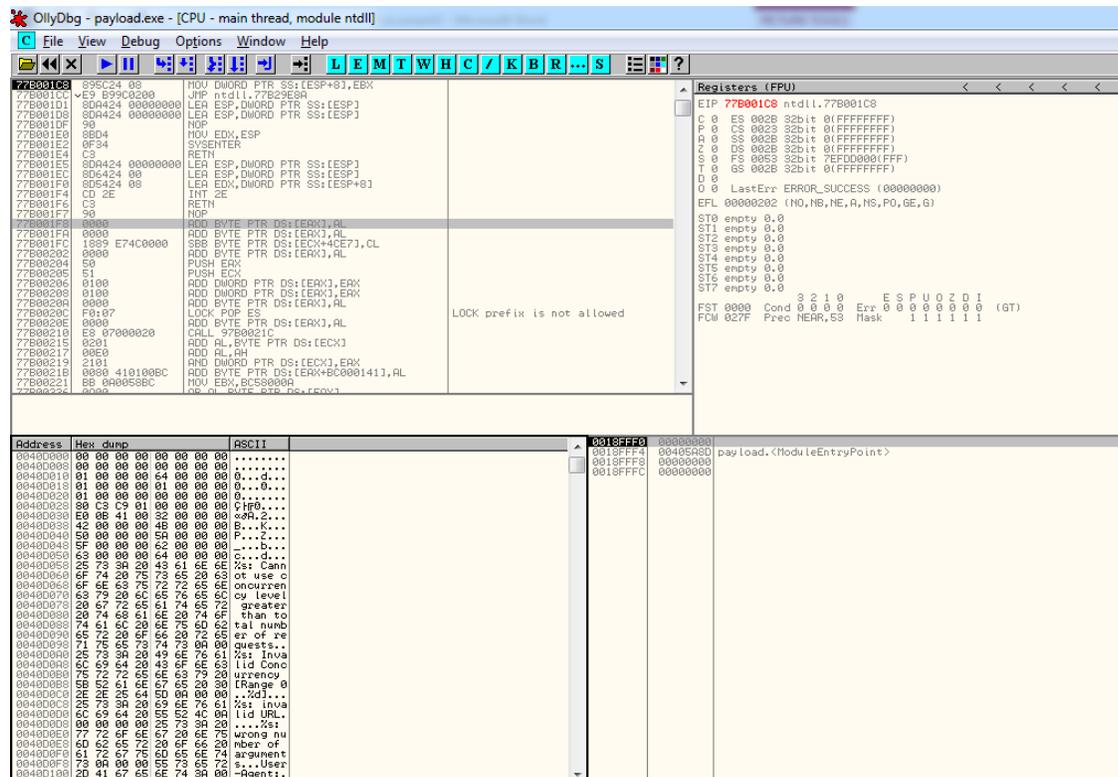
Terlihat tulisan user attacker Ganteng1, menurut saya, file payload2 ini telah dicrack (diserang) dan diberikan malware, sehingga membuat file payload2 menjadi corrupt.

Setelah itu lakukan perintah GHex pada kedua file payload dan payload2 untuk melihat keamanan pada kedua file tersebut. Dapat dilihat GHex pada payload dan payload2 pada gambar 1.3 di bawah.



Pada gambar 1.4 terlihat sedikit kode encrypt didalamnya, itu dikarenakan file payload2 telah diserang malware dan corrupt. Sehingga karakter pada file payload2 telah hilang.

Selanjutnya dilakukan dengan menggunakan tools ollydbg, untuk ollydbg sendiri tidak dapat membaca file payload2, sehingga ollydbg dilakukan pada file payload saja. Dan dapat dilihat pada gambar 1.5 dibawah.

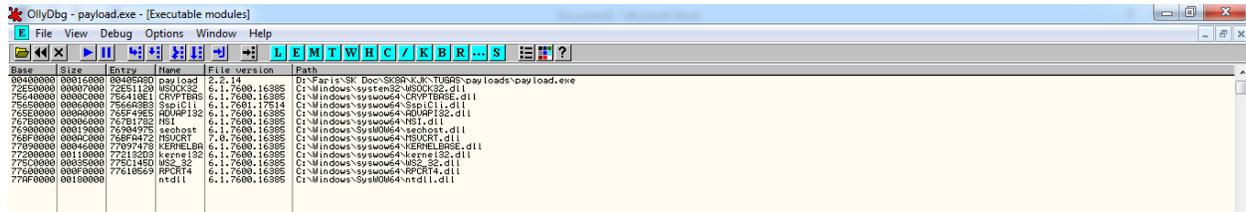


Gambar 1.5. Ollydbg pada payload

Pada ollydbg gambar 1.5, itu sendiri menu CPU, yang dimana menu CPU itu sudah include pilihan lainnya seperti main thread, module, memory, dan lain-lain. Terdapat juga Hexdump didalamnya, yang dimana hexdump sendiri adalah bilangan heksadesimal dari data computer, dari RAM, atau dari file atau perangkat penyimpanan. Hexdump sendiri direpresentasikan sebagai angka heksadesimal dua digit, yang dimana seperti gambar 1.5 hexdump memiliki 2 angka yang masing-masing dipisahkan oleh kolom putih atau spasi.

Untuk Executable modules sendiri berfungsi untuk mencatat apa saja yang masuk pada ollydbg yang sedang standby saat itu. Dapat dilihat pada kolom executable terdapat apa saja yang masuk

kedalam proses saat ini, seperti contoh file payload yang terekam oleh executable. Dapat dilihat pada gambar 1.6 dibawah.



**Gambar 1.6.** Executable Modules