BAB V
IMPLEMENTASI DAN PEMBAHASAN

5.1. Implementasi

Pada bab ini akan di terangkan proses dari fase selanjutnya adalah implementasi dan penerapan dari detail rancangan topologi dan rancangan sistem pada lingkungan nyata sebagai simulasi dan LAN. Detail rancangan akan digunakan sebagai instruksi atau panduan tahap implementasi agar sistem yang dibangun dapat relevan dengan sistem yang sudah dirancang. Proses implementasi terdiri dari installasi dan konfigurasi

5.2. Implementasi Topologi Jaringan

Penulis mengumpulkan seluruh perangkat yang dibutuhkan,Perangkat ini meliputi *hardware* dan *software*. Setelah itu, penulis menempatkan seluruh perangkat sesui dengan topologi yang sudah dibuat. Setelah semua unit terhubung satu sama proses selanjutnya adalah mengkonfigurasi setiap unit agar dapat berkomunikasi Satu dengan yang lainnya. Perangkat *switch* yang digunakan tidak membutuhkan konfigurasi, karena perangkat tersebut tidak dapat di konfigurasi. Sejumlah parameter dari unit mesin *host* yang harus dikonfigurasi adalah alamat *internet protocol*, *subnet mask,* alamat IP *gateway,* dan alamat IP DNS. Setelah instalasi dan konfigurasi selesai dilakukan, proses selanjutnya adalah pengujian untuk memastikan fungsionalitas koneksi, hal ini dimaksudkan untuk menjamin agar mesin yang satu dapat berkomunikasi dengan unit mesin lain.

5.3. Implementasi Dan Konfigurasi IDS

IDS atau system pendeteksi intrusi yang dibangun dengan menggunakan beberapa komponen utama, yaitu : snort (mesin inti IDS), *Barnyard* (menangani *output plug-in Snort*) BASE (mempresentasikan *output snort*), *Wireshark* (untuk melihat grafik dan monitoring jaringan). IDS dibangun dengan menggunakan

system operasi berbasis *open source* yaitu *linux Ubuntu* 9.10, berikut ini adalah sejumlah proses yang dikerjakan sebelum mengimplementasikan komponen.

5.3.1. Installasi paket *dependency*

Paket dependency merupakan paket komponen sistem yang dibutuhkan sebelum komponen utama snort terinstal yang terdiri dari;

1) *Sudo apt-get install mysql-common*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
Hit http://old-releases.ubuntu.com karmic-updates/multiverse Sources
Hit http://old-releases.ubuntu.com karmic/multiverse Sources
Hit http://old-releases.ubuntu.com karmic-security/main Packages
Hit http://old-releases.ubuntu.com karmic-security/restricted Packages
Hit http://old-releases.ubuntu.com karmic-security/universe Packages
Hit http://old-releases.ubuntu.com karmic-security/universe Sources
Hit http://old-releases.ubuntu.com karmic-security/multiverse Packages
Hit http://old-releases.ubuntu.com karmic-security/multiverse Sources
Fetched 198B in 23s (9B/s)
Reading package lists... Done
root@dian-laptop:/home/newbie/Downloads# clear

root@dian-laptop:/home/newbie/Downloads# apt-get install mysql-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  mysql-common
1 upgraded, 0 newly installed, 0 to remove and 346 not upgraded.
Need to get 71.2kB of archives.
After this operation, 0B of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com karmic-updates/main mysql-common 5.1.37
-1ubuntu5.5 [71.2kB]
Fetched 71.2kB in 20s (3,403B/s)
(Reading database ... 114040 files and directories currently installed.)
Preparing to replace mysql-common 5.1.37-1ubuntu5 (using .../mysql-common_5.
1.37-1ubuntu5.5_all.deb) ...
Unpacking replacement mysql-common ...
Setting up mysql-common (5.1.37-1ubuntu5.5) ...
root@dian-laptop:/home/newbie/Downloads#
```

Gambar 5.1 proses install *mysql-common*

2) *Sudo apt-get install mysql-client*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
1.37-1ubuntu5.5_all.deb) ...
Unpacking replacement mysql-common ...
Setting up mysql-common (5.1.37-1ubuntu5.5) ...
root@dian-laptop:/home/newbie/Downloads# apt-get install mysql-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libdbd-mysql-perl libdbi-perl libmysqlclient16 libnet-daemon-perl libplrpc-perl mysql-client-5.1
Suggested packages:
  dbishell
The following NEW packages will be installed:
  libdbd-mysql-perl libdbi-perl libnet-daemon-perl libplrpc-perl mysql-client mysql-client-5.1
The following packages will be upgraded:
  libmysqlclient16
1 upgraded, 6 newly installed, 0 to remove and 345 not upgraded.
Need to get 11.2MB of archives.
After this operation, 23.1MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com karmic-updates/main libmysqlclient16 5.1.37-1ubuntu5.5 [1,904kB]
Get:2 http://old-releases.ubuntu.com karmic/main libnet-daemon-perl 0.43-1 [46.9kB]
Get:3 http://old-releases.ubuntu.com karmic/main libplrpc-perl 0.2020-2 [36.0kB]
Get:4 http://old-releases.ubuntu.com karmic/main libdbi-perl 1.609-1 [800kB]
Get:5 http://old-releases.ubuntu.com karmic/main libdbd-mysql-perl 4.011-1ubuntu1 [136kB]
Get:6 http://old-releases.ubuntu.com karmic-updates/main mysql-client-5.1 5.1.37-1ubuntu5.5 [8,210kB]
Get:7 http://old-releases.ubuntu.com karmic-updates/main mysql-client 5.1.37-1ubuntu5.5 [65.3kB]
Fetched 11.2MB in 38s (292kB/s)
(Reading database ... 114040 files and directories currently installed.)
Preparing to replace libmysqlclient16 5.1.37-1ubuntu5 (using .../libmysqlclient16_5.1.37-1ubuntu5.5_i386.deb) ...
Unpacking replacement libmysqlclient16 ...
Selecting previously deselected package libnet-daemon-perl.
Unpacking libnet-daemon-perl (from .../libnet-daemon-perl_0.43-1_all.deb) ...
Selecting previously deselected package libplrpc-perl.
Unpacking libplrpc-perl (from .../libplrpc-perl_0.2020-2_all.deb) ...
Selecting previously deselected package libdbi-perl.
```

Gambar 5.2 proses install *mysql-client*

3) *Sudo apt-get install mysql-server*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install mysql-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libhtml-template-perl mysql-server-5.1 mysql-server-core-5.1
Suggested packages:
  libipc-sharedcache-perl tinyca mailx
The following NEW packages will be installed:
  libhtml-template-perl mysql-server mysql-server-5.1 mysql-server-core-5.1
0 upgraded, 4 newly installed, 0 to remove and 345 not upgraded.
Need to get 11.2MB of archives.
After this operation, 25.8MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com karmic-updates/main mysql-server-core-5.1 5.1.37-1ubuntu5.5 [3,841kB]
Get:2 http://old-releases.ubuntu.com karmic-updates/main mysql-server-5.1 5.1.37-1ubuntu5.5 [7,187kB]
Get:3 http://old-releases.ubuntu.com karmic/main libhtml-template-perl 2.9-1 [65.8kB]
Get:4 http://old-releases.ubuntu.com karmic-updates/main mysql-server 5.1.37-1ubuntu5.5 [65.5kB]
Fetched 11.2MB in 50s (221kB/s)
Preconfiguring packages ...
Selecting previously deselected package mysql-server-core-5.1.
(Reading database ... 114296 files and directories currently installed.)
Unpacking mysql-server-core-5.1 (from .../mysql-server-core-5.1_5.1.37-1ubuntu5.5_i386.deb) ...
Selecting previously deselected package mysql-server-5.1.
Unpacking mysql-server-5.1 (from .../mysql-server-5.1_5.1.37-1ubuntu5.5_i386.deb) ...
Selecting previously deselected package libhtml-template-perl.
Unpacking libhtml-template-perl (from .../libhtml-template-perl_2.9-1_all.deb) ...
Selecting previously deselected package mysql-server.
Unpacking mysql-server (from .../mysql-server_5.1.37-1ubuntu5.5_all.deb) ...
Processing triggers for man-db ...
Processing triggers for sreadahead ...
Setting up mysql-server-core-5.1 (5.1.37-1ubuntu5.5) ...
Setting up mysql-server-5.1 (5.1.37-1ubuntu5.5) ...
```

Gambar 5.3 installasi *mysql-server*

4) *Sudo apt-get install php5-dev*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install php5-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  autoconf autoconf2.13 automake automake1.4 autotools-dev libltdl-dev libssl-dev libssl0.9.8 libtool m4 php5-common shtool
  zlib1g-dev
Suggested packages:
  autobook autoconf-archive gnu-standards autoconf-doc gettext libtool-doc automaken gfortran fortran95-compiler gcj php5-suhosin
The following NEW packages will be installed:
  autoconf autoconf2.13 automake automake1.4 autotools-dev libltdl-dev libssl-dev libtool m4 php5-common php5-dev shtool
  zlib1g-dev
The following packages will be upgraded:
  libssl0.9.8
1 upgraded, 13 newly installed, 0 to remove and 344 not upgraded.
Need to get 8,741kB of archives.
After this operation, 19.1MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com karmic-updates/main libssl0.9.8 0.9.8g-16ubuntu3.5 [2,927kB]
Get:2 http://old-releases.ubuntu.com karmic/main m4 1.4.13-2 [241kB]
Get:3 http://old-releases.ubuntu.com karmic/main autoconf 2.64-1ubuntu1 [558kB]
Get:4 http://old-releases.ubuntu.com karmic/main autoconf2.13 2.13-59 [351kB]
Get:5 http://old-releases.ubuntu.com karmic/main autotools-dev 20090427.1 [63.7kB]
Get:6 http://old-releases.ubuntu.com karmic/main automake 1:1.11-1 [559kB]
Get:7 http://old-releases.ubuntu.com karmic/main automake1.4 1:1.4-p6-13 [233kB]
Get:8 http://old-releases.ubuntu.com karmic/main libltdl-dev 2.2.6a-4 [191kB]
Get:9 http://old-releases.ubuntu.com karmic/main zlib1g-dev 1:1.2.3.3.dfsg-13ubuntu3 [163kB]
Get:10 http://old-releases.ubuntu.com karmic-updates/main libssl-dev 0.9.8g-16ubuntu3.5 [1,980kB]
Get:11 http://old-releases.ubuntu.com karmic/main libtool 2.2.6a-4 [522kB]
Get:12 http://old-releases.ubuntu.com karmic-updates/main php5-common 5.2.10.dfsg.1-2ubuntu6.10 [426kB]
Get:13 http://old-releases.ubuntu.com karmic/main shtool 2.0.8-1 [161kB]
Get:14 http://old-releases.ubuntu.com karmic-updates/main php5-dev 5.2.10.dfsg.1-2ubuntu6.10 [367kB]
Fetched 8,741kB in 33s (260kB/s)
Preconfiguring packages ...
(Reading database ... 114472 files and directories currently installed.)
```

Gambar 5.4 installasi *php5-dev*

5) *Sudo apt-get install php5-ldap*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install php5-ldap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap php5
Suggested packages:
  apache2-doc apache2-suexec apache2-suexec-custom php-pear
The following NEW packages will be installed:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap php5 php5-ldap
0 upgraded, 11 newly installed, 0 to remove and 344 not upgraded.
Need to get 4,532kB of archives.
After this operation, 12.3MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com karmic/main libapr1 1.3.8-1 [116kB]
Get:2 http://old-releases.ubuntu.com karmic-updates/main libaprutil1 1.3.9+dfsg-1ubuntu1.1 [85.4kB]
Get:3 http://old-releases.ubuntu.com karmic-updates/main libaprutil1-dbd-sqlite3 1.3.9+dfsg-1ubuntu1.1 [27.1kB]
Get:4 http://old-releases.ubuntu.com karmic-updates/main libaprutil1-ldap 1.3.9+dfsg-1ubuntu1.1 [25.1kB]
Get:5 http://old-releases.ubuntu.com karmic-updates/main apache2.2-bin 2.2.12-1ubuntu2.4 [1,310kB]
Get:6 http://old-releases.ubuntu.com karmic-updates/main apache2-utils 2.2.12-1ubuntu2.4 [156kB]
Get:7 http://old-releases.ubuntu.com karmic-updates/main apache2.2-common 2.2.12-1ubuntu2.4 [285kB]
Get:8 http://old-releases.ubuntu.com karmic-updates/main apache2-mpm-prefork 2.2.12-1ubuntu2.4 [2,376B]
Get:9 http://old-releases.ubuntu.com karmic-updates/main libapache2-mod-php5 5.2.10.dfsg.1-2ubuntu6.10 [2,505kB]
Get:10 http://old-releases.ubuntu.com karmic-updates/main php5 5.2.10.dfsg.1-2ubuntu6.10 [1,120B]
Get:11 http://old-releases.ubuntu.com karmic-updates/main php5-ldap 5.2.10.dfsg.1-2ubuntu6.10 [18.8kB]
Fetched 4,532kB in 1min 3s (71.5kB/s)
Selecting previously deselected package libapr1.
(Reading database ... 116543 files and directories currently installed.)
Unpacking libapr1 (from .../libapr1_1.3.8-1_i386.deb) ...
Selecting previously deselected package libaprutil1.
Unpacking libaprutil1 (from .../libaprutil1_1.3.9+dfsg-1ubuntu1.1_i386.deb) ...
Selecting previously deselected package libaprutil1-dbd-sqlite3.
```

Gambar 5.5 installasi *php5-ldap*

6) *Sudo apt-get install php5-mysql*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
                                                                                                          [ OK ]

Setting up libapache2-mod-php5 (5.2.10.dfsg.1-2ubuntu6.10) ...

Creating config file /etc/php5/apache2/php.ini with new version
 * Reloading web server config apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
                                                                                                          [ OK ]

Setting up php5 (5.2.10.dfsg.1-2ubuntu6.10) ...
Setting up php5-ldap (5.2.10.dfsg.1-2ubuntu6.10) ...

Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@dian-laptop:/home/newbie/Downloads# php5-mysql
php5-mysql: command not found
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install php5-mysql
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  php5-mysql
0 upgraded, 1 newly installed, 0 to remove and 344 not upgraded.
Need to get 66.2kB of archives.
After this operation, 246kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com karmic-updates/main php5-mysql 5.2.10.dfsg.1-2ubuntu6.10 [66.2kB]
Fetched 66.2kB in 19s (3,385B/s)
Selecting previously deselected package php5-mysql.
(Reading database ... 117121 files and directories currently installed.)
Unpacking php5-mysql (from .../php5-mysql_5.2.10.dfsg.1-2ubuntu6.10_i386.deb) ...
Setting up php5-mysql (5.2.10.dfsg.1-2ubuntu6.10) ...

root@dian-laptop:/home/newbie/Downloads#
```

Gambar 5.6 installasi *php5-mysql*

7) *Sudo apt-get install libpcap-dev-libpcap0-8- libpcre0.8-dev*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
                                                                                                          [ OK ]

Setting up libapache2-mod-php5 (5.2.10.dfsg.1-2ubuntu6.10) ...

Creating config file /etc/php5/apache2/php.ini with new version
 * Reloading web server config apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
                                                                                                          [ OK ]

Setting up php5 (5.2.10.dfsg.1-2ubuntu6.10) ...
Setting up php5-ldap (5.2.10.dfsg.1-2ubuntu6.10) ...

Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@dian-laptop:/home/newbie/Downloads# php5-mysql
php5-mysql: command not found
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install php5-mysql
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  php5-mysql
0 upgraded, 1 newly installed, 0 to remove and 344 not upgraded.
Need to get 66.2kB of archives.
After this operation, 246kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com karmic-updates/main php5-mysql 5.2.10.dfsg.1-2ubuntu6.10 [66.2kB]
Fetched 66.2kB in 19s (3,385B/s)
Selecting previously deselected package php5-mysql.
(Reading database ... 117121 files and directories currently installed.)
Unpacking php5-mysql (from .../php5-mysql_5.2.10.dfsg.1-2ubuntu6.10_i386.deb) ...
Setting up php5-mysql (5.2.10.dfsg.1-2ubuntu6.10) ...

root@dian-laptop:/home/newbie/Downloads#
```

Gambar 5.7 installasi *libcap*

8) *Sudo apt-get install libpcre3-dev*

```
root@dian-laptop: /home/newbie/Downloads
File Edit View Terminal Tabs Help
root@dian-laptop: /home/newbie/Downloads    root@dian-laptop: /home/newbie
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install libpcre3
Reading package lists... Done
Building dependency tree
Reading state information... Done
libpcre3 is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 344 not upgraded.
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install libpcre3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libpcrecpp0
The following NEW packages will be installed:
  libpcre3-dev libpcrecpp0
0 upgraded, 2 newly installed, 0 to remove and 344 not upgraded.
Need to get 356kB of archives.
After this operation, 844kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com karmic/main libpcrecpp0 7.8-3 [98.2kB]
Get:2 http://old-releases.ubuntu.com karmic/main libpcre3-dev 7.8-3 [258kB]
Fetched 356kB in 24s (14.8kB/s)
Selecting previously deselected package libpcrecpp0.
(Reading database ... 117375 files and directories currently installed.)
Unpacking libpcrecpp0 (from .../libpcrecpp0_7.8-3_i386.deb) ...
Selecting previously deselected package libpcre3-dev.
Unpacking libpcre3-dev (from .../libpcre3-dev_7.8-3_i386.deb) ...
Processing triggers for man-db ...
Setting up libpcrecpp0 (7.8-3) ...

Setting up libpcre3-dev (7.8-3) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@dian-laptop:/home/newbie/Downloads#
```

Gambar 5.8 installasi *libpcre3-dev*

9) *Sudo apt-get install expect*

```
root@dian-laptop: /home/newbie/Downloads
File Edit View Terminal Tabs Help
root@dian-laptop: /home/newbie/Downloads    root@dian-laptop: /home/newbie
Selecting previously deselected package libpcrecpp0.
(Reading database ... 117375 files and directories currently installed.)
Unpacking libpcrecpp0 (from .../libpcrecpp0_7.8-3_i386.deb) ...
Selecting previously deselected package libpcre3-dev.
Unpacking libpcre3-dev (from .../libpcre3-dev_7.8-3_i386.deb) ...
Processing triggers for man-db ...
Setting up libpcrecpp0 (7.8-3) ...

Setting up libpcre3-dev (7.8-3) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install expect
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  expectk
The following NEW packages will be installed:
  expect
0 upgraded, 1 newly installed, 0 to remove and 344 not upgraded.
Need to get 316kB of archives.
After this operation, 643kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com karmic/main expect 5.43.0-17 [316kB]
Fetched 316kB in 35s (8,847B/s)
Selecting previously deselected package expect.
(Reading database ... 117440 files and directories currently installed.)
Unpacking expect (from .../expect_5.43.0-17_i386.deb) ...
Processing triggers for man-db ...
Setting up expect (5.43.0-17) ...

Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@dian-laptop:/home/newbie/Downloads#
```

Gambar 5.9 installasi *expect*

10) *Sudo apt-get install bison*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /home/newbie/Downloads    root@dian-laptop: /home/newbie
After this operation, 643kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com karmic/main expect 5.43.0-17 [316kB]
Fetched 316kB in 35s (8,847B/s)
Selecting previously deselected package expect.
(Reading database ... 117440 files and directories currently installed.)
Unpacking expect (from .../expect_5.43.0-17_i386.deb) ...
Processing triggers for man-db ...
Setting up expect (5.43.0-17) ...

Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install bison
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  bison-doc
The following NEW packages will be installed:
  bison
0 upgraded, 1 newly installed, 0 to remove and 344 not upgraded.
Need to get 259kB of archives.
After this operation, 1,618kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com karmic/main bison 1:2.4.1.dfsg-1 [259kB]
Fetched 259kB in 23s (11.1kB/s)
Selecting previously deselected package bison.
(Reading database ... 117458 files and directories currently installed.)
Unpacking bison (from .../bison_1%3a2.4.1.dfsg-1_i386.deb) ...
Processing triggers for man-db ...
Setting up bison (1:2.4.1.dfsg-1) ...
update-alternatives: using /usr/bin/bison.yacc to provide /usr/bin/yacc (yacc) in auto mode.
update-alternatives: warning: not replacing /usr/share/man/man1/yacc.1.gz with a link.

root@dian-laptop:/home/newbie/Downloads# s
```

Gambar 5.10 installasi *bison*

11) *Sudo apt-get install libmysql++dev*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /home/newbie/Downloads    root@dian-laptop: /home/newbie
update-alternatives: warning: not replacing /usr/share/man/man1/yacc.1.gz with a link.

root@dian-laptop:/home/newbie/Downloads# sudo apt-get install libmysql++-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libmysql++3 libmysqlclient15-dev libmysqlclient15off
Suggested packages:
  libmysql++-doc mysql-doc-5.0
The following NEW packages will be installed:
  libmysql++-dev libmysql++3 libmysqlclient15-dev libmysqlclient15off
0 upgraded, 4 newly installed, 0 to remove and 344 not upgraded.
Need to get 9,521kB of archives.
After this operation, 27.6MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com karmic/universe libmysqlclient15off 5.1.30really5.0.83-0ubuntu3 [1,839kB]
Get:2 http://old-releases.ubuntu.com karmic/universe libmysql++3 3.0.9-1 [117kB]
Get:3 http://old-releases.ubuntu.com karmic/universe libmysqlclient15-dev 5.1.30really5.0.83-0ubuntu3 [7,273kB]
Get:4 http://old-releases.ubuntu.com karmic/universe libmysql++-dev 3.0.9-1 [292kB]
Fetched 9,521kB in 36s (257kB/s)
Selecting previously deselected package libmysqlclient15off.
(Reading database ... 117497 files and directories currently installed.)
Unpacking libmysqlclient15off (from .../libmysqlclient15off_5.1.30really5.0.83-0ubuntu3_i386.deb) ...
Selecting previously deselected package libmysql++3.
Unpacking libmysql++3 (from .../libmysql++3_3.0.9-1_i386.deb) ...
Selecting previously deselected package libmysqlclient15-dev.
Unpacking libmysqlclient15-dev (from .../libmysqlclient15-dev_5.1.30really5.0.83-0ubuntu3_i386.deb) ...
Selecting previously deselected package libmysql++-dev.
Unpacking libmysql++-dev (from .../libmysql++-dev_3.0.9-1_i386.deb) ...
Processing triggers for man-db ...
Setting up libmysqlclient15off (5.1.30really5.0.83-0ubuntu3) ...
```

Gambar 5.11 proses installasi *libmysql++dev*

12) *Sudo apt-get install libapache2-mod-php5*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /home/newbie/Downloads        root@dian-laptop: /home/newbie
root@dian-laptop:/home/newbie/Downloads#
root@dian-laptop:/home/newbie/Downloads#
root@dian-laptop:/home/newbie/Downloads#
root@dian-laptop:/home/newbie/Downloads#
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install libapache2-mod-php5
Reading package lists... Done
Building dependency tree
Reading state information... Done
libapache2-mod-php5 is already the newest version.
libapache2-mod-php5 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 344 not upgraded.
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install php5-cgi
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  php5-cgi
0 upgraded, 1 newly installed, 0 to remove and 344 not upgraded.
Need to get 4,982kB of archives.
After this operation, 10.6MB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com karmic-updates/main php5-cgi 5.2.10.dfsg.1-2ubuntu6.10 [4,982kB]
Fetched 4,982kB in 39s (126kB/s)
Selecting previously deselected package php5-cgi.
(Reading database ... 117653 files and directories currently installed.)
Unpacking php5-cgi (from .../php5-cgi_5.2.10.dfsg.1-2ubuntu6.10_i386.deb) ...
Processing triggers for man-db ...
Setting up php5-cgi (5.2.10.dfsg.1-2ubuntu6.10) ...

Creating config file /etc/php5/cgi/php.ini with new version
update-alternatives: using /usr/bin/php5-cgi to provide /usr/bin/php-cgi (php-cgi) in auto mode.
update-alternatives: using /usr/lib/cgi-bin/php5 to provide /usr/lib/cgi-bin/php (php-cgi-bin) in auto mode.

root@dian-laptop:/home/newbie/Downloads#
```

Gambar 5.12 installasi *libapache2-mod-php5*

13) *Sudo apt-get install php5-cgi*

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /home/newbie/Downloads        root@dian-laptop: /home/newbie
root@dian-laptop:/home/newbie/Downloads#
root@dian-laptop:/home/newbie/Downloads#
root@dian-laptop:/home/newbie/Downloads#
root@dian-laptop:/home/newbie/Downloads#
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install libapache2-mod-php5
Reading package lists... Done
Building dependency tree
Reading state information... Done
libapache2-mod-php5 is already the newest version.
libapache2-mod-php5 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 344 not upgraded.
root@dian-laptop:/home/newbie/Downloads# sudo apt-get install php5-cgi
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  php5-cgi
0 upgraded, 1 newly installed, 0 to remove and 344 not upgraded.
Need to get 4,982kB of archives.
After this operation, 10.6MB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com karmic-updates/main php5-cgi 5.2.10.dfsg.1-2ubuntu6.10 [4,982kB]
Fetched 4,982kB in 39s (126kB/s)
Selecting previously deselected package php5-cgi.
(Reading database ... 117653 files and directories currently installed.)
Unpacking php5-cgi (from .../php5-cgi_5.2.10.dfsg.1-2ubuntu6.10_i386.deb) ...
Processing triggers for man-db ...
Setting up php5-cgi (5.2.10.dfsg.1-2ubuntu6.10) ...

Creating config file /etc/php5/cgi/php.ini with new version
update-alternatives: using /usr/bin/php5-cgi to provide /usr/bin/php-cgi (php-cgi) in auto mode.
update-alternatives: using /usr/lib/cgi-bin/php5 to provide /usr/lib/cgi-bin/php (php-cgi-bin) in auto mode.

root@dian-laptop:/home/newbie/Downloads#
```

Gambar 5.13 installasi *php5-cgi*

Arti dari perintah *apt-get install* yang tertera diatas adalah perintah untuk menginstal paket baru keseluruhan paket tersebut diinstall pada *root*, karena *root*

merupakan status *user* tertinggi dalam sebuah *system* operasi, artinya semua file *system*, dokumen dan apapun semua dalamnya dapat diakses oleh *root.*

5.3.2. Installasi Paket *Snort*

Aplikasi *snort* yang digunakan pada penulisan skripsi ini adalah snort versi 2.8.4.1 yang Proses instalasi pun bisa juga dilakukan secara manual atau pun otomatis. Dalam penulisan skripsi ini penulis melakukan proses installasi IDS snort secara manual yang teknik penginstallannya menggunakan file yang berekstensi tar.gz dalam paket linux dengan cara mengumpulkan paket-paket yang dibutuhkan untuk komponen system Linux dan IDS, setelah paket terkumpul maka proses instalasi dapat dilakukan dengan cara mengekstrak dan compile setiap paket yang Keseluruhan proses installasi sebagai *root* agar setiap file yang dihasilkan memiliki *permission root*. Adapun proses installasi secara manual adalah sebagai berikut;

a. Copy kan file snort-2.8.4.1.tar.gz ke folder *src*. Lalu ekstrak
   # cp –Rf snort-2.8.4.1.tar.gz /usr/local/src
b. Kemudian masuk ke *direktori*
   # cd /usr/local/src
c. mengekstrak file snort;.
   # tar zxfv snort-2.8.4.1.tar.gz

```
root@dian-laptop: /usr/local/src
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /usr/local/src        root@dian-laptop: /usr/local/src
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_debug.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/snort_dce2.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_list.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_http.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/spp_dce2.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_utils.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_roptions.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/Makefile.am
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_stats.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/spp_dce2.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/snort_dce2.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_memory.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_smb.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_roptions.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_tcp.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_memory.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_config.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_tcp.c
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_event.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/includes/
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/includes/smb.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/includes/dcerpc.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_debug.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/dce2_list.h
snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2/sf_dce2.dsp
snort-2.8.4.1/src/fpdetect.c
snort-2.8.4.1/src/parser.h
snort-2.8.4.1/src/profiler.c
snort-2.8.4.1/src/event.h
snort-2.8.4.1/src/snprintf.c
snort-2.8.4.1/src/mempool.h
snort-2.8.4.1/src/codes.h
snort-2.8.4.1/src/util.h
```

Gambar 5.14 ekstrak *snort*

d. masuk ke dalam folder hasil ekstrak file *snort*

 # cd /usr/local/src/snort-2.8.4.1

e. konfigurasi dengan *mysql*

 # ./configure –with-mysql

```
root@dian-laptop: /usr/local/src/snort-2.8.4.1
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /usr/local/src/snort-2.8.4.1        root@dian-laptop: /usr/local/src
root@dian-laptop:/usr/local/src/snort-2.8.4.1# ./configure --with-mysql
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether to enable maintainer-specific portions of Makefiles... no
checking for style of include used by make... GNU
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking dependency style of gcc... none
checking for ranlib... ranlib
checking for bison... bison
checking for flex... no
checking for lex... no
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking dependency style of gcc... (cached) none
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
checking for a sed that does not truncate output... /bin/sed
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
```

Gambar 5.15 proses konfigurasi *mysql*

 # make

```
root@dian-laptop: /usr/local/src/snort-2.8.4.1
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /usr/local/src/snort-2.8.4.1    root@dian-laptop: /usr/local/src
cp ../include/sf_ip.c sf_ip.c
cp ../include/sfrt.c sfrt.c
cp ../include/sfrt_dir.c sfrt_dir.c
make  all-am
make[6]: Entering directory `/usr/local/src/snort-2.8.4.1/src/dynamic-preprocessors/dcerpc2'
/bin/bash ../../../libtool --tag=CC   --mode=compile gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes  -I/usr/include/m
ysql -DENABLE_MYSQL -fno-strict-aliasing  -g -O2 -Wall -DDYNAMIC_PLUGIN -fno-strict-aliasing -c -o dce2_debug.lo dce2_debug.c
mkdir .libs
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
 -DDYNAMIC_PLUGIN -fno-strict-aliasing -c dce2_debug.c  -fPIC -DPIC -o .libs/dce2_debug.o
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
 -DDYNAMIC_PLUGIN -fno-strict-aliasing -c dce2_debug.c -o dce2_debug.o >/dev/null 2>&1
/bin/bash ../../../libtool --tag=CC   --mode=compile gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes  -I/usr/include/m
ysql -DENABLE_MYSQL -fno-strict-aliasing  -g -O2 -Wall -DDYNAMIC_PLUGIN -fno-strict-aliasing -c -o dce2_utils.lo dce2_utils.c
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
 -DDYNAMIC_PLUGIN -fno-strict-aliasing -c dce2_utils.c  -fPIC -DPIC -o .libs/dce2_utils.o
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
 -DDYNAMIC_PLUGIN -fno-strict-aliasing -c dce2_utils.c -o dce2_utils.o >/dev/null 2>&1
/bin/bash ../../../libtool --tag=CC   --mode=compile gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes  -I/usr/include/m
ysql -DENABLE_MYSQL -fno-strict-aliasing  -g -O2 -Wall -DDYNAMIC_PLUGIN -fno-strict-aliasing -c -o dce2_list.lo dce2_list.c
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
 -DDYNAMIC_PLUGIN -fno-strict-aliasing -c dce2_list.c  -fPIC -DPIC -o .libs/dce2_list.o
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
 -DDYNAMIC_PLUGIN -fno-strict-aliasing -c dce2_list.c -o dce2_list.o >/dev/null 2>&1
/bin/bash ../../../libtool --tag=CC   --mode=compile gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes  -I/usr/include/m
ysql -DENABLE_MYSQL -fno-strict-aliasing  -g -O2 -Wall -DDYNAMIC_PLUGIN -fno-strict-aliasing -c -o dce2_memory.lo dce2_memory.c
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
 -DDYNAMIC_PLUGIN -fno-strict-aliasing -c dce2_memory.c  -fPIC -DPIC -o .libs/dce2_memory.o
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
 -DDYNAMIC_PLUGIN -fno-strict-aliasing -c dce2_memory.c -o dce2_memory.o >/dev/null 2>&1
/bin/bash ../../../libtool --tag=CC   --mode=compile gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes  -I/usr/include/m
ysql -DENABLE_MYSQL -fno-strict-aliasing  -g -O2 -Wall -DDYNAMIC_PLUGIN -fno-strict-aliasing -c -o dce2_stats.lo dce2_stats.c
 gcc -DHAVE_CONFIG_H -I. -I../../.. -I../include -I./includes -I/usr/include/mysql -DENABLE_MYSQL -fno-strict-aliasing -g -O2 -Wall
```

Gambar 5.16 proses *make* file *snort*

 # make install

```
root@dian-laptop: /usr/local/src/snort-2.8.4.1
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /usr/local/src/snort-2.8.4.1    root@dian-laptop: /usr/local/src
ranlib /usr/local/lib/snort_dynamicpreprocessor/libsf_ssh_preproc.a
PATH="$PATH:/sbin" ldconfig -n /usr/local/lib/snort_dynamicpreprocessor
----------------------------------------------------------------------
Libraries have been installed in:
   /usr/local/lib/snort_dynamicpreprocessor

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the `-LLIBDIR'
flag during linking and do at least one of the following:
   - add LIBDIR to the `LD_LIBRARY_PATH' environment variable
     during execution
   - add LIBDIR to the `LD_RUN_PATH' environment variable
     during linking
   - use the `-Wl,--rpath -Wl,LIBDIR' linker flag
   - have your system administrator add LIBDIR to `/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
make[6]: Nothing to be done for `install-data-am'.
make[6]: Leaving directory `/usr/local/src/snort-2.8.4.1/src/dynamic-preprocessors/ssh'
make[5]: Leaving directory `/usr/local/src/snort-2.8.4.1/src/dynamic-preprocessors/ssh'
make[4]: Leaving directory `/usr/local/src/snort-2.8.4.1/src/dynamic-preprocessors/ssh'
Making install in dcerpc
make[4]: Entering directory `/usr/local/src/snort-2.8.4.1/src/dynamic-preprocessors/dcerpc'
make  install-am
make[5]: Entering directory `/usr/local/src/snort-2.8.4.1/src/dynamic-preprocessors/dcerpc'
make DESTDIR=`pwd`/../build install-libLTLIBRARIES
make[6]: Entering directory `/usr/local/src/snort-2.8.4.1/src/dynamic-preprocessors/dcerpc'
test -z "/usr/local/lib/snort_dynamicpreprocessor" || /bin/mkdir -p "/usr/local/src/snort-2.8.4.1/src/dynamic-preprocessors/dcerpc/
../build/usr/local/lib/snort_dynamicpreprocessor"
 /bin/bash ../../../libtool --mode=install /usr/bin/install -c  'libsf_dcerpc_preproc.la' '/usr/local/src/snort-2.8.4.1/src/dynamic
```

Gambar 5.17 proses *make install snort*

f. membuat direktori untuk *logging snort*

#groupadd snort

g. membuat *user snort* di dalam *group snort*

#useradd –g snort snort

h. membuat direktori *snort*

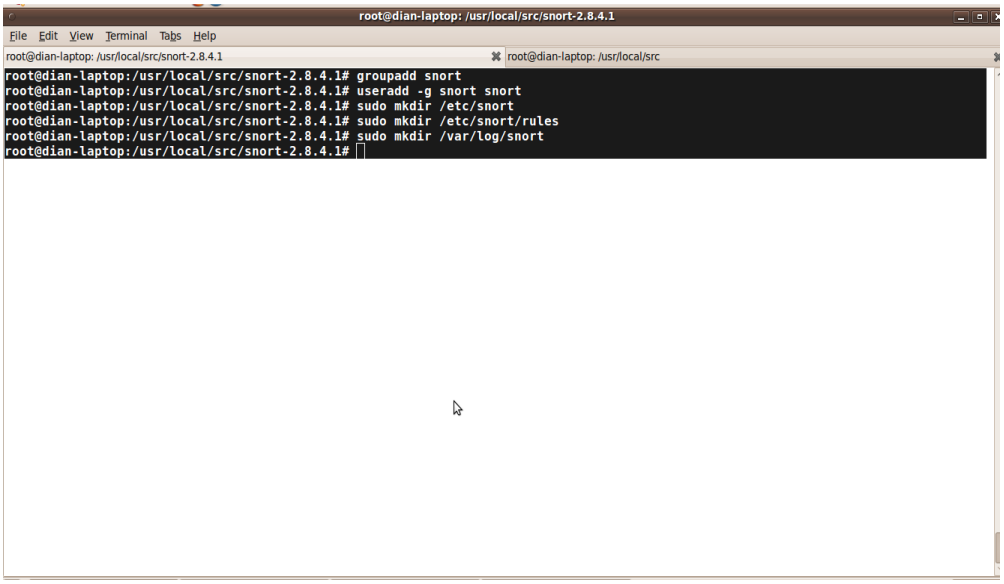
#sudo mkdir /etc/snort

i. membuat direktori rule snort

#sudo mkdir /etc/snort/rules

j. membuat direktori log

#sudo mkdir /etc/var/log/snort



Gambar 5.18 membuat direktori *snort*

5.3.3. Installasi *Rules Snort*

Rule snort dapat didowload di website snort.org dengan melakukan login account terlebih dahulu untuk mendapatkan rules yang sesuai dengan versi snort yang digunakan. Rules snort selalu terupdate dengan versi yang berbeda dikarenakan untuk mendapatkan hasil deteksi yang lebih baik serta untuk menghilangkan bugs yang terdapat di dalam rules-rules versi lama, adapun proses lanjutan konfigurasi rules snort adalah;

a) salin file ke dalam direktori */etc/snort*

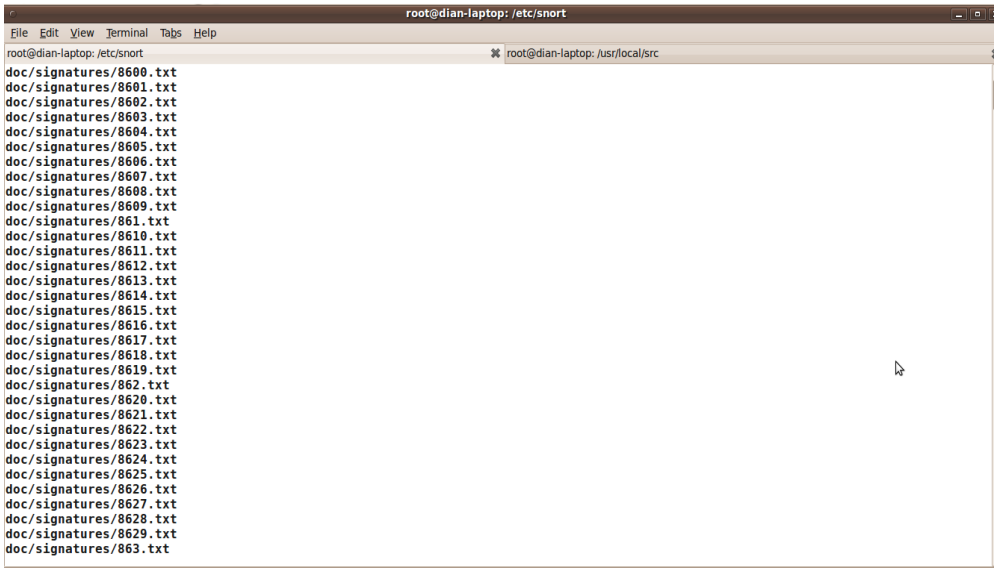
 # cp snortrules-snapshot-CURRENT.tar.gz /etc/snort/

b) masuk kedalam direktori */etc/snort*

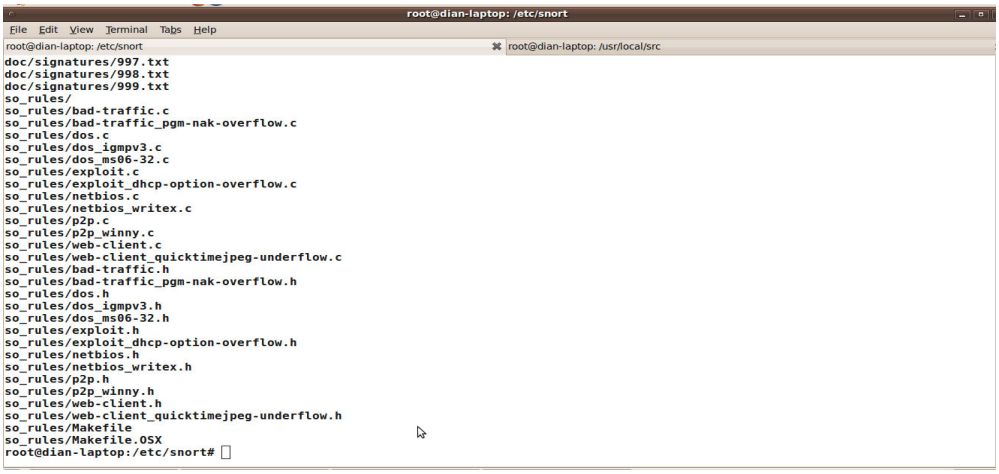
 # cd /etc/snort

c) mengekstrak file Rules Snort pada direktori */etc/snort*

 # tar zxvf snortrules-snapshot-CURRENT.tar.gz



Gambar 5.19 proses ekstrak *rule snort*



Gambar 5.20 proses compile paket *rule snort*

5.3.4. Konfigurasi file *snort.conf*

Selanjutnya adalah proses konfigurasi *snort. File* konfigurasi *snor*t berada di ***/etc/snort/snort.conf.*** berikut adalah sejumlah baris yang perlu dikonfigurasi.

a) Copy snort

#cp /usr/local/src/snort-2.8.0/etc/* /etc/snort

b) masuk kedalam direktori */etc/snort*

 # cd /etc/snort/

c) buka file konfigurasi *snort.conf*

 # vi /etc/snort/snort.conf

d) rubah *path* lokasi *signature / rules snort*

#var RULE_PATH /etc/snort/rules

 # output database: log, mysql, user=snort password=snort dbname=snort host=localhost

d) set alamat IP sistem jaringan Internal

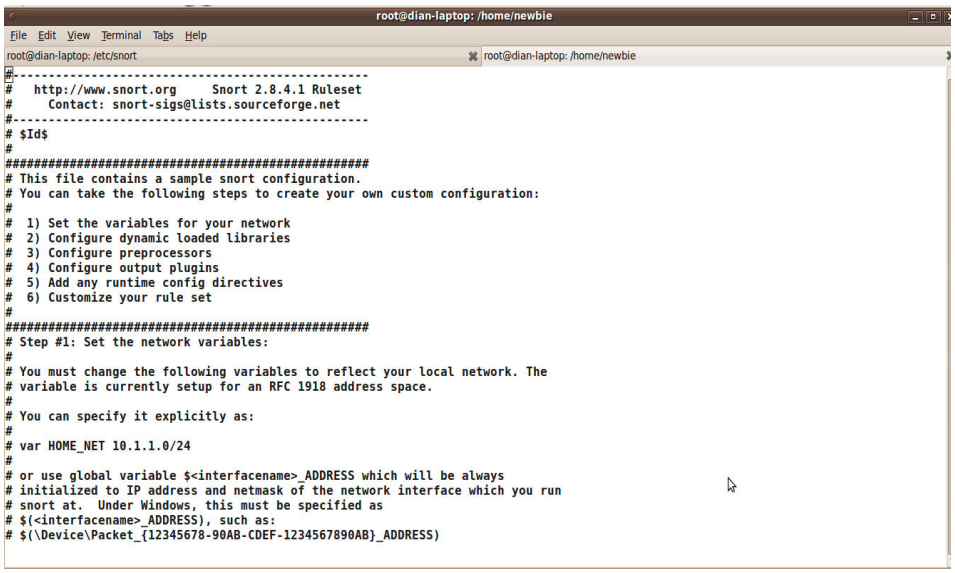
 # var HOME_NET [10.1.1.0/24,192.168.1.0/24]

e) set alamat IP sistem jaringan Eksternal

 # var EXTERNAL_NET !$HOME_NET

f) set direktif *output snort*

 # output database: log, mysql, user=snort password=snort dbname=snort host=localhost



Gambar 5.21 Tampilan awal file *snort.conf*

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /etc/snort        root@dian-laptop: /home/newbie
# Ports you want to look for SHELLCODE on.
portvar SHELLCODE_PORTS !80

# Ports you might see oracle attacks on
portvar ORACLE_PORTS 1521

# other variables
#
# AIM servers.  AOL has a habit of adding new AIM servers, so instead of
# modifying the signatures when they do, we add them to this list of servers.
var AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0
/24,205.188.9.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH /etc/snort/rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# Configure the snort decoder
# ============================
#
# Snort's decoder will alert on lots of things such as header
# truncation or options of unusual length or infrequently used tcp options
#
#
# Stop generic decode events:
#
# config disable_decode_alerts
#
# Stop Alerts on experimental TCP options
#
```

Gambar 5.22 lokasi *signature rules snort*

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /etc/snort        root@dian-laptop: /home/newbie
# output log_tcpdump: tcpdump.log

# database: log to a variety of databases
# ---------------------------------------
# See the README.database file for more information about configuring
# and using this plugin.
#
# output database: log, mysql, user=root password=test dbname=db host=localhost
# output database: alert, postgresql, user=snort dbname=snort
# output database: log, odbc, user=snort dbname=snort
# output database: log, mssql, dbname=snort user=snort password=test
# output database: log, oracle, dbname=snort user=snort password=test

# unified: Snort unified binary format alerting and logging
# ---------------------------------------------------------
# The unified output plugin provides two new formats for logging and generating
# alerts from Snort, the "unified" format.  The unified format is a straight
# binary format for logging data out of Snort that is designed to be fast and
# efficient.  Used with barnyard (the new alert/log processor), most of the
# overhead for logging and alerting to various slow storage mechanisms such as
# databases or the network can now be avoided.
#
# Check out the spo_unified.h file for the data formats.
#
# Two arguments are supported.
#    filename - base filename to write to (current time_t is appended)
#    limit    - maximum size of spool file in MB (default: 128)
#
# output alert_unified: filename snort.alert, limit 128
# output log_unified: filename snort.log, limit 128
```

Gambar 5.23 *set output database snort*

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /etc/snort        root@dian-laptop: /home/newbie
# output log_tcpdump: tcpdump.log

# database: log to a variety of databases
# ---------------------------------------
# See the README.database file for more information about configuring
# and using this plugin.
#
# output database: log, mysql, user=root password=test dbname=db host=localhost
# output database: alert, postgresql, user=snort dbname=snort
# output database: log, odbc, user=snort dbname=snort
# output database: log, mssql, dbname=snort user=snort password=test
# output database: log, oracle, dbname=snort user=snort password=test

# unified: Snort unified binary format alerting and logging
# ---------------------------------------------------------
# The unified output plugin provides two new formats for logging and generating
# alerts from Snort, the "unified" format.  The unified format is a straight
# binary format for logging data out of Snort that is designed to be fast and
# efficient.  Used with barnyard (the new alert/log processor), most of the
# overhead for logging and alerting to various slow storage mechanisms such as
# databases or the network can now be avoided.
#
# Check out the spo_unified.h file for the data formats.
#
# Two arguments are supported.
#    filename - base filename to write to (current time_t is appended)
#    limit    - maximum size of spool file in MB (default: 128)
#
# output alert_unified: filename snort.alert, limit 128
# output log_unified: filename snort.log, limit 128
```

Gambar 5.24 *set format binary alert dan logging snort*

g) Ujicoba jalankan snort,

#/usr/local/bin/snort -dev -c /etc/snort/snort.conf

karena Snort rules yang digunakan biasanya masih banyak bug / error dan harus dibuang supaya hanya rules yang baik yang digunakan

```
root@dian-laptop: /etc/snort
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /etc/snort        root@dian-laptop: /usr/local/src
root@dian-laptop:/etc/snort# /usr/local/bin/snort -dev -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file /etc/snort/snort.conf
PortVar 'HTTP_PORTS' defined :  [ 80 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1521 ]
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Target-based policy: FIRST
    Fragment timeout: 60 seconds
    Fragment min_ttl:   1
    Fragment ttl_limit (not used): 5
    Fragment Problems: 1
Stream5 global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 8192
    Memcap (for reassembly packet storage): 8388608
    Track UDP sessions: INACTIVE
    Track ICMP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
Stream5 TCP Policy config:
    Reassembly Policy: FIRST
    Timeout: 30 seconds
    Min ttl:  1
    Maximum number of bytes to queue per session: 1048576
    Maximum number of segs to queue per session: 2621
```

Gambar 5.25 uji coba *snort*

```
root@dian-laptop: /etc/snort
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /etc/snort        root@dian-laptop: /usr/local/src

[ Port Based Pattern Matching Memory ]
+-[AC-BNFA Search Info Summary]----------------------------
| Instances        : 211
| Patterns         : 27542
| Pattern Chars    : 265664
| Num States       : 98133
| Num Match States : 11118
| Memory           :   3.13Mbytes
|   Patterns       :   0.88M
|   Match Lists    :   0.89M
|   Transitions    :   1.31M
+-----------------------------------------------

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.8.4.1 (Build 38)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/team.html
           Copyright (C) 1998-2009 Sourcefire, Inc., et al.
           Using PCRE version: 7.8 2008-09-05

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 1.10  <Build 16>
           Preprocessor Object: SF_Dynamic_Example_Preprocessor  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 2>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 2>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 7>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 11>
Not Using PCAP_FRAMES
```

Gambar 5.26 hasil uji coba *snort*

Keterangan gambar diatas bahwa hasil uji coba snort berjalan dengan baik tanpa ada pesan error, proses berjalan terhenti menyatakan bahwa karena snort berstatus *daemon* yaitu bergerak di belakang layar sehingga proses aktivitas yang di jalankan snort tidak terlihat.

5.3.5. Setup Database *Snort*

Adapun proses setup database *snort* untuk mysql adalah sebagai berikut.

a) Masuk ke console terminal dan aktifkan mysql;

 # mysql –u –root – p

 # Enter password:

b) Membuat database untuk *snort*

 # create database snort;

mysql> grant ALL on root.* to snort@localhost;

mysql>grant ALL on snort.* to snort@localhost IDENTIFIED BY 'snort' ;

mysql>grant ALL on snort.* to snort IDENTIFIED BY 'snort' ;

mysql>exit

c) Set hak akses untuk user root

 # grant INSERT, SELECT on root.* to snort@localhost;

d) set *password* untuk *user 'snort'* dengan 'password'

 # SET PASSWORD FOR snort@localhost =PASSWORD('password');

e) set hak akses untuk *user 'snort'* di *localhost*

 # grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Help
root@dian-laptop:/home/newbie# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
Server version: 5.1.37-1ubuntu5.5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database snort;
Query OK, 1 row affected (0.00 sec)

mysql> grant ALL on root.* to snort@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> grant ALL on snort.* to snort@localhost IDENTIFIED BY 'snort' ;
Query OK, 0 rows affected (0.00 sec)

mysql> grant ALL on snort.* to snort IDENTIFIED BY 'snort' ;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
root@dian-laptop:/home/newbie#
```

Gambar 5.27 proses pembuatan database snort

f) **Menyiapkan table database snort**

 # mysql -u root -p123 < /usr/local/src/snort 2.8.4.1/schemas/create_mysql snort

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Help
root@dian-laptop:/home/newbie# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
Server version: 5.1.37-1ubuntu5.5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database snort;
Query OK, 1 row affected (0.00 sec)

mysql> grant ALL on root.* to snort@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> grant ALL on snort.* to snort@localhost IDENTIFIED BY 'snort' ;
Query OK, 0 rows affected (0.00 sec)

mysql> grant ALL on snort.* to snort IDENTIFIED BY 'snort' ;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
root@dian-laptop:/home/newbie# mysql -u root -p123456 < /usr/local/src/snort-2.8.4.1/schemas/create_mysql snort
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
root@dian-laptop:/home/newbie# mysql -u root -p123 < /usr/local/src/snort-2.8.4.1/schemas/create_mysql snort
root@dian-laptop:/home/newbie#
```

Gambar 5.28 proses penyiapan database *snort*

g) **Cek Database Snort**

 # Mysql –p

 # Enter Password:

 # Show databases;

 # Use snort;

 # Show tables;

 # exit

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Help
root@dian-laptop:/home/newbie#
root@dian-laptop:/home/newbie#
root@dian-laptop:/home/newbie# mysql -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 40
Server version: 5.1.37-1ubuntu5.5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| snort              |
+--------------------+
3 rows in set (0.00 sec)

mysql> use snort;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------+
| Tables_in_snort  |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
```

Gambar 5.29 login ke database *snort*

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Help
root@dian-laptop:/home/newbie#
root@dian-laptop:/home/newbie#
root@dian-laptop:/home/newbie# mysql -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 40
Server version: 5.1.37-1ubuntu5.5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| snort              |
+--------------------+
3 rows in set (0.00 sec)

mysql> use snort;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------+
| Tables_in_snort  |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
```

Gambar 5.30 menampilkan database snort

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Help
| snort               |
+--------------------+
3 rows in set (0.00 sec)

mysql> use snort;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------+
| Tables_in_snort  |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
| udphdr           |
+------------------+
16 rows in set (0.00 sec)

mysql> exit
Bye
root@dian-laptop:/home/newbie#
```

Gambar 5.31 menampilkan *table database*

Pada sintak diatas terdapat perintah *make* yang berarti untuk *build* program, sedangkan *make install* adalah perintah untuk menginstall program, mkdir adalah perintah untuk membuat direktori *snort.*

5.3.6. Konfigurasi *Barnyard*

Versi aplikasi *Barnyard* yang digunakan pada waktu penulisan skripsi ini adalah ***Barnyard2 versi 1.7***. Keseluruhan proses instalasi dilakukan sebagai *root* agar setiap *file* yang dihasilkan secara otomatis memiliki permission **root.** Ekstrak file *barnyard2-1.7* yang telah didowload kemudian masuk ke folder hasil ekstrak *barnyard2-1.7,* adapun perintahnya adalah;

1) *compile barnyard* dengan fitur *logging* MYSQL

   # ./configure --with-mysql

2) instalasi *Barrnyard*

   # make

   # *make install*

3) masuk kedalam direktori *Barnyard2*

   # cd /usr/local/ barnyard2-1.7

4) salin file konfigurasi *Barnyard.conf ke /etc/snort*

   # cp etc/barnyard2.conf /etc/snort

5.3.7. konfigurasi *barnyard.conf*

Tahap instalasi sudah selesai, selanjutnya adalah konfigurasi file barnyard dengan nama ***barnyard.conf*** yang berada pada direktori ***/etc/snort/barnyard.conf***.

a. Buka file *barnyard.conf*

   # vim /etc/snort/barnyard2.conf

b. rubah konfigurasi *hostname dan interface*

   # config hostname : localhost

   config interface : eth0

c. #rubah *output* database

   #output database: alert, mysql, user=snort password=password

   dbname=snort host=localhost

5.3.8. Konfigurasi *adodb*

Versi aplikasi *adodb* digunakan pada penulisan skripsi ini adalah `*adodb4991.tar.gz* hasil download. Keseluruhan proses installasi dilakukan sebagai `*root* Agar setiap file yang dihasilkan secara otomatis memiliki *permission root.*

a. Copy folder adodb-4991.tgz ke direktori *var/www*

b. Masuk ke dalam direktori *var/www*

   # cd /var/www

c. Mengekstrak adodb

   # tar zxfv adodb-4991

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
root@dian-laptop:/var/www/base# /etc/init.d/apache2 restart
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
                                                                                                                    [ OK ]
root@dian-laptop:/var/www/base# /etc/init.d/mysql restart
 * Stopping MySQL database server mysqld                                                                            [ OK ]
 * Starting MySQL database server mysqld                                                                            [ OK ]
 * Checking for corrupt, not cleanly closed and upgrade needing tables.
root@dian-laptop:/var/www/base# cd /home/newbie/Downloads
root@dian-laptop:/home/newbie/Downloads# ls
adodb4991.tgz   BACKUP 07-08-2014 DARI LAPTOP UBUNTU 9.10  base-1.4.5.tar.gz  ONO W PURBO MATERI
APLIKASI SNORT  barnyard2-1.7.tar.gz                       DIan NITIP         prinscreen hasil oprek repo karmic koala
root@dian-laptop:/home/newbie/Downloads# cp adodb4991.tgz /var/www
root@dian-laptop:/home/newbie/Downloads#
```

Gambar 5.32 Pengcopyan Folder adodb

```
root@dian-laptop: /var/www
File  Edit  View  Terminal  Help
root@dian-laptop:/var/www/base# /etc/init.d/apache2 restart
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
                                                                                                                    [ OK ]
root@dian-laptop:/var/www/base# /etc/init.d/mysql restart
 * Stopping MySQL database server mysqld                                                                            [ OK ]
 * Starting MySQL database server mysqld                                                                            [ OK ]
 * Checking for corrupt, not cleanly closed and upgrade needing tables.
root@dian-laptop:/var/www/base# cd /home/newbie/Downloads
root@dian-laptop:/home/newbie/Downloads# ls
adodb4991.tgz   BACKUP 07-08-2014 DARI LAPTOP UBUNTU 9.10  base-1.4.5.tar.gz  ONO W PURBO MATERI
APLIKASI SNORT  barnyard2-1.7.tar.gz                       DIan NITIP         prinscreen hasil oprek repo karmic koala
root@dian-laptop:/home/newbie/Downloads# cp adodb4991.tgz /var/www
root@dian-laptop:/home/newbie/Downloads# cd /var/www
root@dian-laptop:/var/www#
```

Gambar 5.33 Proses Masuk Direktori Lain

```
root@dian-laptop: /var/www
File  Edit  View  Terminal  Help
adodb4991.tgz  base  base-1.4.5.tar.gz  index.html
root@dian-laptop:/var/www# tar zxvf adodb4991.tgz
adodb/adodb-active-record.inc.php
adodb/adodb-csvlib.inc.php
adodb/adodb-datadict.inc.php
adodb/adodb-error.inc.php
adodb/adodb-errorhandler.inc.php
adodb/adodb-errorpear.inc.php
adodb/adodb-exceptions.inc.php
adodb/adodb-iterator.inc.php
adodb/adodb-lib.inc.php
adodb/adodb-memcache.lib.inc.php
adodb/adodb-pager.inc.php
adodb/adodb-pear.inc.php
adodb/adodb-perf.inc.php
adodb/adodb-php4.inc.php
adodb/adodb-time.inc.php
adodb/adodb-time.zip
adodb/adodb-xmlschema.inc.php
adodb/adodb-xmlschema03.inc.php
adodb/adodb.inc.php
adodb/license.txt
adodb/pivottable.inc.php
adodb/readme.txt
adodb/rsfilter.inc.php
adodb/server.php
adodb/toexport.inc.php
adodb/tohtml.inc.php
adodb/xmlschema.dtd
adodb/xmlschema03.dtd
adodb/perf/perf-db2.inc.php
adodb/perf/perf-informix.inc.php
adodb/perf/perf-mssql.inc.php
adodb/perf/perf-mssqlnative.inc.php
adodb/perf/perf-mysql.inc.php
```

Gambar 5.34 proses compile file adodb

5.3.9. Konfigurasi *BASE*

Aplikasi BASE yang digunakan adalah BASE versi 1.3.9. Keseluruhan proses instalasi dilakukan sebagai *root* agar setiap *file* yang dihasilkan secara otomatis memiliki *permission root.*

a) Instalasi *PEAR*

 # Sudo apt-get install php-pear

b) Installasi modu*l PEAR*

 # pear install Number_Roman-1.0.2

 # pear install Number_Words-0.16.2

 # pear install Image_Canvas-0.3.2

 # pear install Image_Graph-0.7.2

 # pear install –alldeps mail

```
root@dian-laptop: /home/newbie/Downloads
File  Edit  View  Terminal  Help
Get:1 http://old-releases.ubuntu.com karmic-updates/main php5-mysql 5.2.10.dfsg.1-2ubuntu6.10 [66.2kB]
Fetched 66.2kB in 19s (3,385B/s)
Selecting previously deselected package php5-mysql.
(Reading database ... 117121 files and directories currently installed.)
Unpacking php5-mysql (from .../php5-mysql_5.2.10.dfsg.1-2ubuntu6.10_i386.deb) ...
Setting up php5-mysql (5.2.10.dfsg.1-2ubuntu6.10) ...

root@dian-laptop:/home/newbie/Downloads# sudo apt-get install php-pear
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  php5-cli
The following NEW packages will be installed:
  php-pear php5-cli
0 upgraded, 2 newly installed, 0 to remove and 344 not upgraded.
Need to get 2,842kB of archives.
After this operation, 7,827kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com karmic-updates/main php5-cli 5.2.10.dfsg.1-2ubuntu6.10 [2,513kB]
Get:2 http://old-releases.ubuntu.com karmic-updates/main php-pear 5.2.10.dfsg.1-2ubuntu6.10 [330kB]
Fetched 2,842kB in 49s (57.1kB/s)
Selecting previously deselected package php5-cli.
(Reading database ... 117128 files and directories currently installed.)
Unpacking php5-cli (from .../php5-cli_5.2.10.dfsg.1-2ubuntu6.10_i386.deb) ...
Selecting previously deselected package php-pear.
Unpacking php-pear (from .../php-pear_5.2.10.dfsg.1-2ubuntu6.10_all.deb) ...
Processing triggers for man-db ...
Setting up php5-cli (5.2.10.dfsg.1-2ubuntu6.10) ...

Creating config file /etc/php5/cli/php.ini with new version
update-alternatives: using /usr/bin/php5 to provide /usr/bin/php (php) in auto mode.

Setting up php-pear (5.2.10.dfsg.1-2ubuntu6.10) ...
root@dian-laptop:/home/newbie/Downloads# ^[[2~
```

Gambar5.35 installasi paket *php-pear base*

```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
root@dian-laptop:/var/www/base# gedit base_conf.php
root@dian-laptop:/var/www/base# pear list
Installed packages, channel pear.php.net:
=========================================
Package          Version State
Archive_Tar      1.3.3   stable
Console_Getopt   1.2.3   stable
PEAR             1.9.0   stable
Structures_Graph 1.0.2   stable
XML_Util         1.2.1   stable
root@dian-laptop:/var/www/base# pear install Numbers_Roman-1.0.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Numbers_Roman-1.0.2.tgz ...
Starting to download Numbers_Roman-1.0.2.tgz (6,210 bytes)
.....done: 6,210 bytes
install ok: channel://pear.php.net/Numbers_Roman-1.0.2
root@dian-laptop:/var/www/base# pear install Numbers_Words-0.16.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Numbers_Words-0.16.2.tgz ...
Starting to download Numbers_Words-0.16.2.tgz (52,956 bytes)
............done: 52,956 bytes
downloading Math_BigInteger-1.0.2.tgz ...
Starting to download Math_BigInteger-1.0.2.tgz (27,854 bytes)
...done: 27,854 bytes
install ok: channel://pear.php.net/Math_BigInteger-1.0.2
install ok: channel://pear.php.net/Numbers_Words-0.16.2
root@dian-laptop:/var/www/base# pear install Image_Canvas-0.3.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
WARNING: "pear/Image_Color" is deprecated in favor of "pear/Image_Color2"
downloading Image_Canvas-0.3.2.tgz ...
Starting to download Image_Canvas-0.3.2.tgz (54,698 bytes)
............done: 54,698 bytes
downloading Image_Color-1.0.4.tgz ...
Starting to download Image_Color-1.0.4.tgz (9,501 bytes)
...done: 9,501 bytes
```

Gambar 5.36 installasi modul *pear*

c) *pear install Number Roman-1.0.2*

```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
root@dian-laptop:/var/www/base# gedit base_conf.php
root@dian-laptop:/var/www/base# chown -Rf www-data.www-data /var/www/base
root@dian-laptop:/var/www/base# gedit base_conf.php
root@dian-laptop:/var/www/base# pear list
Installed packages, channel pear.php.net:
=========================================
Package           Version State
Archive_Tar       1.3.3   stable
Console_Getopt    1.2.3   stable
PEAR              1.9.0   stable
Structures_Graph  1.0.2   stable
XML_Util          1.2.1   stable
root@dian-laptop:/var/www/base# pear install Numbers_Roman-1.0.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Numbers_Roman-1.0.2.tgz ...
Starting to download Numbers_Roman-1.0.2.tgz (6,210 bytes)
.....done: 6,210 bytes
install ok: channel://pear.php.net/Numbers_Roman-1.0.2
root@dian-laptop:/var/www/base# pear install Numbers_Words-0.16.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Numbers_Words-0.16.2.tgz ...
Starting to download Numbers_Words-0.16.2.tgz (52,956 bytes)
.............done: 52,956 bytes
downloading Math_BigInteger-1.0.2.tgz ...
Starting to download Math_BigInteger-1.0.2.tgz (27,854 bytes)
...done: 27,854 bytes
install ok: channel://pear.php.net/Math_BigInteger-1.0.2
install ok: channel://pear.php.net/Numbers_Words-0.16.2
root@dian-laptop:/var/www/base# pear install Image_Canvas-0.3.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
WARNING: "pear/Image_Color" is deprecated in favor of "pear/Image_Color2"
downloading Image_Canvas-0.3.2.tgz ...
Starting to download Image_Canvas-0.3.2.tgz (54,698 bytes)
.............done: 54,698 bytes
downloading Image_Color-1.0.4.tgz ...
```

Gambar 5.37 installasi *paket number roman* php

d) *pear install Number_word-0.16.2*

```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
root@dian-laptop:/var/www/base# gedit base_conf.php
root@dian-laptop:/var/www/base# chown -Rf www-data.www-data /var/www/base
root@dian-laptop:/var/www/base# gedit base_conf.php
root@dian-laptop:/var/www/base# pear list
Installed packages, channel pear.php.net:
=========================================
Package           Version State
Archive_Tar       1.3.3   stable
Console_Getopt    1.2.3   stable
PEAR              1.9.0   stable
Structures_Graph  1.0.2   stable
XML_Util          1.2.1   stable
root@dian-laptop:/var/www/base# pear install Numbers_Roman-1.0.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Numbers_Roman-1.0.2.tgz ...
Starting to download Numbers_Roman-1.0.2.tgz (6,210 bytes)
.....done: 6,210 bytes
install ok: channel://pear.php.net/Numbers_Roman-1.0.2
root@dian-laptop:/var/www/base# pear install Numbers_Words-0.16.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Numbers_Words-0.16.2.tgz ...
Starting to download Numbers_Words-0.16.2.tgz (52,956 bytes)
.............done: 52,956 bytes
downloading Math_BigInteger-1.0.2.tgz ...
Starting to download Math_BigInteger-1.0.2.tgz (27,854 bytes)
...done: 27,854 bytes
install ok: channel://pear.php.net/Math_BigInteger-1.0.2
install ok: channel://pear.php.net/Numbers_Words-0.16.2
root@dian-laptop:/var/www/base# pear install Image_Canvas-0.3.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
WARNING: "pear/Image_Color" is deprecated in favor of "pear/Image_Color2"
downloading Image_Canvas-0.3.2.tgz ...
Starting to download Image_Canvas-0.3.2.tgz (54,698 bytes)
.............done: 54,698 bytes
downloading Image_Color-1.0.4.tgz ...
```

Gambar 5.38 installasi paket *number words* php

e) *Pear install Image_Canvas-0.3.2*

```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
.....done: 6,210 bytes
install ok: channel://pear.php.net/Numbers_Roman-1.0.2
root@dian-laptop:/var/www/base# pear install Numbers_Words-0.16.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Numbers_Words-0.16.2.tgz ...
Starting to download Numbers_Words-0.16.2.tgz (52,956 bytes)
.............done: 52,956 bytes
downloading Math_BigInteger-1.0.2.tgz ...
Starting to download Math_BigInteger-1.0.2.tgz (27,854 bytes)
...done: 27,854 bytes
install ok: channel://pear.php.net/Math_BigInteger-1.0.2
install ok: channel://pear.php.net/Numbers_Words-0.16.2
root@dian-laptop:/var/www/base# pear install Image_Canvas-0.3.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
WARNING: "pear/Image_Color" is deprecated in favor of "pear/Image_Color2"
downloading Image_Canvas-0.3.2.tgz ...
Starting to download Image_Canvas-0.3.2.tgz (54,698 bytes)
.............done: 54,698 bytes
downloading Image_Color-1.0.4.tgz ...
Starting to download Image_Color-1.0.4.tgz (9,501 bytes)
...done: 9,501 bytes
install ok: channel://pear.php.net/Image_Color-1.0.4
install ok: channel://pear.php.net/Image_Canvas-0.3.2
root@dian-laptop:/var/www/base# pear install Image_Graph-0.7.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Image_Graph-0.7.2.tgz ...
Starting to download Image_Graph-0.7.2.tgz (368,056 bytes)
.........................................................................done: 368,056 bytes
install ok: channel://pear.php.net/Image_Graph-0.7.2
root@dian-laptop:/var/www/base# pear install --alldeps mail
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
WARNING: "pear/Auth_SASL" is deprecated in favor of "pear/Auth_SASL2"
downloading Mail-1.2.0.tgz ...
Starting to download Mail-1.2.0.tgz (23,214 bytes)
........done: 23,214 bytes
```

Gambar 5.39 installasi paket *Image_Canvas* php

f) *Pear install Image_Graph-0.7.2*

```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
Starting to download Image_Canvas-0.3.2.tgz (54,698 bytes)
.............done: 54,698 bytes
downloading Image_Color-1.0.4.tgz ...
Starting to download Image_Color-1.0.4.tgz (9,501 bytes)
...done: 9,501 bytes
install ok: channel://pear.php.net/Image_Color-1.0.4
install ok: channel://pear.php.net/Image_Canvas-0.3.2
root@dian-laptop:/var/www/base# pear install Image_Graph-0.7.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Image_Graph-0.7.2.tgz ...
Starting to download Image_Graph-0.7.2.tgz (368,056 bytes)
.........................................................................done: 368,056 bytes
install ok: channel://pear.php.net/Image_Graph-0.7.2
root@dian-laptop:/var/www/base# pear install --alldeps mail
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
WARNING: "pear/Auth_SASL" is deprecated in favor of "pear/Auth_SASL2"
downloading Mail-1.2.0.tgz ...
Starting to download Mail-1.2.0.tgz (23,214 bytes)
........done: 23,214 bytes
downloading Net_SMTP-1.6.2.tgz ...
Starting to download Net_SMTP-1.6.2.tgz (13,077 bytes)
...done: 13,077 bytes
downloading Net_Socket-1.0.14.tgz ...
Starting to download Net_Socket-1.0.14.tgz (5,600 bytes)
...done: 5,600 bytes
downloading Auth_SASL-1.0.6.tgz ...
Starting to download Auth_SASL-1.0.6.tgz (9,119 bytes)
...done: 9,119 bytes
install ok: channel://pear.php.net/Mail-1.2.0
install ok: channel://pear.php.net/Net_Socket-1.0.14
install ok: channel://pear.php.net/Auth_SASL-1.0.6
install ok: channel://pear.php.net/Net_SMTP-1.6.2
root@dian-laptop:/var/www/base# pear install Mail
pear/Mail is already installed and is the same as the released version 1.2.0
install failed
```

Gambar 5.40 installasi paket *Image_Graph* php

g) *Pear install –alldeps mail*

```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
install ok: channel://pear.php.net/Image_Color-1.0.4
install ok: channel://pear.php.net/Image_Canvas-0.3.2
root@dian-laptop:/var/www/base# pear install Image_Graph-0.7.2
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Image_Graph-0.7.2.tgz ...
Starting to download Image_Graph-0.7.2.tgz (368,056 bytes)
.......................................................................done: 368,056 bytes
install ok: channel://pear.php.net/Image_Graph-0.7.2
root@dian-laptop:/var/www/base# pear install --alldeps mail
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
WARNING: "pear/Auth_SASL" is deprecated in favor of "pear/Auth_SASL2"
downloading Mail-1.2.0.tgz ...
Starting to download Mail-1.2.0.tgz (23,214 bytes)
........done: 23,214 bytes
downloading Net_SMTP-1.6.2.tgz ...
Starting to download Net_SMTP-1.6.2.tgz (13,077 bytes)
...done: 13,077 bytes
downloading Net_Socket-1.0.14.tgz ...
Starting to download Net_Socket-1.0.14.tgz (5,600 bytes)
...done: 5,600 bytes
downloading Auth_SASL-1.0.6.tgz ...
Starting to download Auth_SASL-1.0.6.tgz (9,119 bytes)
...done: 9,119 bytes
install ok: channel://pear.php.net/Mail-1.2.0
install ok: channel://pear.php.net/Net_Socket-1.0.14
install ok: channel://pear.php.net/Auth_SASL-1.0.6
install ok: channel://pear.php.net/Net_SMTP-1.6.2
root@dian-laptop:/var/www/base# pear install Mail
pear/Mail is already installed and is the same as the released version 1.2.0
install failed
root@dian-laptop:/var/www/base# pear upgrade PEAR
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
WARNING: "pear/Console_Getopt" is deprecated in favor of "pear/Console_GetoptPlus"
downloading PEAR-1.9.5.tgz ...
Starting to download PEAR-1.9.5.tgz (290,006 bytes)
```

Gambar 5.41 installasi paket *alldeps_Mail* php

h) *Pear install Mail_Mime*

```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
.......................................done: 290,006 bytes
downloading Archive_Tar-1.3.12.tgz ...
Starting to download Archive_Tar-1.3.12.tgz (19,863 bytes)
...done: 19,863 bytes
downloading Structures_Graph-1.0.4.tgz ...
Starting to download Structures_Graph-1.0.4.tgz (30,318 bytes)
...done: 30,318 bytes
downloading Console_Getopt-1.3.1.tgz ...
Starting to download Console_Getopt-1.3.1.tgz (4,471 bytes)
...done: 4,471 bytes
downloading XML_Util-1.2.3.tgz ...
Starting to download XML_Util-1.2.3.tgz (17,134 bytes)
...done: 17,134 bytes
upgrade ok: channel://pear.php.net/Archive_Tar-1.3.12
upgrade ok: channel://pear.php.net/Structures_Graph-1.0.4
upgrade ok: channel://pear.php.net/Console_Getopt-1.3.1
upgrade ok: channel://pear.php.net/XML_Util-1.2.3
upgrade ok: channel://pear.php.net/PEAR-1.9.5
PEAR: Optional feature webinstaller available (PEAR's web-based installer)
PEAR: Optional feature gtkinstaller available (PEAR's PHP-GTK-based installer)
PEAR: Optional feature gtk2installer available (PEAR's PHP-GTK2-based installer)
PEAR: To install optional features use "pear install pear/PEAR#featurename"
root@dian-laptop:/var/www/base# pear install Mail_Mime
WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to update
downloading Mail_Mime-1.8.9.tgz ...
Starting to download Mail_Mime-1.8.9.tgz (33,796 bytes)
.........done: 33,796 bytes
install ok: channel://pear.php.net/Mail_Mime-1.8.9
root@dian-laptop:/var/www/base# root@dian-laptop:/var/www/base# pear install Numbers_Roman-1.0.2
bash: root@dian-laptop:/var/www/base#: No such file or directory
root@dian-laptop:/var/www/base# WARNING: channel "pear.php.net" has updated its protocols, use "pear channel-update pear.php.net" to
 update
WARNING:: command not found
root@dian-laptop:/var/www/base# downloading Numbers_Roman-1.0.2.tgz ...
downloading: command not found
```

Gambar 5.42 installasi paket *Mail_Mime* php

i) Installasi BASE 1.4.5

Copy folder Base-1.4.5.tar.gz ke direktori */var/www*

#cp base-1.4.5.tar.gz /var/www/

Masuk ke direktori */var/www*

#cd /var/www

Compile folder base

#tar zxvf base-1.4.5.tar.gz

Mengganti folder base

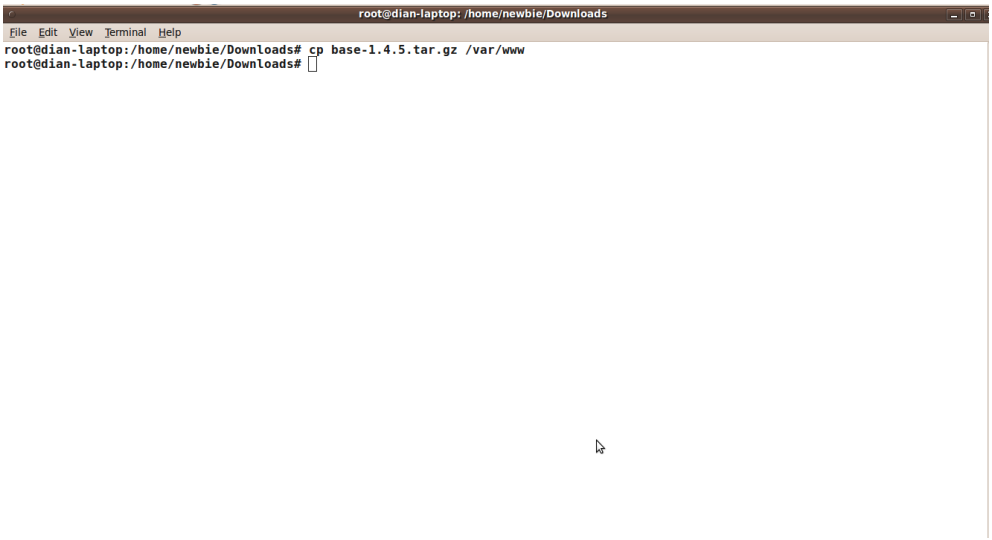
#mv base-1.4.5 base

Masuk ke folder hasil compile base

#cd /var/www/base

Mengcopy file *base_conf.php.dist* menjadi *base_conf.php*

#cp base_conf.php.dist base_conf.php



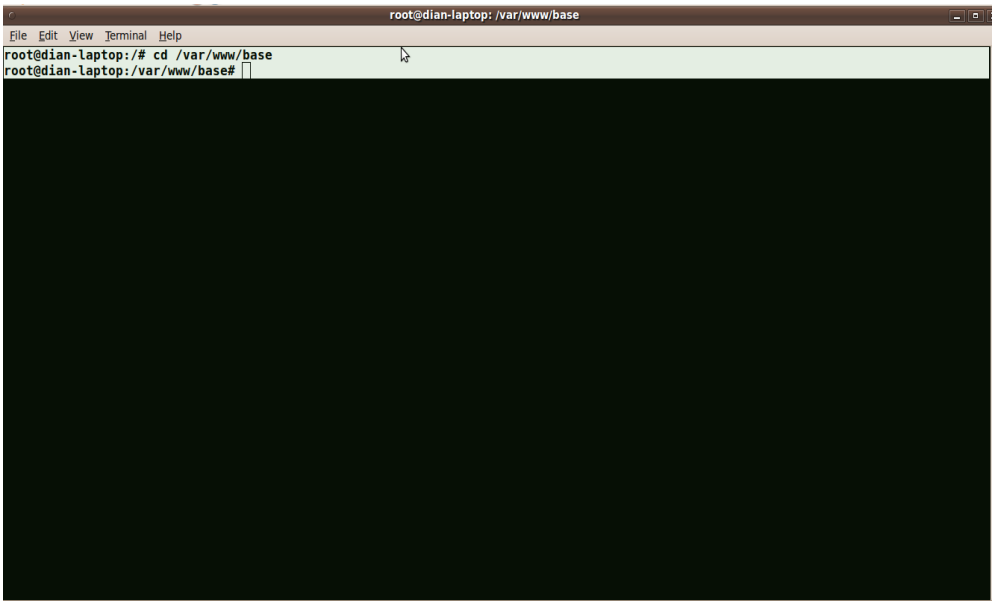
Gambar 5.43 mengcopy folder base ke direktori lain

```
root@dian-laptop: /var/www
File  Edit  View  Terminal  Help
root@dian-laptop:/home/newbie/Downloads# cp base-1.4.5.tar.gz /var/www
root@dian-laptop:/home/newbie/Downloads# cd /var/www
root@dian-laptop:/var/www# tar zxvf base-1.4.5.tar.gz
base-1.4.5/
base-1.4.5/admin/
base-1.4.5/admin/base_roleadmin.php
base-1.4.5/admin/base_useradmin.php
base-1.4.5/admin/index.php
base-1.4.5/base_ag_common.php
base-1.4.5/base_ag_main.php
base-1.4.5/base_common.php
base-1.4.5/base_conf.php.dist
base-1.4.5/base_db_common.php
base-1.4.5/base_db_setup.php
base-1.4.5/base_denied.php
base-1.4.5/base_footer.php
base-1.4.5/base_graph_common.php
base-1.4.5/base_graph_display.php
base-1.4.5/base_graph_form.php
base-1.4.5/base_graph_main.php
base-1.4.5/base_hdr1.php
base-1.4.5/base_hdr2.php
base-1.4.5/base_local_rules.php
base-1.4.5/base_logout.php
base-1.4.5/base_mac_prefixes.map
base-1.4.5/base_main.php
base-1.4.5/base_maintenance.php
base-1.4.5/base_payload.php
base-1.4.5/base_qry_alert.php
base-1.4.5/base_qry_common.php
base-1.4.5/base_qry_form.php
base-1.4.5/base_qry_main.php
base-1.4.5/base_qry_sqlcalls.php
base-1.4.5/base_stat_alerts.php
base-1.4.5/base_stat_class.php
```

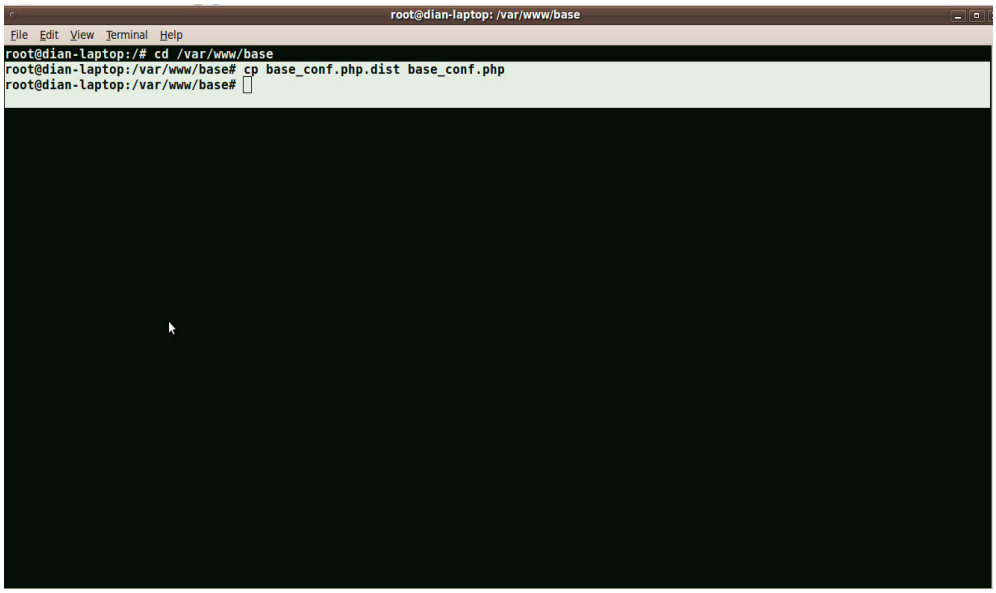
Gambar 5.44 proses compile file base

```
root@dian-laptop: /var/www
File  Edit  View  Terminal  Help
base-1.4.5/languages/turkish.lang.php
base-1.4.5/rpm/
base-1.4.5/rpm/base.spec
base-1.4.5/rpm/base_maintenance.pl.patch
base-1.4.5/scripts/
base-1.4.5/scripts/base_maintenance.pl
base-1.4.5/setup/
base-1.4.5/setup/base_conf_contents.php
base-1.4.5/setup/index.php
base-1.4.5/setup/setup1.php
base-1.4.5/setup/setup2.php
base-1.4.5/setup/setup3.php
base-1.4.5/setup/setup4.php
base-1.4.5/setup/setup5.php
base-1.4.5/setup/setup_db.inc.php
base-1.4.5/sql/
base-1.4.5/sql/acid2base_tbls_mssql.sql
base-1.4.5/sql/acid2base_tbls_mysql.sql
base-1.4.5/sql/acid2base_tbls_pgsql.sql
base-1.4.5/sql/create_base_tbls_mssql.sql
base-1.4.5/sql/create_base_tbls_mssql_extra.sql
base-1.4.5/sql/create_base_tbls_mysql.sql
base-1.4.5/sql/create_base_tbls_oracle.sql
base-1.4.5/sql/create_base_tbls_pgsql.sql
base-1.4.5/sql/create_base_tbls_pgsql_extra.sql
base-1.4.5/sql/upgrade_0.9.x_to_1.0-mysql.sql
base-1.4.5/styles/
base-1.4.5/styles/acid_style.css
base-1.4.5/styles/base_black_style.css
base-1.4.5/styles/base_red_style.css
base-1.4.5/styles/base_style.css
base-1.4.5/world_map6.png
base-1.4.5/world_map6.txt
root@dian-laptop:/var/www# mv base-1.4.5 base
root@dian-laptop:/var/www#
```

Gambar 5.45 mengganti folder base



Gambar 5.46 masuk ke direktori base



Gambar 5.47 copy file base_conf.php.dist

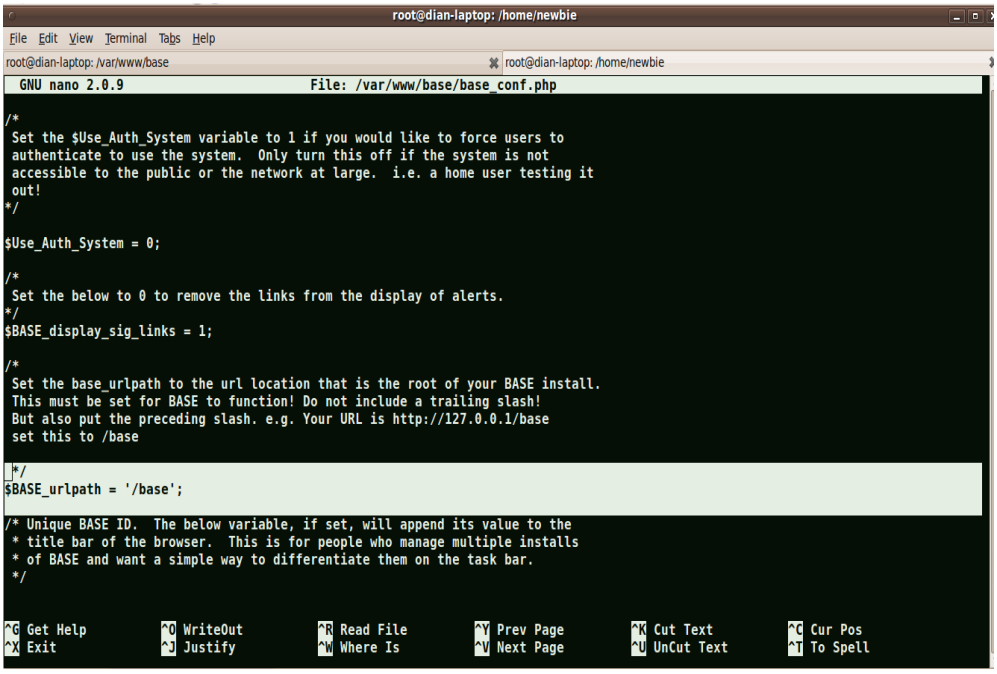
j) **Edit Konfigurasi *Base***

#Vi base_conf.php

isi dengan

$BASE_urlpath = "/base";

$DBlib_path = "/usr/share/php/adodb/";
$DBlib_path = "/var/adodb/"; - gunakan ini untuk instalasi adodb manual
$DBtype = "mysql";
$alert_dbname = 'snort';
$alert_host = 'localhost';
$alert_port = ;
$alert_user = 'snort';
$alert_password = 'snort';
$archive_exists = 0;
$archive_dbname = 'snort';
$archive_host = 'localhost';
$archive_port = ;
$archive_user = 'snort';
$archive_password = 'snort';



Gambar 5.48 edit konfigurasi lokasi

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /var/www/base        root@dian-laptop: /home/newbie
  GNU nano 2.0.9                File: /var/www/base/base_conf.php

$base_custom_footer = '';

/* Path to the DB abstraction library
 *  (Note: DO NOT include a trailing backslash after the directory)
 *   e.g. $foo = '/tmp'      [OK]
 *        $foo = '/tmp/'     [OK]
 *        $foo = 'c:\tmp'    [OK]
 *        $foo = 'c:\tmp\'   [WRONG]
 */
$DBlib_path = '/var/www/adodb';


/* The type of underlying alert database
 *
 *  MySQL       : 'mysql'
 *  PostgresSQL : 'postgres'
 *  MS SQL Server : 'mssql'
 *  Oracle      : 'oci8'
 */
$DBtype = 'mysql';

/* Alert DB connection parameters
 *   - $alert_dbname   : MySQL database name of Snort alert DB
 *   - $alert_host     : host on which the DB is stored
 *   - $alert_port     : port on which to access the DB
 *   - $alert_user     : login to the database with this user
 *   - $alert_password : password of the DB user
 *

^G Get Help   ^O WriteOut   ^R Read File   ^Y Prev Page   ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is    ^V Next Page   ^U UnCut Text ^T To Spell
```

Gambar 5.49 edit lokasi path database

```
root@dian-laptop: /home/newbie
File  Edit  View  Terminal  Tabs  Help
root@dian-laptop: /var/www/base        root@dian-laptop: /home/newbie
  GNU nano 2.0.9                File: /var/www/base/base_conf.php

 *  This information can be gleaned from the Snort database
 *  output plugin configuration.
 */
$alert_dbname   = 'snort';
$alert_host     = 'localhost';
$alert_port     = '';
$alert_user     = 'snort';
$alert_password = 'snort';

/* Archive DB connection parameters */
$archive_exists   = 0;
$archive_dbname   = 'snort';
$archive_host     = 'localhost';
$archive_port     = '';
$archive_user     = 'snort';
$archive_password = 'snort';

/* Type of DB connection to uses
 *   1  : use a persistant connection (pconnect)
 *   2  : use a normal connection (connect)
 */
$db_connect_method = 1;

/* Use referential integrity
 *   1  : use
 *   0  : ignore (not installed)
 *
 * Note: Only PostgreSQL and MS-SQL Server databases support

^G Get Help   ^O WriteOut   ^R Read File   ^Y Prev Page   ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is    ^V Next Page   ^U UnCut Text ^T To Spell
```

Gambar 5.50 edit konfigurasi database

Beri ijin Apache Web Server mengakses folder BASE

 # chown -Rf www-data.www-data /var/www/base

```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
root@dian-laptop:/var/www/base# gedit base_conf.php
root@dian-laptop:/var/www/base# chown -Rf www-data.www-data /var/www/base
root@dian-laptop:/var/www/base#
```

Gambar 5.51 perintah apache web server untuk mengakses BASE

Sesuai kan pada file konfigurasi snort mysql untuk nama *database, host, user,* dan password yang ada pada *file snort.conf*

k) Kemudian *restart apache* dan *snort*

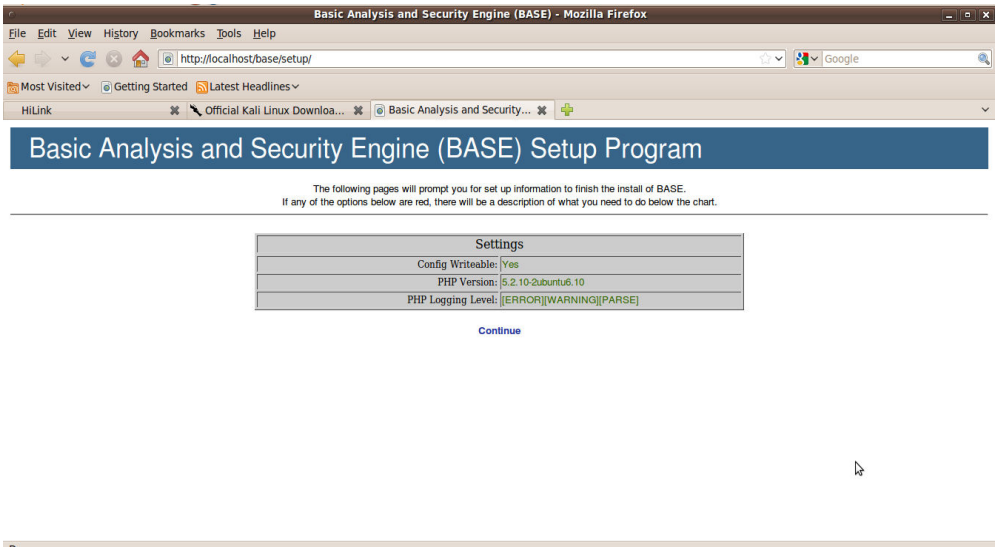
 # /etc/init.d/apache2 restart

 # /etc/init.d/snort restart

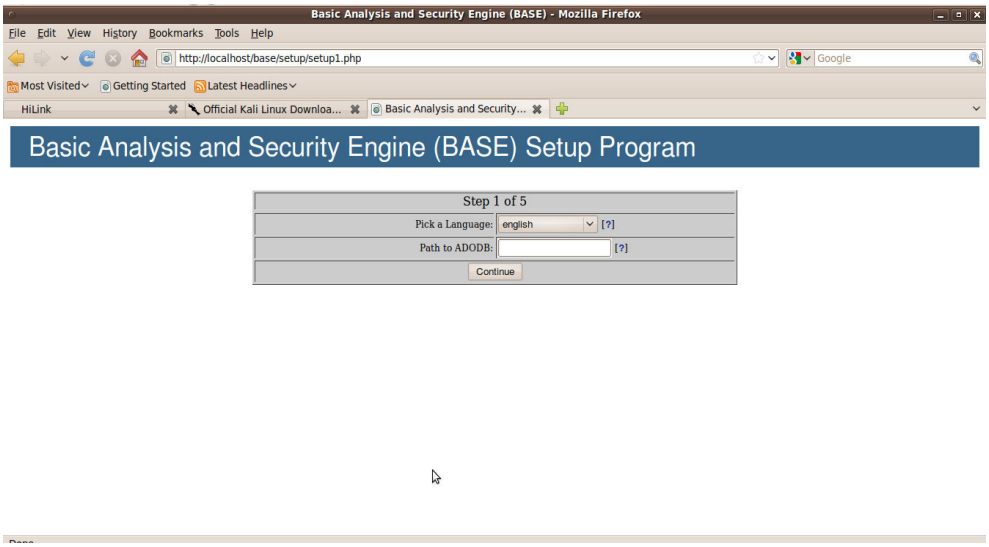
```
root@dian-laptop: /var/www/base
File  Edit  View  Terminal  Help
root@dian-laptop:/var/www/base# /etc/init.d/apache2 restart
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
                                                                                                                    [ OK ]
root@dian-laptop:/var/www/base# /etc/init.d/mysql restart
 * Stopping MySQL database server mysqld                                                                            [ OK ]
 * Starting MySQL database server mysqld                                                                            [ OK ]
 * Checking for corrupt, not cleanly closed and upgrade needing tables.
root@dian-laptop:/var/www/base#
```

Gambar 5.52 *restart apache dan mysql*

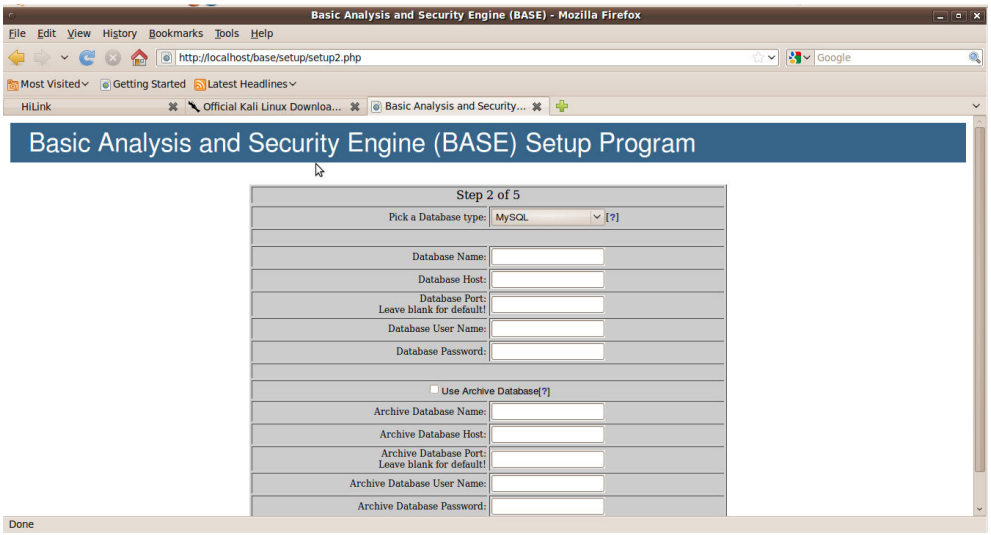
l) akses ke *http://localhost/acidbase*



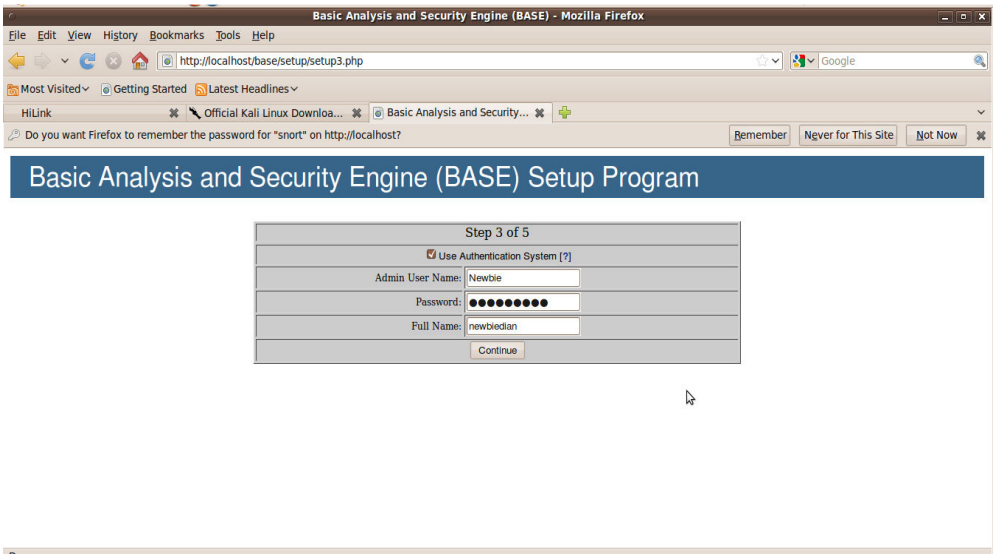
Gambar 5.53 tampilan browser base setup 1



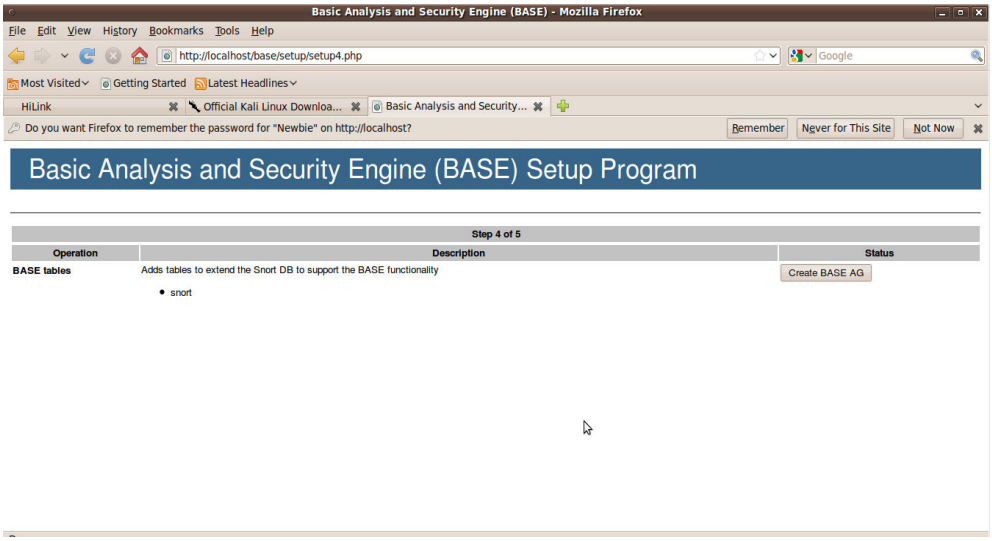
Gambar 5.54 tampilan browser base setup 2



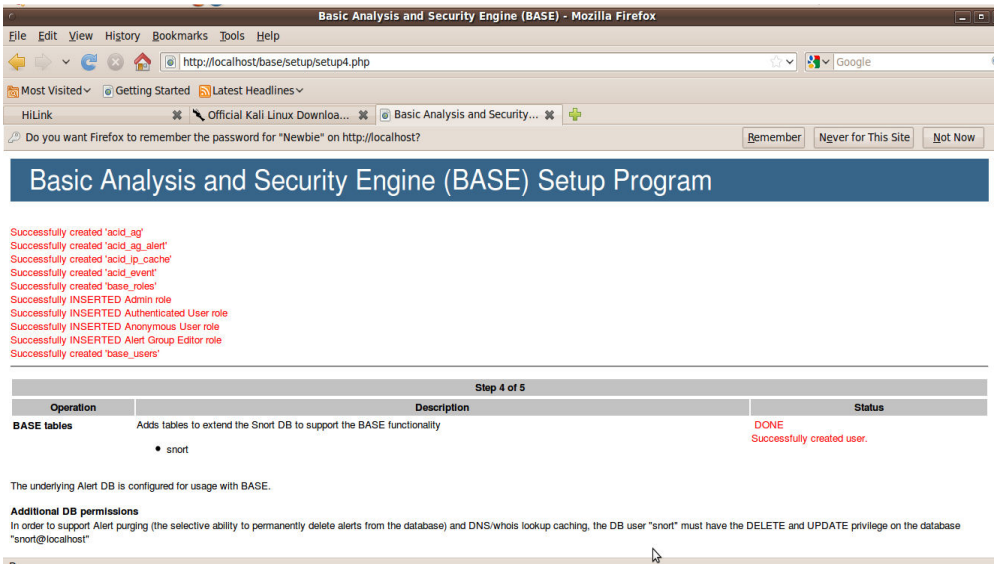
Gambar 5.55 tampilan browser base setup 3



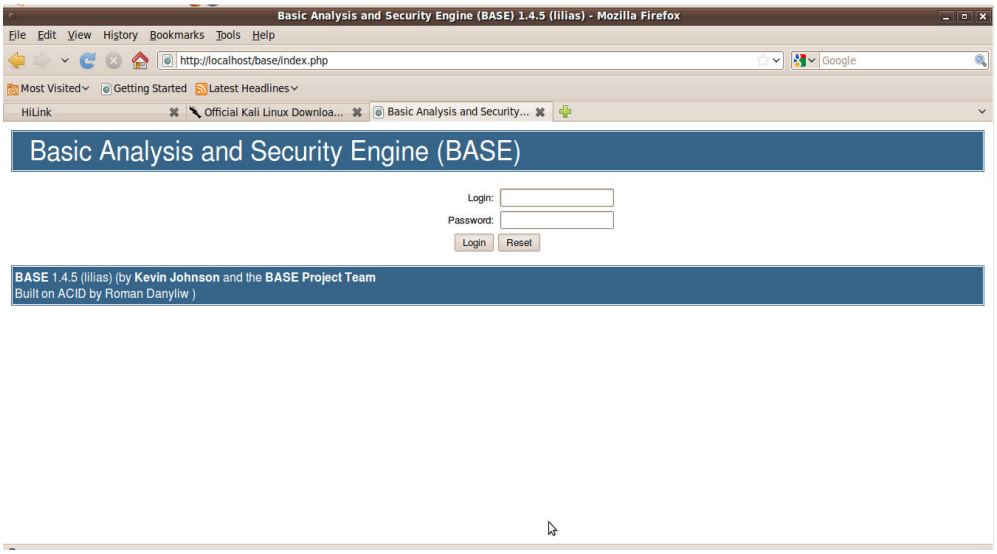
Gambar 5.56 tampilan browser base setup 4



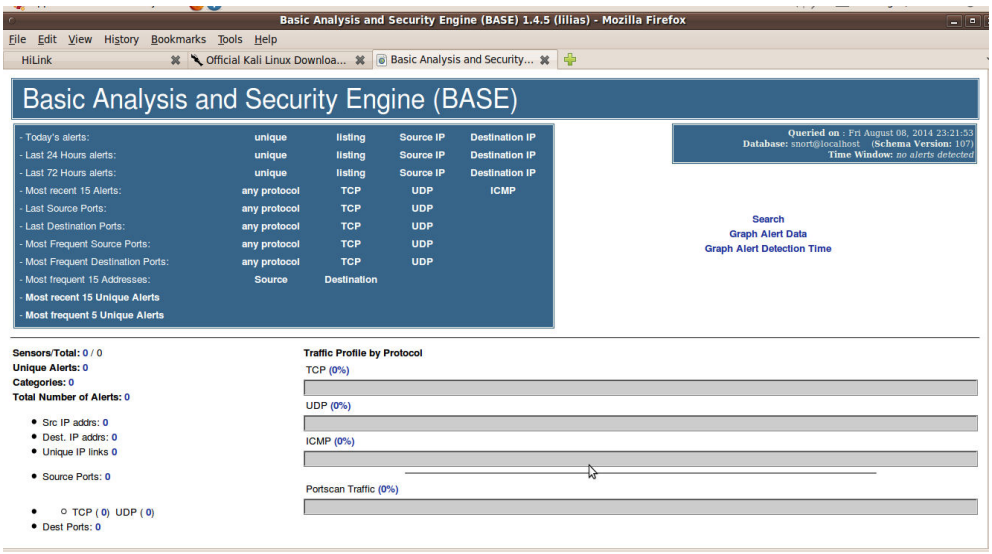
Gambar 5.57 tampilan browser base setup 5



Gambar 5.58 tampilan browser base setup 6



Gambar 5.59 tampilan login browser base



Gambar 5.60 tampilan muka browser base

Pengujian BASE yang dilakukan penulis adalah dengan melakukan pada browser yaitu menggunakan *browser Mozilla firefox* dengan memasukkan alamat *URL* https://localhost/base, Pada beberapa bagian tampilan menu setup, diisi

sesuai dengan file konfigurasi yang terdapat di file konfigurasi base_conf.php pada folder BASE seperti gambar 5.55

5.4. Pengoperasian *Snort*

Secara umum *snort* dapat di operasikan dalam tiga (3) buah *mode*, yaitu

a. *Sniffer mode*, untuk melihat paket yang lewat di jaringan.
b. *Packet logger mode*, untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
c. *Intrusion Detection mode*, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan setup dari berbagai *rules* / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

5.4.1. *Sniffer Mode*

Dalam menjalankan snort pada *sniffer mode* terdapat, beberapa contoh perintah yang bisa digunakan,

a. *#snort –v*
b. *#snort –vd*
c. *#snort –vde*
d. *#snort –v –d –e*

dengan menambahkan beberapa *switch* –v, -d, -e akan menghasilkan beberapa keluaran yang berbeda, yaitu

a. -v, untuk melihat *header TCP/IP* paket yang lewat.
b. -d, untuk melihat isi paket.
c. -e, untuk melihat *header link* layer paket seperti *ethernet header.*

5.4.2. *Packet Logger Mode*

Untuk mencatat semua paket yang lewat di jaringan untuk dianalisa dikemudian hari.Tentunya cukup melelahkan untuk melihat paket yang lewat sedemikian cepat di layar terutama jikakita menggunakan *ethernet* berkecepatan

100Mbps, layar anda akan scrolling dengan cepat sekalisusah untuk melihat paket yang di inginkan. Cara paling sederhana untuk mengatasi hal ini adalahmenyimpan dulu semua paket yang lewat ke sebuah file untuk di lihat kemudian, sambil santai.Beberapa perintah yang mungkin dapat digunakan untuk mencatat paket yang ada adalah

a. *./snort –dev –l ./log*

b. *./snort –dev –l ./log –h 192.168.0.0/24*

c. *./snort –dev –l ./log –b*

perintah yang paling penting untuk me-log paket yang lewat adalah *-l ./log* yang menentukan bahwa paket yang lewat akan di log / di catat ke file ./log. Beberapa perintah tambahan dapat digunakan seperti –h 192.168.0.0/24 yang menunjukan bahwa yang di catat hanya packet dari host mana saja, dan –b yang memberitahukan agar file yang di log dalam format binary, bukan ASCII. untuk membaca file log dapat dilakukan dengan menjalankan snort dengan di tambahkan perintah –r nama file log-nya, seperti,

./snort –dv –r packet.log

./snort –dvr packet.log icmp

5.4.3. *Intrusion Detection Mode*

Pada mode ini snort akan berfungsi untuk mendeteksi serangan yangdilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini diperlukan setup dariberbagai rules / aturan yang akan membedakan sebuah paket normal dengan paket yangmembawa serangan. Mode operasi snort yang paling rumit adalah sebagai pendeteksi penyusup (intrusion detection) dijaringan yang kita gunakan. Ciri khas mode operasi untuk pendeteksi penyusup adalah dengan menambahkan perintah ke snort untuk membaca file konfigurasi –c nama-file-konfigurasi.conf. Isi file konfigurasi ini lumayan banyak, tapi sebagian besar telah di set secara baik dalam contoh snort.conf yang dibawa oleh source snort. Beberapa contoh perintah untuk mengaktifkan snort untuk melakukan pendeteksian penyusup,seperti *:./snort –dev –l ./log –h 192.168.0.0/24 –c snort.conf*

./snort –d –h 192.168.0.0/24 –l ./log –c snort.conf

Untuk melakukan deteksi penyusup secara prinsip snort harus melakukan logging paket yang lewat dapat menggunakan perintah –l nama-file-logging, atau membiarkan snort menggunakan default file logging-nya di *directory /var/log/snort*. Kemudian menganalisa catatan / logging paket yang ada sesuai dengan isi perintah snort.conf. Ada beberapa tambahan perintah yang akan membuat proses deteksi menjadi lebih effisien, mekanisme pemberitahuan *alert* di Linux dapat di set dengan perintah –A sebagai berikut :

a. -A *fast, mode alert* yang cepat berisi waktu, berita, IP & port tujuan.
b. -A *full, mode alert* dengan informasi lengkap.
c. -A unsock, mode alert ke unix socket
d. -A none, mematikan mode alert.

Untuk mengirimkan alert ke *syslog* UNIX kita bisa menambahkan switch –s, seperti tampak pada beberapa contoh di bawah ini :

./snort –c snort.conf –l ./log –s –h 192.168.0.0/24

./snort –c snort.conf –s –h 192.168.0.0/24

Untuk mengirimkan *alert binary ke workstation windows*, dapat digunakan perintah di bawah ini :

./snort –c snort.conf –b –M WORKSTATIONS

Agar snort beroperasi secara langsung setiap kali workstation / server di boot, kita dapat menambahkan ke file */etc/rc.d/rc.local* perintah di bawah ini */usr/local/bin/snort –d –h 192.168.0.0/24 –c /root/snort/snort.conf –A full –s –D* atau */usr/local/bin/snort –d –c /root/snort/snort.conf –A full –s –D* dimana –D adalah switch yang menset agar snort bekerja sebagai *Daemon* (bekerja dibelakang layar) .

5.5. Monitoring

Dalam skripsi ini tahap *monitoring* digunakan untuk proses pengetesan dari sistem IDS (*Intrusion Detection System*) yang telah dibuat. Dimulai dari melakukan pengetesan koneksi antar perangkat yang saling terhubung, pengujicobaan terhadap aplikasi yang digunakan hingga melakukan proses

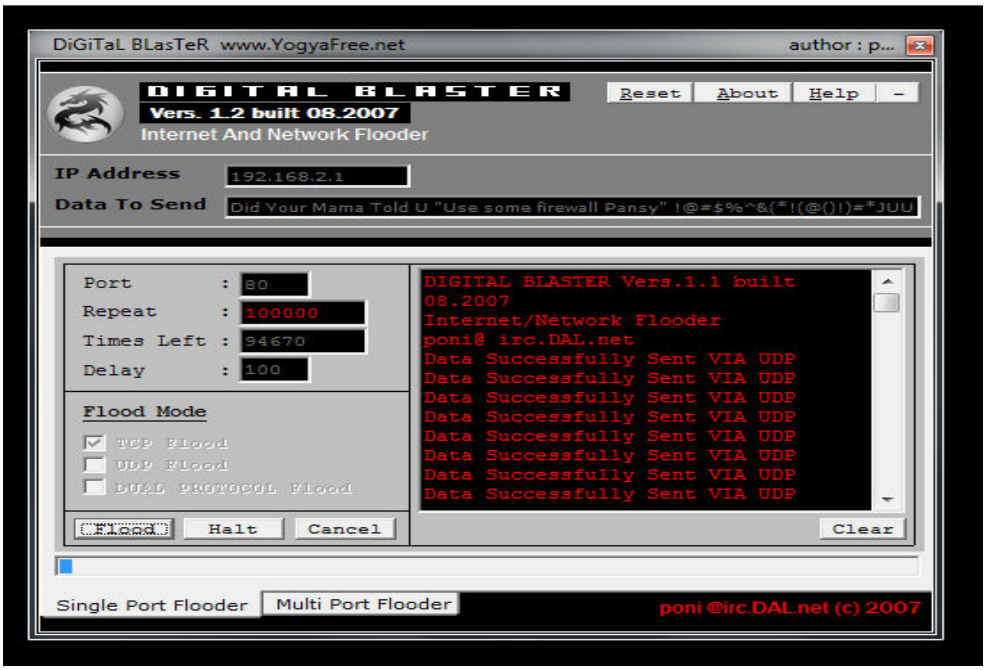
penyadapan data yang berada di jaringan yang ada. Berikut adalah deskripsi proses pengujiannya :

5.5.1. Pengujian Sistem IDS

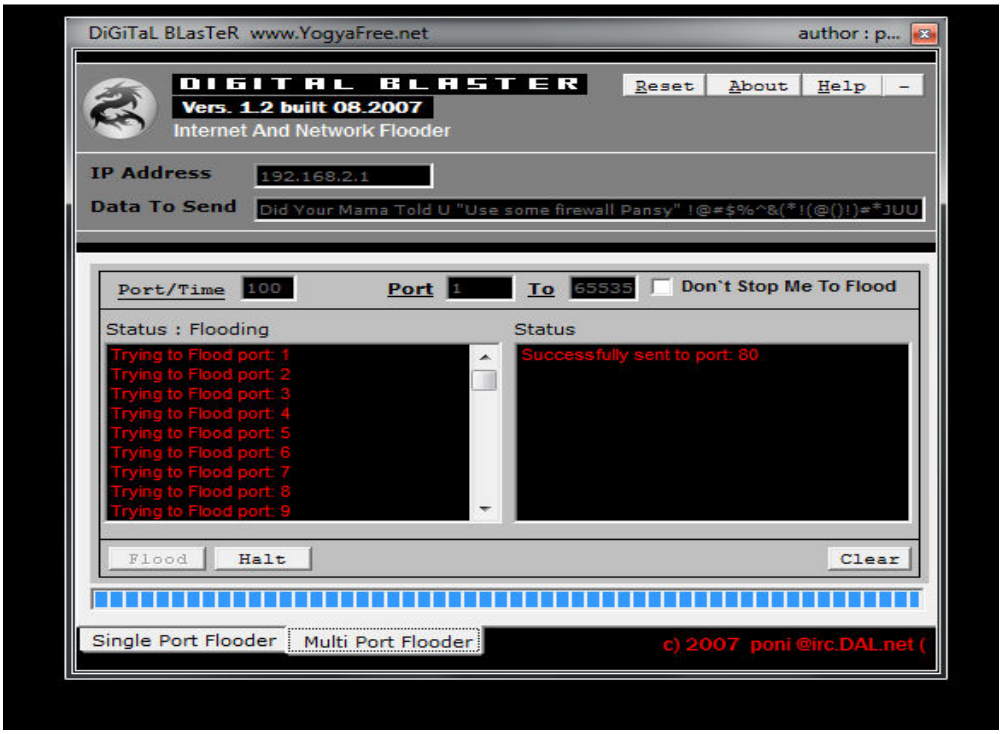
Pada pembahasan ini, penulis menggunakan beberapa aplikasi yang digunakan untuk melakukan penyerangan terhadap jaringan yang ada. Hal ini ditujukan untuk mengetahui jenis serangan apa saja yang sering dilakukan oleh para cracker serta serangan tersebut dilakukan melalui port mana saja yang sering digunakan. Jenis serangan yang akan penulis coba lakukan adalah berupa pembebanan *bandwith* , ICMP

5.5.2. Pengujian IDS Dengan *TCP Flooding*

Tahapan ini penulis mencoba melakukan penyerangan dari windows ke komputer *server linux* dengan metode penyerangan terhadap pembebanan jalur komunikasi TCP/IP atau biasa dikenal dengan teknik TCP *flooding*. Dengan mencoba melakukan serangan kedalam jaringan LAN dengan menggunakan aplikasi *Digital Blaster.*



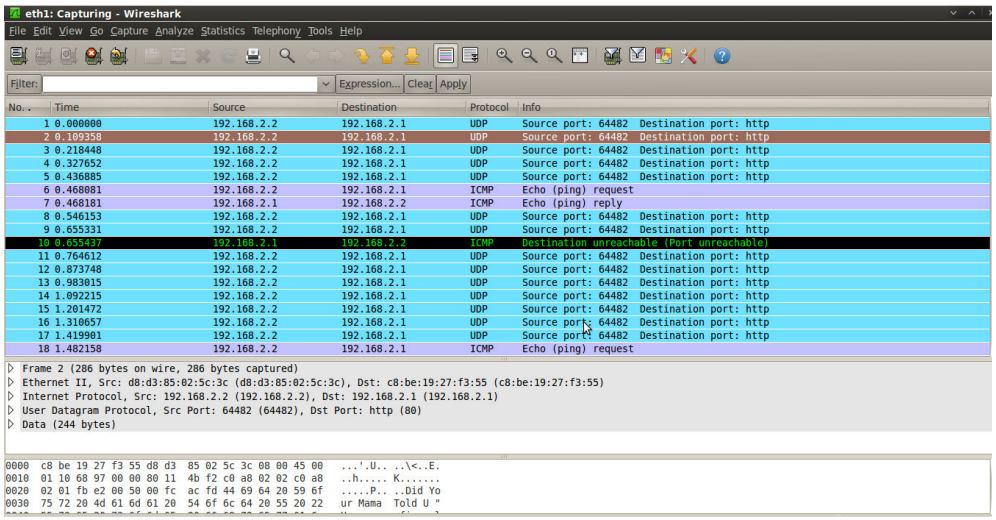
Gambar 5.61 proses TCP dan UDP *Flood* ke server linux



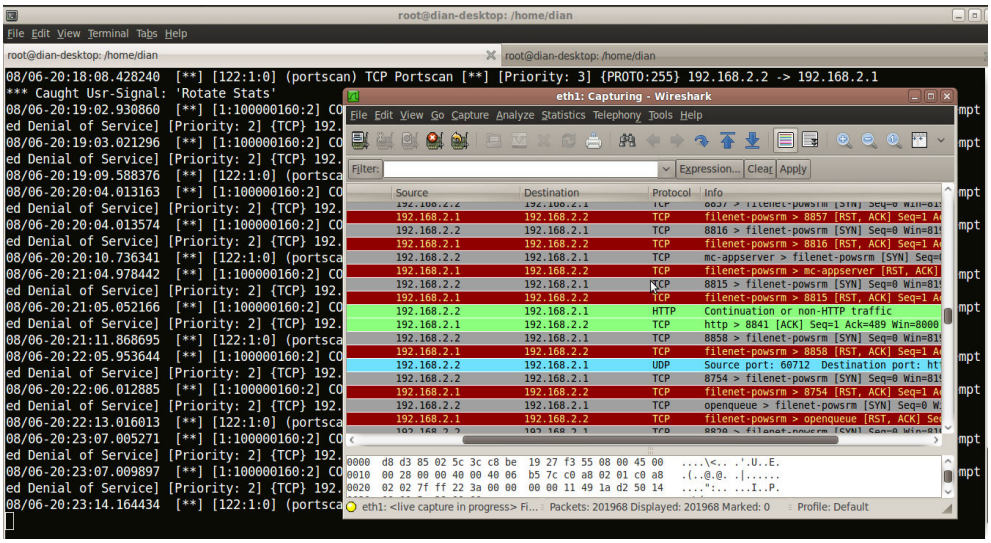
Gambar 5.62 proses *scanning* Port TCP dan UDP Flood ke server linux

DIGITAL BLASTER Vers.1.1 built 08.2007
Internet/Network Flooder
poni@ irc.DAL.net
Proceeding To Flood : 192.168.2.1 at port:80
Failed to Flood : 192.168.2.1 :80Host Is Not Active / Port Is Not Open
Connected to 192.168.2.1:80
Data Successfully Sent VIA UDP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Data Successfully Sent VIA UDP
Data Successfully Sent VIA UDP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Data Successfully Sent VIA UDP
Data Successfully Sent VIA UDP

Keterangan hasil gambar diatas bahwa proses pengiriman pembebanan bandwitch yang dilakukan dengan digital blaster menggunakan teknik flooding akan terus berjalan tanpa henti hanya dengan memasukan ip addres dari komputer target maka proses penyerangan pun akan berjalan sehingga. Hasil yang akan didapat dari proses penyerangan ini adalah proses kerja pada komputer target akan menjadi berat dan lama, terutama pada saat melakukan koneksi kedalam jaringan internet. Aktivitas ini akan didetaksi oleh aplikasi *sniffing monitoring* dan IDS yang terpasang pada jaringan komputer yang menjadi target.



Gambar 5.63 perekaman data hasil monitoring *Wireshark*



Gambar 5.64 hasil Deteksi Snort IDS dan *Wireshark*

```
root@dian-desktop: /home/dian
File Edit View Terminal Help

root@dian-desktop:/home/dian#  snort -i eth1 -q -c /etc/snort/snort.conf -A console
command line overrides rules file alert plugin!
08/06-20:08:07.694010  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.2:1036 -> 192.168.2.1:80
08/06-20:08:19.346500  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.1:80 -> 192.168.2.2:1039
08/06-20:08:43.468755  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 192.168.2.2 -> 192.168.2.1
08/06-20:08:45.041157  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168
.2.2:1206 -> 192.168.2.1:161
08/06-20:08:45.042726  [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.
2:1207 -> 192.168.2.1:162
08/06-20:08:45.552217  [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.
2:1207 -> 192.168.2.1:162
08/06-20:08:45.552239  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168
.2.2:1206 -> 192.168.2.1:161
08/06-20:08:46.066811  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168
.2.2:1206 -> 192.168.2.1:161
08/06-20:08:46.066919  [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.
2:1207 -> 192.168.2.1:162
08/06-20:08:51.911132  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.2.2:1756 -> 192.168.2.1:705
08/06-20:08:52.509132  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.2.2:1756 -> 192.168.2.1:705
08/06-20:08:53.008296  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.2.2:1756 -> 192.168.2.1:705
08/06-20:08:53.273550  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.2:1828 -> 192.168.2.1:776
08/06-20:08:53.273661  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
```

Gambar 5.65 hasil deteksi IDS *TCP Flooding*

Pada gambar di atas merupakan hasil perekaman data yang ditangkap dengan menggunakan aplikasi *wireshark* terhadap serangan TCP *flooding*. Terlihat dari serangan tersebut besarnya paket dan protokol apa yang digunakan. Pada gambar tersebut data yang tertangkap merupakan data yang melalui protokol UDP dan ICMP, jenis serangan yang digunakan adalah *Dual Protocol Flood*, jadi serangan menggunakan dua buah protokol sekaligus yaitu protokol UDP dan TCP. Dari proses *scanning* terlihat semua aktifitas yang telah terekam pada aplikasi wireshark, yaitu :

a. *source* : merupakan sumber dari paket data yang terkirim.
b. *destination* : merupakan tujuan dari paket data yang terkirim.
c. *protocol* : merupakan jalur aktifitas yang digunakan dalam proses penyerangan.
d. *info* : merupakan catatan apa saja yang terjadi pada aktifitas tersebut.

Pada gambar Terlihat bahwa serangan yang dilakukan oleh penyusup dapat terlihat dengan menggunakan aplikasi *wireshark*, yaitu serangan dengan menggunakan protokol UDP dan TCP yang memiliki *source port* 1133 dan *destination port* 80. *Port* 1133 yang termasuk kedalam jenis protokol TCP dan

UDP. Sedangkan *port* 80 merupakan protokol yang biasa digunakan pada jalur internet atau HTTP (*Hypertext Transfer Protocol*) yang termasuk kedalam protokol TCP. Dari serangan dengan menggunakan teknik ini dapat menyebabkan suatu jaringan komputer menjadi berat dalam melakukan koneksi antar komputer baik dalam jaringan internet atau jaringan lokal. Untuk tahapan ini sumber daya yang dapat diambil masih dalam katagori kecil, karena yang diserang hanya koneksi jaringannya saja dan tidak ada data atau *file* yang dicuri.

5.5.3. PING *Attack* (ICMP *Traffic*)

Pada kasus ini penulis menganalisis jenis serangan berprotokol ICMP. Pada dasarnya, *traffic* ICMP yang diproduksi oleh perintah ping, dianggap sebagai satu serangan karena dapat dipergunakan penyerang atau penyusup untuk mendapatkan informasi mengenai mesin target, memastikan apakah *host* target dalam keadaan aktif atau tidak. Yang pertama dilakukan penulis adalah melakukan ping dari *client* ataupun dari mesin penyerang kedalam computer server sekaligus mesin sensor IDS yang memiliki IP *address* 192.168.2.1 dengan mencoba mengirim paket sebesar 74000 sehingga server bisa merequest paket tersebut tanpa henti.

C:\Users\Dian Nugeraha>ping 192.168.2.1 -t74000

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

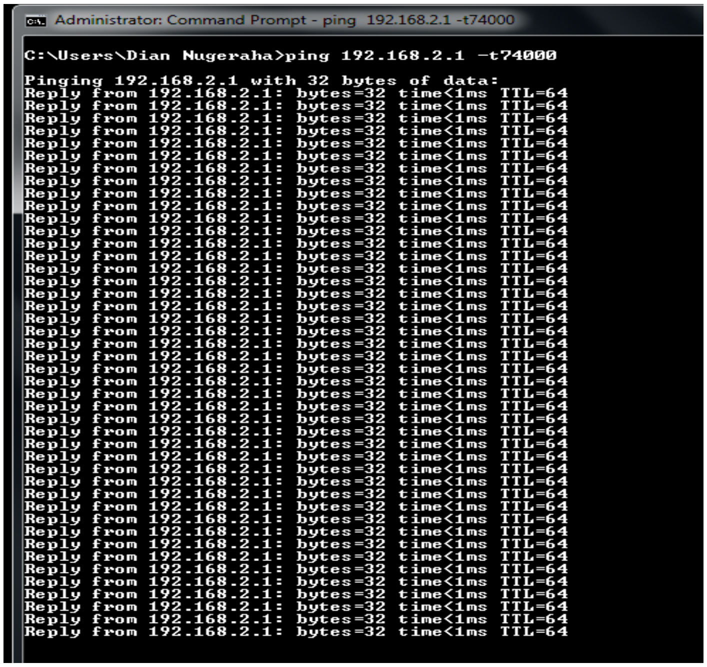
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

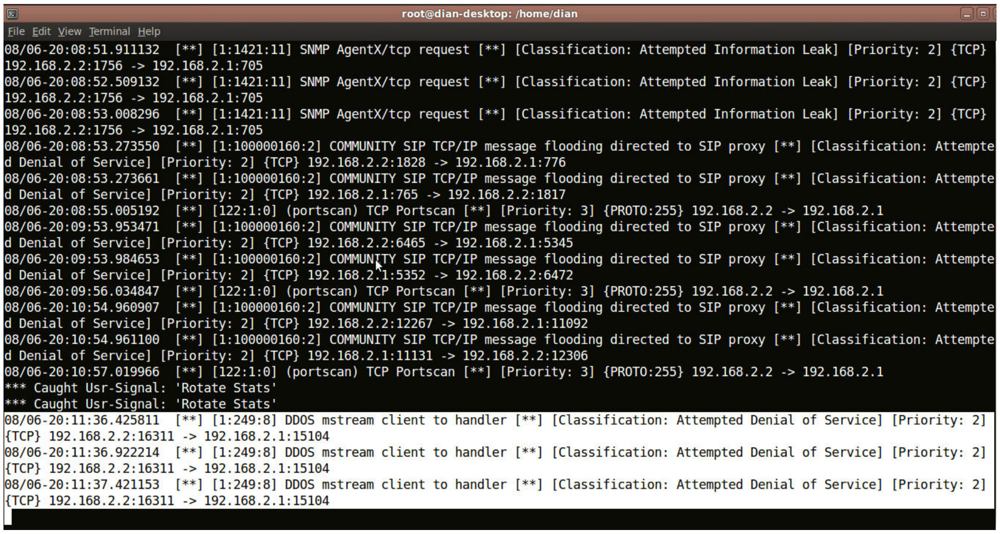
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Reply from 192.168.2.1: bytes=32 time<1ms TTL=64



```
C:\Users\Dian Nugeraha>ping 192.168.2.1 -t74000

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
```

Gambar 5.66 proses ping attack sebesar 74000

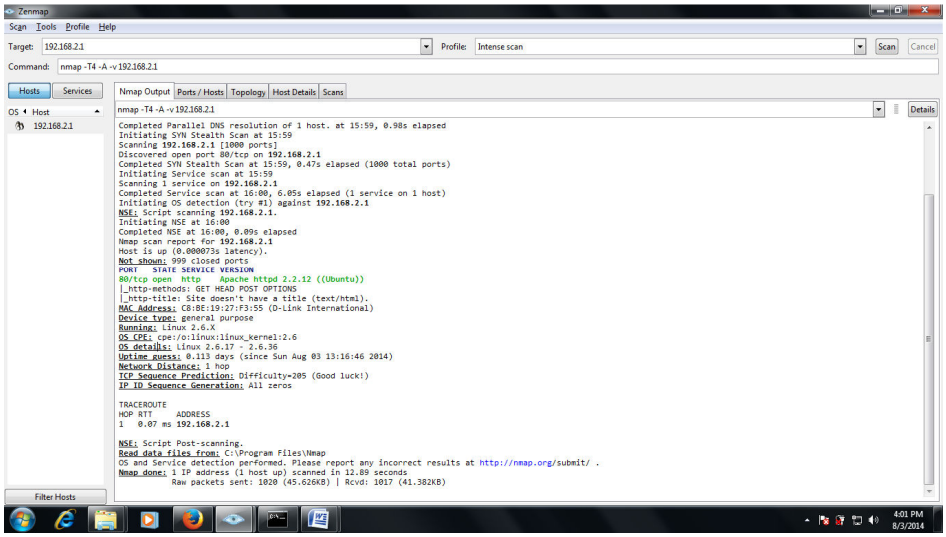


```
08/06-20:08:51.911132  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.2.2:1756 -> 192.168.2.1:705
08/06-20:08:52.509132  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.2.2:1756 -> 192.168.2.1:705
08/06-20:08:53.008296  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.2.2:1756 -> 192.168.2.1:705
08/06-20:08:53.273550  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.2:1828 -> 192.168.2.1:776
08/06-20:08:53.273661  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.1:765 -> 192.168.2.2:1817
08/06-20:08:55.005192  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 192.168.2.2 -> 192.168.2.1
08/06-20:09:53.953471  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.2:6465 -> 192.168.2.1:5345
08/06-20:09:53.984653  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.1:5352 -> 192.168.2.2:6472
08/06-20:09:56.034847  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 192.168.2.2 -> 192.168.2.1
08/06-20:10:54.960907  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.2:12267 -> 192.168.2.1:11092
08/06-20:10:54.961100  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempte
d Denial of Service] [Priority: 2] {TCP} 192.168.2.1:11131 -> 192.168.2.2:12306
08/06-20:10:57.019966  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 192.168.2.2 -> 192.168.2.1
*** Caught Usr-Signal: 'Rotate Stats'
*** Caught Usr-Signal: 'Rotate Stats'
08/06-20:11:36.425811  [**] [1:249:8] DDOS mstream client to handler [**] [Classification: Attempted Denial of Service] [Priority: 2]
{TCP} 192.168.2.2:16311 -> 192.168.2.1:15104
08/06-20:11:36.922214  [**] [1:249:8] DDOS mstream client to handler [**] [Classification: Attempted Denial of Service] [Priority: 2]
{TCP} 192.168.2.2:16311 -> 192.168.2.1:15104
08/06-20:11:37.421153  [**] [1:249:8] DDOS mstream client to handler [**] [Classification: Attempted Denial of Service] [Priority: 2]
{TCP} 192.168.2.2:16311 -> 192.168.2.1:15104
```

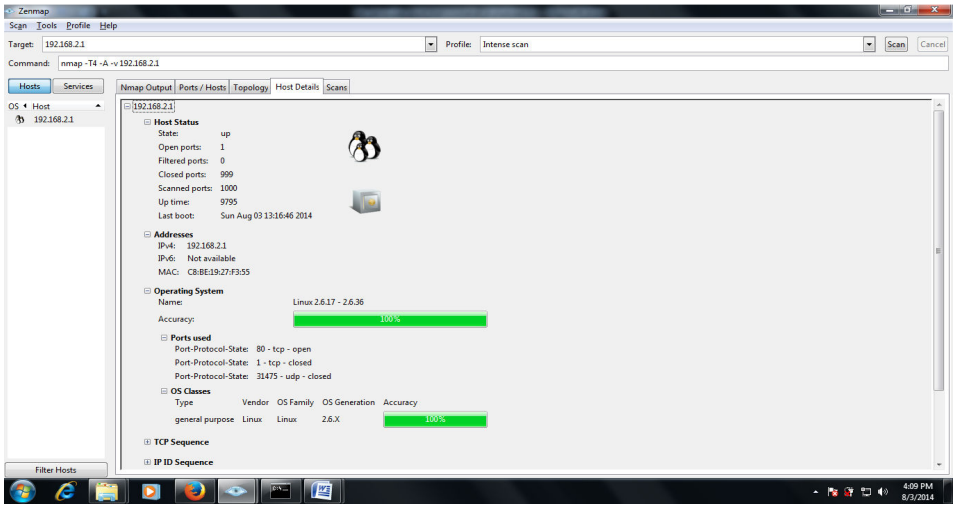
Gambar 5.67 hasil deteksi snort IDS Ping Attack

5.5.4. Nmap *Port Scanning Attack*

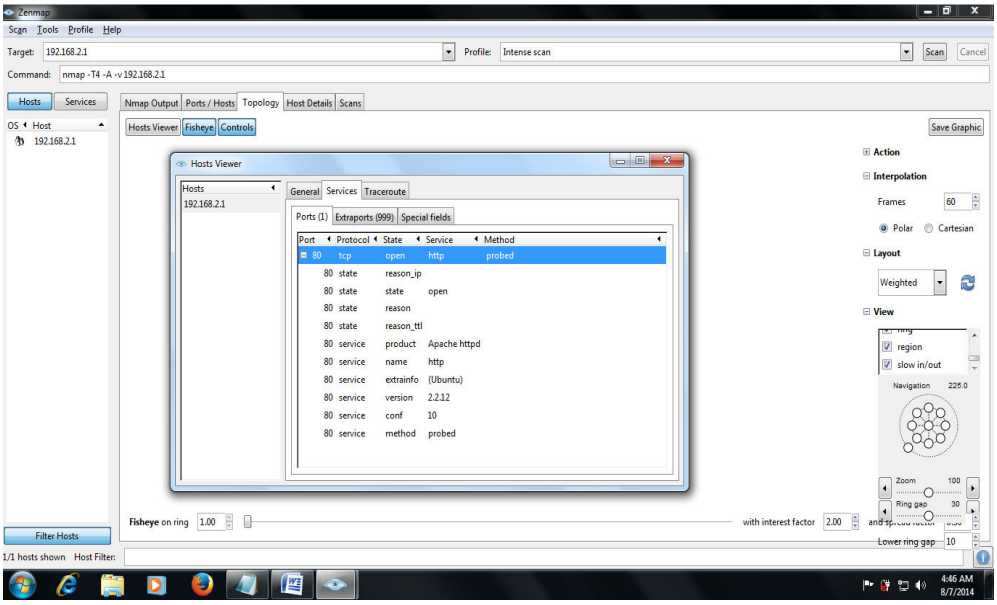
Pada kasus ini, penulis akan mencoba melakukan *Scanning Port* ke komputer server dengan menggunakan Nmap yang bertujuan mencari port2 apa saja yang terbuka atau yang sedang di jalankan oleh server.



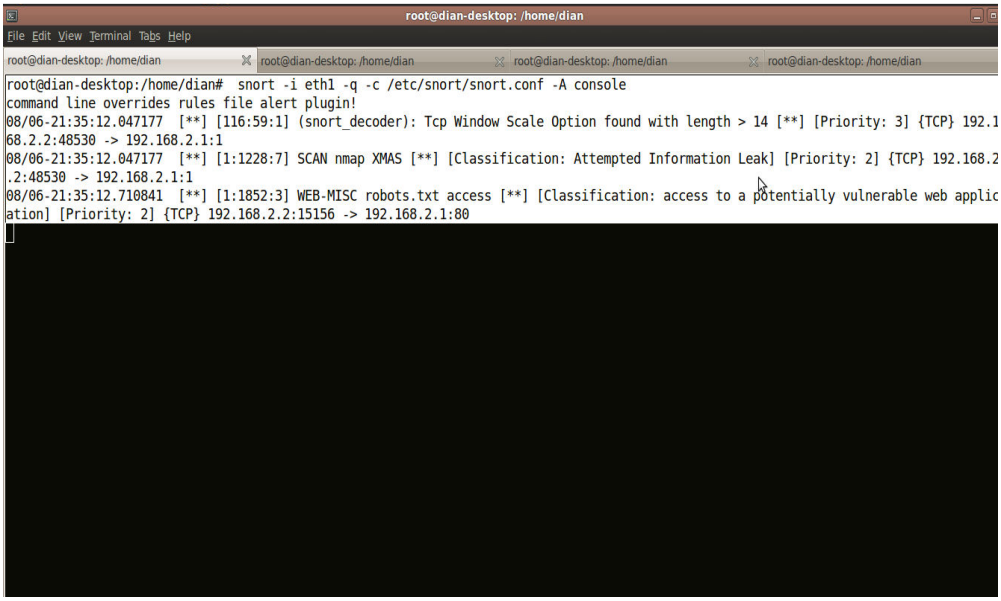
Gambar 5.68 proses scanning nmap ke server



Gambar 5.69 Hasil info deteksi nmap ke server



Gambar 5.70 Hasil info deteksi port yang terbuka



Gambar 5.71 hasil deteksi Nmap

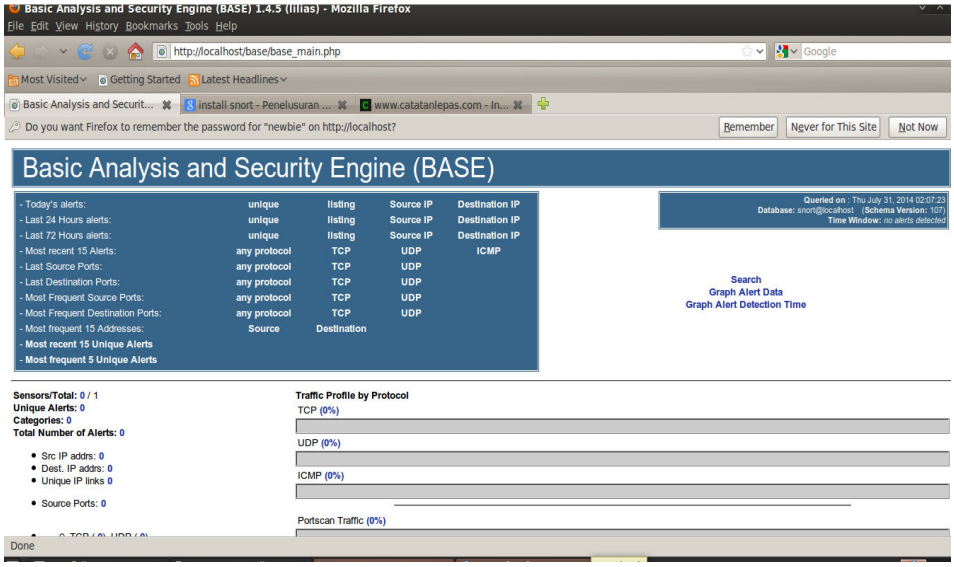
```
root@dian-desktop: /home/dian
File Edit View Terminal Tabs Help
root@dian-desktop: /home/dian   root@dian-desktop: /home/dian   root@dian-desktop: /home/dian   root@dian-desktop: /home/dian
root@dian-desktop:/home/dian#  snort -i eth1 -q -c /etc/snort/snort.conf -A console
command line overrides rules file alert plugin!
08/06-21:35:12.047177  [**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**] [Priority: 3] {TCP} 192.1
68.2.2:48530 -> 192.168.2.1:1
08/06-21:35:12.047177  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2
.2:48530 -> 192.168.2.1:1
08/06-21:35:12.710841  [**] [1:1852:3] WEB-MISC robots.txt access [**] [Classification: access to a potentially vulnerable web applic
ation] [Priority: 2] {TCP} 192.168.2.2:15156 -> 192.168.2.1:80
08/06-21:42:06.317165  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 192.168.2.2 -> 192.168.2.1
08/06-21:42:06.453415  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempt
ed Denial of Service] [Priority: 2] {TCP} 192.168.2.2:41237 -> 192.168.2.1:1658
08/06-21:42:06.453928  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempt
ed Denial of Service] [Priority: 2] {TCP} 192.168.2.1:5357 -> 192.168.2.2:41237
08/06-21:42:06.533658  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.16
8.2.2:41237 -> 192.168.2.1:161
08/06-21:42:06.611346  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
 192.168.2.2:41237 -> 192.168.2.1:705
```

Gambar 5.72 hasil deteksi IDS Scanning Port Nmap

Pada gambar diatas menunjukan proses *Scanning* yang di lakukan Nmap adalah mencari suatu informasi yang berhubungan dengan target seperti port yang terbuka dan informasi OS yang digunakan serta service apa saja yang dijalankan di server. Dan terlihat proses aktivitas yang dilakukan oleh Nmap terdeteksi oleh snort IDS pada Komputer server.

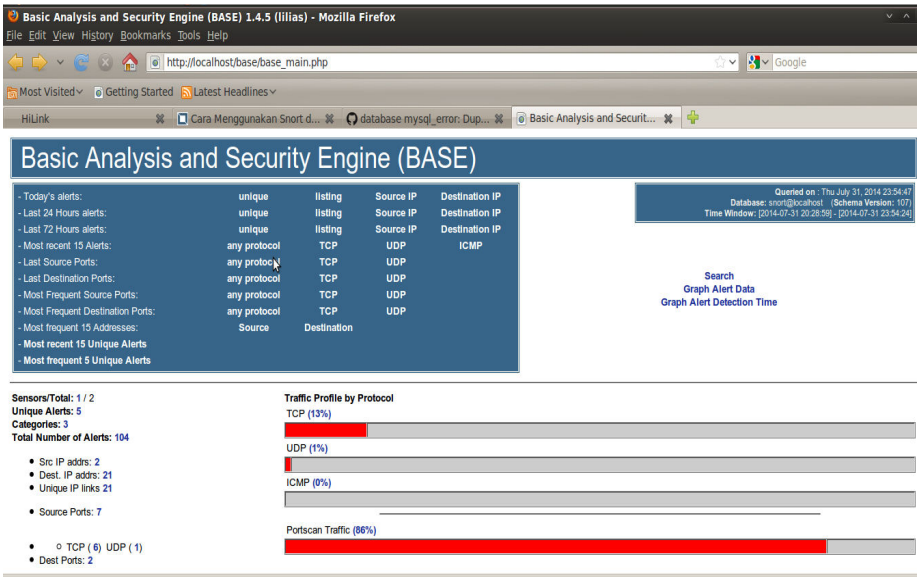
5.6. Analisis Data Menggunakan BASE

Pada sub-bab ini penulis akan mendeskripsikan proses analisis data kejadian melalui fungsionalitas BASE.



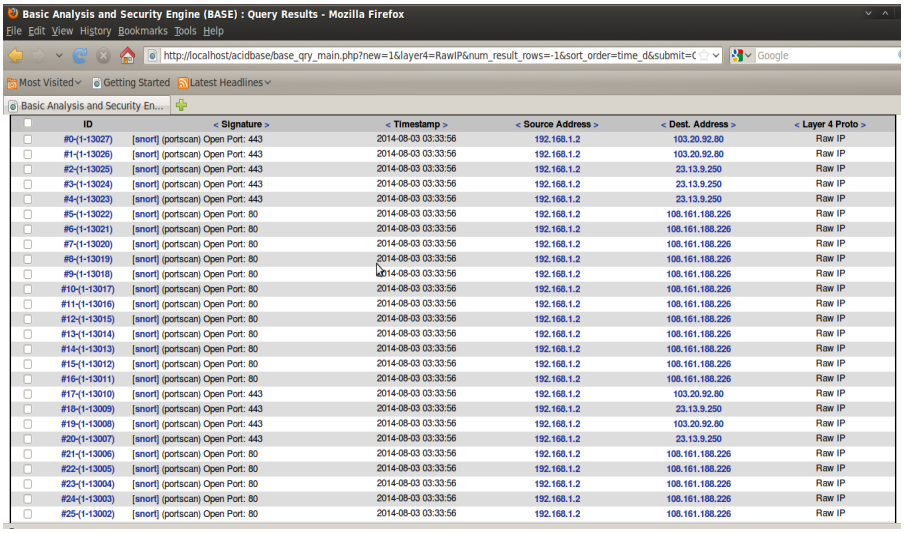
Gambar 5.73 Halaman Utama Base

Pada kuadran kiri atas terdapat *link* yang mendeskripsikan sejumlah informasi seperti *alert* yang terjadi selama 24 jam terakhir dan72 jam terakhir yang dapat ditampilkan berdasarkan parameter unik, *listing*, alamat IP sumber dan tujuan. Selain itu terdapat juga informasi seperti 15 *alert* terbaru, *port* sumber atau tujuan terbaru. Pada kuadran kanan atas terdapat informasi waktu pengambilan data ke *database*, nama *database,* versi skema, dan informasi waktu tambahan. Sealain itu juga terdapat tiga *link* yang mendefinisikan fitur pencarian, pembuatan grafik data *alert,* dan pembuatan grafik untuk terdeteksinya *alert.* Pada kuadran kanan bawah terdapat deskripsi profil *traffic* berdasarkan protokol, dan pada kuadran kiri bawah terdapat berbagai informasi seperti jumlah sensor, *alert* unik, kategorisasi, jumlah total *alert,* dan sebagainya.



Gambar 5.74 *Alert* yang ditampilkan

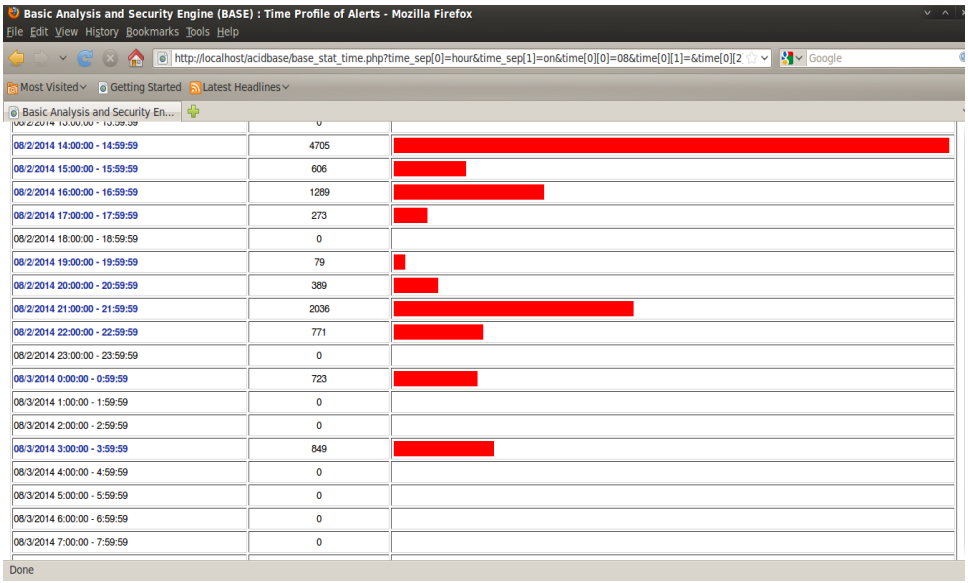
Pada gambar diatas terlihat proses penyerangan yang terjadi proses yang dianggap sebagai alert ke dalam server maka BASE akan menampilkan alert atau peringatan yang sesuai dengan protocol yang digunakan berdasarkan traffic. Pada fitur yang menampilkan profil *traffic* berdasarkan protocol TCP, BASE mendeskripsikan sejumlah daftar *log* dan *alert* pada protokol TCP



ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-13027)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	103.20.92.80	Raw IP
#1-(1-13026)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	103.20.92.80	Raw IP
#2-(1-13025)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	23.13.9.250	Raw IP
#3-(1-13024)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	23.13.9.250	Raw IP
#4-(1-13023)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	23.13.9.250	Raw IP
#5-(1-13022)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#6-(1-13021)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#7-(1-13020)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#8-(1-13019)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#9-(1-13018)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#10-(1-13017)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#11-(1-13016)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#12-(1-13015)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#13-(1-13014)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#14-(1-13013)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#15-(1-13012)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#16-(1-13011)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#17-(1-13010)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	103.20.92.80	Raw IP
#18-(1-13009)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	23.13.9.250	Raw IP
#19-(1-13008)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	103.20.92.80	Raw IP
#20-(1-13007)	[snort] (portscan) Open Port: 443	2014-08-03 03:33:56	192.168.1.2	23.13.9.250	Raw IP
#21-(1-13006)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#22-(1-13005)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#23-(1-13004)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#24-(1-13003)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP
#25-(1-13002)	[snort] (portscan) Open Port: 80	2014-08-03 03:33:56	192.168.1.2	108.161.188.226	Raw IP

Gambar 5.75 Tampilan Daftar *Alert* Dan *Traffic*

Terlihat berturut-turut dari kira ke kanan adalah nomer identitas *alert*, informasi *signature alert* yang ter-*generate, timestamp* (waktu terjadinya *alert*), alamat IP sumber, alamat IP tujuan, dan protokol yang digunakan



Gambar 5.76 *alert time* yang ditampilkan

5.7. Pencegahan Serangan Menggunakan IPTables

Setelah penulis melakukan beberapa proses penyerangan dan menganalisa baik terhadap komputer target maupun terhadap computer penyerang, penulis menemukan data dari komputer penyerang yang dapat digunakan untuk melakukan pencegahan terhadap penyerangan tersebut. Adapun data yang berhasil diperoleh adalah;

1) ***Nmap Scanning***

08/04-13:23:06.412888 [**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**] [Priority: 3] {TCP} ***192.168.2.2****:37497 -> 192.168.2.1:1*

08/04-13:23:06.412888 [**] *[1:1228:7]* ***SCAN nmap XMAS*** *[**] [Classification: Attempted Information Leak] [Priority: 2]* ***{TCP} 192.168.2.2:37497 -> 192.168.2.1:1***

08/04-13:23:07.070012 [**] [1:1852:3] WEB-MISC robots.txt access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2] {TCP} ***192.168.2.2****:1512 -> 192.168.2.1:80*

08/04-13:22:12.081949 [**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length > 14 [**] [Priority: 3] {TCP} 192.168.2.2:53200 -> 192.168.1.2:1

*08/04-13:22:58.838165 [**] [122:1:0] (portscan) **TCP Portscan [**] [Priority: 3] {PROTO:255} 192.168.2.2 -> 192.168.2.1***

08/04-13:22:58.956928 [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempted Denial of Service] [Priority:

2) ***Ping Attack***

root@dian-desktop:/var/log/snort# snort -i eth1 -q -c /etc/snort/snort.conf -A console

command line overrides rules file alert plugin!

08/04-12:52:04.673042 *[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP}* ***192.168.2.2:59066 -> 192.168.2.1:80***

08/04-12:52:15.076259 *[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempted Denial of Service] [Priority: 2]* ***{TCP} 192.168.2.1:80 -> 192.168.2.2:41715***

08/04-12:53:04.961470 *[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempted Denial of Service] [Priority: 2]* ***{TCP} 192.168.2.2:41728 -> 192.168.2.1:80***

08/04-12:53:15.069633 *[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempted Denial of Service] [Priority: 2] {ICMP} 192.168.2.1 -> 192.168.2.2*

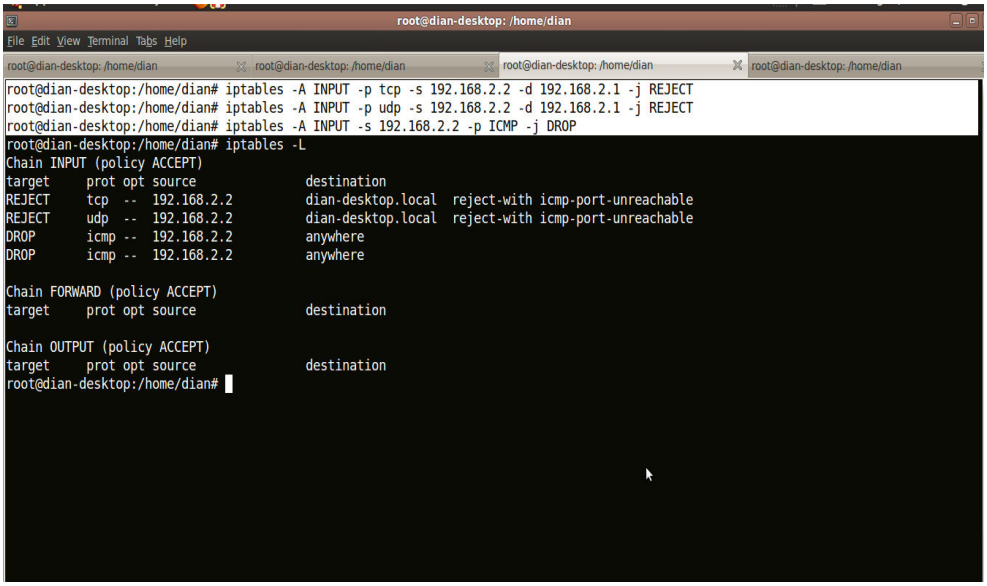
3) ***TCP / UDP Flood***

08/04-13:17:06.031843 [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 192.168.2.2 -> 192.168.2.1

08/04-13:17:06.915459 [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 192.168.2.2:49881 -> 192.168.2.1:7730

08/04-13:17:06.983331 [**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 192.168.2.1:7680 -> 192.168.2.2:49830

Metode yang digunakan, alamat *internet protokol*, alamat MAC, dan *port* yang digunakan untuk melakukan penyerangan. Dari data yang diperoleh, maka penulis dapat melakukan pencengahan terhadap penyerangan tersebut. Dalam melakukan pencegahan ini, penulis melakukannya dengan melakukan konfigurasi perintah pada komputer firewall server yang bertindak sebagai *gateway* dengan cara memasukan *source* yang diperoleh dari komputer penyusup seperti alamat ip dan *protocol* yang digunakan dengan menggunakan fitur dari mesin *firewall* yaitu iptables, sehingga yang dihasilkan dari konfigurasi ini adalah penyerang tidak dapat melakukan aktivitas yang sama terhadap computer server seperti melakukan ping atau aktivitas seperti *port scanning* dan yang lainnya



Gambar 5.77 Blok Target Dengan IPTables

Pada gambar diatas penulis mengisukan sebuah perintah untuk melakukan pemblokiran terhadap komputer penyerang. Penulis menggunakan perintah

#iptables –A INPUT –p tcp –s 192.168.2.2 –d 192.168.2.1 –j REJECT

#iptables –A INPUT –p udp –s 192.168.2.2 –d 192.168.2.1 –j REJECT

Keterangan dari pada sintak adalah :

a. ***-A (append)***

Perintah ini digunakan untuk menerapkan satu aturan baru yang akan ditempatkan di baris yang paling bawah dari aturan – aturan yang telah dibuat sebelumnya.

b. **INPUT**

Aturan yang digunakan oleh *firewall* untuk mengatur paket – paket data yang menuju *Firewall.*

c. **–p (jenis protokol)**

Parameter ini berungsi untuk membuat aturan berdasarkan jenis *protocol* yang digunakan, misalnya TCP,UDP,ICMP

d. **–s [alamat IP sumber]**

Parameter –s berfungsi untuk membuat aturan mengacu pada alamat IP asal paket yang dikirimkan

e. **–d [alamat IP tujuan]**

Parameter –d berfungsi untuk membuat aturan mengacu pada alamat IP tujuan dari paket yang dikirimkan.

f. **–j *[jump]***

sejumlah keputusan untuk diterapkan terhadap suatu paket yang diawali dengan –j [jump]. Yang meliputi

1) ***DROP***

Apabila ditemukan paket yang sesuai dengan aturan untuk di-DROP, maka *firewall* akan langsung membuang paket tersebut tanpa mengirimkan pesan *ERROR* apapun ke pengirim

2) ***REJECT***

Apabila ditemukan paket yang sesuai dengan aturan untuk di-*REJECT,* maka *firewall* akan langsung membuang paket tersebut namun disertai dengan mengirimkan pesan *ERROR ICMP " port unreachable"*

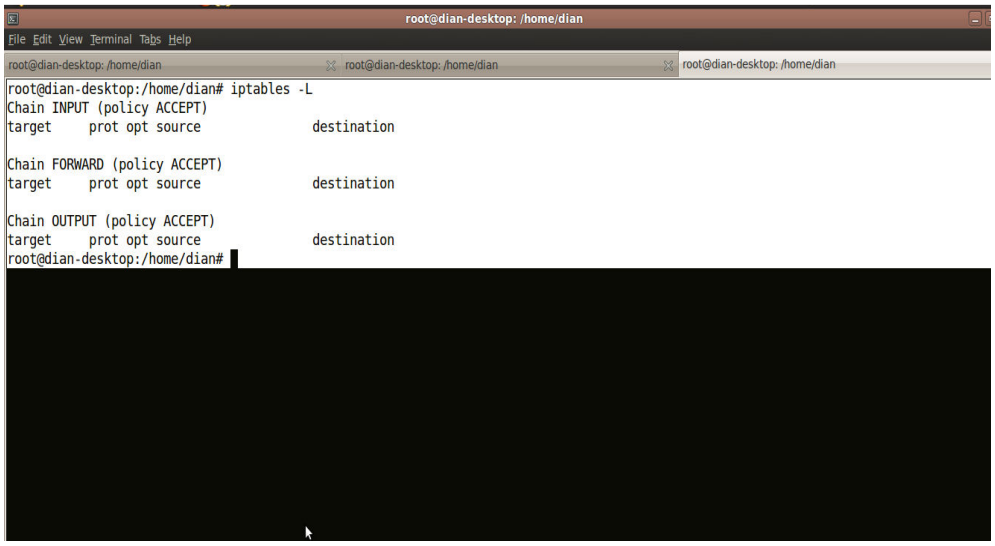
3) ***ACCEPT***

Apabila ditemukan paket yang sesuai dengan aturan untuk di-*ACCEPT*, maka *firewall* akan langsung menerima untuk kemudian meneruskan paket tersebut.

g. **–L *[list]***

Perintah ini digunakan untuk menampilkan semua aturan yang telah dibuat sebelumnya

Contoh : ***iptables –L***



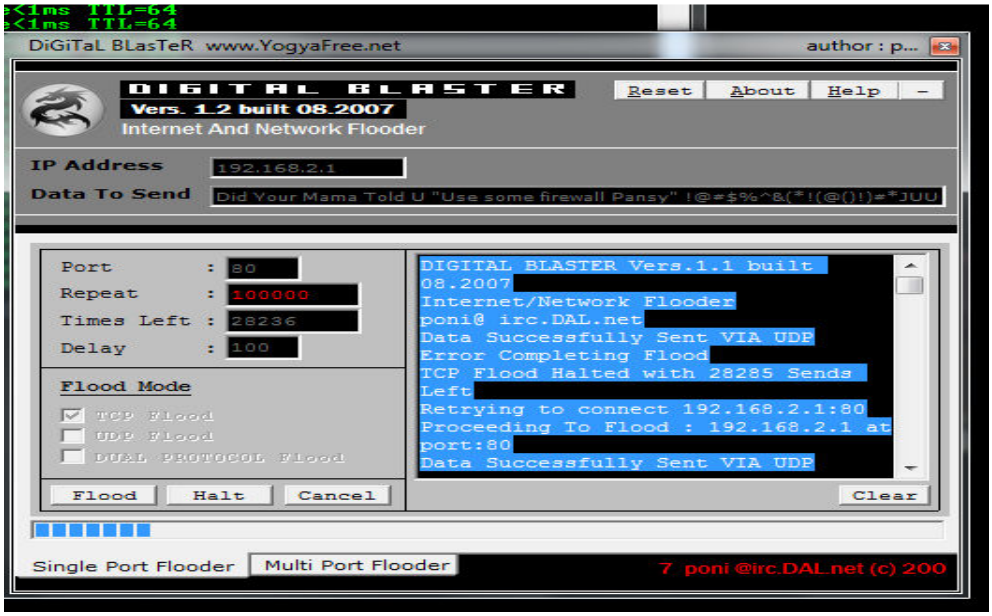
Gambar 5.78 menampilkan aturan iptables yang dibuat

Maka perintah ini dapat digunakan untuk melihat aturan yang telah diterapkan pada *Firewall*. Pada Gambar *chain INPUT*, *chain FORWARD* dan chain *OUTPUT* masih kosong, karena belum diisi aturan yang baru.

```
root@dian-desktop: /home/dian
File Edit View Terminal Tabs Help
root@dian-desktop: /home/dian   root@dian-desktop: /home/dian   root@dian-desktop: /home/dian   root@dian-desktop: /home/dian
root@dian-desktop:/home/dian# iptables -A INPUT -p tcp -s 192.168.2.2 -d 192.168.2.1 -j REJECT
root@dian-desktop:/home/dian# iptables -A INPUT -p udp -s 192.168.2.2 -d 192.168.2.1 -j REJECT
root@dian-desktop:/home/dian# iptables -A INPUT -s 192.168.2.2 -p ICMP -j DROP
root@dian-desktop:/home/dian# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  --  192.168.2.2          dian-desktop.local  reject-with icmp-port-unreachable
REJECT     udp  --  192.168.2.2          dian-desktop.local  reject-with icmp-port-unreachable
DROP       icmp --  192.168.2.2          anywhere
DROP       icmp --  192.168.2.2          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@dian-desktop:/home/dian#
```

Gambar 5.79 hasil aturan yang telah dibuat

Pada gambar diatas menunjukan bahwa suatu aturan baru telah dibuat dalam penggunaan iptables sehingga hasil dapat di tampilkan dengan menggunakan perintah # iptables –L. Saat perintah iptables dilakukan, maka hasil eksekusi perintah akan terlihat reaksi yang ditimbulkan pada mesin penyerang atau *client* saat sedang melakukan proses penyusupan menggunakan *tool-tools scanning* ataupun yang lain sehingga menimbulkan pesan *error.*



Gambar 5.80 proses *flooding* terhenti setelah di *REJECT*

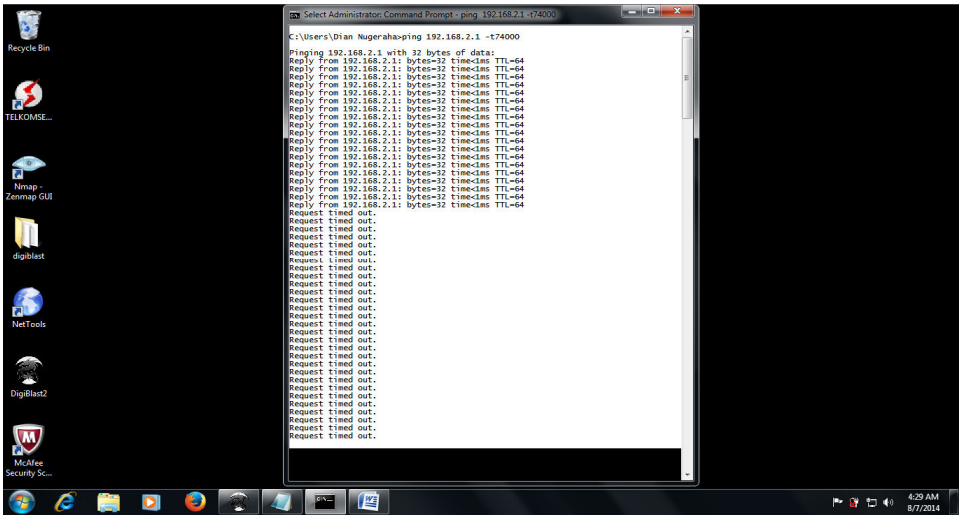
DIGITAL BLASTER Vers.1.1 built 08.2007
Internet/Network Flooder
poni@ irc.DAL.net
Proceeding To Flood : 192.168.2.1 at port:80
Failed to Flood : 192.168.2.1 :80Host Is Not Active / Port Is Not Open
Connected to 192.168.2.1:80

Data Successfully Sent VIA UDP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Data Successfully Sent VIA UDP
Data Successfully Sent VIA UDP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Data Successfully Sent VIA UDP
Data Successfully Sent VIA UDP
Flooding 192.168.2.1
Data Successfully Sent VIA TCP/IP
Flooding 192.168.2.1
Connection Closed.
Error Completing Flood
TCP Flood Halted with 99932 Sends Left

```
Retrying to connect 192.168.2.1:80
Proceeding To Flood : 192.168.2.1 at port:80
Failed to Flood : 192.168.2.1 :80Host Is Not Active / Port Is Not Open
Connected to 192.168.2.1:80
```

Sedangkan perintah yang digunakan untuk memblok suatu serangan ping attack adalah *:*

```
#iptables -A INPUT -s 192.168.2.2 -p ICMP -j DROP
```



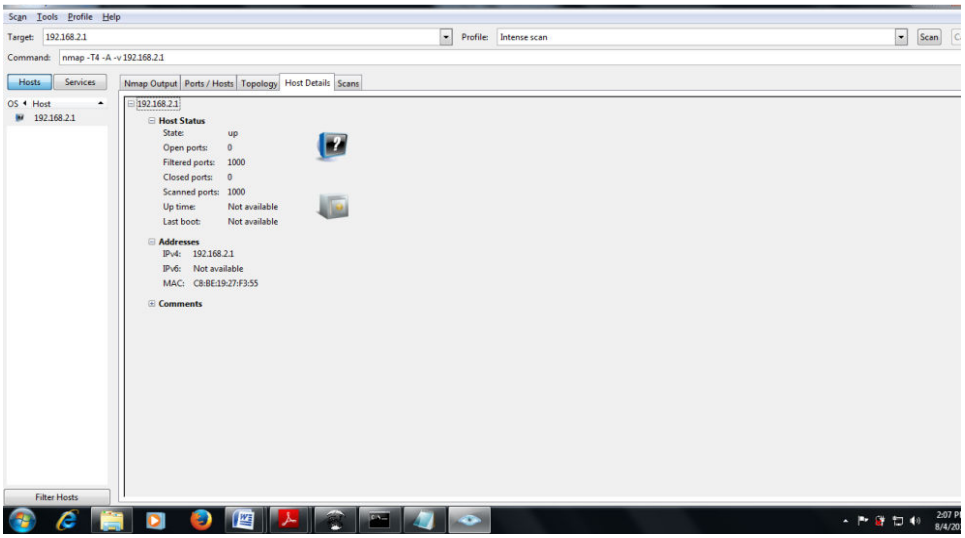
```
C:\Users\Dian Nugeraha>ping 192.168.2.1 -t74000

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Gambar 5.81 hasil DROP *Ping Attack*

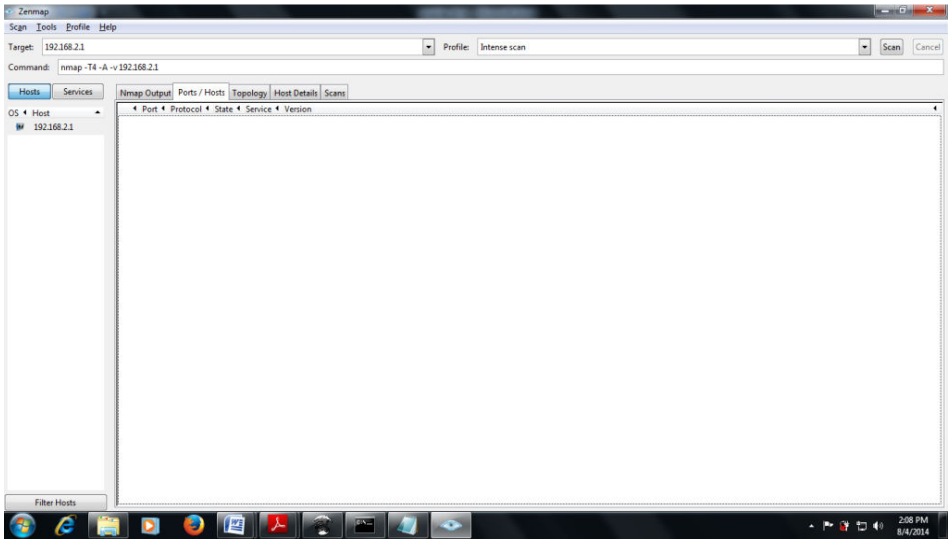
```
C:\Users\Dian Nugeraha>ping 192.168.2.1 -t74000
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Request timed out.
```

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out

Terlihat pada gambar proses ping ke computer server terhenti setelah pada komputer penyerang mencoba melakukan ping attack dengan mengirimkan paket sebesar 74000 menjadi terhenti sehingga terlihat proses request ke server menjadi Request timed out.



Gambar 5.82 hasil scan Nmap tidak menampilkan info server



Gambar 5.83 hasil scan Nmap tidak menampilakan port yang terbuka

5.8. Keuntungan dan Hasil Menggunakan IDS (*Intrusion Detection System*)

Setelah penulis melakukan berbagai proses dalam penerapan IDS, maka penulis mendapatkan kemudahan dalam penerapannya. Dapat diperoleh hasil dari penerapan IDS ini, yaitu suatu jaringan computer dapat dipantau hanya dengan melalui sebuah mesin atau komputer yang bertindak sebagai sensor didalam jaringan dan tehubung kedalam sebuah jaringan, itu dapat melihat semua kejadian yang sedang terjadi didalamnya. Selain keuntungan yang didapat dalam penerapan IDS ini, penulis juga mendapatkan hasil dari sistem IDS dalam mengamankan jaringan, yaitu jika terdapat sebuah masalah pada jaringan (proses intrusi) maka dapat diketahui secara langsung oleh IDS ini yang menggunakan Snort. Dari mana serangan itu datang, melalui *port* berapa, dan protokol apa yang digunakan. Tahap akhir ini tidak ada tindakan yang dilakukan, sehingga pada skripsi ini tahap yang dilakukan hanya sampai pada tahap *monitoring*.

5.9. KESIMPULAN DAN SARAN

Dari hasil pembahasan yang terdapat dari bab sebelumnya maka penulis menarik kesimpulan apa yang sudah didapat dari hasil praktek atau percobaan terhadap sistem IDS (*Intrusion Detection System*). Dan juga saran tentang apa yang harus dikembangakan lagi terhadap masalah system IDS ini.

5.9.1. KESIMPULAN

Rumusan kesimpulan dari keseluruhan proses penelitian yang telah dilakukan dari pembahasan yang sudah diuraikan, maka penulis mencoba membuat kesimpulan sebagai berikut;

1. Sistem IDS (*Intrusion Detection System*) yang diterapkan telah berhasil dibangun dan dikembangkan dengan baik keseluruhan mesin sensor IDS dapat bekerja dengan efektif sebagai system keamanan jaringan computer yang berbasis open source dalam mendeteksi sebuah intruder atau penyusup pada mesin sensor IDS. Dimanan dalam mendeteksi suatu serangan dianalisis pada BASE (*Basic Analysis Security Engine*)
2. Sistem IDS dalam mendeteksi serangan yang terjadi adalah dengan melakukan *scanning* terhadap sejumlah *source* dan lalu lintas yang terjadi di dalam jaringan, sehingga seluruh kejadian yang dianggap sah maupun tidak sah dapat di lihat melalui kegiatan *monitoring* dengan menggunakan aplikasi yang digunakan untuk melakukan pemantauan jaringan yang merupakan hasil *capture* menggunakan *snort*
3. Mekanisme *system* kerja *snort* dan BASE yang telah berhasil di implementasikan dengan baik. Dalam pengujian *system* snort dan BASE yaitu dengan menggunakan *ping attack* dan *port scanning* (Nmap), dan *Digital Blaster.*
4. Pencegahan yang dapat dilakukan terhadap serangan adalah dengan menggunakan iptables. Untuk mengatasi serangan dari intruder yaitu dengan cara melakukan *ping attack* dan Nmap ke sebuah mesin server, maka penulis akan menuliskan membuat aturan baru iptable, dimana aturan baris perintah tersebut untuk memblok berdasarkan alamat IP *Address*. Saat aturan dimasukan

ke dalam *rules* iptables maka akan terlihat pada mesin penyerang atau *client* yang menyatakan *Request time out*

5. Kelebihan dalam menggunak IDS ini adalah suatu jaringan computer dapat dipantau hanya dengan sebuah mesin atau Komputer yang bertindak sebagai sensor di dalam jaringan dan berhubungan ke dalam sebuah jaringan dan dapat melihat semua aktifitas di dalam sebuah jaringan. Selain keuntungan didapat dalam penerapan IDS ini, penulis juga mendapatkan hasil dari *system* IDS dalam mengamankan jaringan. Yaitu jika terdapat sebuah masalah pada jaringan (proses intrusi) maka dapat diketahui secara langsung oleh IDS ini yang menggunakan snort, melalui port, protocol ,IP Address yang digunakan

5.9.2. SARAN

Saran-saran yang diberikan pada penelitian ini adalah sebagai berikut

1. Dalam segi pendeteksian dapat dilakukan dengan baik karena dapat melihat lalu lintas jaringan yang sedang terjadi, akan tetapi dari sisi pencegahan masih harus dikembangakan lagi dalam melindungai asset yang terdapat pada komputer yang menjadi tujuan dari penyerangan
2. IDS hanya bisa melakukan monitoring jaringan, akan lebih baik jika IDS yang diterapkan dapat melakukan pencegahan dari serangan yang terjadi secara otomatis.