BAB IV
IMPLEMENTASI DAN PENGUJIAN

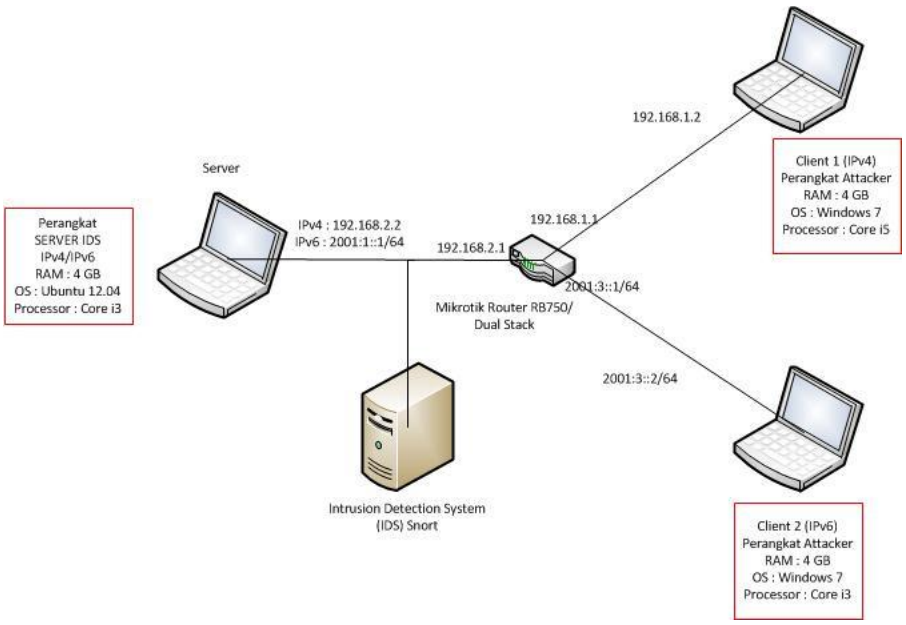
Pada bagian ini akan dilakukan implementasi sistem yang sudah dibuat berdasarkan perancangan pada bab sebelumnya. Pengujian sistem dilakukan dengan melakukan beberapa serangan dan untuk mengetahui apakah IDS dapat bekerja dengan baik.

4.1 Implementasi

Tahap implementasi merupakan tahap penerapan dari proses analisis yang sudah dilakukan agar sistem yang dibangun dapat dimengerti oleh mesin dan sesuai dengan lingkungan yang sebenarnya. Penerapan metode yang digunakan pada penelitian, selanjutnya akan diimplementasi pada setiap perangkat yang terlibat untuk menghasilkan sistem yang sesuai dengan tahap perancangan.

4.1.1 Implementasi Arsitektur Jaringan Pengujian

Implementasi ini merupakan penerapan dari perancangan arsitektur jaringan, pada perancangan tersebut digambarkan bagaimana setiap komputer dan perangkat lainnya terhubung. Berikut ini adalah Gambar 4.1. arsitektur pengujian yang akan diimplementasikan yang telah diberikan pengalamatan untuk setiap komputernya.



Gambar 0.1 Arsitektur Jaringan Pengujian

4.1.1.1 Implementasi Perangkat Keras

Implementasi ini merupakan penjelasan mengenai spesifikasi perangkat keras yang digunakan pada arsitektur jaringan yang akan diimplementasikan. Pada gambar arsitektur pengujian (Gambar 4.1) terdapat beberapa perangkat keras yaitu hub, komputer Mikrotik RouterOS, komputer *attacker*, komputer client, kabel UTP. Setiap perangkat keras tersebut memiliki spesifikasi yang dijelaskan pada Tabel 4.1 sampai dengan Tabel 4.3

Table 0.1 Spesifikasi Router [19**]**

Product Code	RB750
Architecture	MIPS-BE
CPU	AR7241 400MHz
Current Monitor	No
Main Storage/NAND	64MB
RAM	32MB
SFP Ports	0
LAN Ports	5
Gigabit	No
Switch Chip	1

MiniPCI	0
Integrated Wireless	No
MiniPCIe	0
SIM Card Slots	No
USB	No
Memory Cards	No
Power Jack	10-28V
802.3af Support	No
POE Input	10-28V
POE Output	No
Serial Port	No
Voltage Monitor	No
Temperature Sensor	No
Dimentions	113x89x28mm
Operating System	RouterOS
Temperature Range	-40C .. +55C
RouterOS License	Level4

Table 0.2 Spesifikasi Perangkat Keras Komputer *Client 1* s.d *client 2*

Perangkat Keras	*Client* 1	*Client* 2
Processor	*Core* i5 2.4GHz	*Core*i3 2.4GHz
Hardisk	500 Gb	500 Gb
Ram	4 Gb	2 Gb

Table 0.3 Spesifikasi Perangkat Keras *Server*

No	Perangkat Keras	Server
1	*Processor*	Corei3 2.4 GHz
2	*Hardisk*	500 Gb
3	Ram	2 Gb

4.1.1.2 Implementasi Perangkat Lunak

Implementasi ini merupakan penjelasan dari aplikasi dan sistem operasi yang digunakan pada setiap perangkat keras dari arsitektur jaringan. Berikut ini adalah aplikasi dan sistem operasi yang digunakan pada setiap perangkat, yang dipaparkan pada Tabel 4.4 sampai dengan Tabel 4.5

Table 0.4 Implementasi Perangkat Lunak *Server*

No	Spesifikasi	Server
1	Sistem Operasi	Linux Ubuntu 12.04
2	Database	MySQL 5.5.37
3	Web Server	Apache/2.4.7
4	Aplikasi IDS	Snort 2.9.6
5	Configure Router	Winbox
6	Accelerator winbox	wine
7	Notification	Gammu (SMSGateway)

Table 0.5 Implementasi Perangkat Lunak *Client*

No	Spesifikasi	Client 1	Client 2
1	Sistem Operasi	Windows 7 Ultimate	Windows 7 Ultimate
2	Tools	Zenmap 6.40	Terminal

4.1.1.3 Implementasi dan Konfigurasi Arsitektur Jaringan

Implementasi ini merupakan bagaimana cara mengkonfigurasi mikrotik router dan pengalamatan pada masing-masing perangkat komputer.

1. Konfigurasi Mikrotik RouterOS
2. Konfigurasi IP Address Perangkat Keras Intruder
3. Konfigurasi IP address pada Linux Ubuntu (Komputer Client) IPv4 IPv6

4.1.2 Implementasi Aplikasi

Implementasi ini merupakan penjelasan mengenai cara menginstalasi aplikasi IDS snort, pengimplementasian perancangan dari *rule* snort, dan pengimplementasian perancangan aplikasi monitoring IDS snort.

4.1.1.4 Implementasi Snort

Implementasi ini dilakukan pada komputer Client 1 (IPv4) dan client 2 (IPv6) pada sistem operasi linux ubuntu 12.04, berikut ini adalah tahapan-tahapan instalasi aplikasi snort yang digunakan sebagai aplikasi IDS.

1. Download package LAMP (Apache, MySQL, PHP), digunakan untuk menjalankan aplikasi snort. Pada terminal (User root) ketikkan perintah:

```
Apt-get -y install apache2 libapache2-mod-php5
mysql-server mysql-common mysql-client php5-mysql
libmysqlclient-dev php5-gd php-pear libphp-adodb
php5-cli
```

Ikuti perintah selanjutnya sesuai dengan instruksi pada aplikasi yang diinstall.

2. Install library pendukung snort. Pada terminal (user root) ketikkan perintah:

```
apt-get -y install libwww-perl libnet1 libnet1-dev
libpcre3 libpcre3-dev autoconf libcrypt-ssleay-perl
libtool libssl-dev build-essential automake gcc
make flex bison
```

Ikuti perintah selanjutnya sesuai dengan intruksi pada aplikasi yang di *install.*

3. Download aplikasi pendukung snort dan snort 2.9.6 untuk menjalankan snort ada beberapa *library* yang perlu di-*download*, library tersebut antara lain :

   a. Libdnet yang dapat di-download di http://libdnet.googlecode.com/files/libdnet-1.12.tgz.

b. Daq-2.0.2 yang dapat di-download di http://sourceforge.net/projects/snort/files/snort/daq-2.0.2.tar.gz/download.
c. Libpcap 1.3.0 yang dapat di-download di http://www.tcpdump.org/release/libpcap-1.3.0.tar.gz.
d. Snort 2.9.6 yang dapat di-download di https://www.snort.org/downloads/snort/snort-2.9.6.1.tar.gz.

4. Instalasi Snort

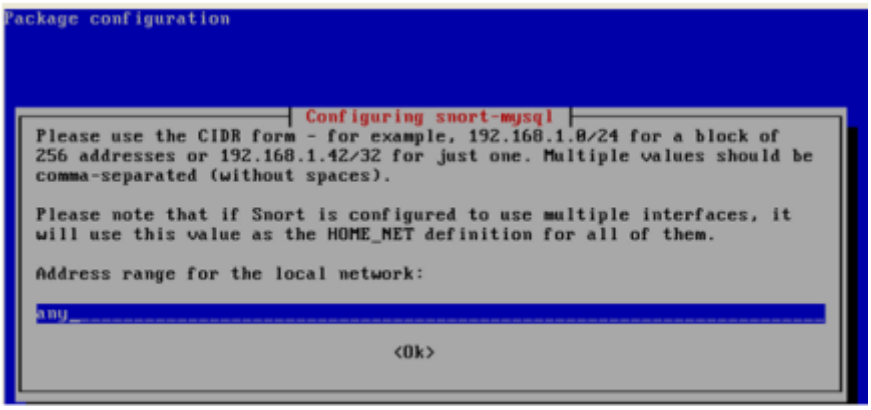
Dari hasil *download* aplikasi pendukung snort dan snort 2.9.6 tersebut di *copy* ke *folder* usr/local/snort. Pada *terminal* ketikkan perintah:

Beberapa langkah persiapan yang perlu dilakukan

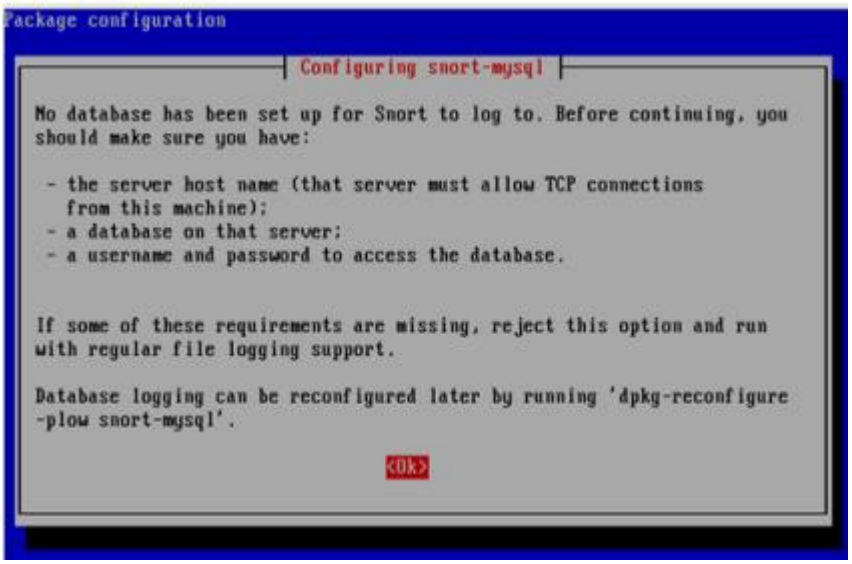
1) Apt-get install snort-mysql

```
apt-get install snort-mysql_
```

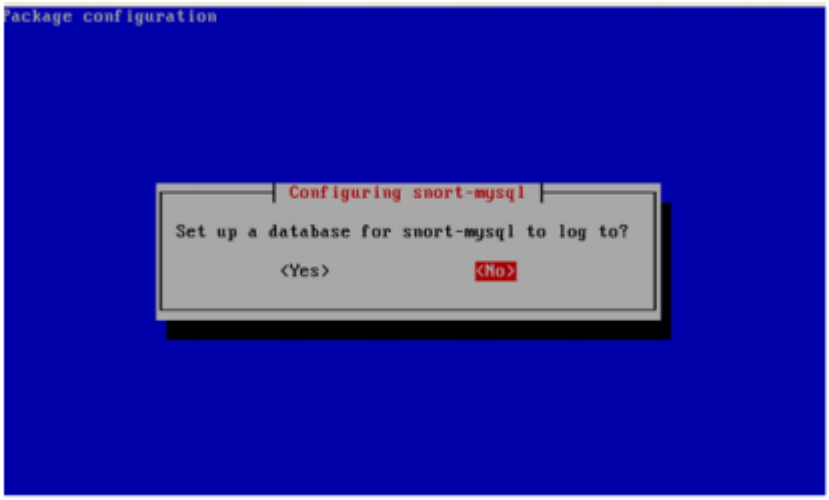
2) Muncul Pop-up, pada tetfield masukkan any, lalu tekan OK



3) Tekan OK



4) SetUp a database, pilih No

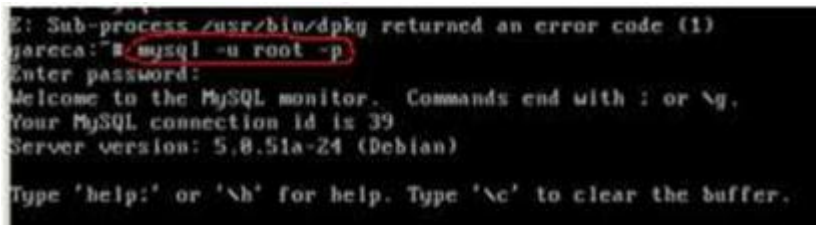


Untuk Sementara akan terjadi eror, tetapi tidaj masalah.

Langkah selanjutnya akan masuk ke MySQL

1) Ketikkan : mysql _u root –p lalu masukkan password user root

Sebagai contoh :admin



2) Masukkan : Create database snort;

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

mysql> _
```

3) Ketikkan : grant all on snort.* to snortuser@localhost identified by ‘snortpassword’;

```
mysql> grant all on snort.* to snortuser@localhost identified by 'snortpassword'
;
Query OK, 0 rows affected (0.00 sec)
```

4) Ketikkan : lush privileges; <-perintah untuk reload privileges

```
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
gareca:~$ _
```

5) Lalu exit

Selanjutnya adalah mengimport table ke dalam mysql,

1) Ketikkan : cd/usr/share/doc/snort-mysql

```
cd /usr/share/doc/snort-mysql
```

2) Ketikkan : gzip –d/usr/share/doc/snort-mysql/create_mysql.gz

```
# gzip -d /usr/share/doc/snort-mysql/create_mys
```

3) Ketikkan : mysql –u root –p snort < /usr/share/doc/snort-mysql/create_mysql
4) Masukkan password yang telah diketahui . contoh :admin

a. Install libdnet 1.12

```
# cd usr/local/snort
# tar zxvf libdnet-1.12.tgz
# cd libdnet-1.12
# ./configure
# make
# make install
# ln -s /usr/local/lib/libdnet.1.0.1
  /usr/lib/libdnet.1
```

b. Install daq 2.02

```
# cd usr/local/snort
# tar zxvf daq-2.0.2.tar.gz
# cd daq-2.0.2
# ./configure
# make
# make install
```

c. Install libcap 1.3.0

```
# cd usr/local/snort
# tar zxvf libpcap-1.3.0.tar.gz
# cd libpcap-1.3.0
# ./configure
# make
# make install
# echo "/usr/local/lib" >> /etc/ld.so.conf
# ldconfig -v
```

d. Install Snort 2.9.6

```
# cd usr/local/snort
# tar zxf snort-2.9.6.0.tar.gz
# cd snort-2.9.6.0
# ./configure -prefix=/usr/local/snort -enable-
  sourcefire
# make
# make install
# mkdir /var/log/snort
# mkdir /var/snort
# groupadd snort
# useradd -g snort snort
# chown snort:snort /var/log/snort
```

2. Menjalankan Snort

Aplikasi snort dijalankan di dalam *terminal*, untuk menjalankan aplikasi snort ketikkan perintah :

```
# /usr/local/snort/bin/snort -vde -A full -i eth0
  -c /usr/local/snort/etc/snort.conf
```

4.1.1.5 Implementasi Rules Snort

Rule snort digunakan untuk mendeteksi adanya serangan atau aktivitas yang dilakukan oleh client-client terhadap *server*. Berikut ini adalah *rule-rule* yang digunakan untuk mendeteksi aktivitas-aktivitas tersebut.

1. *Rule* Deteksi *Port Scanning*

```
(msg:"SCAN FIN"; flow:stateless; flags:F,12;
reference:arachnids,27; classtype:attempted-recon;
sid:621; rev:7;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"SCAN NULL"; flow:stateless; ack:0; flags:0;
seq:0; reference:arachnids,4; classtype:attemptedrecon;
sid:623; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"SCAN SYN FIN"; flow:stateless; flags:SF,12;
reference:arachnids,198; classtype:attempted-recon;
sid:624; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"SCAN XMAS"; flow:stateless; flags:SRAFPU,12;
reference:arachnids,144; classtype:attempted-recon;
sid:625; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"SCAN TONX nmap XMAS"; flow:stateless;
flags:FPU,12; reference:arachnids,30;
classtype:attempted-recon; sid:1228; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"SCAN synscan portscan"; flow:stateless;
flags:S,12; id:39426; reference:arachnids,441;
classtype:attempted-recon; sid:630; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 22
(msg:"SCAN SSH Version map attempt";
flow:to_server,established;
content:"Version_Mapper"; nocase;
classtype:network-scan; sid:1638; rev:5;)
alert udp $EXTERNAL_NET any -> $HOME_NET 1900
(msg:"SCAN UPnP service discover attempt";
content:"M-SEARCH "; depth:9;
content:"ssdp|3A|discover"; classtype:network-scan;
sid:1917; rev:6;)
```

2. *Rule* Deteksi DDOS (*SYN Flooding*, *Ping large Packet*)

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any
(msg:"ICMP Large ICMP Packet"; dsize:>800;
reference:arachnids,246; classtype:bad-unknown;
sid:499; rev:4;)
alert tcp any any -> any any (flags: S; msg:"DDOS
SYN Flooding"; flow: stateless; threshold: type
both, track by_src, count 70, seconds 10;
sid:10001;rev:1;)
```

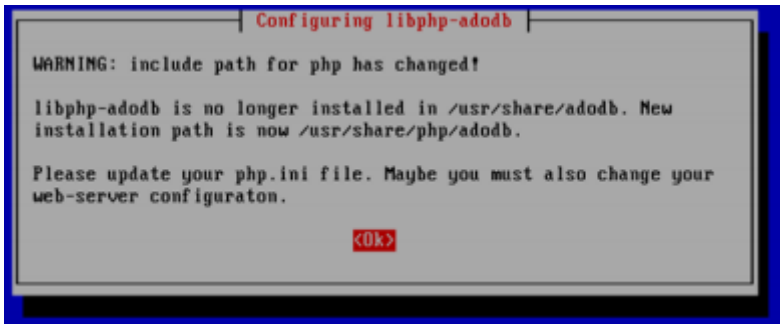
4.1.1.6 Implementasi antarmuka AcidBASE

1. Menginstall acidBASE

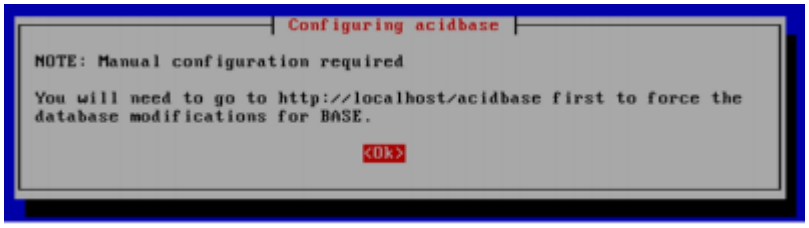
Install paket BASE merupakan langkah pembangunan sistem keamanan ini. BASE akan membaca rules yang tertulis oleh snort, maka BASE harus dikonfigurasikan dengan database Snort. Karena BASE merupakan program web-based, maka aplikasi ini ditanamkan pada direktori

1) Ketikkan : `apt-get install acidbase`

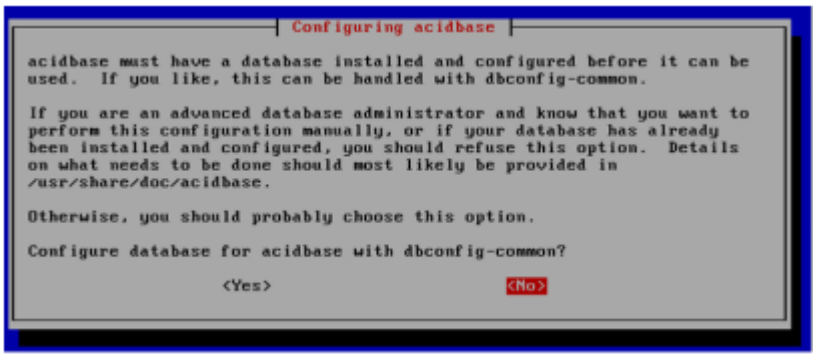
2) Muncul Pop up, OK



3) Pilih OK

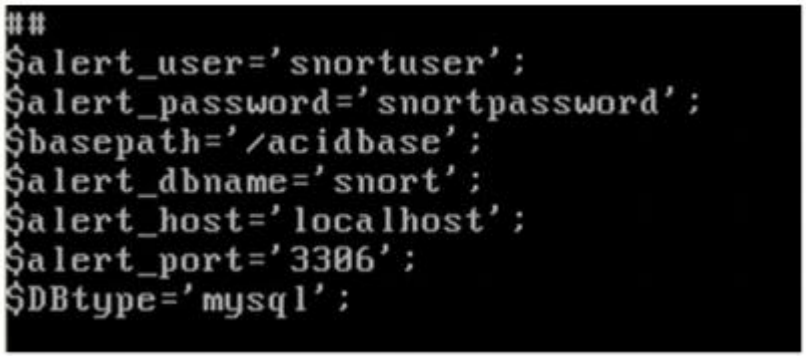


4) Create database, pilih NO



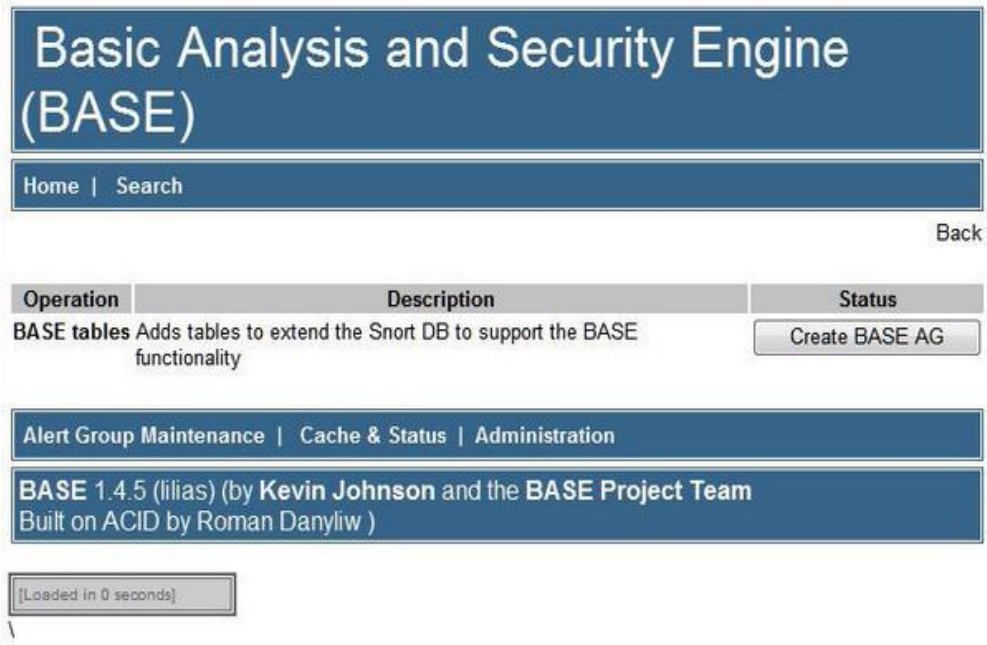
5) Ketikkan : /etc/acidbase/database.php

6) Isi bagian ‘’ seperti gambar dibawah:



7) Save and exit

8) ketikkan : /etc/acidbase/apche.conf



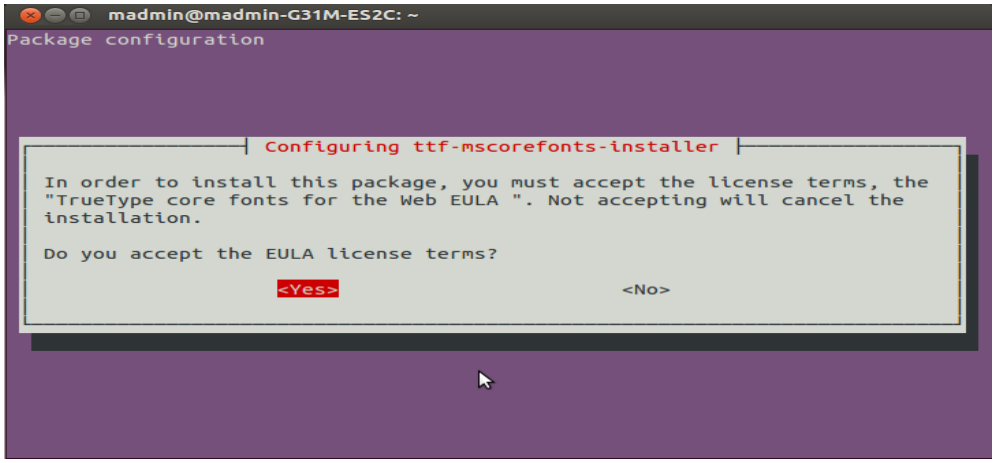
Gambar 0.2 Tampilan Implementasi IDS pada service acidBASE

4.1.1.7 Implementasi dan Konfigurasi Arsitektur jaringan

Implementasi ini merupakan penjelasan bagaimana cara mengkonfigurasi router dan pengalamatan pada masingmasing perangkat komputer

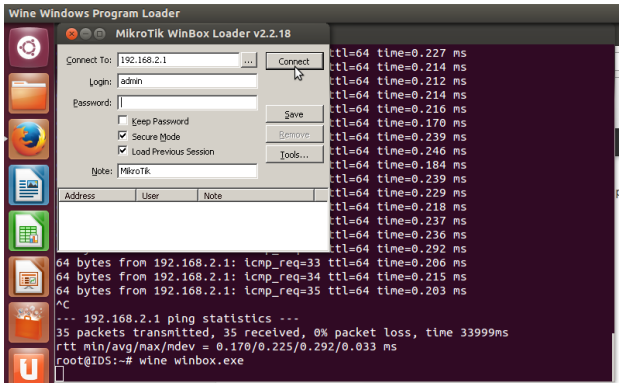
4.1.1.1.1 Konfigurasi Mikrotik Router RB750

1. Winbox adalah aplikasi untuk mengkonfigurasi mikrotik router. Tetapi winbox hanya tersedia untuk platform windows dengan ekstensi *exe.
2. Sebelum dapat menjalankan winbox pertama yang harus dipasang adalah aplikasi Wine. Wine adalah emulator di ubuntu untuk menjalankan winbox
3. Masuklah pada terminal ubuntu ctrl+alt+T
4. Install wine dengan perintah : **sudo apt-get install wine**
5. Tunggulah sampai download selesai
6. Pilih (yes)



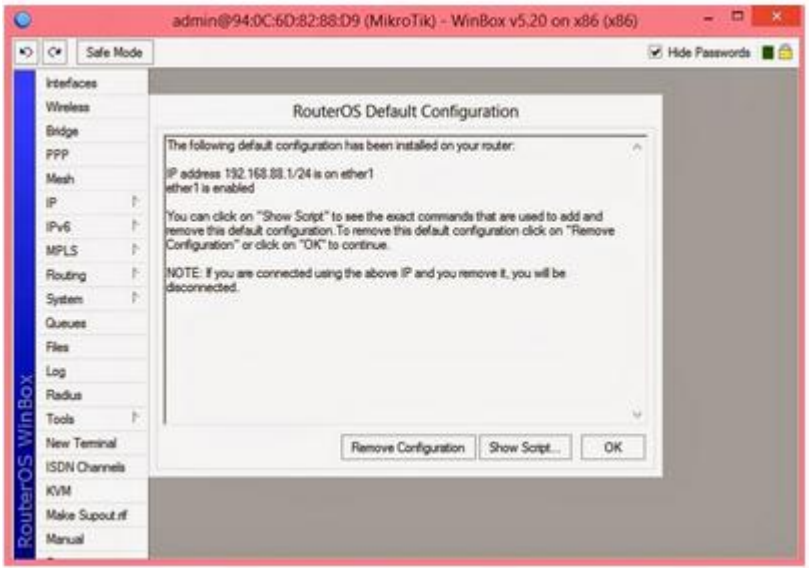
Gambar 0.3 Konfigurasi installasi Wine

7. Ketikkan **Wine winbox.exe** untuk menjalankan winbox
8. Download winbox dengan mengetikkan **wget http://www.mikrotik.com/download/winbox.exe**
   Lakukan instalasi winbox maka akan muncul gambar seperti



Gambar 0.4 Tampilan GUI winbox

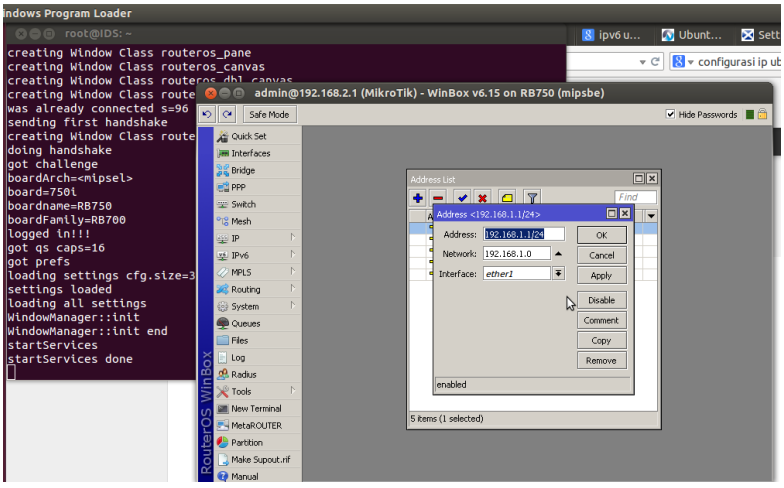
9. login ke mikrotik via winboxx untuk mengkonfigurasi mikrotik GUI.
   Masukkan alamat 192.168.2.1 klik connect.



Gambar 0.5 Halaman Utama winbox

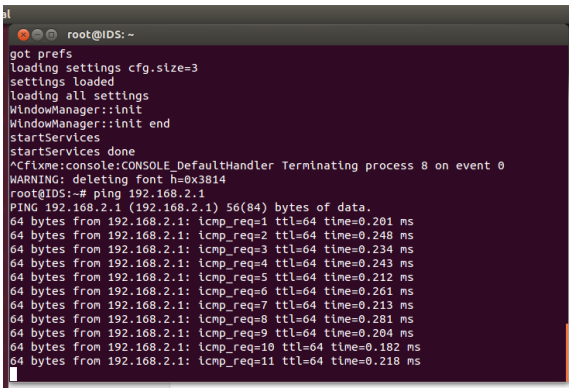
10. Setelah login, maka untuk melihat interfaces yang aktif siap dioperasikan. Pilih menu interface

11. Pada interface ada menu IP >addresses
    Berilah alamat address pada setiap socket ethernet pada router



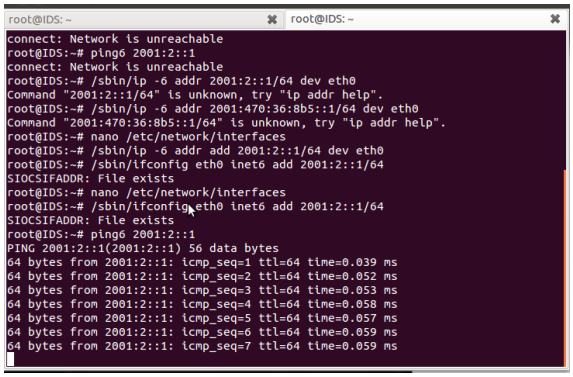
Gambar 0.6 Konfigurasi Ethernet pada Router Mikrotik

12. Mencoba untuk melakukan ping agar dapat diketahui apakah server sudah terhubung dengan mikrotik ataukah belum



Gambar 0.7 Konfigurasi sambungan miktrotik ke Client IPv4

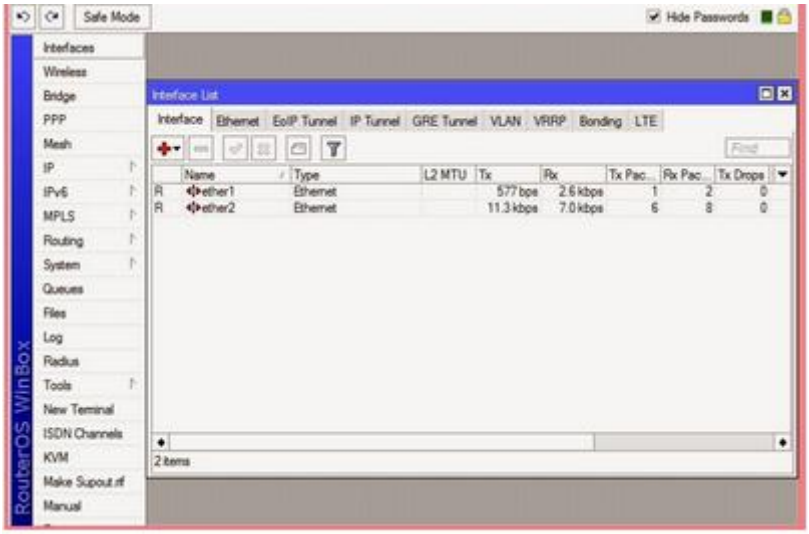
13. Pada gambar diatas telah dilakukan ping 192.168.2.1 yaitu ping terhadap IP mikrotik



Gambar 0.8 Konfigurasi pada client IPv6

4.1.1.1.2 Konfigurasi NAT

1. Setting IP address, pilih menu IP > Interfaces list



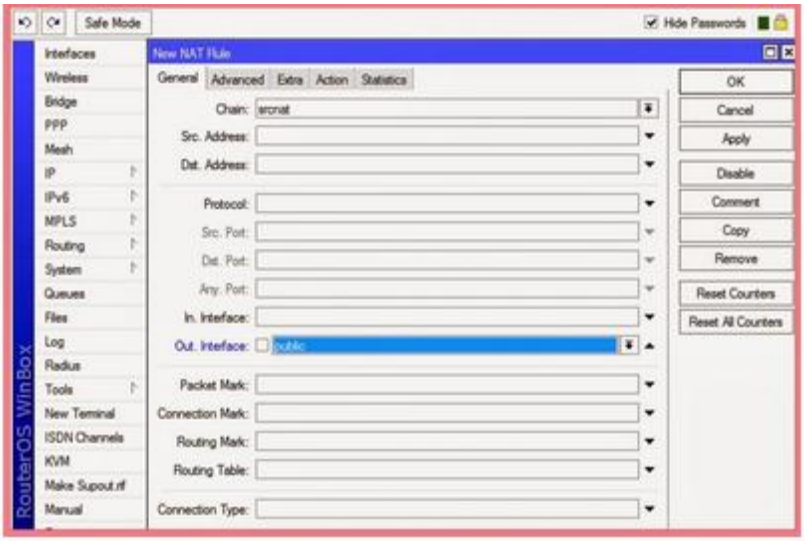
Gambar 0.9 Konfigurasi NAT Pada Winbox

2. Setting Firewall. Pilih menuIP > Firewall. Pilih Tab NAT. Klik add

   + Chain: srcnat (biarkan saja)

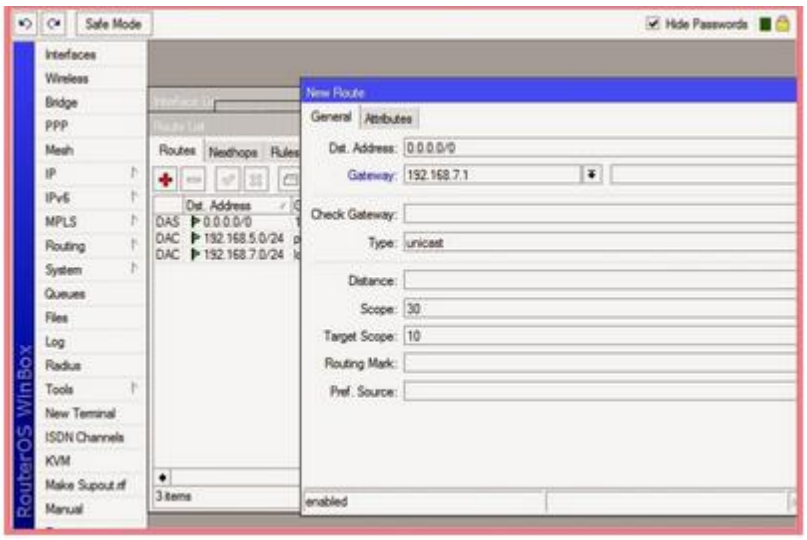
   Out.Interface: public

   Pilih Tab Action. Setting Action: masquerade

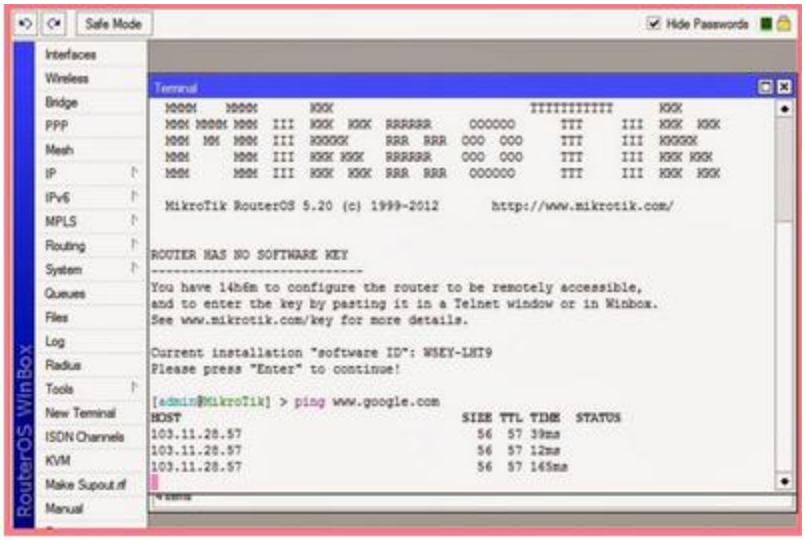


Gambar 0.10 Setting NAT di Mikrotik

3. Setting Routes. Pilih menu IP > routes. Klik add + Gatewayy:192.168.1.1 (gateway ISP saya) OK.



Gambar 0.11 Setting Router Mikrotik



Gambar 0.12 Testing Sambungan ke Server

3. Setting DHCP Server. Pilih menu IP > DHCP server. Klik DHCP setup. DHCP Server Interface: LOCAL (NEXT)

DHCP Address Space (NEXT)

Gateway for DHCP Network

Addresses to Give out

DHS Srevers: (NEXT)

4.1.1.1.3 Konfigurasi IPv6 pada Router

Prinsip-prinsip dasar IPv6 yang persis sama dengan IPv4

Contoh Routing IPv6:

```
[admin@MikroTik] > ipv6 route add dst-address=2001::/16
gateway=fc00:dead:beef::2
[admin@MikroTik] > ipv6 route print detail
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, o - ospf, b - bgp, U - unreachable
0 A S  dst-address=2001::/16 gateway=fc00:dead:beef::2 reachable
    ether1 distance=1 scope=30 target-scope=10
```

Perbedaan IPv4 dan IPv6 hanyalah pada alamat lokal yang dapat digunakan sebagai nethops rute

```
[admin@MikroTik] > ipv6 route add dst-address=2002::/16
gateway=fe80::21a:4dff:fe56:1f4d%ether1
[admin@MikroTik] > ipv6 route print detail
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, o - ospf, b - bgp, U - unreachable
 ...
 1 A S  dst-address=2002::/16
        gateway=fe80::21a:4dff:fe56:1f4d%ether1 reachable distance=1
        scope=30 target-scope=10
```

RouterOS memungkinkan untuk mengatur lebih dari satu alamat gateway untuk untuk satu rute. Dalam hal ini rute yang dipasang di kernel untuk masing-masing interface itu berbeda.

```
[admin@MikroTik] > ipv6 address p
```

```
Flags: X - disabled, I - invalid, D - dynamic, G - global, L - link-local
 #    ADDRESS                                     INTERFACE
ADVERTISE
 0  G fc00:1::1/64                                ether1            no
 1  G fc00:2::1/64                                ether2            no
[admin@MikroTik] > ipv6 route add dst-address=2001::/16
gateway=fc00:1::2,fc00:2::2
[admin@MikroTik] > ipv6 route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, o - ospf, b - bgp, U - unreachable
 #      DST-ADDRESS              GATEWAY                       DISTANCE
 0 A S  2001::/16                fc00:2::2 reachable ether1,  1
                                 fc00:1::2 reachable ether2
```

dua rute yang ditambahkan, tidak satu

```
# ip -6 route
2001::/16 via fc00:2::2 dev eth1  proto static  metric 1024  mtu 1500
advmss 1440 metric10 4294967295
2001::/16 via fc00:1::2 dev eth0  proto static  metric 1024  mtu 1500
advmss 1440 metric10 4294967295
...
```

4.2 Pengujian

Pengujian merupakan proses pengeksekusian dari implementasi yang telah dilakukan untuk menilai dan menemukan kesalahan kesalahan yang terdapat pada sistem. Dengan adanya pengujian diharapkan sistem memiliki kualitas yang baik dan dapat dijadikan bahan referensi dalam proses pengembangan sistem lebih lanjut.

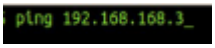
4.1.3 Pengujian Arsitektur Jaringan

Pengujian ini merupakan proses pengecekan terhadap keberhasilan dan instalasi arsitektur jaringan. Pengujian yang dilakukan yaitu dengan melakukan pengecekan terhadap status keterhubungan dari satu *node* ke *node* lain dan pengaksesan konten-konten yang ada di *server* oleh *Client*

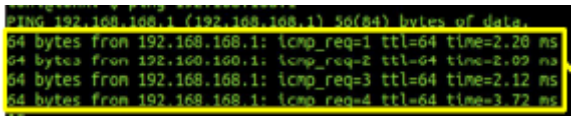
4.1.1.8 Pengujian Keterhubungan antar perangkat

Pengujian ini merupakan pengujian yang dilakukan untuk mengecek setiap *node* atau perangkat dalam arsitektur jaringan saling terhubung. Pengujian dilakukan dengnan menggunakan aplikasi ping. Berikut ini cara pengujian keterhubungan yang dilakukan dan hasil dari pengujian tersebut dijelaskan pada penjelasan berikut.

1) Membuakan aplikasi *command prompt* pada windows atau *terminal* pada linux.
2) Mengetikkan perintah ping



3) Mengecek respon yang diberikan oleh *IP Address* yang dituju



Dari hasil pengujian yang dilakukan maka di dapatkan hasilnya pada Tabel. 4.7

Table 0.6 Hasil Pengujian Keterhubungan Perangkat

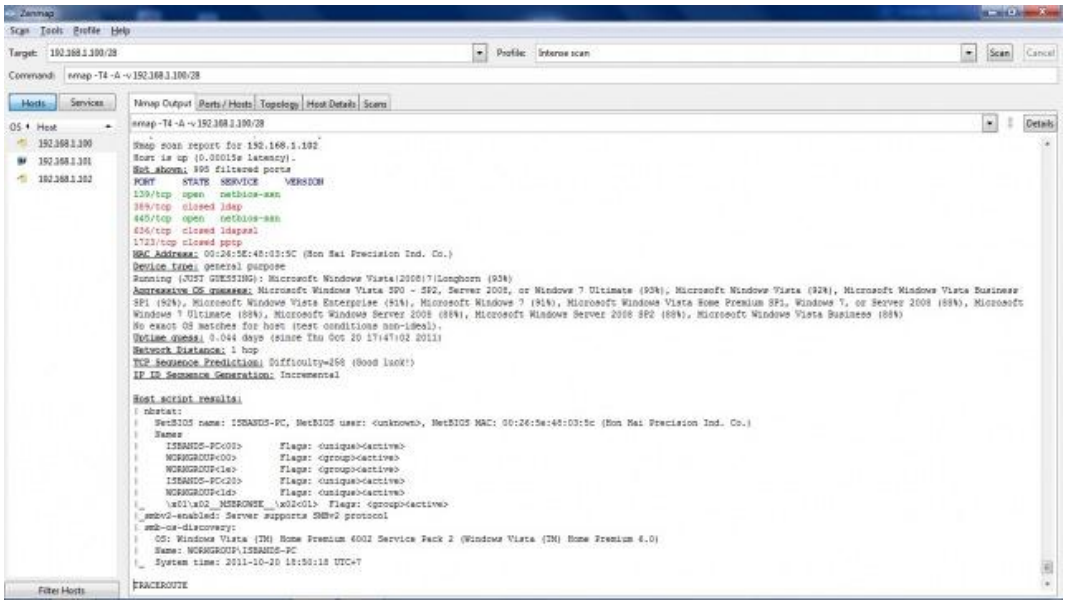
	Client 1	Client 2
IDS SERVER	Ok	Ok
SERVER	Ok	Ok

4.1.4 Pengujian dan Penilaian IDS Snort

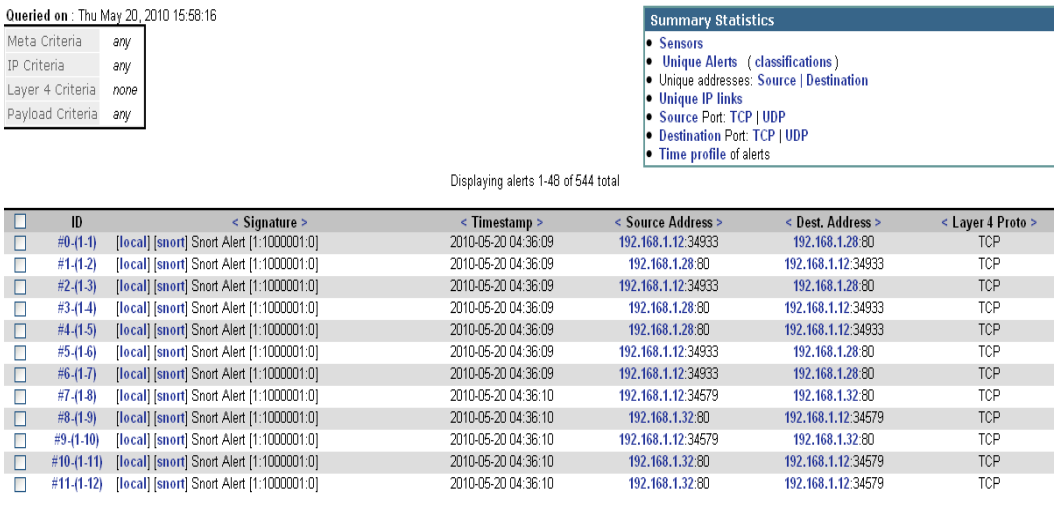
Pengujian ini merupakan proses untuk menguji aplikasi IDS snort yang terpasang pada sebuah jaringan komputer. Parameter yang diujikan yaitu kecepatan akses setelah IDS diterapkan pada jaringan, kecepatan itu diantara komunikasi client ke server dan sebaliknya, kemudian parameter ketepatan dari IDS Snort untuk mendeteksi jenis serangan. Berikut ini akan dijelaskan pengujian-pengujian tersebut

4.1.1.9 Pengujian penyerangan pada IPv4

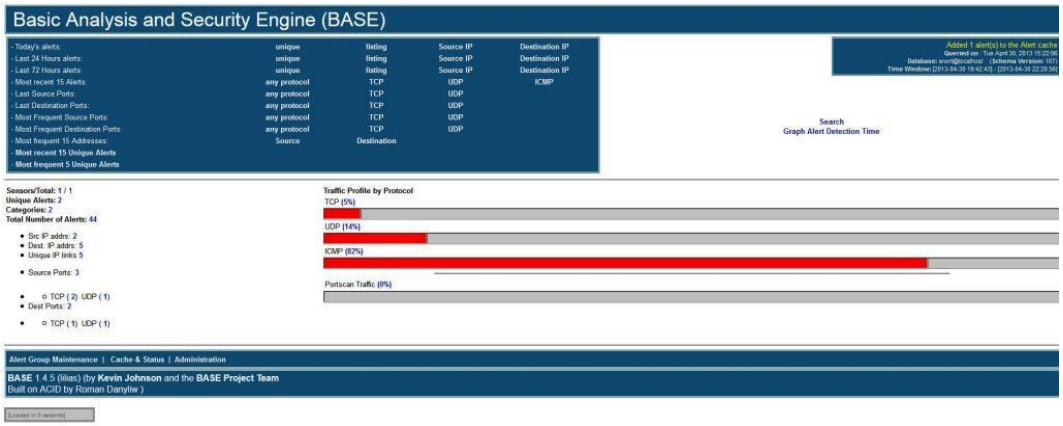
Gambar dibawah menunjukkan penyerangan yang dilakukan kepada server menggunakan *port scanning* dengan aplikasi zenmap



Gambar 0.13 Penyerangan dengan Zenmap



Gambar 0.14 Implementasi Notifikasi serangan yang terjadi pada Server



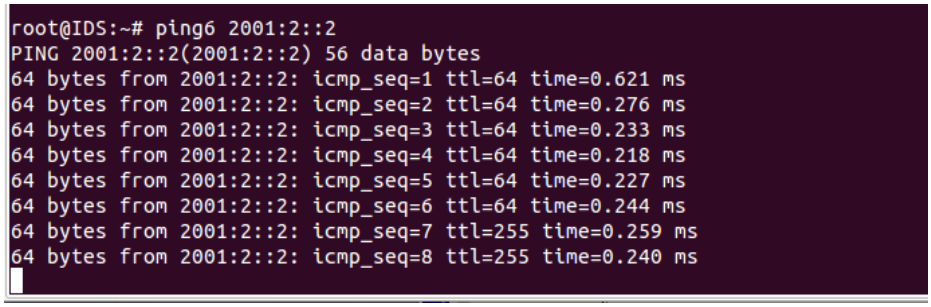
Gambar 0.15 Notifikasi serangan Dengan Grafik



Gambar 0.16 Persentase serangan

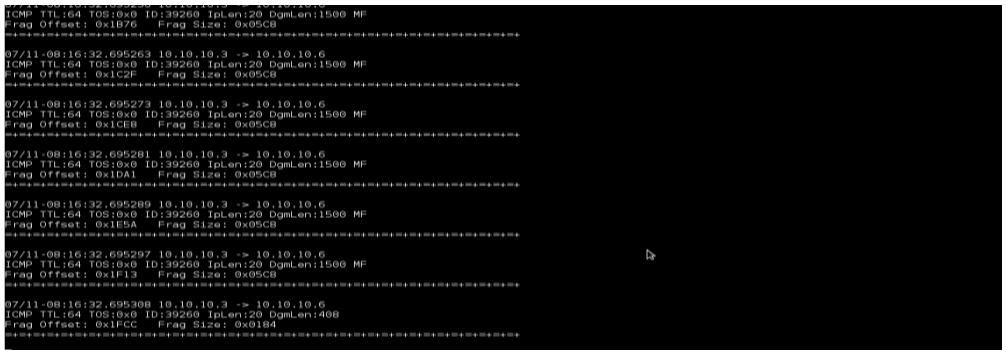
4.1.1.10 Pengujian penyerangan pada IPv6

Gambar dibawah ini merupakan pengujian yang dilakukan pada IPv6 menggunakan *ping of death*.



Gambar 0.17 Serangan pada IPv6

Serangan dapat dilakukan pada IPv6 tetapi acidBASE pada server dalam bentuk GUI tidak terlihat, dibawah ini merupakan bentuk serangan dalam bentuk console. Yang disesuaikan dengan *rule* pada snort



Gambar 0.18 Serangan kepada IPv6 IDS server