Laporan Resmi Praktikum Kemanan Data

Network Intrusion Detection System Menggunakan Snort

Dimas Rizky H.P. – 2110141011

***Dasar Teori***

**Network IDS**

*Network IDS (NIDS)* adalah intrussion detection system yang berjalan pada jaringan atau network. Intrussion detection sendiri adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus yang otomatis.

Ada beberapa tipe dasar dari IDS diantaranya adalah :

* Rule-based systems - berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalulintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan.
* Adaptive systems - mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada, tapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk bentuk penyusupan yang baru.

Jenis yang sering digunakan adalah rule-based system. Rules-based system juga memiliki odua pendekatan, yaitu penceganan (preemptory) dan reaksi (reactionary) yang perbedaannya ada di masalah waktu.

Network IDS memiliki tiga jenis IDS, yaitu

* Signature Based
* Anomaly Based
* Hybrid Based

Program signature based yang terkenal adalah Snort, sedangkan program IDS anomaly-based yang sering digunakan adalah BRO-IDS. Hybrid based merupakan gabungan antara keduanya, program yang terkenal adalah suricata

**Snort**

Snort merupakan signature based IDS yang bekerja pada network dengan cara menginspeksi packet yang melewati sensor nya dan akan memeberitahu network administrator jika ada packet yang mencurigakan atau yang menyalahi rule.

Snort memiliki tiga buah mode yaitu,

* **Sniffer Mode**, untuk melihat packet yang lewat di jaringan

Untuk menjalankan snort pada sniffer mode tidaklah sukar, beberapa contoh perintahnya

terdapat di bawah ini,

#snort –v

#snort –vd

#snort –vde

#snort –v –d –e

dengan menambahkan beberapa switch –v, -d, -e akan menghasilkan beberapa keluaran

yang berbeda, yaitu

-v, untuk melihat header TCP/IP paket yang lewat.

-d, untuk melihat isi paket.

-e, untuk melihat header link layer paket seperti ethernet header.

* **Packet Logger Mode**, untuk mencatat semua paket yang lewat di jaringan untuk dianalisa di kemudian hari

Tentunya cukup melelahkan untuk melihat paket yang lewat sedemikian cepat di layar

terutama jika kita menggunakan ethernet berkecepatan 100Mbps, layar anda akan

scrolling dengan cepat sekali susah untuk melihat paket yang di inginkan. Cara paling

sederhana untuk mengatasi hal ini adalah menyimpan 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

./snort –dev –l ./log

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

./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

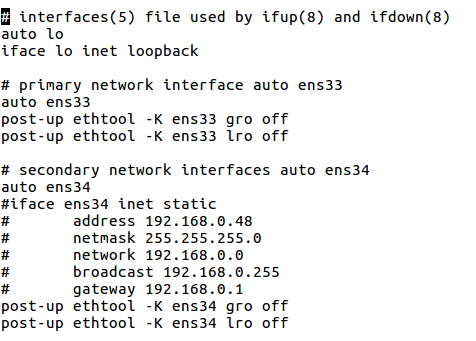
./snort –dvr packet.log icmp

***Laporan Pendahuluan***

***Instalasi Snort***

1. Konfigurasi Network Interface

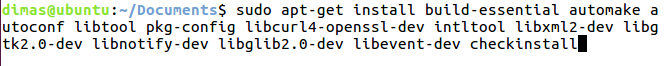
Untuk menjalankan Snort, sangat disarankan untuk menon-aktifkan fitur pada network card yang dinamakan LRO dan GRO, untuk menon-aktifkan fitur ini, lakukan editing pada file */etc/network/interfaces* sehingga seperti *gambar 1.0* di bawah ini.



*Gambar 1.0, non-aktif GRO dan LRO*

1. Install Snort Library Pre-Requisites

Snort membutuhkan beberapa library untuk berjalan sehingga sebelum menginstall snort perlu dilakukan download beberapa library yang dibutuhkan, jalankan perintah pada *gambar 2.0* sampai dengan *gambar 2.2,* di bawah ini untuk menginstall library yang dibutuhkan oleh snort.



*Gambar 2.0*, *instalasi library yang dibutuhkan oleh snort(1)*

**

*Gambar 2.1, instalasi library yang dibutuhkan oleh snort(2)*

**

*Gambar 2.2, instalasi library yang dibutuhkan oleh snort(3)*

Selain itu, juga dibutuhkan Snort DAQ (Data Acquisition Library). Untuk install DAQ harus terlebih dahulu melakukan download DAQ yang ada pada repository snort terbaru. Jalankan perintah pada *gambar 2.3* sampai dengan *gambar 2.5* untuk melakukan download dan instalasi DAQ.



*Gambar 2.3, download DAQ*

**

*Gambar 2.4, unpack package daq*

**

*Gambar 2.5, instalasi DAQ*

1. Instal Snort

Instalasi snort tahapnya sama dengan pada saat menginstall DAQ, download package snort, ekstraksi packet tarbalnya, lalu lakukan build dan install pada package snort nya. Langkah-langkahnya dapat dilihat pada *gambar 3.0* sampai dengan *gambar 3.2*.



*Gambar 3.0, download package snort*

**

*Gambar 3.1, ekstraksi package snort*

**

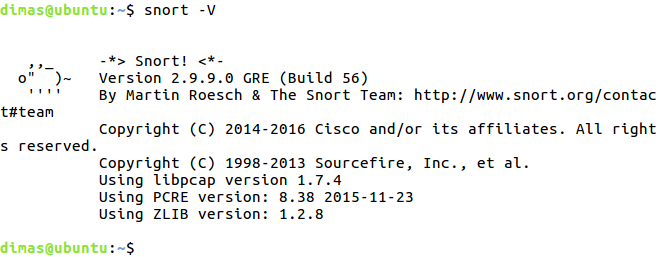
*Gambar 3.2, build dan instalasi package snort*

Setelah melakukan instalasi, lakukan update pada shared library agar snort dapat dijalankan oleh seluruh user, caranya adalah dengan menjalankan perintah seperti pada *gambar 3.3*

**

*Gambar 3.3, update shared library dari direktory bin ke sbin*

Untuk mengetahui apakah snort sudah terinstall atau belum, dapat dilakukan dengan cara menjalankan perintah *$snort –V*  untuk melakukan cek versi pada snort yang diinstall tadi.



*Gambar 3.4, cek versi snort*

1. Konfigurasi Snort

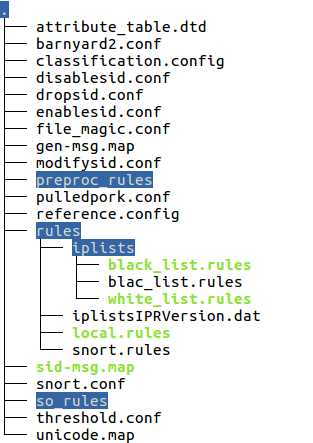
Konfigurasi perlu dilakukan pada beberapa direktori snort, dan file konfigurasi snort agar snort dapat berjalan dengan baik. Beberapa langkah yang harus dilakukan antara lain sebagai berikut,

* + Membuat user dan group snort
    - :~# groupadd snort
    - :~# useradd snort -r -s /sbin/nologin -c SNORT\_IDS -g snort
  + Membuat direktori snort
    - :~# mkdir /etc/snort
    - :~# mkdir /etc/snort/rules
    - :~# mkdir /etc/snort/rules/iplists
    - :~# mkdir /etc/snort/preproc\_rules
    - :~# mkdir /usr/local/lib/snort\_dynamicrules
    - :~# mkdir /etc/snort/so\_rules
  + Membuat file untuk rules dan ip list
    - :~# touch /etc/snort/rules/iplists/black\_list.rules
    - :~# touch /etc/snort/rules/iplists/white\_list.rules
    - :~# touch /etc/snort/rules/local.rules
    - :~# touch /etc/snort/sid-msg.map
  + Membuat direktori untuk log
    - :~# mkdir /var/log/snort
    - :~# mkdir /var/log/snort/archived\_logs
  + Mengatur permission masing-masing direktori
    - :~# chmod -R 5775 /etc/snort
    - :~# chmod -R 5775 /var/log/snort
    - :~# chmod -R 5775 /var/log/snort/archived\_logs
    - :~# chmod -R 5775 /etc/snort/so\_rules
    - :~# chmod -R 5775 /usr/local/lib/snort\_dynamicrules
  + Mengubah ownership masing-masing direktori
    - :~# chown -R snort:snort /etc/snort
    - :~# chown -R snort:snort /var/log/snort
    - :~# chown -R snort:snort /usr/local/lib/snort\_dynamicrules

Setelah melakukan pembuatan direktori untuk source aplikasi snort, selanjutnya adalah melakukan copy pada direktori snort yang telah didownload ke direktori snort yang ada pada direktori /etc. Langkahnya adalah dengan masuk ke direktori package snort yang didownload tadi lalu menjalankan perintah-perintah berikut ini,

* + :~# cd snort\_src/snort-2.9.8.3/etc/
  + :~/snort\_src/snort-2.9.8.3/etc/# cp \*.conf\* /etc/snort
  + :~/snort\_src/snort-2.9.8.3/etc/# cp \*.map /etc/snort
  + :~/snort\_src/snort-2.9.8.3/etc/# cp \*.dtd /etc/snort
  + :~/snort\_src/snort-2.9.8.3/etc/# cd
  + :~# cd snort\_src/snort-2.9.8.3/src/dynamic-preprocessors/build/usr/local/lib/snort\_dynamicpreprocessor/
  + :~./././# cp \* /usr/local/lib/snort\_dynamicpreprocessor/

Secara umum, langkah di atas adalah mengkopikan semua yang ada pada direktori package snort yang sudah didownload ke direktori snort yang ada pada */etc/snort*, sehingga pada direktori snort nantinya akan terdapat file file seperti pada *gambar 4.0* di bawah ini



*Gambar 4.0, struktur direktori /etc/snort*

Setelah seluruh direktori selesai disalin, selanjutnya adalah melakukan konfigurasi pada file */etc/snort/snort.conf*. Langkah yang harus dilakukan dapat dilihat pada *gambar 4.1* sampai dengan  *gambar 4.3*

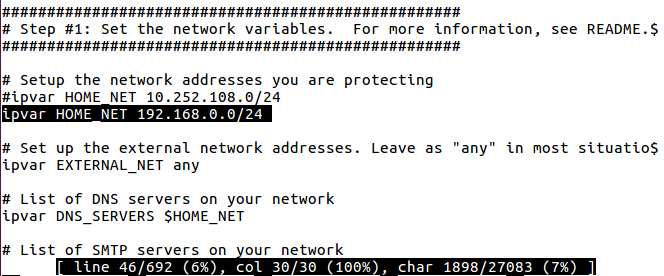


*Gambar 4.1, melakukan konfigurasi pada string $RULE\_PATH*

Lakukan edit pada file konfigurasi snort yang ada pada */etc/snort/snort.conf* menggunakan perintah

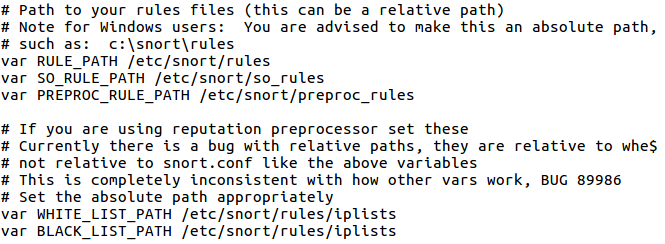
* + :~# nano –c /etc/snort/snort.conf

Editing dilakukan pada **baris ke 45, 104 dan 546**, masing –masing dapat dilihat pada *gambar 4.2, 4.3, dan 4.4,*

**

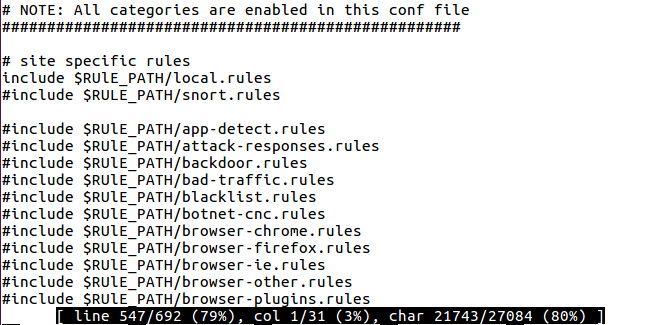
*Gambar 4.2, konfigurasi pada baris ke 45*

Pada baris ini, isikan HOME\_NET dengan network yang ingin dilindungi atau network yang ingin dimonitor. Pada kasus jaringan ini, menggunakan network *192.168.0.0/24.*



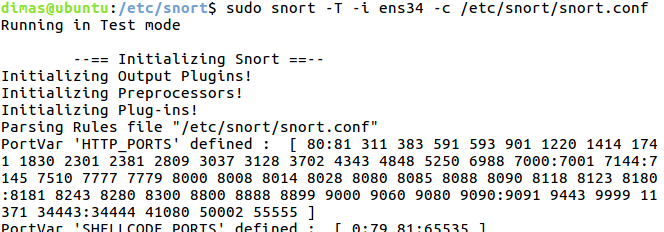
*Gambar 4.3, definisikan path untuk masing masing parameter*

Pada baris ini yang harus dilakukan adalah mendefinisikan path untuk masing masing parameter *RULE\_PATH, SO\_RULE\_PATH, PREPROC\_RULE\_PATH, WHITE\_LIST\_PATH, dan BLACK\_LIST\_PATH.*

**

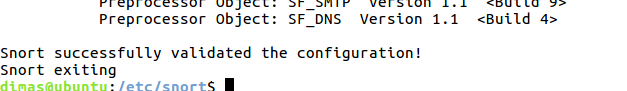
*Gambar 4.4, uncomment pada include rule path local.rules*

Pada langkah ini, hapus tanda # untuk rule path local.rules, file local.rules ini nanti lah yang akan menjadi file tempat rule custom dituliskan. Langkah selanjutnya adalah melakukan test apakah file konfigurasi yang dibuat sudah valid atau tidak dengan menjalankan perintah yang ada pada *gambar 4.5,*

**

*Gambar 4.5, run snort pada test mode untuk melakukan validasi konfigurasi*

Jika konfigurasi yang dilakukan valid, maka akan keluar output seperti pada *gambar 4.6.* Jika yang keluar bukan output tersebut, maka masih ada yang error pada file konfigurasi yang ada pada */etc/snort/snort.conf*.

**

*Gambar 4.6, konfigurasi snort sukses*

1. Membuat Rule Sederhana

Setelah konfigurasi berhasil dilakukan dan valid, langkah yang dapat dilakukan selanjutnya adalah untuk membuat rule sederhana. Rule ini dapat dituliskan pada file */etc/snort/rules/local.rules*. Pada percobaan kali ini akan dibuat rules sederhana yang mendeteksi adanya ping yang dilakukan pada jaringan yang dimonitor. Rulesnya adalah sebagai berikut

* + alert icmp any any -> $HOME\_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

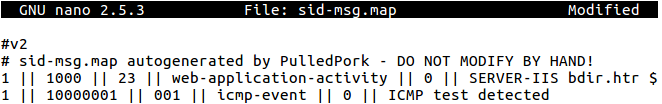


*Gambar 5.0, rule pada /etc/snort/rules/local.rules*

Terdapat aturan dalam penulisan rule ini, yaitu untuk field (sid), nomor rule baru yang didefinisikan secara custom nilainya harus lebih dari 1000000 (1 juta). Hal ini dikarenakan untuk sid 1 – 1000000, telah disediakan untuk rule rule snort yang didefinisikan terlebih dahulu oleh community snort.

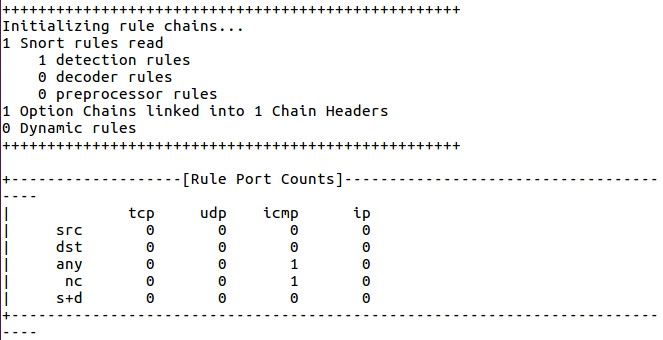
Pada file */etc/snort/sid-msg.map* juga harus dituliskan informasi map untuk rules yang telah kita buat. Pada percobaan ini rulenya adalah

* + 1 || 10000001 || 001 || icmp-event || 0 || ICMP Test detected || url,tools.ietf.org/html/rfc792



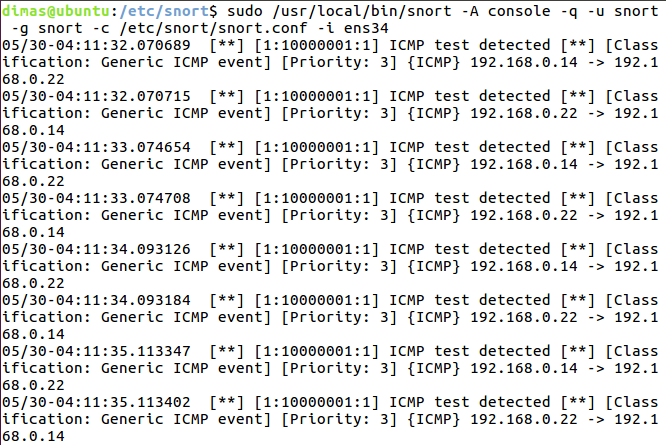
*Gambar 5.1, rule pada /etc/snort/sid-msg.map (perhatikan entry dengan sid 10000001*

Setelah penulisan rule, lakukan snort test mode untuk cek valid tidaknya rule yang telah dibuat. Untuk menjalankan test mode dapat dilihat pada *gambar 4.5* sebelumya. Bedanya, jika dilihat pada bagian rule, akan muncul spesifikasi rule yang ada, seperti pada *gambar 5.2*

**

*Gambar 5.2, muncul overview rule pada saat dijalankan test mode*

Untuk test rule yang telah dibuat, dapat dilakukan dengan cara menjalankan snort pada mode NIDS, yang akan dilakukan oleh snort pada mode NIDS adalah akan mengamati traffic yang ada pada sebuah jaringan yang sudah ditentukan dan jika ada packet yang memenuhi rule yang aktif, maka snort akan mencetak output pemberitahuan bahwa rule yang ada terpenuhi. Untuk melakukan test, setelah snort berjalan dengan mode NIDS, lakukan ping pada interface yang digunakan oleh snort. Perintah yang harus dijalankan dan apa saja outputnya dapat dilihat pada *gambar 5.3*.



*Gambar 5.3, snort berjalan pada NIDS mode*

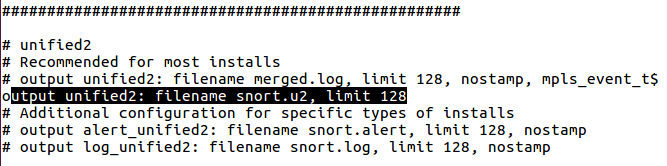
1. Instalasi Barnyard

Barnyard digunakan untuk mengatasi kelemahan snort yaitu log nya sulit dibaca. Barnyard akan menerjemahkan log snort yang ada lalu mengirimkannya ke mysql agar nantinya dapat dibaca dan dianalisa dengan leluasa.

Untuk menginstall barnyard diperlukan juga untuk melakukan instalasi mysql versi 5.7. Langkah instalasi mysql, sama seperti yang ada pada saat praktikum konfigurasi web server menggunakan perintah *$sudo apt-get install mysql-server* lalu pilih versi 5.7 dan spesifikan password untuk user root mysql. Setelah itu berlanjut ke instalasi barnyard

* + Ubah konfigurasi snort

Pada file */etc/snort/snort.conf* lakukan penambahan pada baris 520 seperti yang ada pada *gambar 6.0.*

**

*Gambar 6.0, tambahkan baris konfigurasi*

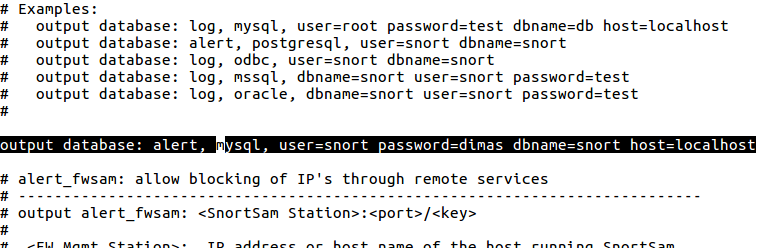
* + Update library dumbnet dan setting library mysql
    - Jalankan perintah
    - *ln –s /usr/include/dumbnet.h /usr/include/dnet.h*
    - lalu
    - *./configure --with-mysql --with-mysql-libraries=/usr/lib/i386-linux-gnu (jika menggunakan linux 32 bit)*
    - *./configure --with-mysql --with-mysql-libraries=/usr/lib/x86\_64-linux-gnu (jika menggunakan linux 64 bit)*
  + Download dan build barnyard
    - Jalankan perintah di bawah ini
    - $cd /home
    - $wget [https://github.com/firnsy/barnyard2/archive/7254c24702392288fe6be948f88afb74040f6dc9.tar.gz \-O barnyard2-2-1.14-336.tar.gz](https://github.com/firnsy/barnyard2/archive/7254c24702392288fe6be948f88afb74040f6dc9.tar.gz%20\-O%20barnyard2-2-1.14-336.tar.gz)
    - $tar –zxvf barnyard2-2-1.14-336.tar.gz
    - $mv barnyard2-7254c24702392288fe6be948f88afb74040f6dc9 barnyard2-2-1.14-336
    - $cd barnyard2-2-1.14-336
    - $autoreconf -fvi -I ./m4
    - $make && make install
  + Copy beberapa file barnyard
    - Jalankan perintah ini
    - :~/home/barnyard2-2-1.14-336# cp etc/barnyard2.conf /etc/snort
    - :~/home/barnyard2-2-1.14-336# mkdir /var/log/barnyard2
    - :~/home/barnyard2-2-1.14-336# chown snort.snort /var/log/barnyard2
    - :~/home/barnyard2-2-1.14-336# touch /var/log/snort/barnyard2.waldo
    - :~/home/barnyard2-2-1.14-336# chown snort.snort /var/log/snort/barnyard2.waldo
  + Buat database
    - Masuk ke direktori package barnyard yang telah diinstal
    - $cd /home/barnyard2-2-1.14-336/schemas
    - Lalu jalankan command
    - $mysql –u root –p
    - Masukan password root yang dibuat pada saat instalasi mysql tadi, lalu jalankan query query berikut ini
    - mysql> create database snort;
    - mysql> use snort;
    - mysql> source create\_mysql;
    - mysql> CREATE USER 'snort' IDENTIFIED BY 'jarkom123';
    - mysql> grant create, insert, select, delete, update on snort.\* to snort;
    - mysql> exit
  + Konfigurasi barnyard
    - Lakukan perubahan pada file */etc/snort/barnyard2.conf* pada baris 71,75 dan 348 seperti pada *gambar 6.1 sampai dengan gambar 6.3*



*Gambar 6.1, baris 71*

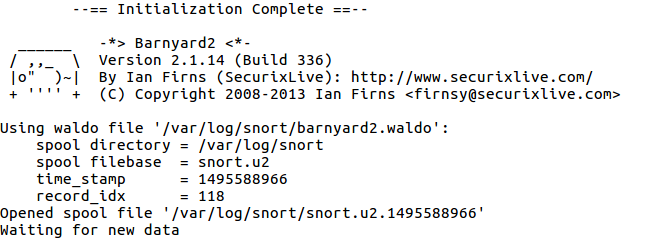
**

*Gambar 6.2, baris 75*

**

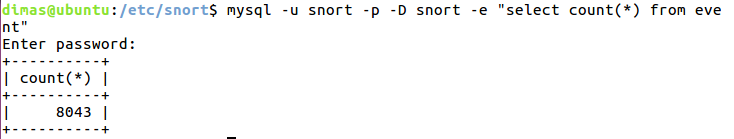
*Gambar 6.3 baris 348*

* + Ubah permission konfigurasi barnyard
    - Ubah permission dengan perintah
    - $chmod o-r /etc/snort/barnyard2.conf
  + Jalankan snort dan barnyard
    - Jalankan barnyard pada alert mode, dengan perintah
    - *$ /usr/local/bin/snort –q –u snort –g snort –c /etc/snort/snort.conf –i ens34*
    - Lalu lakukan ping pada interface yang menjalankan snort. Langkahnya sama dengan langkah pada *gambar 5.3,* namun bedanya command ini berjalan di daemon, sehingga tidak akan muncul output apapun
    - Setelah ping selesai dilakukan hentikan command dengan ctrl+c
    - Selanjutnya jalankan perintah ini
    - $barnyard2 –c /etc/snort/barnyard2.conf –d /var/log/snort –f snort.u2 –w /var/log/snort/barnyard2.waldo –g snort –u snort
    - Tunggu hingga proses selesai sampai dengan string “waiting for new data” lalu ctrl-c untuk menghentikan proses



*Gambar 6.4, inisialisasi barnyard*

* + Cek database mysql
    - Lakukan cek pada database dan lihat apakah event ping masuk ke tabel event dengan perintah
    - $mysql –u snort –p –D snort –e “select count(\*) from event”

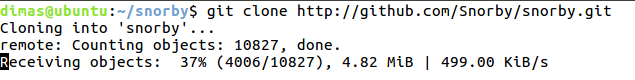


*Gambar 6.5, masuk ke mysql*

1. Instalasi Snorby

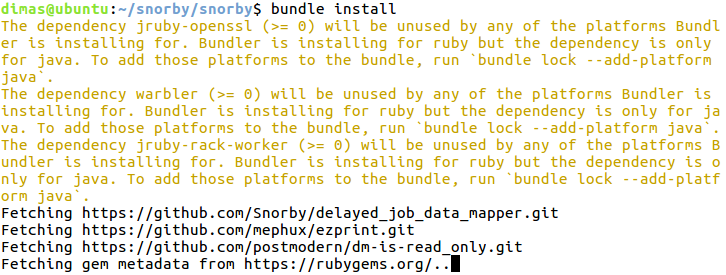
Snorby merupakan GUI untuk snort NIDS yang dapat menampilkan laporan snort ke dalam bentuk graphical user interface. Instalasasinya membutuhkan beberapa prasyarat library diantaranya adalah ruby. Langkah instalnya adalah

* + Instalasi library yang dibutuhkan snorby
    - Jalankan perintah untuk instalasi depedency ini
    - $ apt-get install apache2 git imagemagick wkhtmltopdf ruby1.9.3 libyaml-dev libxml2-dev libxslt1-dev zlib1g-dev build-essential openssl libssl-dev libmysqlclient-dev libreadline6-dev
    - $gem install rails
    - $gem update
  + Install snorby
    - $ cd /home/<user>
    - $mkdir snorby-data
    - $git clone <http://github.com/Snorby/snorby.git>



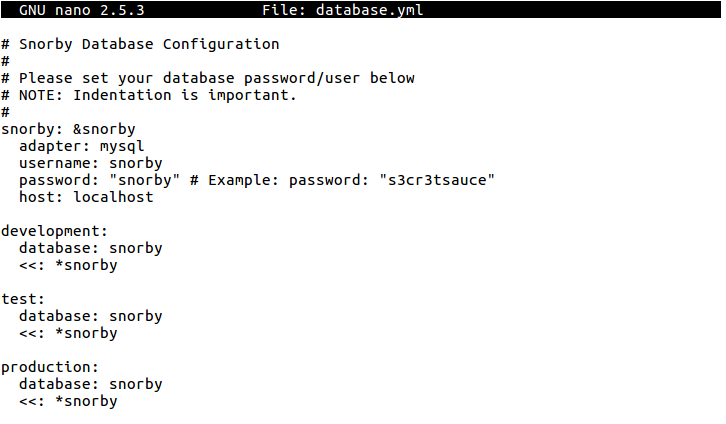
*Gambar 7.1, download snorby*

* + - $cd snorby && bundle install



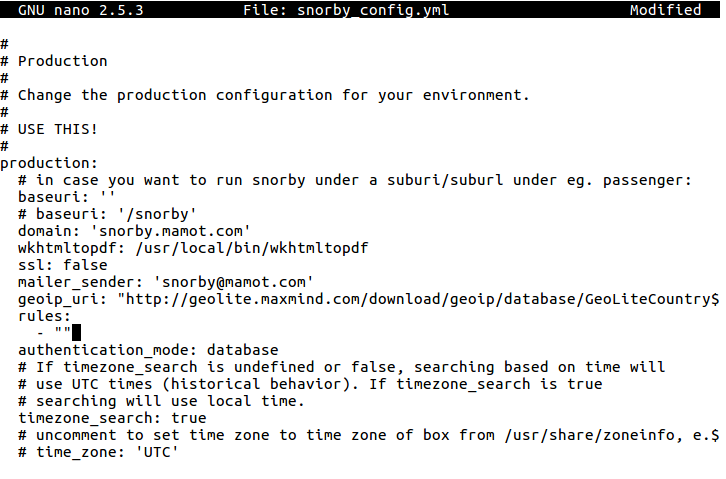
*Gambar 7.2, instalasi snorby*

* + Membuat file konfigurasi
    - Buat dua file di bawah ini pada direktori config/ yang ada di dalam snorby
    - File 1 bernama database.yml

**

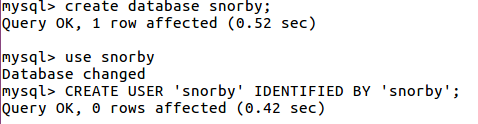
*Gambar 7.3, database.yml*

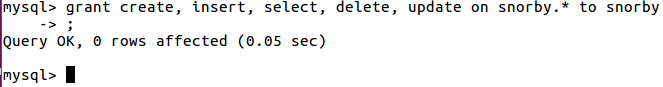
* + - File 2 bernama snorby\_config.yml



*Gambar 7.4, snorby\_config.yml*

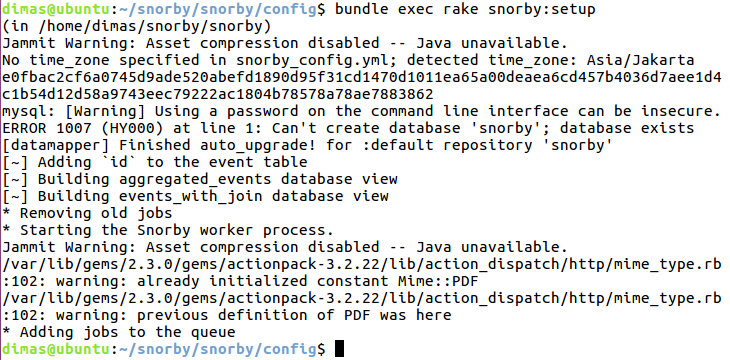
* + Membuat database account
    - Untuk mengkoneksikan snorby dengan mysql server, perlu dibuat user baru yang diberi nama snorby dan memiliki hak akses ke database bernama snorby. Password nya harus sama dengan yang sudah didefinisikan pada database.yml





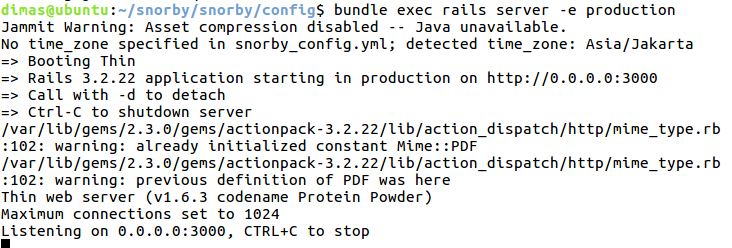
*Gambar 7.5, buat user snorby*

* + - Lalu jalankan setup untuk snorby dengan perintah ini
    - Bundle exec rake snorby:setup



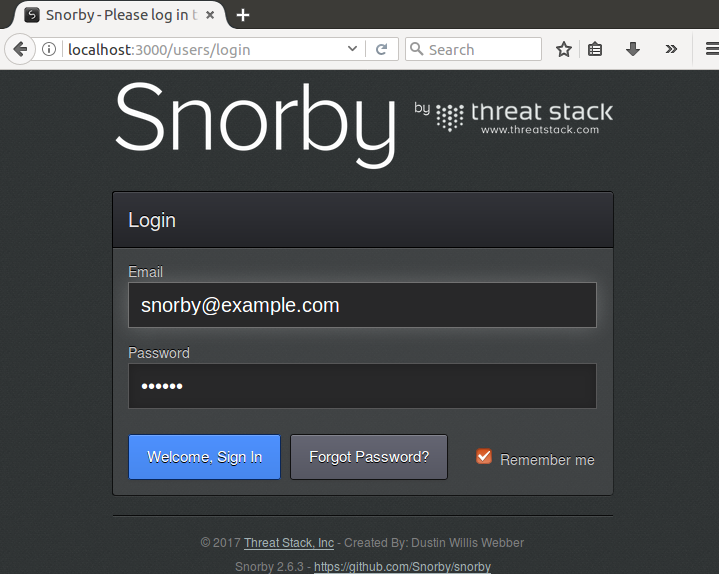
*Gambar 7.6 Setup snorby*

* + Menjalankan snorby
    - Untuk menjalankna snorby jalankan perintah
    - $bundle exec rails server –e production

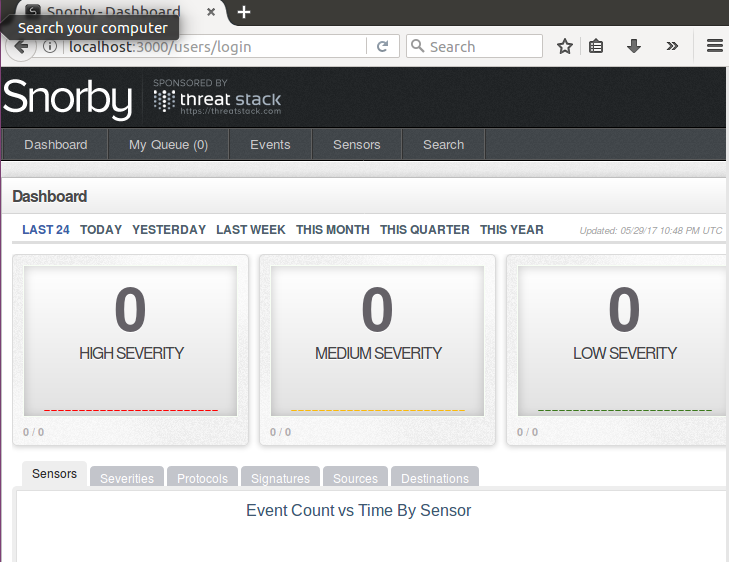


*Gambar 7.7 Snorby berjalan di port 3000*

* + - Jika telah berjalan, maka snorby dapat diakses di <http://localhost:3000>



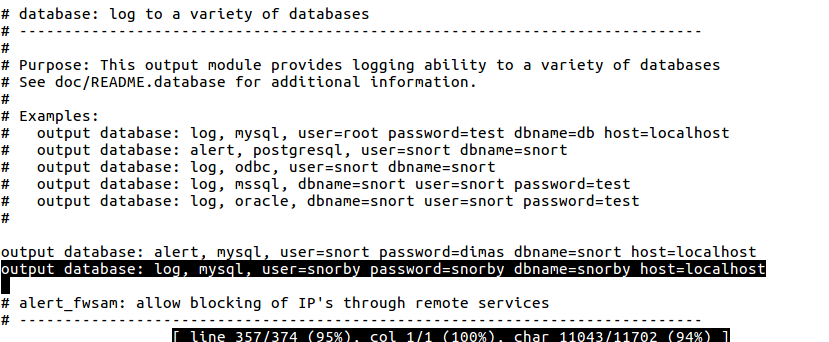
*Gambar 7.8, login snorby*

**

*Gambar 7.9, masih kosong*

Dapat dilihat pada *gambar 7.9* data pada snorby masih kosong karena belum dimasukan feed dari barnyard2 ke snorby. Langkah selanjutnya adalah konfigurasi barnyard ke snorby

* + Push event barnyard2 ke database snorby
    - Tambahkan baris berikut ke file /etc/snort/barnyard2.conf
    - output database: log, mysql, user=snorby password=s3cr3t dbname=snorby host=localhost
    - tambahkan pada baris 356



*Gambar 7.10 tambahkan konfigurasi*

* + - lalu restart service barnyard2
    - Akan terlihat pada snorby hasil dari log barnyard yang ada