# SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SNORT

**Denny Wijanarko**

*Jurusan Teknologi Informasi, Politeknik Negeri Jember*
*E-mail: dennywijanarko@gmail.com*

***ABSTRACT***

*Network security is an aspect that is always enhanced by the network administrator, the efforts both by optimizing hardware or software. Snort is a detection sensor against abuse on the network, this system functioned as a snort NIDS (Network intrusion Detection System), which works to detect any attempted intrusion (intrusions). The detection is done based on the rule that has been described by the administrator in the directory rule contained in the configuration file. Snort will analyze every packet and can record every activity performed on a network and report them if there is a potential intrusion on the network. Merging snort with SMS gateway can make the system more responsive to the potential for abuse, the log of alerts will be forwarded to the admin via SMS media, so that administrators can determine the condition of the managed network.*

**Kata Kunci**: *Snort, SMS Gateway, Keamanan*

## PENDAHULUAN

Keamanan data merupakan masalah penting bagi setiap institusi. Setiap institusi atau lembaga harus memiliki pencegahan terhadap keterbukaan akses dari pihak yang tidak berhak. Peran pertahanan sistem, pada umumnya terletak pada administrator sebagai pengelola jaringan yang memiliki akses penuh terhadap infrastruktur jaringan yang dibangunnya.

Seorang administrator bertanggung jawab terhadap semua jenis pengamanan pada jaringan, serta pemeliharaan validitas dan integritas yang diperlukan oleh pengguna. Sebuah jaringan komputer harus mampu memberikan rasa aman terhadap akses yang dilakukan oleh seorang user, dengan memberikan jaminan informasi atau data pribadi aman dari pengaksesan seorang intruder (penyerang). Keamanan sebuah server akan sulit terpantau selama
24 jam, secara manual oleh administrator jaringan. Maka sangat perlu perangkat lunak ataupun perangkat keras yang dapat membantu administrator dalam melakukan kegiatan monitoring terhadap jaringan.

IDS (*Intrusion Detection Sistem*) merupakan sebuah sistem monitoring jaringan yang berfungsi membantu administrator dalam mengamankan jaringan. IDS bisa berupa sebuah perangkat keras atau perangkat lunak.

Contoh dari IDS berbasis *opensource* yaitu snort. Snort merupakan sebuah aplikasi berbasis IDS yang mampu mengenali pola serangan berdasarkan rule yang dibuat. Setiap serangan yang diidentifikasi oleh snort akan menghasilkan alert yang nantinya alert tersebut akan diletakkan pada sebuah database sebagai kepentingan identifikasi oleh administrator.

Salah satu cara agar administrator dapat mengetahui kondisi jaringan secara langsung adalah dengan mengirimkan pesan notifikasi kepada admin tentang bahaya terjadi serangan, pesan tersebut dapat dikirim menggunakan layanan SMS gateway prinsip kerja dari SMS gateway ini adalah mengirimkan notifikasi sesuai dengan format yang ditentukan oleh administrator apabila database pada snort terisi oleh notifikasi serangan. Dengan mengirimkan notifikasi secara langsung, maka administrator akan langsung mengetahui kondisi serta ancaman terhadap jaringan yang dikelolanya.

## TINJAUAN PUSTAKA

Jaringan komputer dapat dikatakan sebagai interkoneksi antara dua atau lebih komputer melalui sebuah media transmisi baik kabel maupun nirkabel (*wireless*).

Secara umum jaringan komputer terbagi menjadi tiga kategori berdasarkan letak geografisnya yaitu:

1. LAN (*Local Area Network*) berada pada cakupan area yang kecil umumnya berada pada satu ruangan.
2. MAN (*Metropolitan Area Network*) Yang meliputi area yang lebih besar dari LAN, cakupan area lebih luas dan dalam lingkungan yang lebih besar
3. WAN (*Wide Area Network*) berada pada kawasan yang lebih luas daripada MAN, teknologi yang digunakan biasanya berupa *wireless*, ataupun menggunakan media kabel fiber optik.

**Keamanan Jaringan Komputer**

Komputer yang terhubung dengan jaringan memiliki resiko ancaman keamanan lebih besar daripada komputer yang tidak terhubung dengan jaringan. Dengan beberapa cara, jaringan komputer dapat lebih dioptimalkan dari resiko ancaman pihak yang tidak memiliki hak akses terhadap sumber yang ada pada jaringan tersebut, namun hal tersebut akan berbanding terbalik dengan kenyamanan akses pengguna, dimana tingkat keamanan yang tinggi akan membuat pengguna tidak nyaman, sedangkan tingkat keamanan yang rendah maka akses semakin nyaman. Beberapa aspek yang perlu diperhatikan untuk merancang keamanan jaringan komputer. terdapat empat aspek yaitu *privacy, integrity, authentication,* dan *availability.*

**Data Base Mysql**

Mysql adalah salah satu aplikasi manajemen database SQL. aplikasi ini bersifat gratis dan *opensource*, dalam database mysql terdapat beberapa penggunaan data dan semuanya dapat terorganisir. Mysql tidak hanya tersedia pada system operasi unix atau linux, mysql juga dapat digunakan di atas platform windows.

**SMS Gateway**

SMS gateway merupakan sebuah aplikasi yang difungsikan sebagai manajemen terhadap fitur SMS, yang dapat bermanfaat sebagai alat bantu untuk mengirimkan SMS notifikasi secara masal ataupun untuk pemanfaatan notifikasi oleh program aplikasi. SMS gateway dapat bermanfaat sebagai media interaksi antara program aplikasi dengan pengguna melalui fitur notifikasi sehingga program aplikasi ataupun perusahaan yang memanfaatkan SMS gateway dapat menjadi lebih interaktif.

**Intrusion Detection System (IDS)**

IDS merupakan aplikasi software ataupun dapat berbentuk hardware yang dapat melihat pola dari serangan-serangan yang terdapat pada jaringan Komputer. Pola tersebut berupa paket yang lewat yang teridentifikasi oleh IDS sebagai paket yang mengandung serangan ataupun ancaman pada sebuah jaringan. Terdapat dua kategori IDS yaitu network based IDS dimana jenis ini dapat menganalisa semua paket di dalam jaringan dan yang kedua disebut client based IDS yang dapat menganalisis *log file* yang berisi pola mencurigakan dari sebuah serangan terhadap suatu *client* yang lewat pada sebuah jaringan.

**Snort IDS**

Snort merupakan sebuah alat yang berfungsi untuk mencegah sebuah instruksi atau serangan pada jaringan. Dalam praktiknya snort sangat handal dalam membentuk *logging* paket-paket dan analisis trafik-trafik secara *real time* dalam jaringan yang berbasis TCP/IP.

Martin Roesch merupakan orang yang pertama kali menulis snort dan sekarang dikelola oleh Sourcefire, di mana Roesch bertindak sebagai pendiri dan CTO (Chief of Technical Officer). Versi enterprise dari snort terintegrasi dengan hardware tertentu dan jasa dukungan komersialnya dijual oleh Sourcefire.

Snort merupakan gabungan dari system analisis protocol dan system pendeteksi penyusupan (*Intrusion Detection System-IDS*), dan sangat bermanfaat sebagai system pendeteksi serangan terhadap host pada jaringan.

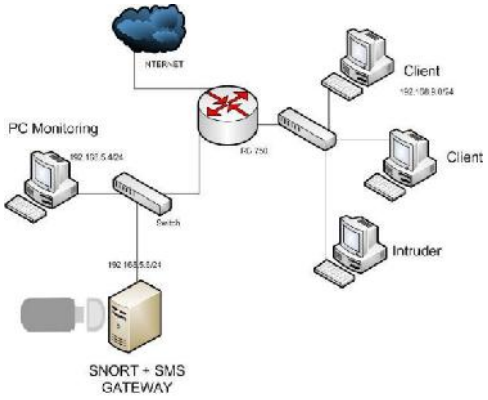
## METODOLOGI PENELITIAN

3.1 Analisis Kebutuhan

Penulis menggunakan Linux debian sebagai sistem operasi server. Switch yang diperlukan sebagai konsentrator

penghubung antara server dengan client dalam sebuah jaringan agar keduanya dapat terhubung dengan baik.

3.2 Perancangan Skema Jaringan Snort
Pada tahapan ini penulis melakukan perancangan terhadap sistem yang diinginkan. Dalam perancangan ini dibutuhkan laptop/computer server. Komputer server inilah yang nantinya dapat mendeteksi pola serangan yang dilakukan komputer client terhadap server, pada server juga dilengkapi dengan SMS Gateway menggunakan modem Huawei, penulis menggunakan modem sebagai interface dari aplikasi Gammu. Server yang digunakan menggunakan sistem operasi linux debian.




Gambar 1 Topologi Jaringan

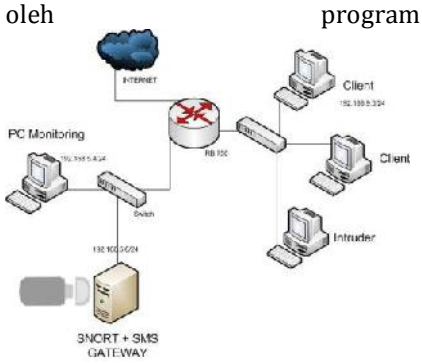
3.3 Konfigurasi Jaringan
Pada tahapan ini penulis melakukan konfigurasi awal sistem operasi server
.Server yang sudah terinstal akan dilengkapi dengan beberapa aplikasi jaringan yang lain sebagai penunjang sistem seperti samba, ftp, ssh dan lainnya. Penulis juga melakukan pemberian IP address kepada network interface server sesuai dengan rancangan topologi yang telah dibuat.
Konfigurasi yang dilakukan selanjutnya adalah melakukan instalasi snort, sebelum melakukan instalasi program, penulis telah menyiapkan beberapa dependensi yang diperlukan untuk keperluan instalasi. Setelah snort terinstal dengan baik maka hal selanjutnya yang diperlukan adalah menghubungkan database dengan program snort, sehingga semua aktivitas paket data dalam jaringan dapat direkam secara baik dan ditempatkan pada database yang telah ditentukan.

Setelah snort bekerja dengan baik maka hal yang diperlukan berikutnya adalah menempatkan sebuah program PHP dan melakukan konfigurasi terhadap gammu sebagai aplikasi SMS gateway agar dapat mengirimkan alert berdasarkan database yang diperlukan kepada administrator jaringan, sehingga administrator dapat mengetahui bahwa jaringan yang dikelola terdapat masalah yang harus diidentifikasi.

3.4 Pengujian
Penulis melakukan beberapa tahap pengujian terhadap sistem yang telah dibuat. Pengujian awal adalah dengan menguji apakah program snort yang telah dikonfigurasikan dapat bekerja dengan baik berdasarkan rule yang ditetapkan. Selain itu snort juga harus dapat melakukan pencatatan *alert* dari serangan kedalam database yang telah ditentukan.
Pengujian selanjutnya adalah dengan melakukan pengujian pada SMS gateway yang telah dikonfigurasikan pada gammu, apabila sistem dapat mengirimkan pesan alert kepada administrator maka sistem telah berjalan dengan baik.

## HASIL DAN PEMBAHASAN

Snort sebagai sistem deteksi intrusi pada jaringan menggunakan SMS Gateway adalah sistem yang dibuat dengan tuan memberikan notifikasi peringatan kepada admin apabila terjadi pencatatan sebuah event alert, sehingga admin dapat melakukan tindakan berdasarkan jenis alert yang teridentifikasi oleh program snor




Gambar 2 Topologi sistem

Pada topologi pembuatan sistem digunakan pengalamatan network yang berbeda antara server snort dengan client yang bertindak sebagai penguji sistem, dengan tujuan snort tetap dapat

mendeteksi ancaman intrusi dari network luar, atau dalam konfigurasi snort hal tersebut disebut sebagai external network.

Dalam perancangan sistem ini terdapat beberapa komponen dari penggunaan teknologi IDS snort dan SMS gateway di antaranya yaitu:

a. Sensor Snort

Sensor berfungsi memantau serta menganalisis paket pada jaringan berdasarkan rule yang terdapat pada direktori rule snort. Istilah IDS biasanya digunakan untuk IDS yang berfungsi memantau jaringan.

b. Database Server

Sebuah server database yang berfungsi untuk menyimpan semua kejadian yang dihasilkan dari pencatatan intrusi oleh snort, agar laporan tersebut dapat dimanfaatkan oleh program SMS Gateway untuk diteruskan kepada admin menggunakan program tertentu.

c. Gammu

Gammu merupakan aplikasi SMS Gateway yang berfungsi sebagai management SMS, dimana pada sistem ini gammu dimanfaatkan sebagai alat notifikasi terhadap event yang masuk kedalam database. Sehingga admin dapat mengetahui kondisi sensor secara realtime

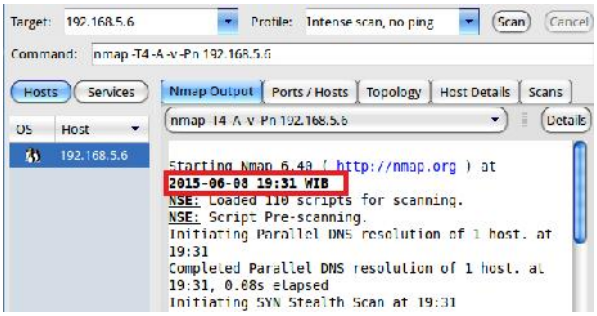
d. Program PHP

Pada sistem ini digunakan pemrograman PHP untuk melakukan perbandingan tabel antara tabel sensor snort dengan tabel pembanding apabila terdapat perbedaan maka program PHP akan mengambil sebuah tindakan untuk memberikan instruksi kepada gammu agar mengirimkan notifikasi berbentuk SMS.

## PENGUJIAN SNORT

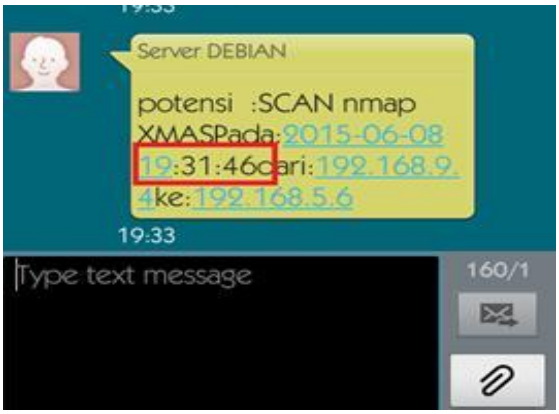
Untuk menguji sistem diperlukan sebuah skenario dengan melakukan uji coba scan menggunakan tool nmap-Zenmap GUI. Hal tersebut menandakan telah terjadi upaya penyerangan terhadap server yang dilakukan oleh salah satu client dengan melakukan scanning port dengan level TCP/IP

Pada gambar 2 terlihat pengujian menggunakan tool zenmap oleh client yang bertindak sebagai intruder berhasil mengetahui port yang terbuka pada server snort, serta waktu scan pada saat dilakukan upaya scan tersebut. Upaya tersebut dilakukan oleh client dengan IP 192.168.9.0.

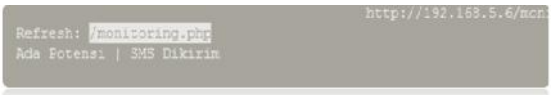



Gambar 3 Scan Zenmap

Dari upaya tersebut program PHP pada web server berhasil mendeteksi penambahan event serangan pada database sehingga browser pada server memunculkan peringatan SMS notifikasi seperti yang terlihat pada gambar 3 dan gambar 4 yang menunjukkan SMS telah terkirim kepada admin dengan detail jenis serangan, waktu serangan, dan IP sumber.




Gambar 4 SMS Notifikasi




Gambar 5 Program PHP pada browser

Pada gambar dapat terlihat notifikasi SMS dapat berhasil dikirimkan dengan keterangan jenis potensi yang berhasil ditangkap serta waktu terjadinya serangan. Dapat dipastikan bahwa server tersebut rentan terhadap aksi penyerangan pada protokol TCP/IP yang dilakukan intruder

dikarenakan banyak port yang berstatus terbuka.

## KESIMPULAN

Intrusion Detection System (IDS) berguna untuk sistem pendeteksian penyalahgunaan aktivitas pada jaringan komputer yang dilakukan sebagai upaya pelumpuhan sebuah server pada jaringan. IDS yang digunakan menggunakan snort. Dalam percobaan yang dilakukan dapat berhasil menangkap penggunaan tool scan jaringan yang berupaya mengetahui port- port yang terbuka pada server. upaya tersebut berhasil direkam oleh *sensor snort* dan disimpan dalam database yang kemudian diteruskan menggunakan aplikasi SMS gateway, dengan begitu sistem snort yang dibangun dapat bersifat lebih responsif terhadap upaya percobaan penyerangan karena admin dapat mengetahui secara *real time* terhadap kondisi jaringan yang dikelola

## DAFTAR PUSTAKA

[1] Nugroho, B. 2015. *Panduan Membuat Aplikasi Program Toko Berbasis Web Dengan PHP-Mysql dan Dreamweaver*. Yogyakarta: Penerbit Gava Media

[2] Rafiudin, R. 2012. *Mengganyang Hacker Dengan Snort*. Yogyakarta: Penerbit Andi

[3] Sofana, I. 2012. *Cisco CCNA dan Jaringan Komputer*. Bandung: Penerbit Informatika.