Sistem Deteksi Intrusi dengan Snort
(Intrusion Detection System with Snort)

Harjono[1)], Agung Purwo Wicaksono[2)]

[1) 2)]*Teknik Informatika, F. Teknik, Universitas Muhammadiyah Purwokerto*
Jl. Raya Dukuhwaluh PO. Box 202 Purwokerto 53182
[1)]harjono@ump.ac.id

Abstrak— **Jaringan komputer memberikan banyak kemudahan dalam pengaksesan informasi antar perangkat. Namun adanya jaringan juga berdampak pada kemungkinan terjadinya gangguan terhadap keamanan sistem . Penelitian ini bertujuan untuk mengembangkan sistem deteksi intrusi dengan menggunakan Snort. Pengembangan Sistem melalui tahapan analisis kebutuhan, perancangan sistem, instalasi sistem, konfigurasi sistem, dan Pengujian sistem. Hasilnya sistem IDS snort sudah berjalan dan dapat mengenali paket data yang melintas dan menghasilkan alert sesuai dengan rule yang ada. Alert yang dihasilkan tersebut dapat ditampilkan dan dianalisis dalam tampilan web.**

Kata-kata kunci— **Jaringan komputer, Keamanan, IDS Snort**

Abstract— Computer networks provide much convenience in accessing information between devices. But the existence of the network also affects the possibility of disruption to the system security. This study aims to develop an intrusion detection system using Snort. System development through the stages of requirements analysis, system design, system installation, system configuration, and system testing. The result has been running Snort IDS system and can identify data packets that pass and generate alerts in accordance with existing rules. Generated alerts can be displayed and analyzed in the web-based.

Keywords— *Computer network, Security, IDS Snort.*

I. PENDAHULUAN

Seiring dengan perkembangan komputer, perkembangan jaringan, murahnya harga perangkat, dan perkembangan aplikasi baru maka jaringan komputer semakin banyak digunakan. Jaringan komputer awalnya relatif aman karena secara fisik terpisah antara satu jaringan dengan jaringan lainnya. Namun setelah dihubungkannya satu jaringan dengan jaringan yang lain hingga terbentuk jaringan yang luas (*Wide Area Network*) maka faktor keamanan menjadi berkurang. Apalagi WAN tersebut sudah terhubung ke seluruh penjuru dunia hingga terbentuk internet.

Jaringan komputer yang terhubung ke internet memberikan banyak kemudahan dalam pengaksesan informasi dari seluruh dunia. Namun terhubungnya jaringan dengan internet justru memperbesar kemungkinan terjadinya gangguan terhadap keamanan sistem. Sebuah komputer menjadi mudah diakses dan beresiko untuk disusupi oleh pihak-pihak yang menginginkan untuk mengakses komputer tersebut. Akibatnya sistem komputer beresiko terhadap ancaman atau serangan. Hal tersebut sangat berbahaya bagi sistem komputer perusahaan yang berisi data rahasia dan hanya boleh diakses oleh orang tertentu saja. Bentuk ancaman yang mungkin terjadi adalah penyadapan atau pencurian data rahasia. Bentuk ancaman lainnya seperti dalam penelitian [1] dan juga dalam [2] adalah serangan dari *malware.* Oleh karena itu sistem jaringan komputer harus dilengkapi dengan sistem yang dapat mendeteksi adanya penyusupan atau intrusi (*intrusion*). Sistem tersebut dikenal dengan istilah *Intrusion Detection System* (IDS).

Deteksi intrusi adalah proses memantau peristiwa yang terjadi dalam sistem komputer atau jaringan dan menganalisis kemungkinan adanya insiden. Insiden merupakan pelanggaran atau ancaman pelanggaran kebijakan keamanan komputer, kebijakan penggunaan yang dapat diterima, atau praktik keamanan standar. Insiden memiliki banyak penyebab, seperti *malware* (misalnya *worm* dan *spyware*), penyerang mendapatkan akses tidak sah ke sistem dari internet, dan pengguna resmi dari sistem yang menyalahgunakan hak-hak mereka atau mencoba untuk mendapatkan tambahan hak yang bukan wewenangnya. Sebuah sistem deteksi intrusi (IDS) adalah sistem (*hardware* dan *software*) yang mengotomatisasi proses deteksi intrusi [3].

Snort adalah salah satu IDS yang *open source*. Snort terdiri beberapa komponen. Komponen-komponen ini bekerja sama untuk mendeteksi serangan tertentu dan menghasilkan *output* dalam format yang

diperlukan oleh sistem pendeteksi . Snort dirancang untuk beroperasi berbasis *command line* dan telah diintegrasikan ke beberapa aplikasi pihak ketiga dan mendukung *cross platform*. Snort menganalisis semua lalu lintas jaringan untuk menyadap (*sniff*) dan mencari beberapa jenis penyusupan dalam sebuah jaringan.

II. METODE

Perangkat lunak yang digunakan dalam penelitian ini adalah Snort yang berfungsi sebagai IDS. Perangkat lunak Snort berjalan di atas sistem operasi *Linux Ubuntu* 14.04 LTS. Selain itu juga diperlukan perangkat lunak pendukung yaitu Barnyard2, Apache, MySQL, dan BASE. Adapun perangkat keras yang diperlukan berupa komputer dengan spesifikasi yang cukup untuk menjalankan *snort* di atas Sistem Operasi *Linux Ubuntu* 14.04 LTS. Selain itu juga digunakan komputer untuk pengujian dan perangkat jaringan lainnya.

Data yang dipakai pada penelitian ini adalah data sekunder yang diambil dari penelitian [1] berupa topologi jaringan UMP. Penelitian diawali dengan melakukan analisis sistem berupa analisis kebutuhan, kemudian dilakukan perancangan sistem. Langkah selanjutnya adalah instalasi Sistem.Tahapan pertama dalam melakukan instalasi adalah instalasi serta konfigurasi perangkat jaringan yang diperlukan; kemudian instalasi Sistem Operasi Linux Ubuntu 14.04 LTS, Snort, Barnyard2, Apache, MySQL, BASE, dan library pendukung lainnya. Setelah instalasi, kemudian dilakukan konfigurasi agar antar komponen bisa saling terhubung dan bekerja sama. Langkah berikutnya adalah pengujian sistem. Pengujian dilakukan dengan cara melakukan serangan terhadap sistem yang dimonitor IDS.

III. HASIL DAN PEMBAHASAN

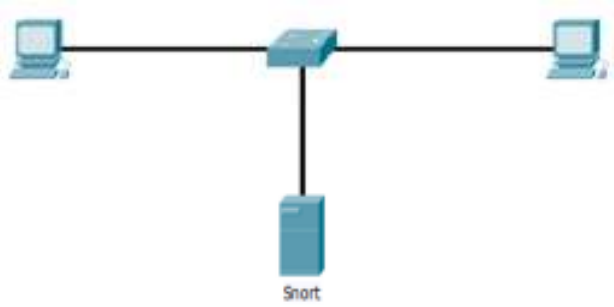
A. Analisis Kebutuhan Sistem

Analisis kebutuhan sistem merupakan proses identifikasi dan evaluasi permasalahan-permasalahan sistem yang ada sehingga dapat dikembangkan sistem baru yang sesuai dengan yang diharapkan. Sistem deteksi intrusi dengan snort dibangun untuk kebutuhan sebagai berikut :

- Sistem mampu mengidentifikasi adanya usaha-usaha intrusi atau penyusupan pada jaringan.
- Sistem dapat menyimpan *log* ke dalam *database*.
- Sistem dapat menampilkan *log* dari *database* melalui antarmuka web.

B. Perancangan Sistem

Sistem deteksi intrusi dengan snort ditempatkan dalam jaringan untuk mendeteksi adanya intrusi pada sistem yang dipantau. Oleh karenanya snort harus bisa menyadap semua data dari sistem yang dipantau, baik data yang masuk maupun data yang keluar. IDS snort dihubungkan dengan *span port* dari switch yang dapat menangkap lalu lintas data dari jaringan yang dipantau seperti pada Gambar 1.



Gambar 1. Rancangan Sistemada

C. Instalasi Sistem

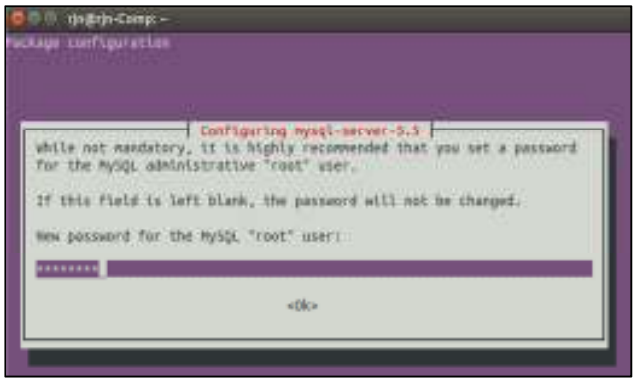
Tahap awal dalam melakukan instalasi IDS adalah menyiapkan dan melakukan instalasi perangkat jaringan seperti pada gambar 1. IDS snort digunakan untuk memantau serangan yang ditujukan pada sistem dengan IP 192.168.137.224. Oleh karena itu snort harus diinstal pada sistem dan dihubungkan dengan *spanning port* pada switch yang dapat memantau lalu lintas data yang menuju dan meninggalkan komputer 192.168.137.224.

Tahap berikutnya adalah melakukan instalasi sistem operasi yang digunakan untuk menjalankan snort, yaitu linux Ubuntu 14.04 LTS. Setelah sistem operasinya terinstal, langkah selanjutnya adalah melakukan instalasi snort. Instalasi dilakukan secara *online* terhubung internet. Instalasi berikutnya adalah instalasi Barnyard2. Barnyard2 merupakan *tool open source* sebagai penerjemah (*interpreter*) *alert unified* dan log dari Snort. Barnyard2 dapat meningkatkan efisiensi Snort dengan cara mengurangi beban pada sensor deteksi. Barnyard2 bekerja dengan membaca Snort's *unified logging output files* dan memasukannya kedalam *database*. Jika *database* tidak tersedia maka Barnyard2 akan memasukan semua data ketika *database* tersedia kembali sehingga tidak ada alert atau log yang hilang.

Selanjutnya dilakukan instalasi MySQL, yang digunakan untuk menyimpan dan mengelola *database*. Gambar 2 menunjukkan proses kofigurasi password untuk user MySQL.

Istalasi berikutnya adalah instalasi apache sebagai web server dan BASE yang merupakan tool untuk

melakukan analisis trafik yang dihasilkan snort. Proses instalasi BASE seperti terlihat pada Gambar 3.



Gambar 2. Konfigurasi Password User MySQL

Gambar 3. Instalasi BASE

D. Konfigurasi Sistem

Setelah proses instalasi selesai, tahap berikutnya adalah melakukan konfigurasi sistem. Yang pertama harus dilakukan konfigurasi terhadap file snort.conf yang berada pada direktori /etc/snort/ dengan menggunakan perintah:

sudo gedit /etc/snort/snort.conf

Snort harus dikonfigurasi untuk memantau lalu-lintas data dari sistem yang dikehendaki yaitu alamat jaringan 192.168.137.0/24.

Konfigurasi terhadap Barnyard2 juga dilakukan pada file barnyard2.conf yang berada pada direktori /etc/snort. Konfigurasi ini dilakukan supaya barnyard2 dapat membaca log yang dihasilkan snort dan memasukkannnya ke dalam *database*. Di sini harus ditentukan *user, password*, *dbname*, serta *host* yang sesuai dengan kofigurasi pada MySQL.

E. Pengujian Sistem

Pengujian sistem dilakukan untuk mengetahui apakah sistem dapat berjalan sesuai dengan yang diharapkan. Untuk mengetahui apakah snort berjalan dan dapat mendeteksi intrusi pada sistem yang dipantau, dilakukan dengan cara melakukan *ping* dan juga mengakses web pada sistem yang dipantau. Namun sebelumnya harus dilakukan konfigurasi rule snort. Agar ketika pengujian dapat dihasilkan *alert* yang sesuai. Guna tujuan di atas maka dilakukan perubahan terhadap file /etc/snort/rules/local.rules dengan dua *rule* berikut.

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Test
    NOW!!!"; classtype:not-suspicious; sid:1000001;
    rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:"HTTP Test
    NOW!!!";classtype:not-suspicious;
    sid:1000002; rev:1;)
```

Rule pertama akan menghasilkan *alert* jika ada lalu lintas ICMP dari sembarang IP dan sembarang port yang menuju HOME_NET (yaitu 192.168.137.0/24) sembarang port, dan menampilkan pesan "*ICMP Test NOW*!!!" dengan klasifikasi *Not Suspicious* dan *sid* 1000001:1. Sedangkan rule kedua menghasilkan alert jika ada traffic TCP dari sembarang IP dan sembarang port yang menuju HOME_NET (yaitu 192.168.137.0/24) port 80, dan menampilkan pesan "*HTTP Test NOW*!!!" dengan klasifikasi *Not Suspicious* dan *sid* 1000002:1.

Saat dilakukan ping dari komputer dengan IP 192.168.137.233 dihasilkan alert pada IDS snort seperti berikut.

```
08/07-10:11:44.462390 [**] [1:1000001:1] ICMP Test
NOW!!! [**] [Classification: Not Suspicious Traffic]
[Priority: 3] {ICMP} 192.168.137.233 ->
192.168.137.224
```

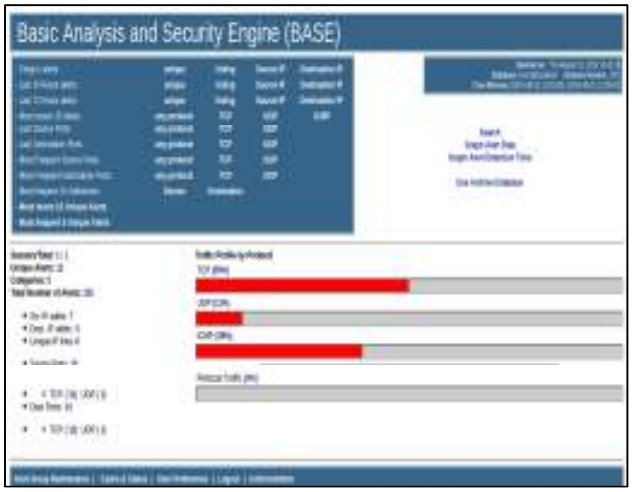
Dan saat dilakukan test HTTP dari komputer dengan IP 192.168.137.233 dihasilkan alert berikut.

```
08/07-10:16:33.566905 [**] [1:1000002:1] HTTP Test
NOW!!! [**] [Classification: Not Suspicious Traffic]
[Priority: 3] {TCP} 192.168.137.233:49699 ->
192.168.137.224:80
```

Dari pengujian tersebut terlihat bahwa sistem IDS snort sudah berjalan dan dapat mengenali paket data yang melintas dan menghasilkan *alert* sesuai dengan *rule* yang telah dibuat sebelumnya. Adapun tampilan BASE setelah dilakukan uji penetrasi terlihat seperti Gambar 4.

Terlihat dari tampilan Base menunjukkan alert yang dihasilkan oleh IDS snort. Klasifikasi traffic berdasarkan protokolnya ditunjukkan dengan bar merah. Masing-masing dapat dilihat rinciannya seperti Gambar 5 yang menunjukan rincian dari protokol TCP. Kolom pertama dan kedua menunjukkan id alert dan signature. Kolom ketiga menunjukan waktu terjadinya intrusi.

Kolom keempat dan kelima menunjukkan alamat sumber dan tujuan beserta nomor portnya. Sedangkan kolom terakhir menunjukkan protokolnya.



Gambar 4. Tampilan BASE

Gambar 5. Rincian Alert untuk Protokol TCP

Untuk sistem deteksi intrusi dengan snort ini, rule yang digunakan dapat diperoleh di web snort yaitu di www.snort.org. Rule tersebut harus selalu diperbarui (*update*) agar jika ada intrusi jenis baru dapat dideteksi oleh snort. Berbeda dengan sistem pendeteksi serangan menggunakan *honeypot* seperti pada penelitian [1} dan [2], pada sistem dengan snort ini lebih banyak menghasilkan *false positif*. *False positif* ini adalah adanya paket data yang sebenarnya bukan paket berbahaya tetapi oleh snort dianggap berbahaya atau sebuah intrusi. Akibatnya log atau alert yang dihasilkan oleh snort jauh lebih banyak dibandingkan dengan log yang dihasilkan oleh honeypot.

IV. PENUTUP

A. Kesimpulan

Dari hasil penelitian, dapat ditarik kesimpulan bahwa telah berhasil dibangun sebuah sistem deteksi intrusi dengan snort yang dapat mendeteksi intrusi pada sistem yang dipantau. Sistem dapat menghasilkan *log* yang tersimpan di dalam *database*. Selain itu, *Alert* yang dihasilkan dapat ditampilkan dan dianalisis dalam tampilan web.

B. Saran

Sistem deteksi intrusi bersifat pasif, artinya sistem ini hanya dapat mendeteksi jika ada serangan saja dan tidak dapat melakukan tindakan pencegahan. Untuk berikutnya dapat dikembangkan sebuah sistem yang dapat mendeteksi serangan sekaligus malakukan tindakan pencegahan terhadap serangan serupa.

DAFTAR PUSTAKA

[1] Harjono dan Pinandita, T. 2012. Deteksi Malware di Jaringan Lokal Universitas Muhammadiyah Purwokerto Menggunakan Dionaea. *Laporan Penelitian*. FT-UMP. Purwokerto.

[2] Harjono dan Wicaksono, A.P. 2013. Honeyd untuk Mendeteksi Serangan Jaringan di Universitas Muhammadiyah Purwokerto. JUITA ISSN: 2086-9398 Vol. II Nomor 4, Nopember 2013.

[3] Scarfone, K. and Mell, P. 2007. *Guide to Intrusion Detection and Prevention System (IDPS)*. National Institute of Standards and Technology. USA.