Universitas Labuhanbatu
Vol. 6 No.3 / September/2018
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

IMPLEMENTASI SNORT *INTRUSION DETECTION SYSTEM* (IDS) PADA SISTEM JARINGAN KOMPUTER

Muhammad Halmi Dar[1)]
Dosen Manajemen Informatika Fakultas Sains dan Teknologi, Universitas Labuhanbatu
e-mail: mhd.halmidar@gmail.com

Syaiful Zuhri Harahap[2)]
Dosen SistemInformasi Fakultas Sains dan Teknologi, Universitas Labuhanbatu
e-mail: syaifulzuhriharahap@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk merancang sebuah sistem keamanan jaringan komputer dengan menerapkan Snort *Intrusion Detection System* (IDS). Sistem keamanan jaringan yang dibangun mengintegrasikan antara *Intrusion Detection System* (IDS), *Database System*, dan *Monitoring System*. Dalam skema pengujian, sistem terdiri dari dua jenis, yaitu *server* dan *client*. *Server* berfungsi sebagai target serangan dan sekaligus digunakan untuk melakukan pemantauan terhadap jaringan. Sedangkan *client* berfungsi sebagai *intruder* (penyusup). Metode serangan yang diterapkan pada lingkup pengujian adalah *Port Scanning* dan *Denial of Service* (DoS). Dari hasil pengujian yang telah dilakukan, Snort-IDS mampu menganalisis paket-paket yang melewati jaringan dan berusaha menentukan apakah terdapat paket-paket data yang berisi aktivitas mencurigakan atau tidak. Dari data hasil pengujian yang diperlihatkan oleh *Basic Analysis and Security Engine* (BASE), didapatkan bahwa *intruder* melakukan *port scanning* sebanyak 28%, *TCP attack* 62%, *UDP attack* sebanyak 1%, dan *ICMP attack* sebanyak 9%. *Unique Alerts* yang dihasilkan terbagi kepada dua kategori yaitu, *unclassified* sebanyak 28% dengan jumlah 74, dan *attempted-dos* sebanyak 72% dengan jumlah 189.

Kata kunci: Jaringan Komputer, Keamanan Jaringan, Sistem Deteksi Penyusupan, NIDS, Snort, Denial of Service (DoS).

ABSTRACT

This study aims to design a computer network security system by applying the Snort Intrusion Detection System (IDS). Network security system that is built integrates the Intrusion Detection System (IDS), Database System, and Monitoring System. In the test scheme, the system consists of two types, namely server and client. The server functions as a target of attack and is simultaneously used to monitor the network. While the client functions as an intruder. The attack methods applied in the test scope are Port Scanning and Denial of Service (DoS). From the results of tests that have been done, Snort-IDS is able to analyze packets that pass through the network and try to determine whether there are data packets that contain suspicious activity or not. From the test data shown by the Basic Analysis and Security Engine (BASE), it is found that intruders do port scanning as much as 28%, TCP attacks 62%, UDP attacks as much as 1%, and ICMP attacks as

much as 9%. The resulting Unique Alerts are divided into two categories, 28% unclassified with 74, and 72% attempted dosage with 189.

Keywords: Computer Network, Network Security, Intrusion Detection System, NIDS, Snort, Denial of Service (DoS).

1. PENDAHULUAN

Ketika sebuah komputer terhubung dalam jaringan komputer, baik secara lokal maupun melalui internet, komputer tersebut berpotensi untuk disusupi. Melihat begitu berharganya suatu informasi, tidaklah heran jika bermunculan serangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Pihak-pihak tersebut dapat melakukan penyusupan dengan tujuan untuk mencuri, mengubah dan merusak informasi yang ada pada suatu komputer. Penyusupan (*intrusion*) adalah suatu usaha yang dilakukan untuk kompromi terhadap integritas dari suatu sumber daya komputer. Tujuan dari usaha tersebut agar sistem komputer dapat dirusak dan disalahgunakan. Defenisi ini tidak bergantung pada sukses atau gagalnya aksi penyusupan, melainkan ada atau tidaknya aksi yang dilakukan tanpa adanya otoritasi ataupun *abuse of privilege* dari *user* yang sah[1].

Tugas Administrator Jaringan memiliki fungsi vital yang berkaitan dengan keamanan jaringan. Apabila gangguan keamanan yang terjadi sudah dapat melumpuhkan sistem jaringan, maka seorang Administrator Jaringan tidak dapat melakukan pemulihan sistem secara cepat. Salah satu cara yang dapat dilakukan untuk mengatasi masalah tersebut adalah dengan membangun sebuah sistem pendeteksi penyusupan, atau yang dikenal dengan istilah *Intrusion Detection System* (IDS).

Sistem Deteksi Penyusupan (*Intrusion Detection System*) adalah sistem yang mampu melakukan pendeteksian terhadap serangan dan ancaman yang terjadi pada sebuah jaringan komputer, baik yang terhubung pada jaringan lokal maupun dengan jaringan internet[2]. IDS akan memberikan peringatan dini kepada Administrator Jaringan ketika terjadi sebuah aktivitas yang mencurigakan (anomali) pada jaringan komputer. Selain memberikan peringatan dini, IDS juga mampu melacak dan menentukan jenis aktivitas apa saja yang merugikan sebuah sistem jaringan komputer.

Implementasi IDS pada sistem jaringan komputer telah dilakukan oleh beberapa peneliti sebelumnya. Sugiantoro dan Istianto (2010), menerapkan metode keamanan jaringan dengan mengintegrasikan antara *Intrusion Detection System* (IDS), *Firewall System*, *Database System,* dan *Monitoring System* yang dikaitkan dengan tinjauan *agent* bergerak. Dari penelitian tersebut, dihasilkan sebuah arsitektur sistem deteksi penyusupan yang mampu mendeteksi adanya aktivitas yang mencurigakan, dan melakukan tindakan penanggulangan serangan lebih lanjut berbasis agent bergerak[3]. Penerapan IDS dan IPS dalam keamanan jaringan komputer telah dilakukan oleh Rasyid, et.al (2011), hasil yang didapatkan bahwa IDS mampu melakukan pendeteksian terhadap penyusupan pada jaringan komputer, dan memberikan peringatan dini akan adanya penyusupan tersebut[4].

Ada banyak jenis IDS yang berkembang saat ini, antara lain: *RealSecure* dari *Internet Security Systems (ISS), Cisco Secure Intrusion Detection System* dari *Cisco Systems, eTrust Intrusion Detection* dari *Computer Associates*, dan *Symantec Client Security* dari

Symantec. Namun ada IDS yang bersifat *OpenSource* yaitu, Snort. Snort merupakan jenis *Network Intrusion Detection System* (NIDS) yang bekerja dengan menganalisa paket-paket yang melintasi jaringan. Di dalam Snort terdapat *database* yang memuat *rules* yang dikategorikan sebagai penyusupan. Snort menerapkan metode analisa *signatures* dan *anomaly detection*. Metode *signatures* bekerja dengan membandingkan antara *rules* sebuah *traffic* yang sedang dideteksi dengan *traffic* yang mengidentifikasikan terjadinya penyerangan. Sedangkan metode *anomaly* bekerja dengan membandingkan antara *rules* yang berisi *traffic* normal dengan *traffic* yang sedang dideteksi.

2. LANDASAN TEORI

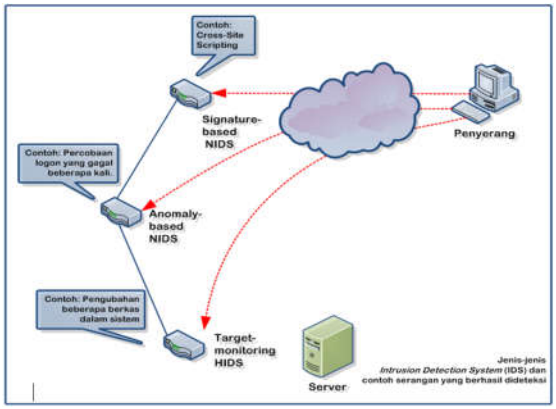
2.1 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah sistem pencegahan dengan menggunakan *software* atau *hardware* yang bekerja secara otomatis untuk memonitor keadaan pada jaringan komputer dan dapat menganalisis masalah keamanan jaringan. IDS adalah *tools*, metode, dan sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer[5].

Kemampuan dari IDS adalah memberikan peringatan dini kepada Administrator Jaringan saat terjadinya sebuah aktivitas tertentu yang tidak diinginkan Administrator sebagai penanggung jawab suatu sistem. Selain memberikan peringatan, IDS juga mampu melacak aktivitas yang merugikan suatu sistem. Suatu IDS dapat melakukan pengamatan (*monitoring*) terhadap paket-paket yang melewati jaringan dan berusaha menemukan apakah terdapat paket-paket yang berisi aktivitas-aktivitas yang mencurigakan.

Intrusion Detection System berfungsi melakukan pengamatan terhadap kegiatan-kegiatan yang tidak lazim pada jaringan sehingga awal dari langkah para penyerang bisa diketahui. Dengan demikian Administrator bisa melakukan tindakan pencegahan dan bersiap atas kemungkinan yang akan terjadi.

Dalam mengenali pola serangan, ada beberapa metode bagaimana IDS bekerja yaitu: *Signature Based* IDS dan *Anomaly Based* IDS.



Gambar 1. Cara kerja IDS

A. *Signature Based* IDS

IDS yang berbasis pada *signature* akan melakukan pengawasan terhadap paket-paket dalam jaringan dan melakukan pembandingan terhadap paket-paket tersebut dengan basis data *signature* yang dimiliki oleh sistem IDS ini atau atribut yang dimiliki oleh percobaan serangan yang pernah diketahui. Cara ini hampir sama dengan cara kerja aplikasi antivirus dalam melakukan deteksi terhadap *malware*. Intinya adalah akan terjadi keterlambatan antara terdeteksinya sebuah serangan di internet dengan *signature* yang digunakan untuk melakukan deteksi yang diimplementasikan didalam basis data IDS yang digunakan. Jadi bisa saja basis data *signature* yang digunakan dalam sistem

IDS ini tidak mampu mendeteksi adanya sebuah percobaan serangan terhadap jaringan karena informasi jenis serangan ini tidak terdapat dalam basis data *signature* sistem IDS ini. Selama waktu keterlambatan tersebut sistem IDS tidak dapat mendeteksi adanya jenis serangan baru.

B. *Anomaly Based* IDS

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai *Anomaly-based* IDS. IDS jenis ini akan mengawasi lalu lintas dalam jaringan dan melakukan perbandingan lalu lintas yang terjadi dengan rata-rata lalu lintas yang ada (stabil). Sistem akan melakukan identifikasi apa yang dimaksud dengan jaringan "normal" dalam jaringan tersebut, berapa banyak *bandwidth* yang biasanya digunakan di jaringan tersebut, protokol apa yang digunakan, port-port dan alat-alat apa saja yang biasanya saling berhubungan satu sama lain didalam jaringan tersebut, dan memberi peringatan kepada administrator ketika dideteksi ada yang tidak normal.

Metode *anomaly-based* IDS menawarkan kelebihan dibandingkan *signatue-based* IDS, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam *database signature* IDS. Kelemahannya adalah jenis ini sering mengeluarkan pesan *false positive*. Sehingga tugas Administrator menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya *false positive* yang muncul.

2.2 Snort

Snort merupakan sebuah aplikasi sekuriti yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Dalam praktiknya, snort sangat andal untuk membentuk *logging* paket-paket dan analisis trafik-trafik secara *real-time* dalam jaringan-jaringan berbasis TCP/IP[6]. Snort ditulis oleh Martin Roesch dan sekarang dikelola oleh Sourcefire, dimana Roesch bertindak sebagai pendiri dan CTO (*Chief of Technical Officer*-Kepala Tim Teknis). Snort tersedia bebas dalam bentuk *source code* di bawah lisensi GNU General Public License.

Secara prinsip, snort dapat dioperasikan dalam tiga mode[7]:

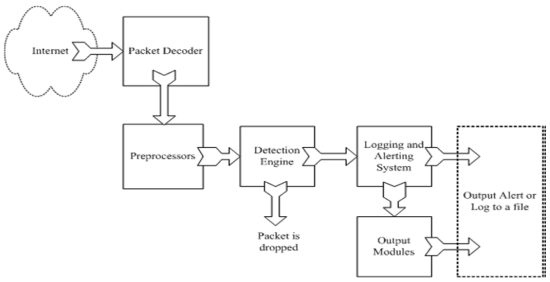
1. *Packet sniffer*: untuk melihat paket-paket yang lewat di jaringan.
2. *Packet logger*: untuk mencatat semua paket-paket yang lewat di jaringan, untuk dianalisis di kemudian hari.
3. NIDS, deteksi penyusup pada network: pada mode ini snort akan berfungsi sebagai pendeteksi serangan yang dilakukan melalu jaringan komputer. Untuk menggunakan mode IDS ini diperlukan pengaturan dari berbagai aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

Snort dibagi menjadi menjadi beberapa komponen. Komponen ini bekerjasama untuk mendeteksi serangan dan untuk menghasilkan output dalam format yang diperlukan dari deteksi sistem. Sebuah IDS berbasis Snort terdiri dari komponen utama sebagai berikut:

- Packet Decoder
- Preprocessors

Informatika : Fakultas Sains dan Teknologi
Universitas Labuhanbatu
Vol. 6 No.3 / September/2018
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

- Detection Engine
- Logging and Alerting System
- Output Modules



Gambar 2. Komponen-komponen snort

Gambar 2 menunjukkan bagaimana komponen-komponen snort disusun. Setiap paket data yang datang dari Internet masuk melalui *packet decoder*. Dalam perjalanan paket data menuju *output modules*, sebagian dari paket dibuang, dan sebagian lainnya menjadi output berupa *log* atau menghasilkan sebuah peringatan.

3. METODE PENELITIAN

Tahapan penelitian yang dilakukan pada pembuatan sistem deteksi penyusupan ini meliputi: analisis kebutuhan sistem, perancangan diagram blok sistem, instalasi dan konfigurasi, dan pengujian sistem.

3.1 Analisis Kebutuhan Sistem

Tujuan utama dari analisis kebutuhan sistem ini adalah untuk mendapatkan informasi rinci yang dibutuhkan sebelum melakukan perancangan dan uji coba sistem. Sistem yang akan dibangun merupakan kombinasi dari perangkat keras dan perangkat lunak.

A. Kebutuhan Perangkat Keras

Perangkat keras yang digunakan dalam perancangan jaringan ini meliputi beberapa komponen. Adapun komponen-komponen utama yang digunakan adalah:

1. Dua buah komputer dengan fungsi sebagai berikut:
   a) *Server* (korban)
   b) *Intruder* (penyusup)
2. Kabel UTP

B. Kebutuhan Perangkat Lunak

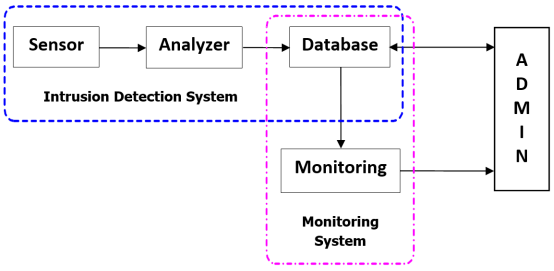
Pemilihan sistem operasi dimaksudkan untuk mempermudah dalam pengimplementasian sistem. Sistem operasi yang digunakan adalah:

1. Distribusi Linux Ubuntu 9.10 (*server*)
2. Windows XP Professional Service Pack 3 (*Intruder*)

Untuk membangun sistem deteksi penyusupan diperlukan beberapa komponen perangkat lunak yang perlu diintegrasikan menjadi satu kesatuan sistem. Komponen-komponen tersebut meliputi: Snort, Apache, MySQL, PHP, ADODB, BASE dan Barnyard2.

3.2 Perancangan Diagram Blok Sistem

Sistem keamanan jaringan yang dibangun membentuk suatu arsitektur sistem yang terintegrasi antara *Intrusion Detection System* (IDS), *Database System,* dan *Monitoring System*. Untuk lebih jelasnya dapat dilihat pada gambar berikut.



Gambar 3. Diagram blok sistem

A. Sistem Deteksi Penyusupan

Intrusion Detection System (IDS) yang dirancang terdiri dari komponen-komponen sebagai berikut:

1. Sensor
   Sensor merupakan deteksi dini dari sistem keamanan yang dirancang. Di dalam modul sensor terdapat dua bagian yaitu *Decoder* dan *Preprocessors* dimana masing-masing mempunyai tugas yang berbeda namun saling berhubungan dalam melakukan kinerjanya.
   a) *Decoder* berfungsi untuk mengambil data dari jaringan sesuai paket data yang di-*capture* dalam bentuk struktur data dan melakukan identifikasi protokol dan *decode* IP, seperti nomor port dan alamat IP.
   b) *Preprocessors* berfungsi mengambil paket yang mempunyai potensi berbahaya untuk kemudian dikirim ke *Analyzer* untuk dikenali polanya, apakah termasuk paket berbahaya atau tidak.

2. Analyzer
   Analyzer berfungsi untuk menganalisa paket data yang dikirim oleh sensor dengan menentukan apakah paket data tersebut tergolong paket serangan atau bukan, cara menentukannya adalah dengan mencocokkan paket data dengan pola yang sama yang ada di *rules files*, jika terdapat kesamaan pola maka *Analyzer* mengirim respons kepada *output plug-ins* untuk kemudian dikirim ke admin.

3. Database
   Snort digunakan untuk sistem deteksi dan analisis paket yang menempatkan aturan-aturannya pada sebuah *list* (daftar) di *database* sistem dengan metode pengolahan paket. Fungsi dasar dari Snort itu sendiri adalah untuk mengumpulkan kode-kode dari suatu paket yang polanya dikenali dari *rule* dan *signature* yang disimpan di dalam suatu folder dalam bentuk *file log* kemudian ditransfer ke *database* dengan menggunakan fasilitas Adodb. *File log* yang disimpan bisa dipelajari untuk melakukan antisipasi di kemudian hari agar kejadian yang sama tidak terulang lagi.

B. Sistem Database

Sistem keamanan yang akan dibangun menggunakan prinsip sentralisasi *database* untuk menyimpan semua *alert* yang berasal dari sensor. Informasi yang tersimpan pada *database* ini juga merupakan input untuk pengawasan keamanan jaringan yang dilakukan oleh sistem monitoring. *Database* yang digunakan adalah Mysql yang diinstall pada sistem operasi Linux Ubuntu 9.10.

C. Sistem Monitoring

Monitoring BASE merupakan aplikasi berbasis *web*, sehingga semua informasi keadaan keamanan jaringan berupa *alert* dari sensor dapat dianalisa melalui aplikasi *web browser* (seperti: Mozilla Firefox, Opera, dll). Informasi ini akan menjadi bahan audit sekuriti. Audit sekuriti perlu dilakukan agar keamanan jaringan tetap terjamin dan untuk mendapatkan solusi keamanan jaringan yang lebih baik.

3.3 Instalasi dan Konfigurasi

Sistem yang akan diimplementasikan membutuhkan beberapa tahapan instalasi dan konfigurasi dari beberapa komponen perangkat lunak[8]. Hal ini dilakukan agar sistem dapat bekerja dengan baik. Berikut diagram tahapan instalasi dan konfigurasi sistem.

Gambar 4. Instalasi dan konfigurasi

A. Instalasi dan Konfigurasi Snort IDS

Dalam menginstall dan mengkonfigurasi Snort IDS diperlukan berbagai macam aplikasi pendukung. Adapun aplikasi-aplikasi pendukung tersebut diantaranya adalah:

1. Pcap (*packet capture*)
2. Pcre (*perl compatible regular expression*)
3. SSH (*secure shell*)

Aplikasi pcap terdiri dari *application programming interface* untuk menangkap lalu lintas paket. Linux menempatkan pcap pada pustaka libpcap. Snort menggunakan libpcap untuk menangkap paket yang melintas dalam suatu jaringan dan mendapatkan daftar antarmuka jaringan yang dapat digunakan. Libpcap juga dapat menyimpan paket yang telah ditangkap ke dalam suatu file dan membaca isi di dalamnya. File yang telah ditangkap, disimpan dalam pustaka yang dapat dihubungkan dengan tcpdump. File yang telah disimpan dalam format libpcap dapat digunakan oleh aplikasi lain.

Library pcre merupakan *library* yang menggunakan pencocokan pola ekspresi yang hampir sama dengan Perl. Sebagai tambahan fungsi pencocokan, pcre memiliki fungsi yang berbeda dalam pencocokan pola kompilasi yang sama. Sedangkan SSH (*secure shell*) merupakan protokol jaringan yang memungkinkan pertukaran data menggunakan saluran yang aman antara dua perangkat jaringan.

B. Instalasi dan Konfigurasi Sistem Database

Konfigurasi paket Snort untuk *login* ke *remote* MySQL *server* pada antarmuka grafis berbasiskan *web* dapat digunakan untuk melihat paket yang telah terdeteksi dan statistiknya.

Pada paket instalasi Snort terdapat sebuah file create_mysql, yang memiliki skema untuk *database*. Pada saat menginstal Linux, file ini akan ditemukan di /usr/share/doc/snort. *Extract* dan *install* file tersebut agar penambahan tabel tambahan yang diperlukan snort dapat digunakan.

C. Instalasi dan Konfigurasi Sistem Monitoring

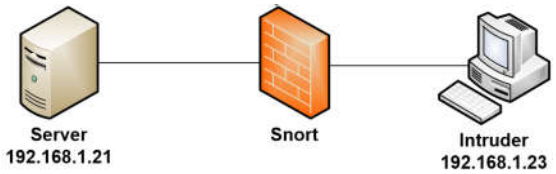
Untuk mengumpulkan dan menyajikan informasi *alert* pada Snort, digunakan BASE. Versi BASE yang digunakan adalah versi 1.4.4. BASE yang merupakan sekumpulan skrip PHP memerlukan program-program pendukung berikut:

- Apache
- PHP versi 4.0 atau yang terbaru.
- ADODB (*Active Data Objects Data Base*)

3.4 Pengujian Sistem

Untuk melakukan pengujian terhadap sistem yang telah dibuat, terlebih dahulu dibuat skema perancangan. Skema ini digunakan untuk mempermudah dalam melakukan analisis pada lingkungan

implementasinya. Skema perancangan tersebut dapat dilihat pada gambar berikut:



Gambar 5. Skema lingkungan pengujian

Jaringan yang digunakan pada lingkungan pengujian adalah sebuah jaringan *Local Area Network* (LAN) dengan dua buah komputer yang masing-masing berfungsi sebagai *Server* dan *Intruder*.

- *Server*. Komputer ini telah dilengkapi dengan program Snort *Intrusion Detection System* (NIDS) dengan alamat IP 192.168.1.21 dan sekaligus digunakan sebagai target serangan.

- *Intruder*. Komputer ini sebagai host yang akan melakukan serangan terhadap *server* dengan alamat IP 192.168.1.23.

Pengujian sistem keamanan dilakukan untuk melihat sejauh mana Snort-IDS mampu mendeteksi aktivitas-aktivitas ilegal yang dilakukan oleh penyusup. Adapun jenis-jenis serangan yang dilakukan untuk menguji sistem ini adalah sebagai berikut:

1. Port Scanning

   Port adalah tempat keluar masuk suatu layanan komputer yang sedang berjalan. Dengan melakukan *port scanning,* didapatkan informasi mengenai port-port apa saja yang terbuka. NetTools adalah *utility* yang digunakan untuk menemukan port yang terbuka. Setelah diketahui port mana saja yang terbuka, maka dapat dilakukan serangan ke tahap selanjutnya.

2. Denial of Service (DoS)

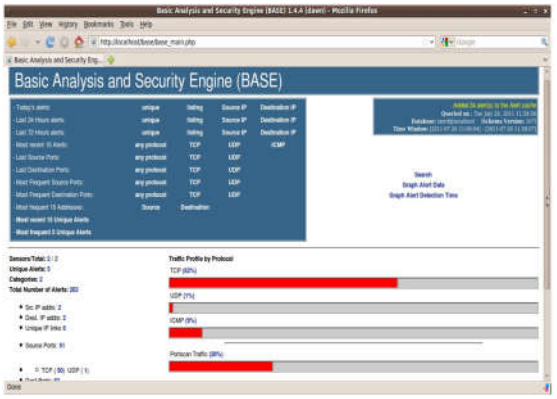
   DoS merupakan suatu metode penyerangan dengan membanjiri permintaan palsu ke mesin *server* secara bertubi-tubi. *Server* dikirimi permintaan secara terus-menerus sehingga *server* tidak dapat melayani permintaan lain atau bahkan sampai *down*, *hang*, atau *crash*. Jenis -jenis serangan kategori DoS yang akan diterapkan adalah:

   a. *Ping Flood*, dengan tujuan meningkatkan kinerja sistem sampai batas maksimal sehingga *traffic* pada jaringan menjadi penuh.
   b. *Syn Attack*, setelah penyusup mendapatkan informasi tentang port yang terbuka, maka serangan dapat dilancarkan dengan memberikan paket Syn yang telah dimanipulasi ke *server*, sehingga memaksa *server* untuk mengakumulasi koneksi yang setengah terbuka yang terus-menerus bertambah sampai sumber daya yang ada pada *server* lumpuh total.
   c. *TCP dan UDP Flooding*, selanjutnya penyusup melancarkan serangan terhadap protokol TCP dan UDP dengan membanjiri protokol tersebut. Tujuannya agar *server hang* atau *crash*.

4. HASIL DAN PEMBAHASAN

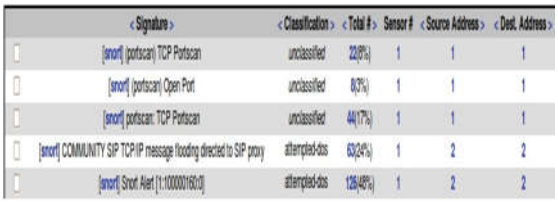
Setelah proses pengujian serangan dilakukan, maka Snort akan mengirim semua proses yang telah dilakukan pada direktori /var/log/snort, kemudian dikirim ke *database mysql* dan setelah itu dapat dilihat pada *Basic Analysis and Security Engine* (BASE) dengan tampilan *web*.

Hasil monitoring BASE dapat dilihat pada gambar di bawah ini:

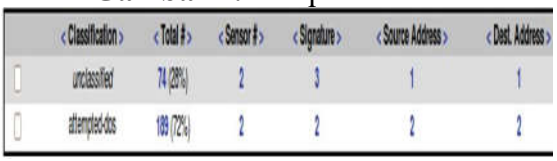


Gambar 6. Hasil monitoring BASE

Gambar di atas memperlihatkan hasil serangan yang terjadi melalui *interface* berbasis web. Dari data tersebut dapat dilihat bahwa *intruder* melakukan *port scanning* sebanyak 28%, TCP sebanyak 62%, UDP sebanyak 1%, dan ICMP sebanyak 9%.



Gambar 7. Unique alerts



Gambar 8. Kategori alerts

Gambar 7 dan 8 memperlihatkan *Unique Alerts* yang dihasilkan, yaitu sebanyak 5 buah, yang terbagi kepada 2 kategori; *unclassified* sebanyak 28% dengan jumlah 74, dan *attempted-dos* sebanyak 72% dengan jumlah 189. Sehingga jumlah *alert* yang dihasilkan adalah sejumlah 263 *alert*.

5. KESIMPULAN DAN SARAN

Snort-IDS bekerja dengan baik dalam mendeteksi serangan. Waktu tanggap Snort-IDS dalam menganalisa paket yang terdeteksi sebagai gangguan cukup cepat, yaitu tidak lebih dari 1 detik per paket gangguan. Dapat disimpulkan bahwa Snort-IDS sangat reaktif dalam menyikapi paket-paket yang terdeteksi sebagai gangguan. Snort-IDS juga mampu mendeteksi penyerangan-penyerangan yang dikategorikan sebagai *Denial of Service* (DoS) seperti *PingFlood, Syn Attack, TCP* dan *UDP Attack*.

Secara *default*, Snort memiliki keterbatasan dari segi *rules* yang ada. Semakin lengkap *rules* yang dimiliki, sistem akan semakin terlindungi dari gangguan penyusupan. Untuk menambahkan *rules*, dibutuhkan pengetahuan yang mendalam tentang protokol dan *payload* serangan. Untuk pengembangan sistem keamanan jaringan yang lebih *secure*, tidak cukup hanya dengan menerapkan *Intrusion Detection System* (IDS). Sistem keamanan jaringan perlu dilengkapi dengan *Intrusion Prevention System* (IPS).

DAFTAR PUSTAKA

[1] J. D. Santoso and M. Suyanto, "Manajemen Keamanan Jaringan Informasi Menggunakan Ids/ips Strataguard 'Studi Kasus STMIK AMIKOM YOGYAKARTA,'" *Data Manaj. dan Teknol. Inf.*, vol. 12, no. 1, 2011.

[2] M. Sc, H. S. Mare, and W. Syafitri, "Sistem Pendeteksian Penyusupan Jaringan Komputer Dengan Active Response Menggunakan Metode

Hybrid Intrusion Detection , Signatures Dan Anomaly Detection," *Sist. Pendeteksian Penyusupan Jar. Komput. Dengan Act. Response Menggunakan Metod. Hybrid Intrusion Detect. Signatures Dan Anom. Detect.*, vol. 2011, no. Snati, pp. 17–18, 2011.

[3] B. Sugiantoro and jazi eko Istianto, "Analisa Sistem Keamanan Intrusion Detection System (IDS), Firewall System, Database System Dan Monitoring System Menggunakan Agent Bergerak," *Analisa*, vol. 2010, no. semnasIF, pp. 21–29, 2010.

[4] J. Al Rasyid, M. I. Herdiansyah, and D. Syamsuar, "ANALISA PENERAPAN IDS DAN IPS DALAM KEAMANAN JARINGAN KOMPUTER," in *SEMNASTIK MTI*, 2011, pp. 403–405.

[5] D. Ariyus, *INTRUSION DETECTION SYSTEM: Sistem Deteksi Penyusupan Pada Jaringan Komputer*, I. Yogyakarta: ANDI, 2007.

[6] R. Rafiudin, *Mengganyang Hacker dengan Snort*. Yogyakarta: ANDI, 2010.

[7] T. S. Project, *SNORT Users Manual 2.8.5*. 2009.

[8] B. Hays, "Installing Snort and Barnyard2 in Ubuntu 9.10." 2010.