BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan internet suatu yang sangat penting pada jaringan publik. Terdapat banyak ancaman – ancaman yang bisa kapan saja menyerang yang tentu akan berdampak gangguan pada layanan yang dimiliki. Dimana setiap tahun serangan terhadap jaringan publik selalu mengalami peningkatan.

> "Rata – Rata serangan DDoS meningkat sebesar 14 persen dari jumlah serangan kurtal ketiga 2014, dan menigkat 245 persen dari tahun sebelumnya"[1].

PT. Time Excelindo sebagai salah satu penyedia jasa layanan internet di Indonesia harus memiliki suatu sistem yang dapat mendeteksi sekaligus mencegah serangan – serangan yang terjadi. Sehingga diharapkan layanan yang dimiliki oleh PT. Time Excelindo maupun pelanggannya tidak terganggu.

Dari data di atas dan sebagai langkah antisipasi untuk menghindari terjadinya serangan terhadap server - server yang dimiliki PT. Time Excelindo maupun pelanggan yang menitipkan servernya di PT. Time Excelindo. Oleh karena itu, peneliti terpikirkan untuk membuat suatu sistem yang dapat mendeteksi maupun mencegah serangan – serangan seperti itu. Pendeteksian dan pencegahan menggunakan aplikasi Snort yang diinstall pada server Linux Ubuntu 16.04 dan terpasang sebagai *transparent bridge*.

Snort merupakan aplikasi berbasis *open source* yang memungkinkan menganalisa trafik dan paket yang melewati jaringan. Trafik yang berjalan pada

jaringan dicocokan dengan *rules* yang ada pada sistem yang kemudian dicatat ke dalam *log*. Ketika terdeteksi trafik yang mencurigakan sesuai dengan *rules* pada database sistem akan mengirimkan sinyal peringatan melalui email ke admin. Admin juga akan mendapatkan laporan tiap bulannya mengenai serangan – serangan yang berhasil tercatat pada *log* yang kemudian dapat digunakan untuk analisa mencegah serangan – serangan berikutnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana mengimplementasikan *Network Intrusion Detection* dan *Prevention System* (NIDPS) dengan menggunakan aplikasi berbasis *open source* Snort di PT. Time Excelindo untuk mendeteksi dan mencegah serangan – serangan *hacking* serta mampu menghasilkan file laporan dari serangan yang telah terjadi.

1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Sistem diletakan antara router core dan router distribusi sebagai *transparent bridge*.
2. Sistem operasi yang digunakan adalah Ubuntu 16.04 LTS.
3. *Software* yang digunakan adalah Snort, Barnyard2, PulledPork, Snorby, dan Splunk.
4. Pencegahan menggunakan mode *inline* dengan *module* DAQ AFPacket.
5. Daftar *rule* yang digunakan dari database snort.org yang di unduh dan di

modifikasi secara otomatis menggunakan aplikasi PulledPork.

6. Jenis serangan yang dilakukan untuk pengujian adalah Apache DoS *Attack* dan FTP *Brute Force Attack*.
7. Server yang digunakan hanya satu dan diletakan di ruang NOC 1 PT. Time Excelindo.
8. IP a*ddress* yang digunakan adalah IPv4.

1.4 Maksud dan Tujuan Penelitian

Tujuan dari penelitian ini dimaksudkan untuk mencapai beberapa hal sebagai berikut :

1. Mendeteksi dan mencegah gangguan – gangguan yang terjadi pada jaringan PT. Time Excelindo.
2. Menghasilkan rekapitulasi dari serangan - serangan yang terjadi ke dalam bentuk dokumen untuk dapat di analisa.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan bermanfaat untuk mendeteksi dan mencegah gangguan maupun serangan yang menyerang server – server yang ada di dalam jaringan PT. Time Excelindo. Manfaat lain penelitian ini juga sebagai langkah awal untuk menganalisa serangan – serangan berikutnya dengan menganalisa hasil rekapitulasi serangan yang telah terjadi.

1.6 Metode Penelitian

Pada penyusunan tugas akhir yang berjudul "Analisa dan Implementasi *Network Intrusion Detection* dan *Prevention System* Berbasis *Open Source* Menggunakan Snort Di PT. Time Excelindo" ini, peneliti melakukan penelitian

menggunakan langkah – langkah sebagai berikut:

1. Studi Literatur

   Menganalisa dan mengumpulkan data untuk dijadikan refrensi baik dari buku maupun artikel – artikel yang ada di internet serta dokumentasi – dokumentasi resmi dari Snort untuk menunjang keberhasilan penelitian ini.

2. Instalasi

   Melakukan instalasi sistem operasi Ubuntu 16.04 LTS, aplikasi utama Snort dan beberapa aplikasi – aplikasi pendukung seperti Barnyard2, PulledPork, Snorby, Splunk, Apache2 dan MySQL agar server dapat berjalan dengan baik.

3. Konfigurasi

   Melakukan konfigurasi baik pada sisi jaringan, konfigurasi sistem operasi serta konfigurasi aplikasi – aplikasi yang telah terinstall.

4. Pengujian

   Pada tahap ini akan dilakukan pengujian terhadap NIDPS Server yang diimplementasikan pada jaringan PT. Time Excelindo. Kemudian mencari kesalahan yang terjadi.

5. Evaluasi

   Melakukan evaluasi terhadap NIDPS Server yang dibuat, kemudian dari kesalahan yang ditemukan, dijadikan saran agar dapat dikembangkan kembali menjadi lebih baik.

1.7 Sistematika Penulisan

Sistematika penulisan dalam penyusunan tugas akhir ini dibagi dalam

lima bab, masing – masing bab dapat diurailkan sebagai berikut:

1. BAB I merupakan pendahuluan yang berisi latar belakang, tujuan penelitian, batasan masalah, metode penelitian dan sistematika penulisan.
2. BAB II membahas tentang dasar – dasar teori yang digunakan dalam penelitian ini, berisi tinjauan pustaka yang peneliti gunakan sebagai dasar teori dalam penyusunan tugas akhir ini.
3. BAB III membahas mengenai analisis dari jaringan milik PT. Time Excelindo tanpa menggunakan NIDPS Server dan NIDPS yang akan dibuat serta hal – hal yang diperlukan dalam pembuatan NIDPS serta hasil dari NIDPS yang dibuat.
4. BAB IV membahas tentang implementasi dari hasil analisis dan perancangan system yang telah dibuat sebelumnya.
5. BAV V berisi mengenai kesimpulan dari penelitian dan saran yang diberikan oleh peneliti untuk pembaca maupun bagi peneliti lain yang ingin mengembangkannya kembali.