BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan internet yang luas merupakan salah satu bukti dari kemajuan teknologi yang begitu pesat. Semua orang bisa bertukar data di manapun dan kapanpun mereka berada sehingga memungkinkan akses informasi yang begitu cepat di berbagai belahan bumi. Namun di lain sisi internet juga memiliki dampak buruk. Hampir semua perangkat yang terhubung dengan jaringan internet memiliki kerentanan yang tinggi untuk diserang oleh pihak-pihak luar yang tidak berkepentingan. Munculnya berbagai jenis teknik serangan yang baru disetiap tahunnya juga semakin memperburuk kondisi tersebut.

Kebutuhan masa kini akan suatu sistem yang mampu melakukan monitoring setiap aktifitas yang terjadi dalam suatu sistem jaringan komputer. Sistem yang mampu meningkatkan kemampuan analisis serta memberikan peringatan secara dini kepada *network administrator* jika terjadi aktifitas mencurigakan yang dikhawatirkan mampu merusak konfigurasi jaringan komputer. Sistem yang secara otomatis mampu melakukan penanganan lebih lanjut ketika terjadi serangan sangatlah dibutuhkan untuk mengurangi efek negatif *hacker* . *Intrusion Detection System (IDS)* menyediakan cara yang tepat untuk menjawab kebutuhan tersebut.

Snort adalah perangkat lunak *IDS* berbasis *open source* yang berfungsi untuk melakukan deteksi serangan yang bekerja dengan melakukan pencocokan paket-paket data yang masuk menggunakan sejumlah *signatures* yang berada dalam *rules* yang ditetapkan [3]. *Snort* juga memiliki kemampuan memberikan notifikasi secara *real-time* jika serangan yang diharapkan terjadi.

Permasalahan yang ada yakni kemampuan dasar *Snort* yang tidak mampu menyajikan notifikasi serangan secara *user-friendly* pada suatu *Dashboard Application* yang mudah dipahami oleh banyak kalangan. *Snort* juga tidak memiliki kemampuan dasar untuk melakukan *blocking* alamat IP secara otomatis

menggunakan *firewall* pada *hardware* yang tersedia jika terjadi suatu serangan oleh alamat IP tertentu. Padahal *blocking* serangan secara otomatis diperlukan untuk menjamin sistem keamananan yang baik dalam suatu jaringan komputer sehingga tidak perlu merepotkan *network administrator* untuk selalu melakukan *monitoring* secara terus-menerus pada IDS terutama jika terjadi berbagai macam jenis serangan dalam satu waktu. Penggunaan *firewall* pada perangkat keras yang ada juga dibutuhkan untuk meningkatkan kehandalan sistem dalam menangkal berbagai jenis serangan sehingga tidak membebani *Server* dalam menjalankan fungsinya.

Oleh karena itu pada penelitian Tugas Akhir ini, dilakukan peningkatan performansi *Snort* dalam melakukan pencegahan terhadap serangan dan meningkatkan performasinya dengan cara melakukan migrasi fungsionalitas dari *software* menuju keranah *hardware* dengan menggunakan ACL Router sebagai perangkat tambahan untuk mengurangi beban kerja *Server*. Dibangun juga beberapa *Dashboard Application* untuk memudahkan *network adminitrator* dalam melakukan monitoring serangan yang terjadi sehingga peningkatan fungsionalitas IDPS yang diharapkan bisa dilakukan.

1.2 Tujuan Penelitian

Tujuan Tugas Akhir ini adalah sebagai berikut:

1. Membangun *Hybrid* IDPS menggunakan *Snort* IDS dengan integrasi ACL *Router* dan *ClamAV Antivirus*.
2. Membangun *Dashboard System* untuk menampilkan *alert* serta kondisi performansi *Server* IDS.
3. Menganalisis performansi *Hybrid* IDPS dari sistem jaringan yang dibuat dalam mencegah berbagai jenis serangan.
4. Meningkatkan performansi IDS *Snort* dan kehandalan sistem dalam mencegah serangan.

1.3 Rumusan Masalah

Beberapa rumusan masalah pada Tugas Akhir adalah sebagai berikut.

1. Bagaimana membangun *Hybrid* IDPS menggunakan *Snort* IDS yang terintegrasi dengan ACL *Router* dan *ClamAV Antivirus.*

2. Bagaimana membangun *Dashboard System* yang mampu menampilkan *alert* serta kondisi performansi *Server* IDS.
3. Bagaimana menganalisis performansi *Hybrid IDPS* dari sistem jaringan yang dibuat dalam mencegah berbagai jenis serangan.
4. Bagaimana meningkatkan performansi IDS *Snort* dan kehandalan sistem dalam mencegah serangan.

1.4 Batasan Masalah

Tugas Akhir ini membatasi masalah pada poin-poin sebagai berikut:

1. Implementasi dan pengujian jaringan *Hybrid IDPS* dilakukan pada jaringan lokal Laboratorium Sistem Komputer.
2. *IDS Snort Server* berjalan pada sistem operasi *Ubuntu 10.04 (Distro Xubuntu-Security Onion).*
3. *Client* akan difungsikan sebagai *attacker* atau *intruder.*
4. Tidak membahas secara mendalam metode serangan yang digunakan.
5. Jenis router yang digunakan adalah produk *Cisco.*
6. Implementasi hanya dilakukan pada IPv4 saja.

1.5 Metode Penelitian

Penelitian ini dilakukan dengan metode-metode sebagai berikut.

1. Studi pustaka

   Studi pustaka ini dimaksudkan untuk mengumpulkan literatur dan proses pembelajaran materi melalui buku maupun jurnal-jurnal ilmiah dari berbagai sumber yang digunakan sebagai acuan penelitian Tugas Akhir ini.
2. Perancangan dan realisasi

   Meliputi aplikasi dari konsep dan teori yang telah diperoleh. Melakukan perancangan jaringan dan mengimplementasikannya sesuai perancangan kemudian melakukan pengujian terhadap hasil perancangan yang telah dikerjakan.
3. Pengujian dan analisis implementasi

   Dalam tahap ini akan diuji menggunakan perangkat serangan untuk berbagai kasus yang disediakan dan mencari kesalahan-kesalahan yang

masih muncul dalam pengimplementasian. Kemudian dilakukan analisis terhadap hasil implementasi dan pengujian implementasi .

1.6 Sistematika Penulisan

Penulisan buku Tugas Akhir ini memiliki topik pembahasan yang sistematika penulisannya terdiri dari lima bab, yaitu:

BAB 1: PENDAHULUAN

Berisi tentang latar belakang pembuatan Tugas Akhir, maksud dan tujuan pembuatan Tugas Akhir, batasan masalah, metodologi penulisan, serta sistematika yang digunakan dalam penulisan laporan Tugas Akhir.

BAB 2: DASAR TEORI

Berisi tentang dasar-dasar teori yang diperlukan serta literatur-literatur yang mendukung dalam pembangunan sistem keamanan yang meliputi konsep dasar mengenai *Network Security, Intrution Detection Prevention System, Access Control List, Snort, ClamAV Antivirus, HAPV, Sguil dan Snortsam.*

BAB 3 : PERANCANGAN DAN IMPLEMENTASI

Berisi tentang perancangan awal sistem yang akan diimplementasikan. Merancang sebuah sistem keamanan yang menggabungkan kemampuan *IDS Snort* dengan *ACL Router* dan *ClamAV Antivirus.* Kemudian dilakukan analisis performasi dari kombinasi sistem keamanan tersebut.

BAB 4 : PENGUJIAN DAN ANALISIS HASIL IMPLEMENTASI

Berisi tentang pengujian dan analisis hasil implementasi yang telah dilakukan. Pengujian dan analisis ini bertujuan untuk mengetahui keandalan sebuah sistem keamanan yang telah dirancang.

BAB 5 : KESIMPULAN DAN SARAN

Berisi tentang kesimpulan yang didapat dari pembahasan dan analisis Tugas Akhir ini, serta saran yang yang dibutuhkan untuk pengembangan selanjutnya.