BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan Komputer adalah sebuah sistem yang menghubungkan dua atau lebih komputer melalui sebuah media transmisi sehingga dapat saling berbagi data atau informasi. Berbagi data atau informasi di dalam sebuah jaringan komputer yang terdapat banyak pengguna pada suatu media transmisi tidak selalu aman, maka dibutuhkan sebuah sistem yang mampu menjamin keamanan saat melakukan pertukaran data atau informasi yang melewati jaringan.

Dalam proses pengamanan sistem di jaringan biasanya masih dilakukan secara manual oleh *Network Administrator*, hal ini mengakibatkan ketergantungan pengamanan sistem pada kecekatan dan ketepatan dari seorang *administrator* dalam menangani gangguan. Langkah-langkah pencegahan membantu menghentikan gangguan dari pengguna yang tidak sah yang disebut "penyusup" untuk mengakses setiap bagian dalam sistem jaringan Komputer.

Pengumpulan informasi, *scanning*, pengambilan alih, memelihara akses dan menutupi jejak merupakan kegiatan seorang penyusup atau peretas, kegiatan tersebut sering kali disebut *hacking*. Sering kali penyusup melakukan serangan terhadap jaringan seperti *Daniel Of Service (DoS), Spoofing, DNS Poisoning, Sniffer, MITM, Session Hijacking, Phissing, Bruteforce*, untuk menerobos masuk kedalam jaringan.

Penyerangan yang dilakukan secara tidak menentu menyebabkan seorang *administrator* harus selalu *standby* mengawasi dan melindungi jaringan. Oleh

karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman keamanan yang mungkin terjadi secara optimal dalam waktu yang cepat dan secara automatis mengatasi penyusupan tersebut sehingga kemungkinan kerusakan akibat penyusupan keamanan jaringan dapat diminimalisir.

Intrusion Detection System (IDS) merupakan sistem keamanan yang mampu mendeteksi adanya serangan pada jaringan dengan merekam setiap aktifitas dan memfiltemya sesuai dengan rule yang diterapkan yang kemudian memberikan alert pada administrator. Menggunakan *iptables* sebagai *firewall* yang berfungsi memfilter paket data kemudian memberikan aksi sesuai dengan pengaturan seperti *accept, drop, dan reject.*

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang diatas maka permasalahan utama adalah "bagaimana membuat rancangan sistem keamanan jaringan menggunakan *Network-based Intrusion Prevention System* dengan metode pencocokan *database* pola serangan *(signature based system)*?"

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas maka didapat batasan-batasan masalah yang digunakan untuk membatasi ruang lingkup masalah dalam melakukan penelitian. Batasan masalah yang digunakan adalah sebagai berikut :

1. Server *Intrusion Prevention System* yang dibangun menggunakan snort dengan sistem operasi Debian 8.
2. Pengujian dilakukan pada jaringan *Local Area Network* dengan topologi yang sudah disesuaikan oleh penulis.

3. Metode pengujian yang digunakan adalah metode *Penetration Testing Life Cycle.*
4. Serangan yang disimulasikan berupa *Scanning* menggunakan *nmap, Bruteforce SSH* menggunakan *hydra, DoS* menggunakan program *hping3.*
5. *Snort rules* yang dibuat berdasarkan database pola serangan dari situs resmi snort.org.
6. Tidak menerapkan semua *rules signature* untuk diujikan.
7. *Rules* yang diujikan menggunakan *local rules* yang dibuat oleh penulis.
8. Sistem Operasi yang digunakan penyerang dalam simulasi adalah Linux Backbox 5.0
9. Tidak melakukan uji coba menggunakan semua jenis serangan yang dilakukan ke system secara lebih mendalam.
10. System dibangun dengan jenis NIPS *(Network-based Intrusion Prevention System).*
11. Metode pendekatan yang diterapan menggunakan *Signature based system.*

1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan penelitian ini berfungsi untuk mengetahui apa yang hendak dicapai dalam penelitian ini. Berikut ini maksud dan tujuan dari penelitian yang dilakukan oleh penulis :

1.4.1 Maksud Penelitian

Adapun maksud dari penelitian adalah untuk memenuhi salah satu syarat kelulusan Strata satu di Universitas Amikom Yogyakarta dengan program studi Informatika di Fakultas Ilmu Komputer.

1.4.2 Tujuan Penelitian

Penelitian yang dilakukan bertujuan untuk menganalisa dan merancang sebuah sistem keamanan jaringan menggunakan NIPS dengan metode pencocokan *database* pola serangan yang mendeteksi serangan penyusupan dan juga melakukan pencegahan terhadap serangan penyusupan tersebut.

1.4.3 Manfaat Penelitian

Dengan melakukan penelitian ini maka diharapkan mendapatkan manfaat-manfaat sebagai berikut :

1. Mampu menerapkan salah satu disiplin ilmu sesuai dengan kompetensi yang didapatkan selama masa perkuliahan dan dapat membantu.
2. Diharapkan bagi pengguna sistem akan merasa terbantu dalam mengawasi menjaga akses jaringan dari pihak yang tidak berhak mengaksesnya *(unauthorized user)*.

1.5 Metode Penelitian

Dalam melakukan penelitian ini, penulis menggunakan beberapa metode penelitian untuk menyusun langkah langkah yang dapat digunakan untuk menyelesaikan penelitian.

1.5.1 Metode Pengumpulan Data

Agar mendapatkan data dan hasil yang benar, relevan tentang penelitian

yang dilakukan, maka dari itu diperlukan metode untuk mencapai tujuan penelitian.

1.5.1.1 Studi Pustaka

Studi Pustaka dilakukan dengan membaca literature dari buku, paper, journal penelitian, dan penelitian sebelumnya yang dapat digunakan sebagai dasar teori dari sistem dalam penelitian yang dilakukan oleh penulis.

1.5.1.2 Observasi

Observasi dilakukan dengan mengamati aktifitas dalam sebuah jaringan, kemudian dilakukan pemilihan komponen yang akan digunakan untuk membangun sistem keamanan.

1.6 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir terdiri dari enam bab. Penjelasan mengenai enam bab ini, yaitu:

BAB I PENDAHULUAN

Bab ini menjelaskan dasar-dasar dari penulisan laporan tugas akhir ini, yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan laporan tugas akhir.

BAB II LANDASAN TEORI

Bab ini membahas teori-teori yang berhubungan dengan spesifikasi pembahasan penelitian yang akan diangkat, yang terdiri dari pembahasan mengenai Pengenalan Jaringan Komputer, *Protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), Model Open System Interconnection (OSI) Layer, Media Access*

Control (MAC) Address, Address Resolution Protocol (ARP), Ancaman Keamanan Jaringan, *Intrusion Detection System (IDS), Intrusion Prevention System (IPS),* Sistem Operasi, dan *Snort.*

BAB III ANALISA DAN PERANCANGAN

Bab ini membahas tentang analisa dan perancangan yang akan digunakan dalam pembuatan sistem, alat-alat yang digunakan, serta sistematika pengujian yang akan dilakukan.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi tentang Implementasi Sistem, Pengujian Network Intrusion Prevention Sistem, serta pembahasan sistem keamanan yang telah diterapkan

BAB V PENUTUP

Bab ini berisi kesimpulan yang dihasikan dari pembahasan tentang sistem yang dikembangkan dan beberapa saran yang berisi perbaikan atas apa yang menjadi kekurangan dalam implementasi sehingga menjadi acuan bagi pengembangan selanjutnya.

DAFTAR PUSTAKA

Berisikan referensi yang digunakan oleh penulis sebagai acuan dan perbandingan landasan teori dalam penulisan skripsi.