

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi informasi yang pesat telah mengubah cara institusi pendidikan beroperasi, termasuk di lingkungan sekolah. Ancaman terhadap jaringan komputer di institusi pendidikan,, sering kali datang dalam bentuk serangan siber seperti *malware*, *ransomware*, atau upaya penyusupan dari pihak tidak berwenang dari serangan atau penyalahgunaan jaringan. Keamanan jaringan komputer berfungsi untuk mengantisipasi resiko-resiko yang akan terjadi pada jaringan komputer yang dapat mengganggu aktivitas yang sedang terjadi pada sistem jaringan komputer [1].

Banyak sekali jenis sistem keamanan jaringan antara lain *firewall*, *cryptographic system*, *IDS*, *SSL*, *antivirus system*, *IPSec*, *authentication* dan lain sebagainya[2], untuk pengimplentasian keamanan jaringan pada sekolah SMKN 1 Kota Jambi menggunakan sistem *Intrusion Detection System* (IDS) untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan [3].

Pada dasarnya *IDS* memiliki dua macam yaitu yang pertama *Host-Based* yang terdiri dari *IDS host-based* bekerja pada host yang akan dilindungi. *IDS* jenis ini dapat melakukan berbagai macam tugas untuk mendeteksi serangan yang dilakukan pada *host* tersebut. Keunggulan *IDS hostbased* adalah pada tugas-tugas yang berhubungan dengan keamanan file. Misalnya ada tidaknya file yang telah diubah atau ada usaha untuk mendapatkan akses ke file-file yang sensitif. Dan yang kedua

Network based : *IDS network based* biasanya berupa suatu mesin yang khusus dipergunakan untuk melakukan monitoring seluruh segmen dari jaringan. *IDS network based* akan mengumpulkan paket-paket data yang terdapat pada jaringan dan kemudian menganalisisnya serta menentukan apakah paket-paket itu berupa suatu paket yang normal atau suatu serangan atau berupa aktivitas yang mencurigakan [4].

Adapun penelitian terdahulu yang membahas tentang pengimplementasian Sistem *IDS*, yang pertama peneliti terdahulu mengimplementasikan *IDS* menggunakan *Software* Securita yang diterapkan pada Linux Debian 9 berdasarkan penyimpanan VPS, pada penelitian ini menggunakan metode *Network Development Life Cycle* pada *software* Securita untuk mendapatkan log aktivitas yang mencurigakan secara detail [5]. Ada juga penerapan *IDS* untuk mendeteksi serangan *Distributed Denial of Service* (DDOS) pada MA Negeri Purwakarta, pada penelitian ini menggunakan *snort* dan *portsentry* untuk mendeteksi serangan yang masuk ke dalam jaringan komputer, dengan mengirimkan *notifikasi* serangan yang masuk ke jaringan komputer, serangan tersebut dapat dicegah dengan menerapkan *portsentry* sehingga serangan seperti *Ping icmp*, *nmap*, dan DDOS tidak dapat masuk ke dalam jaringan komputer [6].

IDS adalah metode yang otomatis memantau lalu lintas jaringan yang mencurigakan. Selain itu, *IDS* dapat mengurangi risiko keamanan sistem jaringan, mendeteksi serangan, dan pelanggaran keamanan. *Snort* adalah alat bantu yang digunakan untuk mendeteksi serangan. *Snort* merupakan aplikasi yang dirancang untuk mengidentifikasi intrusi dan dapat menganalisis lalu lintas secara langsung.

Snort juga terkait dengan Sistem Deteksi Intrusi (*IDS*) dalam menanggapi insiden serangan terhadap host jaringan.[7].

Meskipun banyak sekolah dan institusi pendidikan lain yang telah mengimplementasikan *IDS* untuk meningkatkan keamanan jaringan mereka, evaluasi efektivitas dari sistem ini dalam konteks lingkungan pendidikan seperti SMKN 1 Kota Jambi masih terbatas. jaringan komputer memainkan peran krusial dalam mendukung kegiatan belajar-mengajar, administrasi, serta komunikasi. Namun, meningkatnya ketergantungan pada teknologi ini juga memperbesar risiko ancaman keamanan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan data, pada saat ini belum menerapkan system kemanan jaringan komputer, karena tidak adanya system keamanan jaringan komputer yang diterapkan di SMKN 1 Kota Jambi, masih rentan terkena serangan diantaranya *Ping Attack*, *Network Scanning* dan *DDOS*. Penelitian sebelumnya juga menunjukkan bahwa penerapan *IDS* di lingkungan kecil dan menengah, seperti di institusi pendidikan, sering menghadapi tantangan tersendiri terkait konfigurasi dan efektivitas deteksi ancaman. Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi yaitu dengan menggunakan aplikasi *Intrusion Detection System (IDS)* yaitu *Snort* yang memberikan *alert* .[9]

Dari penjelasan diatas, penulis ingin melakukan implelementasi kemanan jaringan menggunakan sistem *IDS* dan mengevaluasi dari jaringan yang ada di SMKN 1 Kota Jambi, dimana judul yang diangkat ialah **“IMPLEMENTASI DAN**

EVALUASI KEAMANAN JARINGAN MENGGUNAKAN SISTEM *IDS* DI SEKOLAH SMKN 1 KOTA JAMBI”.

1.2 RUMUSAN MASALAH

Hasil dari penelitian ini adalah merancang sistem keamanan jaringan komputer berbasis *Intrusion Detection System* (IDS) menggunakan Snort dan Portsentry untuk mendeteksi serangan intrusi pada jaringan komputer SMKN 1 Kota Jambi seperti ICMP *Ping*, NMAP (*port scanning*) dan DDOS, dengan menerima notifikasi adanya serangan intrusi pada jaringan komputer, serangan tersebut dapat dihindari IDS dengan melakukan portsentry sehingga serangan seperti ICMP *Ping*, NMAP dan DDOS tidak dapat menembus kedalam jaringan komputer.

Berdasarkan permasalahan di atas maka rumusan masalah dari penelitian adalah , yaitu :

1. Bagaimana menerapkan sehingga dapat memonitoring aktifitas jaringan dari serangan.
2. Bagaimana melakukan konfigurasi IDS, sehingga IDS dapat mendeteksi adanya serangan dari para penyusup di SMKN 1 Kota Jambi.

1.3 BATASAN MASALAH

Dalam penelitian ini akan dibatasi pada hal-hal berikut :

1. Penelitian dilakukan di Jaringan Internet SMKN 1 Kota Jambi
2. Sistem ini digunakan untuk melihat Keamanan Jaringan yang ada di SMKN 1 Kota Jambi

3. Merancang sebuah sistem keamanan jaringan berbasis IDS dengan menggunakan *Snort*
4. Sistem Operasi yang digunakan untuk IDS dan sekaligus di jadikan sebuah server adalah Ubuntu 20.04 LTS
5. Sistem pendeteksi intrusi yang dikembangkan berjenis NIDS (*Network Intrusion Detection System*)
6. Simulasi penerapan serangan berasal dari PC *client* yang di install Sistem Operasi Kali Linux
7. Jenis serangan yang diuji ada tiga di antaranya *Port Scanning* dengan jenis *SNY Scan* , DDOS menggunakan jenis *TCP SYN Flood* dan *ICMP Flood*, serta serangan Brute Force dengan jenis *Dictionary Attack*.
8. Data yang digunakan dalam penelitian ini akan diambil dari wawancara dengan guru SMKN 1 Kota Jambi. Penelitian ini tidak mencakup survei atau data dari sumber luar sekolah.
9. Berdasarkan wawancara pengguna jaringan di SMKN 1 Kota Jambi berjumlah 1800 Siswa/I dan 120 Staf, TU serta guru.
10. Penelitian ini akan menggunakan perangkat lunak IDS yang telah dipilih berdasarkan kebutuhan dan sumber daya yang tersedia di SMKN 1 Kota Jambi. Penelitian tidak mencakup evaluasi atau perbandingan dengan teknologi IDS lain di luar yang diimplementasikan.

1.4 TUJUAN PENELITIAN

Adapun tujuan yang ingin dicapai oleh peneliti sebagai berikut :

1. Mengimplementasi sistem deteksi intrusi (IDS) di jaringan SMK N 1 Kota Jambi
2. Mengevaluasi efektivitas sistem IDS dalam mendeteksi dan merespons ancaman di jaringan SMK N 1 Kota Jambi

1.5 MANFAAT PENELITIAN

Adapun manfaat yang dapat diambil dari penelitian dan penulisan tugas akhir ini adalah :

1. Meningkatkan Keamanan Jaringan di SMKN 1 Kota Jambi
2. Memberikan Pengalaman dalam pengimplentasian keamanan jaringan bagi penulis.
3. Kontribusi terhadap Penelitian dan Praktek Keamanan Jaringan
4. Memberikan rekomendasi untuk meningkatkan efektivitas sistem IDS dan keamanan jaringan di SMK N 1 Kota Jambi berdasarkan hasil evaluasi.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan dalam karya ilmiah bertujuan untuk memberikan gambaran umum mengenai keseluruhan penulisan. Sistematika ini meliputi beberapa bagian penting yang saling berkaitan dan menyusun alur logis dari awal

hingga akhir penelitian. Untuk memberikan gambaran umum tentang keseluruhan karya ilmiah, dapat dilihat melalui struktur penulisan yang mencakup :

BAB I : PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang masalah, perumusan masalah, pembatasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini berisi penjelasan mengenai konsep-konsep teoritis yang menjadi dasar pembahasan penelitian yang relevan, dan secara khusus digunakan sebagai landasan untuk menjawab masalah penelitian.

BAB III : METODOLOGI PENELITIAN

Bab ini menjelaskan tahapan-tahapan proses yang dilakukan selama penelitian, metode yang digunakan, serta *software* yang digunakan untuk membangun perangkat yang dibuat.

BAB IV : ANALISA DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang analisis dan tahapan yang sedang berlangsung, analisis untuk kondisi dan langkah-langkah dalam pengimplentasian sistem keamanan di SMKN 1 Kota Jambi.

BAB V : IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas tentang kegiatan implementasi sistem keamanan jaringan yang telah dibuat, termasuk kelebihan dan kekurangan sistem, serta analisis hasil yang dicapai oleh sistem keamanan tersebut.

BAB VI : PENUTUP

Bab ini menyajikan kesimpulan dari penelitian yang telah dilakukan beserta saran-saran yang berguna untuk pengembangan penelitian selanjutnya.