BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Penggunaan jaringan Internet di Indonesia kini sudah sangat berkembang di kalangan masyarakat Indonesia. Internet kini sudah di gunakan di berbagai bidang seperti: bidang pendidikan, bidang kesehatan, bidang olahraga bahkan perusahaan-perusahaan di era sekarang sudah hampir semuanya menggunakan jaringan Internet karna aksesnya yang mudah dan juga murah. Khususnya di bidang pendidikan kini sudah banyak jaringan-jaringan Internet yang di pasang di sekolah-sekolah untuk memudahkan siswanya dalam mengakses Internet untuk digunakan dalam membantu proses pembelajaran.

Menurut data yang diperoleh dari situs APJII (Asosiasi Penyelenggara Data Internet Indonesia). Pada periode 2022-2023 penggunaan Internet di Indonesia kini sudah mencapai 215 Juta Orang (APJII,2023). Sehingga dengan angka pengunaan Internet yang tinggi tersebut tentu akan menimbulkan dampak negatifnya juga, salah satu contohnya yaitu seperti serangan jaringan.

Dalam Bidang Akademik seperti perguruan tinggi atau sekolah bukan tidak mungkin untuk terjadi serangan siber. Universitas atau sekolah juga terdapat banyak data penting disana yang bisa di salah gunakan oleh oknum yang tidak bertanggung jawab seperti data mahasiswa, siswa ataupun guru yang tentu jumlahnhya cukup banyak. Seperti pada tahun 2021 terjadi kebocoran data di universitas Diponegoro sebanyak lebih dari 125 ribu. Data yang dilaporkan bocor termasuk alamat, jalur masuk, *email*, *username*, *password*, IPK, riwayat sekolah, beasiswa, dan lainnya. (Zona Mahasiswa, 2021). SMK PGRI 11 Ciledug merupakan sekolah menengah kejuruan yang memiliki beberapa penjuruan seperti : Multimedia, TKJ, dll. Di SMK PGRI 11 sendiri mempunyai beberapa laboratorium komputer yang terhubung dalam satu jaringan dengan topologi yang digunakan yaitu *star*. Sistem keamanan jaringan pada SMK PGRI 11 hanya menggunakan *firewall* dari awal terbentuknya jaringan, sehingga sistem keamanan jaringannya tidak terlalu maksimal.

Pada SMK PGRI 11 pernah terjadi serangan jaringan seperti DOS (*Denial Of Service)*, yang mengakibatkan situs *web* sekolah tidak dapat diakses beberapa saat, dalam melakukan pelacakannya yaitu dengan melakukan *filtering* pada *firewall* kemudian melakukan pemblokiran pada IP yang mencurigakan. Cara seperti ini tentu akan membutuhkan waktu yang cukup lama dalam mendeteksinya dan ada beberapa bentuk serangan yang tidak dapat terdeteksi, sehingga penangan administrator jaringan dirasa lambat ketika serangan terjadi. Oleh karena itu dibutuhkan sistem keamanan jaringan yang lebih efisien dalam mendeteksi serangan jaringan sehingga tugas seorang administrator jaringan jauh lebih efisien, yaitu dengan cara menggunakan SNORT sebagai *Intrusion Detection System* (IDS). yang nantinya akan terhubung ke dalam telegram sebagai penerima notifikasi otomatis.

Snort merupakan suatu aplikasi yang dimiliki oleh IDS dan NIDS yang memiliki kegunaan sebagai pengamanan pada suatu jaringan terhadap aktifitas data. Snort diretas melalui suatu jaringan, dimana aplikasi ini berbasiskan *opensource*, sehingga bisa digunakan secara gratis . Kemudian aplikasi ini juga memiliki metode *user sysog, file, unix, socket dan database* dimana terdapat kemampuan *realtime alert*. (Aritonang et al., 2020).

Untuk mengatasi masalah tersebut perlu dilakukan penelitian dengan cara melakukan perancangan notifikasi otomatis dengan mengggunakan SNORT dan *bot* telegram. Digunakan pada jaringan LAN (*Local Area Network*) di SMK PGRI 11 Ciledug. Nantinya akan terhubung dengan notifikasi otomatis aplikasi telegram sebagai penerima *alert* sehingga memudahkan administrator jaringan dalam mengidentifikasi serangan jaringan. Berdasarkan latar belakang tersebut maka penelitian ini mengangkat judul "Kajian Perancangan Notifikasi Otomatis Menggunakan Snort Untuk Mengevaluasi Keamanan Jaringan Terhadap Serangan Jaringan".

1.2. Identifikasi Masalah

Berdasarkan hasil uraian latar belakang di atas, maka bisa di jelaskan bahwa pokok permasalahan yang terjadi adalah sebagai berikut:

1. Keberadaan *firewall* mikrotik RB450Gx4 di SMK PGRI 11 kurang mampu untuk mencegah terhadap terjadinya serangan jaringan;
2. Penanganan yang lambat saat terjadi serangan terhadap jaringan oleh administrator jaringan.

1.3. Batasan Masalah

Dari latar belakang diatas, maka dapat di rumuskan batasan-batasan masalah tersebut meliputi:

1. Untuk mendeteksi serangan jaringan *software* yang digunakan snort;
2. Penelitian dibatasi sampai tahap *design* sistem keamanan jaringan di SMK PGRI 11 Ciledug;
3. Sistem keamanan jaringan yang di rancang hanya sebatas mengirimkan notifikasi jika terjadi serangan atau aktifitas tidak wajar pada jaringan;
4. Penerapan metode pengembangan PPDIOO dibatasi sampai tahap *design* (desain).

1.4. Rumusan Masalah

Rumusan masalah yang bisa diambil dari latar belakang, identifikasi masalah dan batasan masalah diatas adalah "Bagaimana Hasil Kajian Perancangan Notifikasi Otomatis Menggunakan SNORT Untuk Mengevaluasi Keamanan Jaringan Terhadap Serangan Jaringan di SMK PGRI 11 Ciledug".

1.5. Tujuan Penelitian

Adapun tujuan dari metode yang digunakan adalah sebagai berikut:

1. Memahami perancangan notifikasi otomatis sistem keamanan jaringan menggunakan Snort;
2. Memahami tantangan implementasi notifikasi sistem keamanan jaringan menggunakan Snort.

1.6. Manfaat Penelitian

Dapat memberikan solusi terkait masalah sistem keamanan jaringan yang ada di SMK PGRI 11 Ciledug,

1. Menjadi sebuah ide untuk mengimplementasikan snort di jaringan sekolah;
2. Dapat dijadikan sebagai bahan pengembangan notifikasi otomatis sistem keamanan jaringan di masa mendatang;
3. Dapat membantu administrator jaringan dalam melakukan identifikasi jika terjadi serangan pada jaringan;
4. Dapat dijadikan bahan referensi untuk penelitian selanjutnya.