BAB I
PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi di *era* revolusi industri 4.0 juga harus diimbangi dengan kemampuan *system* administrator dalam mengola sistem yang sedang dibangun. Selain dapat memberikan informasi yang fleksibel dan terkini, layanan informasi juga harus dapat diandalkan dan aman. Sistem komunikasi dan penyebaran informasi yang tidak lagi dibatasi oleh tempat dan waktu, telah menjadi peluang bagi para pelaku kejahatan di dunia internet, atau biasa disebut dunia *cybercrime*. Oleh karena itu, faktor keamanan jaringan menjadi parameter penting yang harus dipersiapkan dengan baik untuk menghidari upaya ilegal oleh oknum yang tidak bertanggung jawab untuk mencuri data atau merusak sistem yang ada. Berbagai serangan yang sering mengancam jaringan, seperti virus, *sniffing*, *spoofing* merupakan resiko yang harus dihadapi oleh administrator sistem setiap hari. Selain itu, *brute force*, *scanning*, *malware*, dan *Denial of Services* (DOS).

Sistem Deteksi Intrusi (*IDS*) adalah perangkat lunak atau sistem perangkat keras yang beroperasi secara otomatis untuk memantau kejadian di dalam jaringan komputer dan dapat menganalisis isu-isu keamanan jaringan. Sebuah IDS dapat diartikan sebagai alat, metode, atau sumber daya yang memberikan bantuan dalam mengidentifikasi dan melaporkan aktivitas di dalam jaringan komputer[1].

Snort adalah suatu perangkat pemasangan paket pada sistem operasi Linux, yang fungsinya utamanya adalah untuk mengidentifikasi kehadiran ancaman (threats). Snort memiliki kemampuan untuk menganalisis paket data yang bergerak melalui jaringan secara *real-time* dan menghasilkan catatan dalam bentuk basis data. Snort menjadi salah satu contoh dari jenis sistem deteksi intrusi (*IDS*) yang termasuk dalam kategori sistem deteksi intrusi berbasis jaringan (*NIDS*), suatu program sistem yang mampu menemukan tanda-tanda adanya intrusi di dalam jaringan komputer[2].

Telegram adalah aplikasi *messenger* yang akan membantu pihak administrator untuk memonitoring jaringan lebih mudah. Karena setiap serangan yang terdeteksi

oleh Snort akan memberikan *alert* ke Telegram dan di terima oleh pihak administrator. Dari Telegram akan terlihat jenis serangan dan status serangan berbahaya atau tidak bagi administrator[3].

Keamanan data sangat penting dalam lingkungan jaringan, pemantauan sistem 24jam penuh tidak mungkin dilakukan jika harus dilakukan secara manual. Perlu bantuan sistem pengganti manusia untuk pemantauan terus menerus, yang diharapkan dapat mendeteksi dan mencegah serangan terhadap jaringan atau *server*.

Intrusion Detection System (*IDS*) menjadi peluang bagi administrator sistem untuk mendeteksi dan mencegah aktivitas yang mencurigakan.Snort adalah sebuah aplikasi yang bisa digunakan sebagai *Intrusion Detection System* (*IDS*) yang berfungsi untuk mendeteksi adanya serangan atau sebuah aktifitas yang mencurigakan. Telegram disini berfungsi sebagai media notifikasi atau pemberitahuan ke sistem deteksi serangan dan mencatat aktivitasnya.

1.2 Rumusan Masalah

Berdasar latar belakang masalah seperti di 1.1, masalah yang ada yaitu :

1. Apakah IDS Snort mampu mendeteksi adanya serangan ICMP, SSH, Nmap, dan SYN Flood?
2. Seberapa cepat IDS mampu mendeteksi adanya serangan ICMP, SSH, Nmap, dan SYN Flood?

1.3 Batasan Masalah

1. Penelitian ini akan mengujikan implementasi *IDS* dan sistem pemberitahuan dalam lingkungan simulasi jaringan yang dibangun melalui alat virtualisasi seperti VMWare. Lingkungan ini akan mencakup beberapa perangkat (komputer dan server) yang direplikasi untuk mensimulasikan serangan.
2. Penelitian ini difokuskan pada implementasi dan analisis keamanan jaringan *IDS* menggunakan Snort dengan notifikasi Telegram pada *web server*. Pembahasan lebih lanjut tentang jenis serangan yang terdeteksi dan ditangani oleh *IDS* tersebut tidak termasuk dalam ruang lingkup penelitian ini.
3. Analisis lebih lanjut terkait manajemen keamanan jaringan seperti

kebijakan keamanan, manajemen *log*, dan tindakan pencegahan lainnya tidak termasuk dalam penelitian ini.

4. Penelitian ini akan memfokuskan deteksi pada serangan jaringan yang lazim, seperti serangan *Denial of Service* (*DoS*) dan pengintaian port.
5. Penelitian ini akan menggunakan Telegram sebagai media jejaring sosial untuk mengirimkan pemberitahuan serangan kepada administrator jaringan. Kemungkinan integrasi dengan platform lainnya, misalnya Facebook atau Instagram, tidak akan dieksplorasi dalam penelitian ini.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah dapat menjelaskan apa itu *IDS* dan *Snort*. Dapat mendeteksi dan mencegah adanya serangan terhadap *server*. Dapat mengimplementasikan telegram sebagai media notifikasi.

1.5 Manfaat Penelitian

1.5.1 Manfaat Bagi Peneliti

a. Menanmbah wawasan pengetahuan bagi peneliti khususnya pada keamanan jaringan (*Cyber Security*).
b. Menerapkan ilmu pengetahuan yang sudah didapatkan selama menjalani studi perkuliahan.

1.5.2 Manfaat Bagi Akademik

Manfaat yang didapat bagi akademik adalaha menjadi salah satu acuan bagi akademik lainya untuk melanjutkan penelitiaan di masa yang akan datang dan diharapkan dapat menambah bagi pihak akademik yang akan menggunakannya dalam kepentingan menerapkan keamanan jaringan (*Cyber Security*).

1.5.3 Manfaat Bagi Umum

Manfaat bagi umum adalah sebagai ilmu pengetahuan dan ketika ingin mengimplementasikan keamanan jaringan (*Cyber Security*) bagaimana sistemnya berjalan karena dapat membantu personal, perusahaan atau pemerintahan.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi pada penelitian ini sebagai berikut :

BAB I Pendahuluan

Berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II Tinjauan Pustaka

Berisi tentang konsep dasar serta teori-teori yang berkaitan dengan topik penelitian dari sumber pustaka dan referensi yang menjadi landasan dasar dalam perancangan, analisis kebutuhan sampai implementasi.

BAB III Metode Penelitian

Berisi tentang alur penelitian, alat dan bahan serta perancangan skenario kasus yang dibutuhkan dalam perancangan untuk uji coba *Intrusion Detection System*.

BAB IV Pembahasan dan Hasil

Berisi tentang implementasi dari *IDS* menggunakan Snort dengan notifikasi Telegram pada *server* yang telah dilakukan. Selain itu, akan dilakukan uji coba *IDS* snort.

BAB V Penutup

Berisi tentang kesimpulan dari hasil penelitian yang telah dilakukan dan menyampaikan saran agar penelitian selanjutnya dapat dilakukan pengembangan lebih lanjut tentang penelitian ini.