BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Warnet secara umum adalah tempat dimana beberapa komputer menjalin jaringan dengan salah satu komputer bertindak sebagai komputer *server* yang telah di konfigurasi atau disetting dan komputer lainnya bertindak sebagai komputer client. Tarif warnet berbeda-beda dan dalam hitungan per jam, tergantung fasilitas dan kecepatan internet yang disediakan.

Warnet *cyber* adalah warnet yang baru berjalan sekitar satu tahunan yang lalu dan masih dalam proses pengembangan karena warnet ini masih belum sempurna, baik dari sisi bangunan maupun dari sisi sistem yang berjalan dalam memenuhi kebutuhan trafik pengguna pada warnet. Warnet ini dibuat di dekat halaman sekolah SMK Negeri 1 Toboali, sehingga penggunanya cukup banyak dari kalangan pelajar.

Permasalahan yang ada diwarnet *cyber* terletak pada tingkat keamanan *server* warnet yang saat ini berjalan masih belum ada, oleh karena itu dalam beberapa bulan kebelakangan *server* warnet *cyber* mengalami permasalahan karena adanya penyerangan yang dilakukan oleh pihak lain seperti ping flood, smurf attack dan lain - lain.

Ada beberapa alternatif solusi untuk mengatasi permasalahan keamanan warnet yang kurang maksimal salah satunya adalah penerapan metode IDS *(Intrusion Detection System).* Menurut[6] *Intrusion Detection System (IDS)* merupakan perangkat lunak atau perangkat keras sistem yang secara otomatis melakukan proses pemantauan (monitoring) insiden yang terjadi dalam sistem komputer atau jaringan serta menganalisis tanda-tanda adanya masalah terhadap keamanan sistem. Jika terindikasi adanya aktifitas yang mencurigakan terhadap aliran *(traffic)* paket-paket yang keluar dan masuk pada sistem, maka IDS akan merekam aktifitas tersebut.

Dengan adanya laporan dari aktifitas yang mencurigakan dari implementasi IDS, maka admin dapat bertindak untuk memfilter maupun memblokir trafik yang

dicurigai sebagai serangan terhadap warnet. Snort digunakan sebagai tool implementasi dari metode IDS agar admin mendapatkan laporan warning secara real time tentang kondisi jaringan pada saat itu.

Dalam penulisan skripsi ini ada beberapa penelitian yang menjadi acuan, antara lain dilakukan oleh [1]" yang berjudul "Perbandingan Performan *Intrusion Detection (IDS)* Snort Medeteksi Serangan *TCP SYN Flood* Universitas Brawijaya". Penelitian yang dilakukan oleh [2] yang berjudul "Analisis Penerapan dan Uji Perform Intrusion Detection System (IDS) pada Jaringan Berbasis *Softwer Defined Network (SDN)* Universitas Telkom. Kota Bandung. Penelitian yang dilakukan oleh[3] yang berjudul" Implementasi Intrusion Detection System Menggunakan Snort, Barnyard2 dan Base pada Sistem Linux. Penelitian yang dilakukan oleh [4] yang berjudul" Implementasi IDS *(Instrusion Detection System)* pada Keamanan Jaringan Menggunakan Router OS. Penelitian yang dilakukan oleh[5] yang berjudul" Sistem Pengamanan Jaringan Admin *Server* dengan Metode *Instrusion Detection System (IDS)* Snort menggunakan Sistem Operasi ClearOS Universitas Negeri Makasar.

Berdasarkan uraian permasalahan pada paragraf sebelumnya, maka penulis mengambil judul penelitian skripsi **"Implementasi Keamanan Jaringan Mendeteksi adanya Penyusupan pada Server menggunakan IDS dengan Snort di Warnet Cyber Toboali Kabupaten Bangka Selatan".**

1.2 Rumusan Masala

Dengan didasari oleh latar belakang permasalahan di atas, maka permasalahan penelitian yang akan dapat dirumuskan sebagai berikut:

1. Bagaimana membangun sistem keamanan jaringan yang dapat mendeteksi upaya serangan pada penyusupan di *server* warnet *cyber*?
2. Bagaimana mengembangkan sistem pelaporan peringatan serangan pada snort agar mampu memberikan peringatan kepada admin secara cepat?

1.3 Batasan Masalah

Agar penelitian ini berfokus pada pembahasan yang diharapkan maka diperlukan batasan -batasan masalah dalam penelitian sebagai berikut :

1. Sistem operasi yang digunakan linux debian 9.8.0
2. Serangan yang dilakukan untuk menguji keamanan sistem berupa Nmap dan Puty.
3. Mode serangan yang diuji coba adalah ping flood, smurf attack, dan percobaan login menggunakan telnet.

1.4 Tujuan dan Manfaat Penelitian

Tujuan yang ingin dicapai penulis berdasarkan rumusan masalah yang diuraikan di atas adalah :

1. Untuk pengoptimalisasi sistem keamanan jaringan pada suatu sistem operasi linux debian 9.8.0.
2. Untuk mencegah terhadap serangan ping floood, smurf attack dan percobaan login menggunakan telnet.
3. Untuk mendeteksi adanya permasalahan dari serangan ping flood maupun smurf attack dan percobaan login menggunakan telnet.

Manfaat penelitian dan penyusunan laporan skripsi ini diharapkan mampu memberikan manfaat sebagai berikut :

1. Dapat membuat sistem jaringan akan bekerja lebih optimal pada warnet.
2. Dapat memberikan laporan peringatan kepada admin, sehingga dapat ditindaklanjuti secara cepat.

1.5 Sistematika Penulisan

Adapun sistematika penulisan skripsi yang memuat uraian secara garis besar isi laporan skripsi adalah sebagai berikut **:**

BAB I **PENDAHULUAN**

Bab ini menjelaskan tentag latar belakang, rumusan masalah, batasan masalah, manfaat dan tujuan penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II **LANDASAN TEORI**

Bab ini Berisi tentang hasil–hasil penelitian terdahulu yang berkaitan dengan penelitian yang dilakukan. Serta teori-teori yang digunakan dalam penelitian, perancangan dan pembuatan sistem keamanan jaringan pada *server* warnet *cyber* Toboali Kabupaten Bangka Selatan".

BAB III **METODOLOGI PENELITIAN**

Bab ini membahas tentang metologi penelitian yang akan digunakan dalam pembuatan aplikasi ini.

BAB IV **PEMBAHASAN DAN HASIL**

Bab ini membahas tentang proses pembuatan perancangan serta hasil dan aplikasi.

BAB V **PENUTUP**

Bab ini berisi kesimpulan dan saran yang di dapat dari pembahasan bab-bab sebelumnya.