# BAB 1

**PENDAHULUAN**

## Latar Belakang

Keamanan jaringan komputer sangat penting untuk mencegah penggunaan sumber daya jaringan dari pihak luar dan melakukan antisipasi terhadap risiko ancaman. Untuk menjamin pemeliharaan trafik pada suatu jaringan komputer, diperlukan *software* jaringan yang bisa berguna sebagai pemantau aktivitas jaringan. (Utomo, Sholeh, & Avorizano, 2017)

Metode paling umum untuk mencegah serangan jaringan dari pihak luar adalah dengan menunjuk seorang administrator. Karena administrator jaringan tidak dapat selalu mengawasi jaringan, maka ada sistem, khususnya”IDS..(*Intrusion..Detection System*), yang memiliki kemampuan untuk melakukan deteksi terhadap perilaku yang mencurigakan pada suatu jaringan dan melakukan automasi terhadap fungsi kerja administrator.

IDS (*Intrusion Detection System*) merupakan sebuah program yang dapat secara otomatis mendeteksi ancaman eksternal. Snort adalah perangkat lunak yang dapat mendeteksi aktivitas mencurigakan dalam suatu jaringan. (Atmaja, Prasetya, & Kresnha, 2018). Ketersediaan aplikasi Telegram sebagai sosial media *messenger* yang memudahkan administrator untuk memantau jaringan dari luar ruangan *server* sangat penting jika kita ingin menjaga keamanan suatu data atau jaringan yang kita miliki. Apalagi di era sekarang ini yang sudah tidak asing lagi dengan Telegram messenger, dan banyak administrator yang bisa mengunduh Telegram dan memanfaatkannya secara efektif.

Ketika ada ancaman terhadap target dalam hal ini *host server* yang dilindungi oleh aplikasi, aplikasi ini berusaha untuk memberikan peringatan dini. Aplikasi perpesanan Telegram mengirimkan peringatan dini dalam bentuk pesan percakapan ke *handphone* dari pihak administator jaringan.

Dalam penelitian yang dilakukan oleh (Marta, Hartawan, & Satwika, 2020) dengan judul analisis sistem monitoring keamanan *server* dengan SMS *alert* berbasis Snort.Dalam penelitian ini, sistem monitoring berbasis Snort dapat bekerja dengan baik sebagai pemberi peringatan dini adanya upaya serangan terhadap *server* dengan mengirimkan sebuah SMS alert. Selain itu, terdapat penelitian terkait juga mengenai membangun sistem mobile monitoring keamanan web aplikasi menggunakan Suricata dan *bot Telegram channel* oleh (Utomo, Sholeh, & Avorizano, 2017). Dalam penelitian ini, sistem monitoring untuk keamanan web aplikasi menggunakan Suricata berhasil mendeteksi beberapa jenis serangan serta mengirimkan notifikasi melalui *telegram* *messenger.*

Oleh karena itu penelitian ini dilakukan untuk mengembangkan penelitian tersebut, namun yang membedakan dari penelitian ini adalah menggunakan Snort sebagai alat *Intrusion..Detection System* *(IDS)* dan aplikasi *bot telegram* sebagai media notifikasi adanya serangan.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yan dijelaskan diatas penulis mendapatkan rumusan masalah sebagai berikut :

1. Bagaimana membangun sistem untuk mendeteksi adanya penyusup pada *server* jaringan menggunakan Snort sebagai *Intrusion Detection System*?
2. Bagaimana administrator jaringan dapat mengawasi jaringan secara *real-time*?
3. Bagaimana menggunakan aplikasi bot Telegram untuk mengirim notifikasi kepada administrator jaringan ketika adanya serangan?

## 1.3 Batasan Masalah

Dari permasalahan yang telah dirumuskan, maka penulis membatasi permasalahan dengan ruang lingkup sebagai berikut :

1. Membangun sistem keamanan jaringan berbasis Snort sebagai IDS (*Intrusion Detection System)*
2. Melakukan pengembangan terkait sistem pendeteksi serangan IDS (*Intrusion Detection System*) dengan bantuan Bot Telegram Messanger sebagai media notifikasi adanya serangan.
3. Pengujian sistem monitoring keamanan jaringan dilakukan secara *online*, diujikan pada jaringan lokal, dan pada *traffic* jaringan yang rendah.
4. Bentuk serangan yang akan dideteksi adalah *ICMP Ping, DoS (Denial of Services), Port Scanning, SSH Brute Force,* dan *Remote Telnet Access.*

## 1.4 Manfaat Penelitian

Adapun manfaat yang di dapat dari penelitian ini adalah :

1. Dengan membangun sistem monitoring keamanan jaringan diharapkan dapat membantu administrator untuk mengetahui upaya serangan.
2. Dengan diketahuinya upaya serangan ke suatu jaringan diharapkan administrator dapat mengaudit keamanan jaringan sehingga tidak terulang kembali.
3. Pemberitahuan dengan Bot Telegram bisa membantu pihak administator jaringan dalam melakukan pemantauan jaringan secara *real time*.
4. Sebagai tugas akhir penulis untuk menyelesaikan program sarjana.

## 1.5 Tujuan Penelitian

Berikut ini adalah tujuan penelitian dibuatnya sistem ini :

1. Mengembangkan solusi keamanan jaringan yang dapat diandalkan menggunakan Snort sebagai *Intrusion Detection System*.
2. Menggunakan Bot Telegram Messenger sebagai alat untuk memantau jaringan secara real time.

## 1.6 Sistematika Penulisan

Berikut ini adalah penulisan sistematis untuk memperjelas apa yang ingin dicapai oleh penulis dan untuk memastikan bahwa pembaca memahami apa yang ingin penulis lakukan:

**BAB 1 PENDAHULUAN**

Pada bab ini akan dijelaskan latar belakang masalah, rumusan masalah, batasan masalah, manfaat penelitian, tujuan penelitian, dan sistematika penulisan.

**BAB 2 TINJAUAN PUSTAKA**

Dalam bab ini berisi penjelasan mengenai landasan teori yang berhubungan dengan materi yang dibuah oleh peneliti. Teori tersebut antara lain tentang sistem deteksi intrusi, keamanan jaringan, jenis serangan pada jaringan komputer ,Snort, chatbot, telegram, dan *tools* untuk melakukan uji coba serta mekanisme mengenai bagaimana pengembangan sistem.

**BAB 3 METODOLOGI PENELITIAN**

Pada bab ini terdapat kumpulan dari metode bagaimana penulis mengumpulkan data untuk penelitian, tahapan dalam penelitian, serta metode pengembangan sistem.

**BAB 4 HASIL DAN PEMBAHASAN**

Dalam bab ini menlejaskan terkait hasil yang didapatkan berupa pemecahan masalah dari hasil pengujian sistem monitoring keamanan jaringan yang dijelaskan dalam bentuk gambar dan tabel.

**BAB 5 PENUTUP**

Pada bab ini berisi uraian tentang kesimpulan yang didapat dari penelitian yang telah dilakukan serta mengemukakan saran untuk para pembaca terkait pengembangan penelitian lebih lanjut.