# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Di internet terdapat bahaya besar yang mengintai, yaitu berbagai macam serangan (intrusi) yang berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan. Serangan-serangan itu dapat mengakibatkan kerusakan data dan bahkan kerusakan pada *hardware*. Di Indonesia, misalnya, setiap hari terjadi ratusan ribu serangan terhadap keamanan internet, seperti tindakan menyadap transmisi yang terjadi antara satu pihak dengan pihak yang lain, tindakan yang mengakibatkan terjadinya pemutusan komunikasi antara dua pihak yang seharusnya berinteraksi, dan tindakan lain yang berpotensi untuk menghancurkan informasi yang berjalan di atas infrastruktur internet.

Salah satu jenis serangan yang banyak terjadi adalah yang dikenal sebagai *Remote Code Execution* (eksekusi perintah dari jauh). *Remote Code Execution* dapat terjadi jika terdapat suatu celah yang memungkinkan pihak luar (penyerang) mengakses suatu *server* melalui perintah yang dikirim dari *server* lain. Mengingat besarnya kerugian yang dapat disebabkan oleh terjadinya *Remote Code Execution* maka diperlukan pengetahuan yang lebih mendalam tentangnya agar dapat dilakukan pengamanan maksimal terhadap sistem yang dipakai.

Salah satu upaya untuk meningkatkan keamanan jaringan komputer adalah dengan menerapkan *firewall*, baik yang berupa *software* ataupun *hardware* yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan.

Cara pengamanan yang lain adalah dengan mengimplementasikan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). Berbeda dari *firewall*, IDS adalah sebuah sistem yang digunakan untuk melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik data secara *real-time*, sedangkan IPS bertugas untuk mengambil keputusan berdasarkan data yang sudah terekam oleh IDS.

Penelitian ini dilandasi motivasi untuk mewujudkan suatu cara untuk mendeteksi dan mencegah serangan *Remote Code Execution,* yang didasarkan pada pemanfaatan salah satu *software* IDS yaitu Snort. Snort adalah *software* IDS yang tergolong mudah, *user friendly*, serta dapat di-*download* secara gratis di web resminya. Sedangkan untuk target serangan dipilih Wing FTP Server yang memang setelah diteliti masih memiliki celah untuk diserang dengan serangan *Remote Code Execution*, sehingga cocok digunakan dalam penelitian ini.

## 1.2 Rumusan Masalah

Akan dibangun suatu cara untuk mendeteksi dan mencegah serangan *Remote Code Execution* terhadap Wing FTP Server menggunakan Snort.

## 1.3 Batasan Masalah

Pembatasan masalah ini dimaksudkan agar pembahasan dapat terarah sehingga tujuan yang diharapkan dapat tercapai. Adapun pembatasan tersebut adalah sebagai berikut:

1. Sistem yang dibangun pada penelitian ini hanya untuk memantau aktivitas jaringan komputer jika terjadi serangan *Remote Code Execution* terhadap Wing FTP Server saja.
2. Sistem yang dibangun menggunakan Snort sebagai *Intrusion Detection*

*System* (IDS) dan *firewall* untuk memblokir IP penyerang (*attacker*).

3. Trafik data yang diamati dalam penelitian ini dibatasi pada paket data yang mengarah pada *server Intrusion Detection System* (IDS) yang berhubungan dengan keamanan *server*.

## 1.4 Tujuan Penelitian

Tujuan dari tugas akhir ini adalah mengamati bagaimana suatu serangan *Remote Code Execution* bekerja terhadap Wing FTP Server, dan kemudian melakukan deteksi serangan menggunakan Snort.

## 1.5 Manfaat Penelitian

Manfaat yang diperoleh dari keberhasilan tugas akhir ini adalah :

1. Peneliti mendapatkan ilmu pengetahuan baru yang belum pernah diberikan pada perkuliahan.
2. Hasil penelitian ini dapat digunakan sebagai masukan untuk mengoptimalkan keamanan pada jaringan komputer, khususnya dari serangan *Remote Code Execution*.
3. Sebagai bahan referensi bagi penulisan karya-karya selanjutnya dan menambah sumber pustaka bagi pengembangan sistem keamanan jaringan berbasis *open source* yang aman.
4. Sebagai bahan referensi bagi para akademisi untuk mengembangkan kreatifitasnya dalam menerapkan perancangan keamanan jaringan komputer.

## 1.6 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini secara garis besar adalah sebagai berikut:

BAB I PENDAHULUAN, memuat tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penelitian yang digunakan dalam penelitian.

BAB II TINJAUAN PUSTAKA, berisi tentang telaah penelitian terdahulu yang berhubungan dengan penelitian, landasan teori yang berkaitan dengan masalah yang diteliti dalam penelitian.

BAB III METODE PENELITIAN, merupakan inti dari penelitian, yang di dalamnya mencakup kegiatan penelitian mulai dari awal sampai akhir, diantaranya adalah: gambaran umum penelitian, alokasi waktu, perangkat yang dibutuhkan, metode penelitian, serta alur penelitian.

BAB IV HASIL DAN PEMBAHASAN, berisi tentang hasil daripada penelitian yang dilakukan berikut pembahasannya, yang meliputi beberapa poin diantaranya: tahap pengujian dan implementasi sistem yang sudah dirancang, serta tahap analisa dari sistem.

BAB V KESIMPULAN Bab ini berisi tentang kesimpulan dan saran dari hasil penelitian.