BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Diera teknologi modern saat ini, keamanan jaringan komputer merupakan suatu hal yang sangat penting untuk diperhatikan. Semakin banyaknya penyusupan atau serangan yang dilakukan oleh *hacker* menjadi salah satu faktor utama dalam hal ini [1]. Serangan dan penyusupan terhadap suatu jaringan dipengaruhi juga oleh teknologi yang semakin canggih dan modern. Untuk itu suatu sistem keamanan jaringan diharapkan dapat mendeteksi dan mencegah suatu tindakan penyusupan atau serangan di jaringan oleh pihak-pihak luar yang tidak bertanggung jawab.

Bentuk serangan dari luar jaringan yang bersifat merugikan antara lain adalah *port scanning* dan *Denial of Service* (DoS). Dimana *port scanning* adalah serangan yang dimanfaatkan untuk mencari titik celah *port* terbuka dari suatu server, untuk kemudian mencari kelemahan yang ada pada server tersebut [2]. Kemudian serangan *Denial of Service* (DoS), yaitu serangan yang membanjiri suatu server dengan cara mengirimkan banyak paket data sehingga server menjadi *down* [2]. Kedua serangan tersebut merupakan suatu serangan yang sangat berbahaya jika tidak dapat ditangani dan dicegah oleh jaringan komputer. Pihak-pihak yang tidak berwenang akan mengambil keuntungan dengan melakukan penyerangan tersebut.

Untuk mencegah berbagai ancaman jaringan, ada beberapa teknik yang bisa diterapkan sebagai suatu bentuk pendeteksian dan pencegahan terhadap suatu aktivitas yang mencurigakan dalam jaringan komputer, yaitu pendeteksian terhadap serangan jaringan menggunakan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). Dimana sistem IDS berfungsi untuk memonitoring lalu lintas pada suatu jaringan komputer dan IPS berfungsi untuk menghentikan percobaan ancaman terhadap suatu jaringan. Kedua fungsi ini, dapat bekerja sama ketika serangan atau penyusupan masuk. Snort merupakan aplikasi *Intrusion Detection Prevention System* (IDPS) yang dapat melakukan monitoring paket data yang masuk kedalam jaringan [3]. Apabila terjadi aktivitas yang mencurigakan pada jaringan, maka Snort akan memberikan pemberitahuan serta pemberhentian

sesuai dengan fungsi *Intrusion Detection Prevention System* (IDPS) akan melakukan identifikasi dan mendeteksi serangan tersebut.

Berdasarkan latar belakang diatas, maka penulis melakukan penelitian yang berjudul "**ANALISIS PERFORMANSI INTRUSION PREVENTION DETECTION SYTEM (IDPS) TERHADAP SERANGAN *PORT SCANNING* DAN UDP *FLOODING***"

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah :

1) Bagaimana performansi *Intrusion Detection Prevention System* (IDPS) dalam menangani serangan didalam jaringan pada komputer ?
2) Bagaimana performansi *tool* Snort dalam mendeteksi dan mencegah serangan *Port scanning* dan *Denial of Service* (DoS)?
3) Bagaimana perancangan *rule* pada *tool* Snort dalam implementasi pendeteksian dan pencegahan terhadap serangan *Port scanning* dan *Denial of Service* (DoS) ?
4) Bagaimana performansi *Intrusion Detection Prevention System* (IDPS) pada sisi *client* dalam menangani serangan *port scanning* dan *Denial of Service* (DoS)?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah :

1) Penerapan *Intrusion Detection Prevention System* (IDPS) dalam penelitian ini hanya untuk melakukan pendeteksian dan pencegahan dari serangan *Port scanning* dan *Denial of Service* (DoS).
2) Penerapan *Intrusion Detection Prevention System* (IDPS) dalam penelitian ini hanya menggunakan *Host Intrusion Detection Prevention System* (HIDPS).
3) Penerapan *Intrusion Detection Prevention System* (IDPS) dalam penelitian ini hanya menggunakan *tool* Snort.
4) Sistem jaringan yang dibuat pada penelitian ini adalah jaringan lokal (Lokal *Area Network*).

5) Menggunakan jenis serangan UDP *flooding* pada *Denial of Service* (DoS) dan *port scanning* untuk uji coba penyerangan.
6) Menggunakan aplikasi Nmap untuk *tool* serangan *port scanning.*
7) Menggunakan aplikasi LOIC untuk *tool* serangan UDP *flooding*.
8) Menggunakan Linux Ubuntu versi 20.04 sebagai sistem operasi yang digunakan oleh web server.
9) Menggunakan Windows 10 sebagai sistem operasi yang digunakan oleh *attacker*.
10) Protokol yang dianalisis pada penelitian ini adalah protokol TCP dan HTTP.
11) Parameter pengukuran pada pengujian hanya menggunakan *Quality of Service* (QOS).

1.4 TUJUAN

Tujuan dari penelitian ini adalah :

1) Untuk mengetahui performansi *Intrusion Detection Prevention System* (IDPS) dalam menangani serangan didalam jaringan pada komputer.
2) Untuk mengetahui performansi *tool* Snort dalam mendeteksi dan mencegah serangan *Port scanning* dan *Denial*) *of Service* (DoS).
3) Untuk mengetahui perancangan *rules* pada *tool* Snort dalam implementasi pendeteksian dan pencegahan terhadap serangan *Port scanning* dan *Denial of Service* (DoS).

1.5 MANFAAT

Manfaat dari penelitian ini adalah :

1) Mampu meningkatkan sistem pendeteksian dan pencegahan serangan pada suatu jaringan dengan menggunakan *Host Intrusion Detection Prevention System* (HIDPS).
2) Mampu meningkatkan sistem keamanan dalam suatu jaringan terhadap serangan *Port scanning* dan *Denial of Service* (DoS).
3) Mampu merancang sebuah sistem keamanan yang dapat mempermudah administrator jaringan dalam mengatasi suatu serangan *Port scanning* dan *Denial of Service* (DoS).

1.6 SISTEMATIKA PENULISAN

Penelitian ini terdiri dari beberapa bab. Bab 1 berisi tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan. Bab 2 berisi tentang kajian pustaka, pengertian jaringan komputer, sistem keamanan jaringan pada komputer, pengertian dan cara kerja Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS), pengertian dan penjelasan tentang *Firewall*, jenis-jenis serangan, serta penjelasan tentang *Port scanning* dan *Denial of Service* (DoS). Pada bab 3 membahas mengenai rancangan alur penelitian, topologi dan konfigurasi jaringan. Bab 4 membahas mengenai analisa dan pembahasan. Bab 5 membahas mengenai kesimpulan dari penelitian serta saran untuk penelitian selanjutnya.