BAB I
PENDAHULUAN

1.1 Latar Belakang

Server merupakan pusat penyedia layanan dan pengolahan data dalam suatu jaringan, permintaan yang dikirim oleh *client* akan diolah *server*. Kinerja *server* bergantung terhadap paket pertukaran data yang dikirim oleh *client* pada jaringan. Keamanan sangat dibutuhkan agar *server* dalam kondisi yang baik. Jika dalam kondisi yang kurang baik serangan dapat dengan gampang masuk dan menyerang jaringan komputer, jika pada jaringan komputer tersebut tidak terdapat sistem keamanan untuk mengatasi serangan yang masuk [1].

Kemanan jaringan menjadi sangat penting dan patut untuk diperhatikan dalam memberikan layanan agar dapat melindungi *server* yang berada dalam jaringan dan meminimalisir terjadinya serangan seperti *Denial of Service* (DoS). *Denial of Service* adalah serangan yang dilakukan para penyerang dengan tujuan agar layanan yang diberikan terganggu, tidak bisa diakses hingga membuat layanan tersebut mati. Serangan yang diberikan ada beberapa macam seperti *ICMP Flood, UDP Flood, SYN Flood, FTP Bruteforce.* Dari permasalahan tersebut solusi yang dapat ditawarkan adalah menggunakan keamanan jaringan dengan sistem *Host-Based Intrusion Prevention System* (HIPS). HIPS adalah kemanan jaringan yang mencegah dan memberikan tindakan pada aktivitas tidak normal seperti serangan menuju ke suatu *host* yaitu *server*. Sistem kemanan jaringan tersebut dibantu dengan metode deteksi *anomaly detection* yang bertujuan untuk memeriksa penyimpangan yang terjadi pada jaringan dengan membandingkan profil jaringan yang normal.

Penelitian ini membatasi permasalahan yang akan dibahas hanya pada konfigurasi HIPS pada Snort. Snort diimplementasikan pada komputer dengan sistem operasi Ubuntu sebagai *bridge* untuk mengelola paket atau aktivitas yang masuk dan keluar dari *server*. Pengujian dilakukan oleh komputer *attacker* dengan melakukan serangan bervariasi seperti *ICMP Flood, UDP Flood, SYN Flood,* dan *FTP Bruteforce* terhadap *server*. Kemudian analisa hasil pengujian terkait peningkatan performansi

dari server seperti *throughput, packet loss, delay, jitter* dan CPU *usage* serta hasil dari pencegahan penyerangan dari HIPS. Penelitian ini diharapkan mampu membantu dalam memantau dan meningkatkan kinerja pelayanan dari *server*.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut rumusan masalah pada penelitian ini adalah:

1) Bagaimanakah cara mensimulasikan sistem keamanan jaringan HIPS dengan metode *anomaly detection*?
2) Bagaimanakah hasil uji dari sistem keamanan jaringan HIPS menggunakan metode *anomaly detection*?
3) Bagaimanakah performansi *server* menggunakan sistem keamanan jaringan HIPS dengan metode *anomaly detection* mengenai CPU *usage*, *throughput, delay, jitter,* dan *packet loss* terhadap serangan yang datang?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1) Dalam penelitian ini menganalisis performansi kinerja *server* dan jaringan menggunakan sistem keamanan jaringan HIPS dengan metode *anomaly-based detection*.
2) Pengujian menggunakan empat jenis serangan yaitu serangan *ICMP Flood*, *UDP Flood*, *SYN Flood,* dan *FTP Bruteforce.*
3) Penelitian dilakukan pada jaringan lokal.
4) Parameter yang diuji yaitu CPU *usage, throughput, delay, jitter,* dan *packet loss*.
5) *Server* menggunakan sistem operasi Windows yang sudah terpasang dan memberikan layanan *FTP Server* dan *Web Server*.
6) Penyerang menggunakan sistem operasi Kali Linux.
7) Penerapan keamanan jaringan HIPS menggunakan aplikasi Snort yang terpasang pada jembatan.

8) Penyerangan menggunakan aplikasi Hping3 dan Hydra yang terpasang pada penyerang.
9) Pengujian dibantu menggunakan aplikasi Wireshark dalam menganalisa data.

1.4 Tujuan Penelitian

1) Dapat mensimulasikan sistem keamanan jaringan HIPS dengan metode *anomaly detection*.
2) Mengetahui serangan yang datang dengan menganalisis pola aktifitas serangan yang tidak teridentifikasi pada keamanan jaringan HIPS menggunakan metode *anomaly detection*.
3) Mengetahui performansi *server* menggunakan keamanan jaringan HIPS dengan metode *anomaly detection* mengenai CPU *usage, throughput, delay*, *jitter,* dan *packet loss.*

1.5 Manfaat Penelitian

Memberikan gambaran performansi mengenai keamanan jaringan menggunakan HIPS serta penggunaan metode *anomaly detection* dapat mendeteksi ancaman dengan cara membandingkan pemakaian saat terjadi kegiatan *anomaly* dengan pemakaian saat kondisi jaringan normal yang dapat dilihat dari pemakaian *resource* yang bekerja seperti CPU *usage*, dan jaringan yang sedang digunakan seperti *throughput, delay*, *jitter,* dan *packet loss*.

1.6 Sistematika Penulisan

Penulisan yang sistematis terbagi menjadi lima bab. Diawali dengan bab satu yang berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan. Pada bab dua membahas mengenai kajian pustaka dan teori-teori yang menjadi acuan bagi penulis dalam penyusunan proposal diantaranya membahas mengenai *Intrusion Detection System* (IDS), *Firewall, Intrusion Prevention System* (IPS), *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS), *Ping of*

Death, UDP Flood, SYN Flood, *ICMP Flood*, *Bruteforce*, Snort, Wireshark, Ethtool, Hping, CUPP, Hydra, dan *Quality of Service*.

Dilanjutkan pada bagian yang membahas mengenai perencanaan penelitian yang memuat alur penelitian, alat yang akan digunakan, proses konfigurasi, serta skenario pengujian yaitu bab tiga. Pada bagian hasil dan pembahasan atau bab empat membahas mengenai hasil pengujian *baseline* dan beberapa serangan yang ditujukan ke target baik sebelum dan sesudah menggunakan metode *anomaly-detection* serta analisis dari pegujian yang dilakukan. Ditutup dengan kesimpulan dan saran yaitu bab lima, membahas mengenai kesimpulan dan saran untuk pengembangan penelitian kedepannya.