BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan jaringan pada *server* merupakan faktor penting dalam jaringan. Keamanan yang baik dapat memberikan rasa percaya pada suatu *server* yang digunakan dan mengurangi kerugian dari serangan yang terjadi pada jaringan suatu *server*. (Pratama dan Handayani, 2019). Keamanan jaringan sangat vital bagi sebuah jaringan komputer. Kelemahan-kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan kerugian berupa kehilangan data, kerusakan sistem *server*, tidak maksimal dalam melayani *user* atau bahkan kehilangan aset-aset berharga institusi. Sudah selayaknya keamanan jaringan harus lebih diperhatikan untuk melindungi sistem dari ancaman serangan yang semakin canggih dan beragam, terlebih lagi ketika jaringan *local* sudah terhubung ke internet maka ancaman keamanan jaringan akan semakin meningkat. (Anugrah dan Rahmanto, 2017).

Kemungkinan adanya serangan atau penyusup dalam sebuah jaringan itu memang ada. Untuk itu dibutuhkan suatu sistem yang dapat mendeteksi serangan atau penyusup dan memberi peringatan kepada *network administrator* bila terjadi serangan ataupun penyusup pada jaringan. Fokus dalam keamanan ini yaitu mengamankan jaringan *server* dan mendeteksi adanya usaha-usaha penyusupan terhadap sebuah sistem. Salah satu metode keamanan untuk mengamankan suatu jaringan adalah menggunakan IDS.

Dengan adanya IDS dalam sebuah jaringan, maka kemungkinan adanya serangan atau penyusup kedalam sebuah jaringan akan semakin kecil karena akan terdeteksi oleh IDS dan juga IDS akan memberi peringatan kepada *network administrator* bila terjadi serangan atau penyusup pada jaringan. Terdapat dua teknik yang digunakan dalam IDS yaitu NIDS (*Network Based Intrusion Detection System*) dan HIDS (*Host Based Intrusion Detection System*). HIDS juga mampu melakukan pemeriksaan sistem tambahan yang hanya bisa dilakukan bila aplikasi IDS dipasang pada *host*, seperti *file integrity checking, registry monitoring, log*

analysis, rootkit detection dan *active respone*. Salah satu *software* yang menggunakan teknik HIDS ialah OSSEC (*Open Source Security*).

Pada peneliti sebelumnya (Bouziani, dkk, 2019) "*A Comparative study of Open Source IDSs according to their Ability to Detect Attacks*", dijelaskannya bahwa frekuensi tindakan jahat terhadap sistem informasi meningkat dalam beberapa tahun terakhir, dan keamanan sistem informasi menjadi sulit karena alat penyerang baru dan skill penyerang, yang dapat membahayakan sistem informasi dan mengarah ke kerugian finansial dan material yang sangat besar.

Oleh karena itu, penulis berinisiatif untuk membuat sistem keamanan jaringan untuk menghindari serangan atau penyusup yang berusaha masuk ke dalam *server* dan mengakses data-data yang ada di *server* tersebut. Dan juga menghindari dari serangan yang menyebabkan turunnya peforma *server* dan bahkan dapat menyebabkan *server* tersebut menjadi lumpuh. Berdasarkan latar belakang diatas penulis mencoba untuk membuat sistem kemanan jaringan menggunakan teknik HIDS dengan judul "**Implementasi Sistem Keamanan Jaringan Menggunakan Teknik Host Based Intrusion Detection System (HIDS) Pada Jurusan Teknik Komputer**"

1.2. Rumusan Masalah

Berdasarkan uraian diatas, maka penulis merumuskan permasalahan yang ada yaitu bagaimana menerapkan sistem keamanan jaringan menggunakan teknik *Host Based Intrusion Detection System* (HIDS).

1.3. Batasan Masalah

Agar penulisan laporan akhir dapat terarah dengan baik dan menghindari pembahasan yang jauh dari pokok permasalahan, maka penulis membatasi yaitu hanya mengenai penerapan sistem kemanan jaringan menggunakan teknik *Host Based Intrusion Detection System* (HIDS) Menggunakan *Software* OSSEC.

1.4. Tujuan

Adapun tujuan dari penulisan laporan akhir ini yaitu menerapkan sistem keamanan jaringan menggunakan teknik *Host Based Intrusion Detection System* (HIDS).

1.5. Manfaat

Adapunt manfaat dari penulisan laporan akhir ini ialah

1. Mencegah dari sembarang orang yang bisa mengakses *server*.
2. Menambah pengetahuan bagi penulis dengan dapat lebih memahami dan menguasai serta menerapkan pada dunia kerja yang sebenarnya.