BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet merupakan sebuah jaringan global, dimana setiap pengguna dapat saling berkomunikasi dan bertukar informasi. Seiring maraknya penggunaan Internet, banyak perusahaan yang kemudian beralih menggunakan internet sebagai bagian dari jaringan mereka untuk menghemat biaya. akan tetapi permasalahan keamanan masih menjadi faktor utama dalam menghadapi kejahatan seperti *Cyber Crime* yaitu proses penyerangan yang dilakukan dengan menyusup ke dalam suatu sistem jaringan komputer secara ilegal tidak atas sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya (Jawa, Dan, and Timur 2019).

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan

tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem juga tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis. Apabila terjadi malfungsi, administrator tidak dapat lagi mengakses sistem secara remote sehingga tidak akan dapat melakukan pemulihan sistem dengan cepat.

Oleh karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat dan secara otomatis sehingga memungkinkan administrator mengakses sistem walaupun terjadi malfungsi jaringan. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

Keamanan komputer atau dalam Bahasa Inggris computer security atau dikenal juga dengan sebutan *cyber security* atau IT *security* adalah keamanan infromasi yang diaplikasikan kepada komputer dan jaringannya. *Computer security* atau keamanan komputer bertujuan membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi , teknologi yang dikenal dan

dikembangkan dengan nama keamanan informasi yang diterapkan pada komputer.

Faktor keamanan begitu penting, dikarenakan tidak semua informasi data bersifat terbuka untuk umum dan tak semua orang berhak mengaksesnya. Adapun salah satu untuk keamanan sistem jaringan komputer yaitu *Intrusion Detection System* (IDS) , *Intrusion Prevention System* (IPS) dan *Honeypot* untuk meningkatkan sistem keamanan. Faktor keamanan begitu penting, dikarenakan tidak semua informasi data bersifat terbuka untuk umum dan tak semua orang berhak mengaksesnya. Salah satu alat bantu keamanan sistem jaringan komputer adalah dengan menggunakan *honeypot* untuk meningkatkan sistem keamanan.

Adapun beberapa sistem keamanan jarigan komputer yang sudah di implementasi kan oleh beberapa peneliti terdahulu seperti **Implementasi *Snort Intrusion Detection System* (IDS) Pada Sistem Jaringan Komputer** hasil pada penelitian tersebut IDS bekerja baik dalam mendeteksi serangan serta membaca suatu serangan dan penyalahgunaan jaringan dan kelemahannya pada keterbatasan pada rules (Dar and Harahap 2017) . **Implementasi Sistem Keamanan Server Menggunakan *Honeypot* Dan *Raspberry Pi* Terhadap *Attacker*** pada

Honeypot sebagai server bayangan apabila ada serangan oleh *Attacker*, dan juga bisa melakukan blocking terhadapat ip address. Selain itu biaya yang dikeluarkan murah karena menggunakan *Risberry PI* (Utomo et al. 2020).

Berdasarkan uraian diatas, untuk meningkatkan sebuah keamanan pada suatu jaringan penulis mau merelasikan sebuah sistem dan mengambil judul "**Analisis Sistem Keamanan Jaringan Menggunakan Metode *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), Dan *Honeypot*".**

1.2 Rumusan Masalah

Adapun masalah sebagai berikut :

1. Bagaimana cara mengatasi suatu kegiatan yang bersifat ilegal pada suatu jaringan yang dilakukan orang tidak dikenal antara lain :
    a. SSH *Brute Force*
    b. Port Scanning

1.3 Batasan masalah

Agar penelitian ini berfokus pada pembahasan yang diharapkan maka diperlukan batasan - batasan masalah dalam penelitian sebagai berikut :

1. Sistem operasi yang digunakan untuk menjalankan Server menggunakan Ubuntu.

2. Serangan yang dilakukan untuk menguji keamanan sistem berupa SSH *Brute Force,* dan *Port Scanning.*

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai penulis dalam penelitian ini adalah sebagai berikut

1. Untuk mengatasi sebuah sistem pada jaringan server yang mencurigakan serta medeteksi dengan cara menerapkan metode *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), dan *Honeypot.*

1.5 Manfaat Hasil Penelitian

Adapun manfaatnya adalah

1. Hasil penelitian ini dapat digunakan sebagai masukan terhadap upaya peningkatan keamanan.
2. Dapat memberikan informasi kepada administrator jaringan tentang teknik atau pola-pola serangan yang digunakan oleh attacker.
3. Dapat memberikan referensi dalam mengembangkan kemampuan kalangan akademis dalam menerapkan teori keamanan jaringan komputer.