BAB 1. PENDAHULUAN

1.1 Latar belakang

Keamanan teknologi dan informasi merupakan hal yang paling mendasar untuk diperhatikan dalam sebuah lingkungan organisasi maupun perorangan. Keamanan jaringan komputer sebagai bagaian dari sistem yang penting untuk menjaga validitas dan integritas serta menjamin ketersedianaan layanan bagi penggunanya. Sistem harus bisa dilindung dari serangan dan usaha peretasan oleh pihak-pihak yang tidak bertanggung jawab.

Beberapa aplikasi atau sistem telah dikembangkan dan dikerahkan untuk memerangi serangan yang terjadi. Misalnya teknik observasi menggunakan firewall atau *Intrusion Prevention System* (IPS) untuk mencegah serangan atau mendeteksi timbulnya serangan menggunakan *Intrusion Detection System* (IDS). Honeypot adalah sebuah sistem atau komputer yang sengaja digunakan sebagai umpan untuk menjadi sasaran penyerang. Komputer ini melayani serangan yang dilakukan oleh penyerang dengan cara menyusup ke server. Honeypot akan memberikan data palsu jika ada sesuatu yang aneh memasuki sistem atau server. Secara teori, honeypot tidak akan mencatat lalu lintas yang sah. Dengan demikian terlihat bahwa orang-orang yang berinteraksi dengan honeypot adalah semua pengguna yang menggunakan sumber daya sistem yang digunakan secara ilegal. Oleh karena itu, honeypot seolah-olah menjadi sistem yang berhasil ditembus oleh penyerang, padahal penyerang tersebut tidak menembus sistem sebenarnya melainkan sistem palsu.

Honeypot Cowrie merupakan alat keamanan jaringan yang bertindak sebagai server palsu. Ini dirancang untuk merekam upaya brute force dan interaksi shell yang dilakukan penyerang. Cowrie juga berperan sebagai proxy untuk SSH dan Telnet, memungkinkan pengamatan perilaku penyerang terhadap sistem lain. Cowrie dikembangkan dari Kippo, honeypot interaksi rendah sebelumnya. Dengan Cowrie, administrator jaringan dapat memahami lebih baik tentang metode, taktik, dan prosedur yang digunakan oleh penyerang, yang sangat membantu dalam meningkatkan keamanan jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka dapat diambil rumusan masalah sebagai berikut:

1. Bagaimana mengimplemtasikan teknik pengalihan arah penyerangan atau menyamarkan serangan terhadap server yang masuk menggunakan *Honypot* dan *Intrusion Detection System* (IDS).
2. Bagaimana mendeteksi serangan atau aktivitas illegal pada server secara otomastis.
3. Bagaimana perfoma sistem keamanan yang dibagun terhadap serangan atau aktivitas pada server.

1.3 Tujuan

Berdasarkan rumusan masalah yang telah dijelaskan, tujuan pembuatan sistem ini adalah untuk merancang sistem keamanan jaringan yang mampu mengalihkan serangan atau penyusupan dengan menggunakan IDS dan *Honeypot* yang digabungkan dengan bot pada Telegram, sehingga dapat mendeteksi gangguan secara otomatis.

1.4 Manfaat

Sistem yang akan dibangun ini meningkatkan keamanan server dengan mengimplementasikan deteksi penyerang server dengan menggunakan IDS dan menerapkan teknik pengalihan serangan/jebakan untuk penyerang dengan Honeypot.

1.5 Batasan Masalah

Bembatasan terhadap masalah yang digunakan pada pembuatan sistem ini antara lain:

1. Server yang digunakan menggunakan sistem operasi Linux Ubuntu.
2. Melakukan simulasi pengujian keamanan server dengan Honeypot dan IDS.
3. Menggunakan Bot pada Telegram sebagai pengirim pesan saat terdapat aktivitas mencurigakan pada sistem.