BAB 1. PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer merupakan sesuatu yang harus diperhatikan. Untuk itu peran administrator jaringan sangat penting dalam menjaga keamanan jaringan komputer. Namun para administrator jaringan tidak dapat selalu berada dekat dengan ruang *server*. Hal ini dikarenakan ruangan *server* dirancang dengan suhu yang dingin dan stabil dimana hal ini tentu tidak baik untuk kesehatan. Sehingga biasanya administrator menjalankan tugasnya dari luar ruangan *server* dengan menggunakan *remote server*. Dengan demikian administrator jaringan cukup melakukan autentikasi ke aplikasi *remote server* untuk mengakses komputer *server*. *Remote server* juga dapat dimanfaatkan jika administrator berada jauh dari jangkauan jaringan lokal dengan menghubungkan aplikasi *remote server* ke internet.

Dengan adanya *remote server* maka diperlukan *port* yang digunakan untuk mengakses komputer *server*. Hal ini tentu mengancam keamanan *server* dikarenakan terdapat *port* yang terbuka untuk digunakan oleh *remote server*. Semakin sering seorang administrator mengakses *remote server* maka celah pada *port* yang digunakan akan semakin mudah dilihat oleh para *attacker*. Jika administrator tidak terhubung terus dengan *server* maka pendeteksian serangan-serangan pada *server* dan jaringan juga akan sulit terdeteksi.

Untuk mengatasi masalah tersebut maka diperlukan pengamanan pada *remote server* dengan menggunakan *Port knocking* dan *Intrusion detection system* (IDS). *Port knocking* digunakan untuk menutup *port* yang digunakan untuk mengakses *remote server*. Namun seorang administrator jaringan dapat melakukan koneksi ke *server* melalui *port* tertutup tersebut. Sedangkan penggunaan IDS adalah untuk mendeteksi adanya gangguan-gangguan pada jaringan komputer dengan cara mendeteksi gangguan-gangguan tersebut berdasarkan pola-pola anomali yang ditimbulkan. Hal ini diperlukan untuk melakukan *monitoring* serangan terhadap *remote server*. Jika terdapat serangan maka IDS akan mengirimkan *alert* pada administrator jaringan. Sehingga

administrator dapat mengetahui keadaan *remote server* selama 24 jam penuh. Hal ini memudahkan administrator sehingga tidak perlu mengakses komputer *server* setiap saat dan jika terdapat serangan, administrator dapat segera melakukan antisipasi.

Kombinasi kedua metode diatas dapat mengatasi masalah yang timbul dari penggunaan *remote server* terutama yang terhubung dengan internet. Memberikan keamanan yang responsif pada *server* jaringan dan memberikan keamanan akses *server* jaringan dari jarak jauh. Dengan begitu administrator tidak perlu selalu berada di depan komputer. Sehingga kesehatan para administrator jaringan akan lebih terjaga.

1.2 Rumusan Masalah

Dari permasalahan pada latar belakang dapat diambil rumusan masalah yaitu bagaimana menerapkan aplikasi *remote server* untuk menghubungkan administrator dan *server*. Dimana celah yang terdapat dalam penggunaan *remote server* dapat diamankan menggunakan metode *Port knocking* dan IDS.

1.3 Batasan Masalah

Dalam penelitian yang akan dilakukan penulis hanya terbatas pada beberapa hal berikut ini:

a. Membangun *remote server* berbasis *telnet* yang terhubung dengan internet.
b. Menggunakan Port knocking untuk menutup port pada telnet.
c. Menerapkan IDS menggunakan aplikasi Snort untuk memantau serangan pada *remote server*.
d. Konfigurasi dilakukan pada komputer *server* dengan sistem operasi Debian 8.0
e. DBMS (*Database Management System*) yang digunakan adalah MySQL

1.4 Tujuan

Adapun tujuan pembuatan tugas akhir yang berjudul "Implementasi *Port Knocking* dan *Intrusion Detection System* (IDS) Untuk Pengamanan Pada *Remote Server*" yaitu dapat membangun *remote server* yang digunakan untuk menghubungkan administrator dan *server*. *Remote server* tersebut nantinya akan

diamankan oleh sistem keamanan jaringan menggunakan *Port knocking* dan *Intrusion Detection System*, sehingga celah dapat diamankan.

1.5 Manfaat

Manfaat dari penelitian ini adalah sebagai berikut:

a. Memudahkan administrator jaringan untuk mengatur jaringan melalui internet
b. Memberikan keamanan dalam menggunakan *remote server*
c. Memudahkan dalam memantau kondisi jaringan
d. Mempercepat respon terhadap serangan dari luar jaringan