# BAB 1. PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan sistem jaringan komputer saat ini khususnya pada penggunaan internet sangat cepat. Sekarang semua komunikasi lebih banyak menggunakan jaringan internet. Bahkan internet bisa dikatakan sebagai kebutuhan karena semua kalangan menggunakannya dari anak-anak sampai orang dewasa. Dengan beragam kegunaan untuk pembelajaran maupun untuk berbisnis. Namun dalam sistem jaringan komputer sudah pasti memiliki kelemahan terutama pada *server*. Karena *server* adalah suatu perangkat yang telah ter-integrasi dengan spesifikasi *hardware* tertentu dan juga *software* yang memiliki berbagai fungsi tertentu sesuai dengan kebutuhan *client.* Oleh karena itu administrator harus memerhatikan masalah yang timbul pada sistem jaringan itu sendiri. Dengan adanya penggunaan *Virtualisasi* diharapkan dapat menggantikan *server* yang awalnya menggunakan PC.

Namun *internet* juga belum begitu mempertimbangkan *security* dan privasi pengguna. Dengan munculnya *attacker* dan *hacker* membuat administrator harus memikirkan tentang keamanan jaringannya. Beberapa keamanan yang pernah digunakan adalah Telnet maupun rlogin tetapi karena tidak melakukan enkripsi terhadap data sebelum dikirim ke *server* maka diganti dengan perangkat lunak yang dianggap lebih aman yaitu *Secure Shell (SSH).* Administrator akan menyediakan layanan *Service Remote Access* agar *server* dapat diakses. Dengan adanya layanan tersebut maka keadaan *port* harus terbuka secara terus-menerus oleh karena itu administrator dapat menggunakan salah satu aplikasi dari *firewall* yaitu *Iptables.* Aplikasi ini dapat melakukan filtering sehingga membuat keberadaannya sungguh fleksibel untuk mengamankan suatu jaringan. Selain itu administrator juga memiliki metode lain untuk menambahkan keamanan jaringan dengan menggunakan metode *port knocking* serta melakukan pengamanan pada lingkungan jaringan saat pengiriman paket dengan menggunakan jaringan VPN

sehingga akan tetap terjaga kerahasiaan paket yang dikirim dan diterima oleh *server* dan *client.*

Metode *port knocking* bekerja dengan sistem "*buka port pada suatu klien,bila klien itu meminta dan tutup kembali bila klien sudah selesai".* Keadaan itu memaksa klien yang ingin mengakses layanan *service* pada *server* harus mengirimkan autentikasi terlebih dahulu ke *server.*

## 1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut,maka dapat di ambil perumusan masalah yaitu :

1. Membangun sistem keamanan SSH (*Secure Shell)* dengan *port knocking* di *server*
2. Membangun sistem jaringan antar *Server* dan *Client* menggunakan jaringan VPN ( *Virtual Private Network)*
3. Mengevaluasi hasil kerja dari *port knocking* dan VPN

## 1.3 Batasan Masalah

Metode yang digunakan dalam permasalahan ini :

1. VPN *server* menggunakan *protokol tunneling (OpenVPN)* dan untuk *Client* menggunakan *ubuntu 14.04 desktop*
2. Sistem yang diamankan adalah port 22 yaitu SSH (*Secure Shell)*
3. Dalam sistem ini tidak ada layanan *server* namun klient hanya meremote *server* melalui port 22.

## 1.4 Tujuan

Adapun tujuan dari laporan akhir ini:

1. Mampu mengamankan port 22 yaitu *secure shell (SSH)* dengan menggunakan metode *port knocking* dan VPN

2. Mampu mengimplementasikan metode *port knocking* dan VPN untuk remote *access secure shell* (*SSH*).
3. Mampu melakukan keamanan port 22 di jaringan lokal dengan menggunakan VPN (Virtual Private Network)

**1.5 Manfaat**

Adapun manfaat dari laporan akhir ini:

1. Dapat mengurangi serangan dari pelaku-pelaku yang berniat buruk untuk keamanan *server* dengan metode *port knocking.*
2. Dapat melakukan konektivitas remote *access secure shell (SSH)* dengan keadaan *port* tertutup dan terbuka dengan waktu yang telah ditentukan.
3. Dapat menjadi acuan referensi bagi mahasiswa yang akan mengerjakan tugas akhir bertema jaringan komputer