BAB I
PENDAHULUAN

1.1 Latar belakang masalah

Pendukung produktivitas perusahaan sekarang ini semakin bervariasi dan berkembang seperti penggunaan teknologi internet sebagai pendukung kinerja perusahaan-perusahaan yang memiliki kantor pusat dan kantor cabang dengan seolah-olah berada pada jaringan lokal melewati jaringan publik (internet) dengan menggunakan teknologi VPN.

VPN (*Virtual Private Network*) merupakan sebuah teknologi komunikasi yang memungkinkan adanya koneksi dari dan ke jaringan publik serta bagaikan menggunakan jaringan lokal itu sendiri meskipun berada di tempat lain. Dengan menggunakan jaringan publik ini, maka *user* dapat mengakses fitur-fitur yang ada di dalam jaringan lokalnya, mendapatkan hak dan pengaturan yang sama bagaikan secara fisik kita berada di tempat dimana jaringan lokal itu berada. Hal yang perlu diingat adalah sebuah *private network* haruslah berada dalam kondisi diutamakan dan terjaga kerahasiaannya. Keamanan data dan ketertutupan transfer data dari akses ilegal serta skalabilitas jaringan menjadi standar utama dalam *Virtual Private Network* ini.

VPN menggunakan beberapa jenis protokol sebagai metode penyampaian data yang melewati tunnel tersebut. Diantaranya protokol PPTP (*Point to Point Tunnelig Protokol)*, L2TP *(Layer 2 Tunneling Protocol)*, IPSec *(IP Security)*, dan L2TP over IPSec. PPTP beroperasi pada *Layer* 2 pada model referensi OSI dan didasarkan pada standar *Point to Point Protocol* (PPP) untuk jaringan *dialup* yang

memungkinkan semua pengguna dengan PPP *client* menggunakan ISP untuk terkoneksi ke internet. L2TP adalah suatu standar yang dikembangkan oleh *Internet Engineering Task Force* (IETF) (RFC 2661) pada *layer* 2, yang merupakan kombinasi dari keunggulan-keunggulan fitur dari protokol L2F dan PPTP. IPSec merupakan suatu standar keamanan komunikasi melalui jalur *internet* dengan autentikasi dan enkripsi untuk semua paket IP yang lewat pada *data stream*. L2TP *over* IPSec merupakan perpaduan antara protokol L2TP dan IPSec dengan tujuan untuk meningkatkan keamanan pertukaran data yang melewati *tunnel* tersebut.

PT Muaramas Ekamukti telah menerapkan VPN dalam pertukaran data operasional perusahaan sehari-hari antara kantor cabang dan kantor pusat. Protokol yang digunakan merupakan protokol Point to Point Tunneling Protocol (PPTP) yang diterapkan dengan menggunakan Ubuntu 13.04 sebagai server. Tujuan dari penggunaan VPN oleh perusahaan adalah pertukaran data yang dapat terjalin secara realtime dengan berada seolah-olah pada jaringan lokal melewati jaringan publik. Namun hal ini, tidak bisa terlepas dari adanya usaha penerobosan keamanan pertukaran data yang terjadi oleh pihak-pihak yang tidak bertanggung jawab.

Penerobosan dapat dilakukan dengan melakukan aksi penyadapan Man In The Middle Attack (MITMA) ke tunneling yang akan terbentuk sewaktu klien VPN akan melakukan koneksi dengan VPN Server. Hal tersebut dapat menyebabkan autentikasi login yang akan dilakukan oleh klien saat akan membentuk suatu tunneling, dapat terbaca oleh penyerang dikarenakan autentikasi

login tersebut akan terlebih dahulu melewati penyerang baru kemudian diteruskan ke server. Karena autentikasi login yang dapat terlihat oleh penyerang, maka akan terdapat kemungkinan yang lebih rentan terhadap penyalahgunaan data tersebut dengan melakukan login ke server menggunakan data yang terbaca oleh penyerang. Ketika penyerang sudah berhasil memasuki server dengan membentuk suatu tunnel yang memalsukan identitas penyerang seolah-olah sebagai klien yang memiliki otorisasi, maka penyerang dapat melakukan berbagai kegiatan terhadap data-data yang terdapat dalam server seperti mengambil data-data yang tersedia pada server , mengubah , ataupun menghapus data tersebut.. Jika hal tersebut terjadi, maka perusahaan dapat terganggu kinerjanya dikarenakan tidak tersedianya data yang dibutuhkan oleh perusahaan.

Proses penyadapan MITMA tersebut dilakukan dengan penyerangan sniffing yaitu penyerang mendengarkan segala lalu lintas data yang terjadi dalam jaringan. Untuk mencegah aksi sniffing tersebut menjadi agak rumit karena sifat dari penyerangan ini adalah pasif. Terdapat beberapa cara yang dapat dilakukan dalam pencegahannya, yaitu secara rutin melakukan pemeriksaan apakah dalam host dalam jaringan, menggunakan SSL atau TLS dalam melakukan pengiriman data namun hal ini tetap dapat terlihat namun masih dalam terenkripsi, serta dapat dilakukan dengan menggunakan VPN protokol tunneling tertentu dalam proses pertukaran data. Sehingga, atas dasar tersebut, maka penulis mengambil judul **“Analisa dan Peralihan Penerapan Teknologi VPN dengan Protokol PPTP Menuju Teknologi VPN dengan Protokol L2TP/IPSec”**

1.2 Rumusan masalah

Berdasarkan latar belakang masalah di atas, maka dapat diuraikan pokok permasalahan penelitian ini adalah:

1. Bagaimana menerapkan teknologi VPN yang aman dari kemungkinan penyadapan MITMA oleh pihak yang tidak berkepentingan ?
2. Bagaimana VPN dapat menjamin keamanan data yang dikirim melewati jaringan publik dalam hal ini internet supaya tidak mudah terbaca oleh pihak yang tidak berkepentingan ?

1.3 Batasan masalah

Berdasarkan latar belakang masalah di atas, maka peneliti membatasi ruang lingkup untuk penelitian ini sebagai berikut:

1. Perancangan jaringan VPN menggunakan sistem operasi *ubuntu server 13.04.*
2. Penerapan teknologi VPN menggunakan metode *tunneling* PPTP dan L2TP/IPSec.
3. Pembacaan trafik data yang dilakukan oleh klien menggunakan *wireshark.*
4. Penyerangan penyadapan autentikasi *login* menggunakan metode *sniffing* yang disediakan oleh *Linux Backtrack/Kali Linux.*
5. Klien menggunakan sistem operasi *windows 7*.

1.4 Tujuan penelitian

Membandingkan protokol PPTP dan protokol IPSec dalam menjaga keamanan data terhadap *tunneling* yang dibentuk sehingga dapat diketahui

protokol yang memiliki tingkat keamanan yang lebih baik untuk dapat diterapkan pada VPN perusahaan.

1.5 Manfaat penelitian

Manfaat yang dicapai dari penelitian ini adalah:

1. Meningkatkan keamanan pertukaran data antara kantor pusat dan kantor cabang dengan memilih protokol VPN yang lebih baik.
2. Memberikan kenyamanan pertukaran data karena telah dilakukan perbaikan terhadap VPN yang dipakai oleh perusahaan sekarang.
3. Mengetahui metode tunneling yang lebih baik untuk digunakan pada penerapan VPN perusahaan.

1.6 Sistematika penulisan

Keseluruhan dari penulisan skripsi ini disusun dengan sistematika sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi gambaran umum penulisan skripsi yaitu latar belakang, ruang lingkup, tujuan dan manfaat, metodologi yang digunakan serta sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini berisi teori-teori pendukung seperti teori dasar jaringan komputer, teori mengenai internet, dan teori mengenai VPN serta protokol yang digunakan pada jaringan VPN.

BAB III METODOLOGI PENELITIAN

Pada bagian ini diuraikan desain, metode, atau pendekatan yang akan digunakan dalam menjawab permasalahan penelitian/studi untuk mencapai tujuan penelitian, serta tahapan penelitian secara rinci, singkat dan jelas.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi tentang proses yang terjadi pada tahap implementasi dan umpan balik yang diperoleh dari hasil perancangan yang diimplementasikan.

BAB V KESIMPULAN DAN SARAN

Pada bab ini merupakan bagian terakhir yang berisi uraian tentang simpulan yang dapat diambil dari uraian bab-bab sebelumnya dan diberikan saran-saran yang diperlukan guna meningkatkan perancangan yang lebih baik lagi.