BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pada era globalisasi seperti sekarang ini, keamanan sistem informasi berbasis internet menjadi suatu yang harus diperhatikan secara sirius, karena jaringan komputer yang sifatnya publik dan global pada dasarnya tidak aman. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi investasi dan sumber daya di dalam jaringan tersebut secara efektif. Sebelum mulai mengamankan suatu jaringan komputer, harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan risiko yang harus diambil maupun yang harus dihindari. Untuk itu, jaringan komputer harus dianalisa untuk mengetahui apa yang harus diamankan, untuk apa diamankan, seberapa besar nilainya, dan siapa yang bertanggung jawab terhadap data dan aset-aset lain di dalam jaringan komputer tersebut.

Unit Pelaksana Teknis atau biasa disingkat (UPT) Laboran merupakan salah satu bagian divisi dalam lingkup Universitas Amikom Yogyakarta yang bertanggungjawab dalam mengelola Laboratorium (LAB) Universitas Amikom Yogyakarta. Dalam mencapai kinerja yang maksimal, UPT menerapkan prosedur standar kerja dalam pengelolaan aset serta demi menunjang kinerja UPT mimiliki fasilitas jaringan internet, layanan tersebut dimanfaatkan untuk koneksi LAB, server, data center, serta karyawan dan mahasiswa apa bila membutuhkan koneksi internet ketika sedang melakukan praktikum didalam LAB. UPT Universita

Amikom Yogyakarta mempunyai jam kerja pelayanan dari 07.00 s/d 17.00 hari kerja sesuai yang telah diatur, oleh sebab itu seluruh karyawan UPT dituntut bekerja sesuai *timeline* dan *jobdesk* masing masing, dalam hal ini karyawan sebagai administrator (admin) yang bertanggung jawab dalam manajemen jaringan UPT harus mampu menjaga keamanan jaringan UPT baik serangan dari lokal maupun dari jaringan yang terhubung ke internet (publik) yang begitu lebih besar tingkat ancaman seranganya.

Dalam menjaga keamanan jaringan UPT admin selalu memonitoring setiap lalulintas *traffic* serta *user* yang sedang aktif pada jaringan UPT, hal tersebut admin setiap hari lakukan ketika sedang berada dalam jaringan lokal yang dimana admin merasa aman. Permasalahan disini ketika admin berada pada jaringan luar UPT atau berada pada jaringan publik (internet), admin sering kali khawatir ketika ingin memoniroting komputer *office*, server atau router serta mengakases data *center* dari jaringan publik dikarenakan tingkat pencurian data, *sniffing packet* dan lebih parahnya orang yang tidak mempunyai hak akses dapat mengetahui *username* dan *password* yang digunakan untuk mengakses *router* atau server, menyadari hal tersebut membuat admin sangat khawatir untuk melakukan remote otentikasi dari jaringan publik. Oleh karena itu, dibuatlah berbagai macam cara agar orang yang tidak dikehendaki tidak dapat melakukan *port scanning*, *sniffing traffic*, serta masuk kedalam sistem jaringan tersebut dan merubah,menghapus data.

Hal inilah yang melatar belakangi untuk melakukan penelitian "Analisa dan Perancangan Keamanan Otentikasi VPN server Menggunakan Metode *Port Knocking* pada UPT Laboratorium Universitas Amikom Yogyakarta" diangkat

sebagai judul skripsi karena berdasarkan pengamatan peneliti penyerang tidak akan mudah membaca *traffic* karena jalur data dienkripsi dengan penggabungan 2 (dua) protokol VPN yaitu sebuah komunikasi yang dapat terkoneksi ke jaringan publik dengan menggunakan *tunnel* untuk dapat bergabung dengan jaringan lokal, serta jika ingin melakukan otentikasi harus mengirimkan ketukan yang sesuai aturan jika salah maka *port* VPN server yang dilindungi oleh *port knocking* tidak akan merespon atau membuka koneksi.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka ditemukan beberapa rumusan masalah diantaranya :

1. Bagaimana menganalisa dan meningkatkan keamanan jalur koneksi antara *client* (admin) dengan router UPT Laboratorium pada jaringan publik ?
2. Bagaimana meningkatkan keamanan otentikasi VPN server ?
3. Bagaimana metode *Port Knocking* mengatasi bentuk serangan terhadap VPN server dan otentikasi router ?
4. Bagaimanan merancang sistem *alarm* deteksi serangan terhadap VPN server untuk meningkatkan keamanan otentikasi ?

1.3 Batasan Masalah

Supaya pembahasan masalah yang dilakukan dapat terarah dengan baik dan tidak menyimpang dari pokok permasalahan, maka peneliti membatasi permasalahan yang akan dibahas, yakni sebagai berikut:

1. Perancangan infrastruktur ini dibangun menggunakan router mikrotik seri RB941-2nD.
2. Perancangan keamanan otentikasi VPN akan menerapkan metode *Port Knocking*.
3. Dalam penelitian ini membahas tentang meningkatkan keamanan otentikasi VPN server, melindungi port otentikasi router, dan meningkatkan kemanan jalur antara *client* (admin) dengan router dengan penggabungan 2 (dua) protokol VPN.
4. Protokol VPN yang akan digunakan dalam perancangan ini adalah L2TP (*Layer Two Tunneling Protocole*) digabungkan dengan IPSec (*Internet Protocole Security*).
5. Dalam perancangan ini juga akan menerapkan list *port* TCP *and* UDP *number* yang akan digunakan sebagai *port* pemicu dan lain sebagainya.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah melakukan analisis dan merancang meningkatkan jalur koneksi yang aman dengan menggunakan VPN sebagai jalur *private* antara *client* dengan router pada jaringan publik, serta meningkatkan keamanan otentikasi VPN server sehingaa *traffic* data *client* dengan router tetap terjaga dan remote otentikasi pada router maupun komputer *office*, dan server yang terhubung dengan router tetap aman kerahasiaannya.

1.5 Manfaat Penelitian

Dari penelitian ini diharapkan dapat memberikan manfaat, sebagai berikut:

1. Universitas Amikom Yogyakarta.

   Menjadi arsip dan referensi untuk mahasiswa angkatan selanjutnya dalam menyusun tugas kuliah, materi perkuliahan, tugas akhir dan skripsi, serta penelitian.

2. UPT Laboratorium Universitas Amikom Yogyakarta

   a. Meningkatkan keamanan jalur koneksi antara *client* dengan router maksudnya ialah dengan penggabungan 2 (dua) protokol VPN dimana *traffic* data tidak mudah untuk di *sniffing* dikarenakan jalur sudah di enkripsi.

   b. Memberikan rasa aman terhadap admin jaringan dalam otentikasi dan jalur koneksi, karena untuk membuka koneksi terhadap VPN server perlu langkah khusus yang hanya admin sendiri yang mengetahui langkah-langkah tersebut.

   c. Meningkatkan keamanan otentikasi router seperti http, ftp, ssh, winbox, dan server dibelakanga router tersebut yang dimana hanya menerima koneksi dari VPN serta port otentikasi yang di lindungi.

3. Peneliti

   a. Meningkatkan pemahaman pengetahuan, pengalaman dalam menganalisa dan merancang infrastuktur jaringan komputer, sehingga nantinya berguna di dunia kerja.

b. Meningkatkan pemahaman dan pengetahuan dalam jaringan komputer khususnya konsep keamanan jaringan.

c. Mengetahui tahapan-tahapan yang harus dilakukan jika melakukan penelitian dan metode apa saja yang digunakan dalam objek penelitian.

1.6 Metode Penelitian

Metode penelitian yang digunakan oleh peneliti dalam melakukan pengumpulan data dan metode pengembangan antara lain :

1.6.1 Metode Pengumpulan Data

Supaya mendapatkan data yang akurat dan relevan tentang penelitian yang akan dilakukan, maka dari itu diperlukan metode untuk mencapai tujuan penelitian, berikut metode penelitian yang digunakan :

1. Metode Pustaka

   Metode pengumpulan data dan referensi melalui berbagai media keputusan, buku, jurnal penelitian, artikel, dan informasi dari internet yang berkaitan dengan judul penelitian.

2. Wawancara

   Penelitian memberikan beberapa pertanyaan langsung kepada admin jaringan UPT Laboratorium Universitas Amikom Yogyakarta untuk mendapatkan data dan informasi yang dibutuhkan dalam penelitian.

3. Observasi

   Penelitian ini dengan terjun langsung ke lokasi penelitian untuk mendapatkan informasi yang belum didapat saat wawancara, ataupun

kepada yang bersangkutan di UPT Laboratorium Universitas Amikom Yogyakarta.

1.6.2 Metode Pengembangan

Penelitian ini menggunakan metode PPDIOO *Network lifecycle* sebagai acuan dalam membuat penelitian ini.

Berikut adalah penjelasan dari masing masing setiap tahapan dalam PPDIOO :

1. Persiapan (*prepare*)

   Dalam tahap ini diawali dengan mencari kebutuhan keseluruhan sistem yang akan dirancang.

2. Perencanaan (*plan*)

   Merecanakan kebutuhan sistem yang akan dibuat dan diharapkan dapat memberikan gambaran terhadapat kebutuhan yang ada.

3. Perancangan (*design*)

   Pada tahap ini dibuat topologi jaringan untuk meningkatkan keamanan otentikasi VPN server dengan metode *port knocking* menggunakan Mikrotik seri RB941-2ND.

4. Implementasi (*implement*)

   Tahap ini menerapkan semua yang telah direncanakan dan didesain sebelumnya.

5. Pengoperasian (*operate*)

   Dalam tahap ini perluya pengujian dan pemantauan sistem yang telah diimplementasikan agar berjalan sesuai dengan perancangan dan analisis.

6. Pengoptimalan (*optimize*)

   Memerlukan perhatian khusus terhadap kebijakan yang perlu dibuat untuk mengatur dan membuat ssistem agar dapat berjalan dengan baik.

1.7 Sistematika Penulisan

Laporan penelitian ini terdiri dari lima bab. Masing-masing bab memiliki pembahasan tersendiri. Berikut sistematika penulisan penelitian yang diuraikan dalam bentuk bab :

BAB I PENDAHULUAN

Bab pendahuluan ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan yang digunakan dalam penulisan skripsi.

BAB II LANDASAN TEORI

Dalam bab ini membahas teori-teori yang menjadi landasan dan mendukung pelaksanaan penulisan penelitian.

BAB III METODE PENELITIAN

Bab ini membahas tentang identifikasi masalah, analisis kebutuhan jaringan, pengambilan data yang diperlukan, kebutuhan *hardware* dan *software*, serta perancangan jaringan yang dilakukan dalam penelitian.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini memaparkan hasil tahapan penelitian mulai dari analisis, desain, implementasi sistem.

BAB V PENUTUP

Bab ini berisi kesimpulan dari penelitian serta saran guna untuk pengembangan sistem ini selanjutnya.