

BAB I

PENDAHULUAN

1.1 Latar Belakang

Semakin tingginya kebutuhan akan jaringan internet membuat terjadinya pengembangan untuk internet. Diantaranya *high speed internet access* dan *secure network*. Dengan begitu kebutuhan akan jaringan internet yang terus meningkat akan dapat terpenuhi, hal ini mempengaruhi tuntutan agar jaringan backbone lebih cepat dan aman, Sehingga para ISP untuk memenuhi kebutuhan tersebut menggunakan teknologi MPLSVPN, karena MPLSVPN mendukung *traffic engineering* dan skalabilitas jaringan yang tinggi[10] dan memiliki juga toleransi yang baik pada jaringan[3] sehingga tidak terlalu mengganggu performansi jaringan yang ada. Dari sisi lain penggunaan VPN hanya menjaga jaringan pada sisi *confidentiality*-nya saja. Sehingga untuk sisi lainnya seperti *integrity* masih rentan akan serangan yang dapat mengganggu jaringan, diantaranya adalah informasi sistem seperti peroutingan yang dapat dengan mudah dimodifikasi dan digunakan untuk mengganggu jaringan dengan misalnya mengubah peroutingan jaringan itu sendiri. Sehingga dibutuhkannya sistem keamanan yang dapat menjaga informasi ini, dan informasi ini dapat dilindungi dengan memberikan sistem autentikasi pada proses informasi sistem itu sendiri, dengan menggunakan *Routing Protocol Authentication* data routing yang ada akan diberikan kunci dan dienkripsi dengan algoritma MD5, sehingga menghasilkan *chipertext* yang hanya dapat didekripsi pada router yang dikenal dan memiliki kunci yang sama/benar, dan paket-paket yang tidak dikenal dapat dicegah masuk ke router, dengan begitu semua paket informasi routing yang merupakan paket untuk menyerang jaringan pada router akan ditolak

Pada Tugas akhir ini dibahas masalah keamanan MPLSVPN-L3VPN dari serangan *man-in-the-middle-attack*, dengan menggunakan *Authentication* pada *routing protocol*-nya. Penulis akan menganalisis implementasi ini untuk mencegah dari serangan pada informasi peroutingan yang digunakan pada jaringan yang dibangun dari serangan *man-in-the-middle* yang akan dilakukan dengan menggunakan tool LOKI dan *wireshark*. Dan hasil yang didapat adalah pemasangan *routing protocol*

authentication dapat mencegah terjadinya *spoofing* paket informasi yang tidak dikenal oleh router, dengan menggunakan kunci yang panjang dan unik, akan menyulitkan untuk melakukan serangan *brutforce* untuk mengetahui kuncinya.

1.2 Tujuan

Tujuan dari tugas akhir ini adalah:

1. Merancang dan membangun jaringan MPLSVPN-L3VPN.
2. Mengimplementasikan *Routing Protocol Authentication* pada komponen MPLSVPN-L3VPN.
3. Melakukan analisis integritas jaringan yang telah dibangun.
4. Melakukan serangan *man-in-the-middle* pada sisi CE, PE, dan P jaringan yang dibangun.
5. Melakukan analisis keamanan pada jaringan *backbone* MPLS VPN *layer 3* dan diimplementasikan *Routing Protocol Authentication*, dan menganalisis Autentikasinya, dan juga menganalisis perubahan QOS setelah penerapan autentikasi pada *routing protocol*.

1.3 Rumusan Masalah

Rumusan masalah pada tugas akhir ini adalah:

1. Bagaimana membangun jaringan MPLS?
2. Bagaimana mengimplementasikan *routing protocol authentication* pada jaringan MPLS.
3. Bagaimana membangun hubungan untuk komunikasi baik dengan VoIP,?
4. Bagaimana melakukan *sniffing* pada jaringan MPLS yang telah dibangun?, dan melakukan *Spoofing* pada jaringan.
5. Bagaimana melakukan analisis QOS pada MPLS yang telah dibangun?

1.4 Batasan Masalah

Batasan masalah dari tugas akhir ini adalah:

1. Jaringan yang dibangun adalah jaringan *private*. hanya membahas informasi yang ada pada jaringan, berbasis Ipv4.
2. Menganalisis keamanan pada sisi integritas jaringan.
3. Menggunakan CISCO IOS di GNS3.
4. Menggunakan mekanisme MPLS, mekanisme *man-in-the-middle*.

5. Hanya membahas penggunaan VoIP.
6. Metode *spoofing* dan *cracking* dengan menggunakan LOKI.
7. Metode *sniffing* dan analisis QOS dengan menggunakan *Wireshark*.

1.5 Metodologi

Metodologi yang digunakan dalam pembuatan tugas akhir ini adalah:

1. Studi Literatur

Melakukan pengumpulan literatur-literatur berupa jurnal, artikel, buku referensi, dan sumber lain untuk memahami dan mendalami konsep.

2. Perancangan dan Realisasi

Merancang dan membangun jaringan backbone dengan 1 PC untuk 6 router cisco pada GNS3, 1 buah server, 2 pc *client*. 1 pc *attacker*.

3. Pengujian dan Analisis implementasi.

4. Pengambilan kesimpulan dan penyusunan laporan.

1.6 Sistematika

Sistematika penulisan Tugas Akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Membahas tentang latar belakang masalah, tujuan, rumusan masalah, batasan masalah, metodologi, dan sistematika penulisan.

BAB II DASAR TEORI

Membahas teori tentang MPLS, VPN, Aspek keamanan, jenis serangan, *routing protocol* dan dengan *authentication*, VoIP, dan Quality of Service.

BAB III PERANCANGAN DAN IMPLEMENTASI

Merancang konfigurasi jaringan MPLS, menerapkan *Routing Protocol Authentication* pada jaringan MPLSVPN-L3VPN.

BAB IV PENGUJIAN DAN ANALISIS HASIL IMPLEMENTASI

Berisi tentang hasil pengujian dan analisis, analisis integritas jaringan dan tentang hasil dari *attack* dan pengaruh keamanan yang dipasang terhadap jaringan.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan yang didapat dari pembahasan dan analisis bab sebelumnya, serta saran yang dibutuhkan untuk pengembangan selanjutnya.