BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan dalam jaringan komputer sangatlah penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Segi – segi keamanan didefinisikan lima poin, yaitu *Confidentiality,* menyaratkan bahwa informasi hanya bisa diakses oleh pihak yang berwenang, *Integrity,* menyaratkan bahwa informasi hanya bisa diubah oleh pihak yang berwenang, *Availability,* menyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang, *Authentication,* menyaratkan bahwa pengiriman sebuah informasi dapat diidentifikasi dengan dan ada jaminan bahwa identitas yang didapat tidak palsu, *Nonrepudiation*,menyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan[1].

Dalam jaringan komputer ada beberapa perangkat yang harus diamankan, salah satunya adalah *Router*. Di dalam *Router*, ada sebuah konfigurasi yang mengatur lalulintas jaringan untuk tujuan *Confidentiality*. Salah satu konfigurasi tersebut adalah konfigurasi *Bandwith* yang memiliki *Resource,* dimana *Resource* tersebut adalah besarnya *Bandwith* yang tersedia. Konfigurasi tersebut bertujuan untuk mengoptimalkan *Bandwith* yang ada.

Dalam penelitian yang dilakukan oleh Prasetyo, Widayanti, dan Setyowibowo tentang *Hotspot Authentication* yang hasilnya adalah *Authentication* tersebut tidak dapat memberikan bukti kekuatan sistem dengan menggunakan

Captcha. Dan metode yang digunakan dalam penelitian ini adalah metode pengumpulan data dan metode pengembangan sistem[2].

Penelitain yang dilakukan oleh Naingolan dan Putra tentang *Voucher* pada *Hotspot* yang salah satu hasilnya adalah dapat menggoptimalkan penggunaan *Resource Bandwith* yang ada. Dan metode yang digunakan dalam penelitian ini adalah metode observasi dan metode studi literatur[3].

Aprianto dan Asmunin meneliti tentang *Port Knocking* yang hasilnya adalah adanya perbedaan antara sebelum menggunakan "Rule" *Port Knocking* dan setelah "Rule" *Port Knocking*. Penelitian ini juga membagi user menjadi dua, pertama *White List* yaitu user yang diperbolehkan untuk mengkaes sistem dan *Black List* yaitu user yang tidak diperbolehkan mengakses sistem[4].

Dari gambaran diatas didapat bahwa pembagian *Resource Bandwith* sangatlah penting, hal tersebut tergambar dari dua penelitian tentang hotspot diatas, dan menggunakan *Authentication* untuk menggunakan internet. Akan tetapi, keamanan pada *Router* juga tidak dapat sepelekan, karena sistem akan jadi kacau jika router dapat diakses oleh pengguna yang tidak berwenang. Maka dari itu peneliti melakukan analisis dan merancang sistem pengamanan akses Authentication mengunakan metode *Port Knocking dan Firewall Action Drop* pada Waroeng Spesial Sambal (Waroeng SS).

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan diatas maka rumusan masalah dalam penelitian ini adalah :

"Bagaimana implementasi *Port Kncoking* pada *Router* Mikrotik dan berapa jauh konfigurasi Router mikrotik dapat diamankan dengan dengan diterapkannya sistem *Port Kncoking* ?"

1.3 Batasan Masalah

1. Penelitian ini menggunakan router Mikrotik RB951ui-2nD
2. Konfigurasi keamanan hanya menggunakan *Port Knocking*.
3. *Port Router* yang diamankan adalah *port Default* yang digunakan oleh SSH, Telnet, Winbox dan Webfig.
4. Software yang digunakan untuk mengakses router menggunakan Winbox, PuTTy, Google Chrome, dan OS Live Backtrack.
5. Proses ujicoba keamanan dilakukan dengan menggunakan 2 komputer dan 1 Router.
6. Topologi yang dirancang hanya dikhususkan di kantor Wareong SS
7. Laptop / *End Device* yang digunakan adalah Laptop yang *Compatible* dengan *Opertating System* Windows 7 atau versi diatas Windows 7.
8. IP yang digunakan dalam penelitian ini adalah IPV4
9. Penelitian dilakukan dengan menggunakan koneksi internet *Indihome*.

1.4 Maksud dan Tujuan Penelitian

Adapun tujuan penelitian ini adalah menerapkan sistem pengamanan akses *Authentication Port Knocking dan Firewall Action Drop* yang tepat pada Waroeng Spesial Sambal (Waroeng SS).

1.5 Manfaat Penelitian

Manfaat yang dapat diambil dari hasil penelitain ini adalah :

1. Dapat membantu meningkatkan keamanan Router
2. Dapat mencegah pihak yang tidak bertanggung jawab untuk tidak mengkonfigurasi router.

1.6 Metode Penelitian

Metode Penelitain yang digunakan untuk mendapatkan informasi tentang permasalahan pada penelitian adalah sebagai berikut :

1.6.1 PPDIOO

PPDIOO(*Prepare Plan Design Implement Operate Optimize*) merupakan metode perancangan jaringan dari Cisco atau biasa disebut sebagai siklus hidup layanan jaringan Cisco yang dirancang untuk mendukung berkembangnya jaringan. Dengan Metode ini Peneliti dapat menyiapkan, merencanakan, mendesain, menerapkan, mengoprasikan serta mengoptimalkan sebuah sistem yang baru.

1.7 Sistematika Penulisan

Adapun sistematika penulisan laporan dalam penyelesaian ini adalah sebagai berikut :

BAB I : PENDAHULUAN

BAB I adalah bagian awal dari laporan skripsi yang membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

BAB II adalah mencakup bagian dari laporan skripsi yang berisi tentang teori-teoi yang mendukung judul skripsi.

BAB III : METODOLOGI PENELITIAN

BAB III adalah membahas tentang penelitian yang dilakukan, baik itu gambaran umum objek penelitian yang berkaitan dengan analisis masalah, analisis hardware dan software, dan perancangan topologi.

BAB IV : HASIL DAN PEMBAHASAN

BAB IV merupakan bagian dari skripsi yang membahas tentang implementasi dari jaringan dengan metode pengamanan *Port Knocking* dan di sertai dengan uji coba sistem.

BAB V : PENUTUP

BAB V merupakan bagian akhir dari laporan skripsi yang berisi tentang kesimpulan dan saran.

DAFTAR PUSTAKA

LAMPIRAN A