

BAB I. PENDAHULUAN

1.1 Latar Belakang

Saat ini keamanan telah menjadi hal yang sangat penting, terutama dalam bidang teknologi informasi. *Eksplorasi* keamanan terhadap banyak server dan jaringan makin hari semakin meningkat. Bahkan orang yang tidak memiliki pengetahuan yang cukup, dalam masalah keamanan jaringan, dapat melakukan penetrasi terhadap sebuah sistem jaringan dengan hanya men-*download exploit tool* untuk sistem yang diserangnya dan kemudian menggunakannya untuk kepentingan sendiri.

Hampir sebagian serangan yang dirancang, merupakan *exploit* untuk *port-port* yang terbuka. Contoh paling nyata adalah *brute force attack*. Serangan ini dilakukan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin untuk memecahkan password, kunci, kode, atau sebuah kombinasi. Selain itu dalam teknik penyerangan, ada suatu fase dimana penyerang harus melakukan identifikasi komputer target. Teknik ini biasanya diawali dengan sesi *port scanning*. Pada sesi ini penyerang mengambil informasi *port - port* apa saja yang terbuka pada mesin target, setelah itu diikuti dengan *OS Finger Printing*. Pada *OS Finger Printing* penyerang dapat mengetahui OS (*Operating Sistem*) yang digunakan oleh target, cukup dengan mempelajari kelakuan port yang terbuka saat membalas paket yang ditujukan ke port tersebut.

Salah satu penanggulangan dengan menutup semua *port* atau biasa disebut juga *closed port system*. Hal ini tentu saja benar dan tidak salah, namun bila semua *port* ditutup maka sama saja menutup koneksi komputer atau *host* tersebut dari dunia luar dalam hal ini *Internet* dan hal ini bukan sesuatu yang diinginkan. Untuk itu diperlukan suatu jalan keluar yang tetap menjamin keamanan mesin dari *eksplorasi* terhadap *port*, tanpa harus mengorbankan tingkat konektivitas sistem yaitu menggunakan metode *port knocking*.

Port Knocking adalah sebuah metode membuka *port* secara eksternal melalui *firewall* dengan cara melakukan usaha koneksi pada suatu *port* yang tertutup dengan urutan yang telah di tentukan. Dengan dasar permasalahan dan kebutuhan untuk mengamankan *server* tanpa harus mengorbankan koneksi internet, penulis berinisiatif untuk menggunakan metode *port knocking* sebagai metode keamanan jaringan pada proyek tugas akhir, proyek tugas akhir tersebut berjudul: “Implementasi Pengamanan *Server* Menggunakan *Port Knocking* Dengan Algoritma Enkripsi Rivest Shamir Adleman (RSA)”

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat di ambil perumusan masalah yaitu bagaimana mengimplemntasikan *port knocking* ke dalam sebuah *server* tanpa mengorbankan koneksi internet.

1.3 Tujuan

Adapun tujuan dari tugas akhir ini antara lain :

- a. Mampu meningkatkan keamanan jaringan menggunakan metode *port knocking*
- b. Mampu mengimplementasikan *port knocking* pada *server* menggunakan *shorewall*.

1.4 Manfaat

Adapun manfaat dari pembuatan tugas akhir ini adalah :

- a. Dapat mengurangi penyerangan pada *server* dengan menutup *port*.
- b. Dengan adanya *port knocking* dapat mengelola *server* dari *client* menggunakan *remote area*.