BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer digunakan di berbagai aspek, contohnya instansi tertentu seperti perusahaan, universitas, kantor pemerintah dan lain sebagainya. Penggunaan jaringan komputer tidaklah optimal jika hanya berupa sistem yang berdiri sendiri, namun perlu berkomunikasi antar komputer yang satu dengan lainnya serta bertukar data melalui jaringan untuk memenuhi kebutuhan seperti basis data *client-server*, akses internet, pertukaran *file*, dan lain-lain.

Umumnya jaringan komputer dilengkapi *firewall* untuk meningkatkan keamanannya, namun penggunaan *firewall* saja tidak dapat mengatasi masalah yang mungkin saja muncul seperti serangan jaringan sehingga diperlukan sebuah mekanisme keamanan tambahan berupa *port knocking*. *Port knocking*memungkinkan terjadinya komunikasi antara *server* dengan *client* melalui jaringan dengan semua *port* tertutup. Beberapa penelitian telah dilakukan untuk mengimplementasikan sistem *port knocking*diantaranya adalah *"Port knocking: Network Authentication Across Closed Ports"*[1],*Knockknock"*[3], *"Network Security using Hybrid port knocking"*[4].

Port knocking[2] merupakan sistem berbasis *firewall* yang memanfaatkan *port* tertutup untuk melakukan autentikasi terhadap pengguna sehingga memungkinkan untuk berkomunikasi. Kelebihannya adalah penyerang tidak dapat dengan mudah menentukan apakah *host* sedang mendengarkan *port knocking*karena autentikasinya dilakukan secara tersembunyi, sistem ini juga fleksibel karena skema autentikasi berupa *knock sequence*. Namun masih terdapat kekurangan yaitu *port knocking*tidak dapat melindungi *port* yang digunakan untuk mengakses aplikasi publik seperti *mail* dan *web client*. Jika

diaplikasikan pada aplikasi publik berarti masih terdapat celah untuk terjadinya serangan sehingga tidak memungkinkan untuk mengaplikasikan sistem *port knocking*pada setiap *mail* dan *web client*.

Hybrid port knocking(HPK) [4], merupakan metode yang menggabungkan 3 konsep yaitu *port knocking*, steganografi, serta *mutual authentication*. HPK dapat digunakan untuk mengautentikasi *host* sehingga layanan pada jaringan lokal tidak terlihat oleh serangan *port scanning*, memberikan *layer* keamanan tambahan sehingga penyerang tidak mudah melakukan serangannya, serta bertindak sebagai pembatas untuk melindungi layanan-layanan yang rentan mendapatkan serangan.

Penelitian *hybrid port knocking*melatarbekangi penulis dalam menganalisa *performance* metode *hybrid port knocking*berbasis enkripsi GnuPG menggunakan RSA and RSA *public-key algorithm*, DSA and ElGamal *public-key algorithm* serta DSA and RSA *public-key algorithm*. Analisa meliputi konsumsi waktu dan memori yang diperlukan oleh metode *hybrid port knocking.*

1.2 Tujuan dan Manfaat

Tujuan dari penelitian ini adalah untuk mengetahui kinerja aplikasi *client-server* menggunakan metode *hybrid port knocking*sebagai sistem keamanan jaringan pada sistem operasi linux.

Manfaat yang diperoleh adalah mengetahui cara kerja *hybrid port knocking*, memperoleh data mengenai waktu pemrosesan *port knockingscript* serta penggunaan memori. Sehingga menambah pengetahuan penulis serta dapat dijadikan referensi ketika bekerja di bidang jaringan komputer.

1.3 Rumusan Masalah

Berdasarkan penelitian *hybrid port knocking*, penulis akan menganalisa *performance* metode *hybrid port knocking*berbasis enkripsi GnuPG menggunakan RSA and RSA

public-key algorithm, DSA and ElGamal *public-key algorithm* serta DSA and RSA *public-key algorithm*. Analisa dilakukan untuk mengetahui berapa lama waktu yang diperlukan untuk memroses setiap baris *port knockingscript* saat dijalankan dan berapa banyak penggunaan memori.

1.4 Batasan Masalah

Pada penulisan skripsi ini ditentukan beberapa batasan masalah diantaranya adalah sebagai berikut:

1. Implementasi *hybrid port knocking*pada aplikasi *client-server* [3] di-*install* sistem operasi *linux* ubuntu 12.04 melalui *virtualbox* versi 4.3.6
2. Metode enkripsi yang digunakan adalah GnuPG (GNU *Privacy Guard*) atau dikenal sebagai gpg versi 1.4.11
3. Bahasa pemrograman adalah *python* 2.7.3.
4. Penggunaan program *scapy* versi 2.2.0 untuk mengirim dan meng-*capture packet.*
5. *Firewall* yang digunakan adalah *iptables*.
6. Pemanfaatan *Python Imaging Library* (PIL) untuk mendukung proses steganografi.
7. Pengujian *profiling* sistem *hybrid port knocking*menggunakan beberapa *tools* diantaranya adalah *line_profiler* dan *memory profiler*.

1.6 Sistematika Laporan

Bab I. Pendahuluan

Bab ini menjelaskan latar belakang, tujuan, rumusan permasalahan, batasan masalah, metodologi, dan sistematika pembahasan.

Bab II. Dasar Teori

Bab ini menjelaskan teori yang mendasari pembuatan skripsi ini, yang mencakup langkah pengerjaannya dan teori yang mendukung.

Bab III. Pemakaian *Software* untuk Lingkungan Uji Coba dan Implementasi

Bab ini menjelaskan pemakaian *software* yang diperlukan untuk lingkungan uji coba baik itu *software* utama maupun pendukung. Selain itu juga berisi penjelasan bagaimana implementasi *hybrid port knocking*pada aplikasi *client-server* melalui *virtual-machine.*

Bab IV. Uji coba dan analisa hasil

Bab ini menjelaskan uji coba dengan menetapkan beberapa parameter dan menganalisa hasil pengujian tersebut.

Bab V. Penutup

Bab ini menjelaskan kesimpulan yang diambil dari skripsi serta saran untuk pengembangan selanjutnya.