BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

SSH merupakan *service* remote login yang cukup aman, bukan hanya sesi yang terenkripsi tapi juga adanya fasilitas otentikasi, sehingga untuk mengakses *service* ini dibutuhkan login, tapi *service* ini masih bisa diserang dengan teknik *brute-force attack*. *Brute-force attack* adalah suatu upaya serangan yang mencoba melakukan login secara otomatis dengan cara mencoba satu-persatu kemungkinan *username* dan *password* menggunakan daftar kombinasi *user* dan *password* yang sudah ada.

Salah satu kasus penyerangan *service* SSH terjadi seperti yang dijelaskan pada situs http://www.shellperson.com, bahwa pada tanggal 10 april 2010 servernya telah berhasil dibobol melalui *service* SSH dengan cara melancarkan serangan *brute-force attack*. Serangan *brute-force attack* ini teridentifikasi ketika sang admin melihat *log* otentikasi. penyerang meninggalkan jejak berupa ribuan percobaan login yang tercatat di file /var/log.auth.log.1 seperti yang dijelaskan pada website tersebut.

Hal ini yang melatar belakangi mengapa "Meningkatkan Keamana *Port* SSH dengan Metode *Port knocking* Menggunakan Shorewall pada Sistem Operasi Linux" diangkat sebagai judul skripsi karena berdasarkan pengamatan penulis jika penyerang mengirimkan ketukan koneksi yang salah maka *port* SSH yang dilindungi oleh *port knocking* tadi tidak akan muncul atau terbuka.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang sudah diuraikan sebelumnya, maka penulis dapat membuat beberapa rumusan masalah yaitu : Bagaimana cara meningkatkan keamanan *service* SSH pada server linux dengan mengunakan metode yang sederhana dan simpel tapi berguna dan aman untuk diimplementasikan.

1.3 Batasan Masalah

Mengingat luasnya materi tentang keamanan *port* SSH yang dibahas, maka penulis akan batasi sebatas :

1. Membahas tentang peningkatan keamanan *port* SSH dengan metode *port knocking*.
2. Membahas implementasi *port knocking* pada server berbasis linux.
3. Metode *port knocking* menggunakan tools administrasi *firewall* bernama *Shorewall*.
4. Pengujian sistem menggunakan serangan *Brute-Force Attack*

1.4 Tujuan Penelitian

Berdasarkan masalah-masalah yang telah diidentifikasi di atas serta latar belakang masalah yang telah diuraikan sebelumnya, maka penulis bertujuan untuk :

1. Untuk memenuhi syarat kelulusan Strata 1 (S1) STMIK AMIKOM Yogyakarta.
2. Menambah pengalaman dalam bidang keaman pada server berbasis linux dan mencoba mengimplementasikan keamanan *port* SSH dengan metode *port knocking* menggunakan shorewall.

1.5 Manfaat Penelitian

Manfaat dari Penelitian ini adalah :

1. Memperoleh gelar sarjana komputer STIMIK AMIKOM Yogyakarta.
2. Meningkatkan keamanan *port* SSH yang berjalan pada sistem operasi linux.
3. Mencegah penyerang dari pemindaian sistem dengan melakukan *port scanning*.
4. Dapat dijadikan bahan reverensi dan dapat diimplementasikan pada server-server berbasis linux.

1.6 Metode Pengumpulan Data

Penulis dalam penelitian ini menggunakan beberapa metode, adapun metode dan langkah-langkah dalam penelitian ini adalah :

1. Kepustakaan

   Mempelajari buku, literatur atau sumber lain termasuk internet tentang keamanan *port* SSH dan hubungannya dengan *port knocking* mneggunakan shorewall.

2. Uji Coba

Uji coba dilakukan dengan skenario sebagai berikut

a) Penginstalan Ubuntu server dan OpenSSH.
b) *Scanning* dan penyerangan terhadap *service* SSH.
c) Instalasi dan konfigurasi *port knocking* menggunakan shorewall.
d) Uji coba penyerangan kembali terhadap *service* SSH yang sudah dilindungi *port knocking*.

1.7 Sistematika Penulisan

Sistematika penulisan laporan penelitian ini akan disusun dalam lima bab sebagai berikut :

BAB I PENDAHULUAN

Bab menerangkan tentang latar belakang masalah, batasan masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, metode pengumpulan data dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang gambaran umum *service* SSH, *Brute Force Attack*, Nmap, THC-Hydra, Shorewall dan *Port knocking*.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi tentang analisis serangan *brute force attack* terhadap *service* SSH, perancangan dan konfigurasi shorewall untuk *port knocking SSH*.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang implementasi *port knocking* dan pengujian sistem keamanan *port* SSH yang dilindungi *port knocking*.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dan saran.

1.8 Jadwal Penelitian

Secara garis besar pelaksanaan penyusunan skripsi yang berjudul "Meningkatkan Keamana *Port* SSH dengan Metode *Port knocking* Menggunakan Shorewall pada Sistem Operasi Linux" terdiri dari beberapa tahap kerja yang sistematis dan berkesinambungan serta saling mendukung. Berikut adalah seluruh jadwal penelitian yang ditampilkan dalam tabel berikut:

Tabel 1.1 Jadwal Penelitian

No	Nama Penelitian	Bulan I				Bulan II				Bulan III			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Persiapan												
2	Perancangan												
3	Pembentukan												
4	Uji Coba												
5	Laporan												
6	Ujian Pendadaran												