

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan dunia teknologi informasi yang begitu cepat, ternyata juga diikuti dengan tingkat penyalahgunaan teknologi itu sendiri. Beberapa tahun belakangan ini, muncul banyak kasus yang berhubungan dengan penyalahgunaan teknologi informasi, seperti pembobolan ATM, pencurian data-data pribadi, penerobosan server publik, penyebaran virus ke dalam jaringan publik serta masih banyak lagi kasus-kasus lainnya yang berhubungan dengan keamanan sistem informasi (Mada Rambu Perdana, 2011).

Untuk mengantisipasi kasus-kasus tersebut, para pakar keamanan sistem informasi menggunakan beberapa metode *offensive security*. Metode ini merupakan metode pengamanan yang jarang digunakan. Metode *offensive security* pada intinya menekankan bahwa untuk mengamankan suatu sistem, perlu adanya suatu pemikiran dan tindakan seperti layaknya seorang penyerang (*attacker*) sehingga dapat diketahui pola dan arah serangan yang biasa dilakukan oleh seorang hacker (*white hat*)

maupun seorang cracker (*black hat*). Salah satu dari bentuk metode *offensive security* ini adalah metode *Network Mapping*.

Menurut Mati Aharoni, dalam bukunya yang berjudul *Offensive Security Lab Exercises (2007)*, sebuah tes penetrasi adalah suatu siklus penelitian dan serangan terhadap target secara terus-menerus. Serangan tersebut harus terstruktur dan dihitung, dan bila mungkin, diverifikasi di laboratorium sebelum diimplementasikan pada target nyata. Langkah awal dalam membangun serangan adalah mengetahui identitas target.

Berdasarkan uraian tersebut, maka akan dibangun suatu aplikasi yang dapat mengeksplorasi informasi dari suatu sistem operasi berupa informasi perangkat keras jaringan, konfigurasi jaringan dan informasi koneksi, berbasis desktop menggunakan bahasa pemrograman java.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah dan melihat begitu penting keamanan suatu sistem informasi, dapat dirumuskan suatu permasalahan yaitu, bagaimana membuat aplikasi yang dapat digunakan untuk mendapatkan informasi yang dibutuhkan (*information gathering*) dan *service enumeration* menggunakan salah satu dari metode *offensive security* yaitu metode *Network Mapping*.

1.3. Ruang Lingkup

Untuk menjaga fokus penelitian, maka ruang lingkup permasalahan mencakup hal-hal sebagai berikut

- a. Aplikasi yang akan dibangun dibatasi pada informasi mengenai konfigurasi jaringan, perangkat keras jaringan dan koneksi yang sedang berjalan pada suatu jaringan.
- b. Aplikasi dapat menemukan informasi mengenai alamat IP, port yang digunakan, layanan (*service*) dengan memasukkan alamat web.

- c. Metode pencarian informasi yang digunakan pada aplikasi yang akan dibangun menggunakan metode *Network Mapping*.
- d. Aplikasi akan dibuat menggunakan bahasa pemrograman *Java Desktop Standard Edition (J2SE)*.

1.4. Tujuan Penelitian

Dari perumusan masalah, maka tujuan dilaksanakannya penelitian ini adalah membuat suatu aplikasi yang dapat membantu pakar keamanan sistem informasi untuk mendapatkan informasi dan layanan yang sedang berjalan pada suatu jaringan.