BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Penggunaan komputer pada saat ini telah menjadi kebutuhan primer, terutama untuk kepentingan koneksi ke jaringan internet. Sedemikian meningkatnya kebutuhan jaringan internet dewasa ini, memicu banyak pihak untuk memberi fasilitas atau layanan jaringan komputer pada area-area publik. Baik itu berbayar, maupun gratis. Ada yang berupa kabel, ada pula yang berupa nirkabel (*wifi*).

Pemanfaatan jaringan komputer pada tempat-tempat publik ini, terkadang memang memberikan daya tarik tersendiri, terutama layanan nirkabel gratis (*free hotspot*). Namun, dalam proses pemanfaatan dan pengembangannya hingga saat ini, masih banyak sekali layanan tersebut yang tidak bisa memberikan kenyamanan penggunanya terhadap ancaman penyusup. Penyusup yang mencoba memanfaatkan jaringan publik untuk melakukan penetrasi pada *client* dalam jaringan ini bisa saja termotivasi oleh kesempatan, yaitu adanya celah kelemahan yang memungkinkan penyusup melakukan penetrasi, atau juga karena keinginan untuk menguji kemampuan atau pengetahuan tentang sebuah celah keamanan.

Penyusup yang berusaha melakukan penetrasi pada *client* dalam jaringan, akan dideteksi dengan adanya sebuah sistem yang dibuat ini. Sistem ini bertujuan untuk mendeteksi penyusup yang mencoba melakukan penetrasi pada komputer *client* yang diserang. Implementasi dari sistem ini kemudian akan diuji, agar dapat

mengetahui seberapa besar kemampuan sistem ini mampu mendeteksi penyusup. Sehingga, dapat dilakukan tindakan pencegahan lanjutan nantinya.

1.2 Rumusan Masalah

1. Apakah sistem deteksi penyusupan ini dapat berjalan dengan menggunakan sistem *firewall* yang sudah ada pada sistem operasi.
2. Karakteristik serangan apa saja yang mampu dideteksi oleh sistem ini.
3. Bagaimana mengintegrasikan sistem ini pada sistem operasi Mandriva 2010.2 (Henry_Farman).

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang disusun, maka pada penelitian ini ada beberapa aspek yang menjadi fokus penelitian. Bagaimana cara sistem ini bekerja, sehingga ditemukan cara untuk mengimplementasikannya menjadi salah satu fokus penelitian. Lalu, observasi kemampuan sistem dalam mendeteksi penyusup, dan pengimplementasian sistem ini memanfaatkan *resource* yang ada pada sistem operasi yang digunakan.

Tidak semua aspek dapat dibahas dalam penelitian ini, karena hal tersebut membutuhkan waktu, dan *resource* yang lebih besar. Oleh karena itu, pada kesempatan ini, hal-hal yang berkaitan dengan bahasa pemrograman yang digunakan, perancangan jaringan antar komputer, rincian serangan yang mungkin terjadi pada sistem, konfigurasi *firewall* lebih lanjut dan analisa sistem operasi Linux yang digunakan, tidak akan menjadi objek yang diteliti.

1.4 Tujuan Penelitian

Penelitian yang dilakukan ini ditujukan sebagai syarat menyelesaikan program studi strata satu Teknik Informatika di STMIK AMIKOM Yogyakarta. Selain itu juga, sebagai solusi penerapan teknologi pengamanan pada komputer-komputer personal (*client*).

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat dimanfaatkan untuk memperoleh gelar Sarjana Komputer dan memberikan solusi pengamanan komputer pada jaringan, sehingga pengguna komputer bisa lebih nyaman dan aman untuk digunakan meskipun menggunakan layanan internet di area-area publik.

1.6 Metode Pengumpulan Data

Penelitian diharapkan akan menemukan hasil yang optimal dan juga akurat, oleh karena itu dalam penelitian ini diterapkan beberapa metode sebagai berikut :

1.6.1 Eksperimen

Metode eksperimen yang diterapkan adalah sebagai berikut :

- Instalasi sistem pendeteksi penyusup yang telah dirancang, dan kemudian menyambungkan komputer pada jaringan.
- Instalasi dan pemanfaatan sistem operasi yang telah memiliki *software-software* yang bisa digunakan untuk pengujian penetrasi. Pada hal ini

digunakan sistem operasi Backtrack. *Software-software* penetrasi yang akan digunakan adalah Nmap, AngryIPScanner, TuxCut, dan EtterCap.

- Merekord kemampuan mendeteksi penyusup, *print-out* dari setiap aktivitas experimen sebagai bahan observasi.

1.6.2 Observasi

Pada metode ini hal-hal yang diobservasi adalah Sistem Operasi yang digunakan untuk pengimplementasian sistem yang digunakan, kemampuan sistem merespon bila diserang oleh penyusup, dan tingkat sensitivitas sistem mengidentifikasi serangan yang dilakukan pada saat penetrasi.

1.6.3 Sumber bacaan/Pustaka

Sebagai landasan dasar pengetahuan penelitian, maka pada penelitian ini juga dibutuhkan sumber-sumber bacaan. Sebagai acuan, maka digunakan sumber bacaan dari Pustaka STMIK AMIKOM Yogyakarta, koleksi pribadi, dan ebook-ebook atau artikel yang ada di internet.

1.7 Sistematika Penulisan

Laporan penelitian yang dibuat secara sistematika ini disusun secara singkat padat dan jelas. Masing-masing bab mempunyai penyelesaian dan dijelaskan permasalahannya sebagai berikut:

BAB 1 PENDAHULUAN

Merupakan bagian pengantar dari pokok permasalahan yang dibahas dalam skripsi ini. Adapun hal-hal yang dibahas berisikan latar belakang masalah, rumusan masalah, tujuan dan

manfaat penelitian, metode pengumpulan data dan sistematika penelitian.

BAB II LANDASAN TEORI

Berisikan tentang menguraikan mengenai tinjauan pustaka tentang sistem yang dirancang, keamanan jaringan, *firewall*, *intrusion detection system*, pengenalan tentang serangan yang mungkin terjadi dan menganalisa jaringan serta *software* yang digunakan dalam pembangunan sistem.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Menguraikan tentang perancangan dalam membangun sistem deteksi penyusupan, analisis kebutuhan sistem, spesifikasi perangkat keras dan perangkat lunak, serta perancangan *software* pendeteksi penyusupan yang telah dibangun.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Membahas kegiatan implementasi yang meliputi tahap instalasi *software*, pembangunan sistem dan pengujian sistem, serta implementasi dan konfigurasinya.

BAB V PENUTUP

Menguraikan tentang kesimpulan dari pelaksanaan seluruh kegiatan dan beberapa saran dari peneliti kepada pihak yang akan membuat skripsi dengan tema yang sama di masa yang akan datang.