BAB I

PENDAHULUAN

A. Latar Belakang

Sekitar tahun 1997 sampai saat ini Universitas Muhammadiyah Yogyakarta terus mengembangkan teknologi jaringan komputer, khususnya Internet. Teknologi jaringan komputer terus dikembangkan karena dapat mendukung kelancaran di bidang akademik dan meningkatkan kualitas perkuliahan. Di bidang akademik misalnya kelancaran proses input data perkuliahan atau *key in*, absensi karyawan, dan pelayanan akademik lainnya. Untuk meningkatkan manajemen dan kualitas perkuliahan di fakultas teknik dikembangkan COMES, di fakultas Ilmu sosial politik, ekonomi, hukum dan pertanian dikembangkan ELCOM, untuk fakultas kedokteran dikembangkan els.umy.ac.id.

Dalam membangun sebuah sistem jaringan komputer, sistem keamanan menjadi suatu hal yang mutlak diperlukan. Keamanan dan kerahasiaan data pada jaringan komputer menjadi sangat penting. Hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi tidak akan berguna lagi apabila ditengah jalan informasi tersebut disadap atau dibajak oleh orang yang tidak berhak. Beberapa jenis alat ini dapat disusupkan ke komputer, antara lain pada saat surfing di internet, chatting, berkomunikasi menggunakan e-mail, dan lain sebagainya.

Hal ini terjadi pada tahun 2007 *website elearning* kampus UMY, http://comes.umy.ac.id dan http://www.fk.umy.ac.id mengalami *down*. Hal tersebut akibat adanya penyusup yang masuk ke dalam sistem kemudian memanfaatkan kelemahan yang ada pada kedua *server* tersebut. Menurut admin yang menangani *server* tersebut penyerangan terjadi karena terdapat *bug* pada *source code* dari bahasa pemrogrammannya, sehingga penyusup dapat mengubah tampilan halaman utama kedua *server* tersebut.

Penyusup dalam melakukan aksinya biasanya melakukan tahapan-tahapan awal dalam melakukan proses penetrasi ke dalam sistem. Salah satunya dimulai dari *scanning* terhadap *host* untuk mendapatkan informasi sistem yang ada, mulai dari jenis sistem operasi yang digunakan, *webserver*, *database*, serta informasi lainnya. Dengan adanya informasi tersebut penyusup melakukan analisa terhadap sistem, apabila terdapat celah, penyusup akan menggunakan celah tersebut untuk membuat pintu belakang (*backdoor*) yang bisa digunakan untuk mengakses sistem sewaktu-waktu tanpa sepengetahuan admin sistem tersebut.

Sistem keamanan yang ideal harus mempunyai sistem deteksi maupun filter dalam menghambat adanya penyusup, akan tetapi sistem keamanan jaringan Universitas Muhammadiyah Yogyakarta masih menggunakan *firewall*, belum dilengkapi dengan sistem deteksi penyusupan. Pola deteksi lebih dilakukan dengan pengamatan terhadap trafik jaringan menggunakan *Router* dengan sistem operasi Mikrotik, pengamatan lebih mengacu pada pemakaian *bandwith* jaringan. Apabila terjadi keanehan terhadap trafik maka admin melakukan *bloking* menggunakan *firewall* yang terintegrasi pada *Router*. *Firewall* yang terintegrasi

tertentu, tetapi tidak dapat mengetahui lebih spesifik tentang serangan tersebut. Ada sejumlah situasi dimana admin ingin melihat isi dari trafik serangan, karena dengan demikian akan dapat diketahui tujuan dari penyerangan pada jaringan komputer sehingga nantinya diharapkan dapat digunakan untuk mengaudit sistem lain misalnya *firewall*.

Penambahan *security tool* juga diperlukan untuk mengantisipasi terjadinya penyusupan pada jaringan komputer. Sedangkan *security tool* yang ada sekarang kebanyakan bersifat komersial seperti, Dragon Squire Host-level IDS, Session Wall, BlackICE, NetPowler IDS dan lain-lainnya. *Security tool* komersial tersebut ditawarkan oleh produsen pembuat sistem sistem keamanan, dengan tambahan *update* sistem yang terbaru, sehingga nanti dapat mengikuti perkembangan dari metode yang digunakan oleh penyusup untuk melakukan penetrasi. Dan tentunya dibutuhkan biaya tambahan untuk dapat memperoleh *update* sistem tersebut.

Sistem pertahanan terhadap aktivitas-aktivitas ilegal diperlukan untuk mencegah adanya penyusup. Karena itu dibutuhkan suatu sistem yang dapat memberikan informasi kepada administator jaringan terhadap ancaman-ancaman yang mungkin terjadi dan sistem yang bersifat *Freeware*, sehingga admin mampu mengambil langkah-langkah penanggulangan.

B. Rumusan Masalah

Dari latar belakang masalah diatas maka dapat diidentifikasi menjadi

a. Sistem keamanan yang ada belum memadai untuk mendeteksi penyusup secara spesifik dan belum mempunyai acuan terbaru dalam mengenali pola-pola serangan terkini.

b. Penyusup melakukan aktivitas ilegal dalam melakukan penetrasi pada sistem yang menjadi target.

c. Sistem keamanan yang ada kebanyakan bersifat komersial dan dibutuhkan biaya tambahan untuk melakukan *update* terhadap sistem yang ada.

C. Batasan Masalah

Sistem keamanan UMY belum dilengkapi dengan sistem pendeteksian jaringan, sehingga firewall yang ada belum memiliki acuan untuk mengkonfigurasinya.

D. Tujuan

Penelitian ini bertujuan untuk :

1. Membangun sistem pendeteksian penyusupan pada jaringan komputer UMY (*intrusion detection system*) yang bersifat *Freeware.*
2. Memperoleh informasi tentang jenis-jenis penyusupan terbaru pada jaringan komputer sehingga dapat digunakan untuk mengaudit sistem yang lain, seperti *firewall.*
3. Mendapatkan sistem operasi yang memiliki perfoma lebih stabil selama sistem melakukan proses pendeteksian.

E. Kontribusi

Dengan adanya implementasi sistem tersebut dapat lebih mempermudah administrator dalam menangani masalah keamanan jaring