BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan Komputer adalah himpunan dari dua atau lebih komputer otonom yang terhubung dan berkomunikasi satu sama lain. Pada sebuah organisasi atau perusahaan, jaringan komputer memiliki manfaat sebagai penunjang layanan layanan yang disediakan oleh server, seperti *data sharing* dan e-mail. Terlepas dari manfaatnya, jaringan komputer tanpa sistem keamanan memiliki kelemahan yang berpotensi menimbulkan ancaman serangan seperti tindakan penyusupan kedalam jaringan tersebut. Sehingga sistem keamanan merupakan suatu hal yang esensial pada jaringan komputer, dalam hal ini jaringan komputer lokal atau *private network* yang terhubung langsung dengan *untrusted network* seperti Internet. Sistem keamanan jaringan komputer harus menjamin beberapa faktor diantaranya kerahasiaan, autentikasi, integritas, ketersediaan dan bebas dari penyangkalan. Tanpa sistem keamanan untuk mencegah ancaman terhadap *private network*, resiko serangan dari Internet menjadi sangat mungkin terjadi. Yang mana dampak kerusakan tidak hanya mengancam server melainkan juga perangkat lain pada *private network* yang bahkan seharusnya tidak dapat diakses publik.

Untuk menangani masalah diatas ada beberapa solusi, salah satunya dengan cara menerapkan metode *Demilitarized Zone* (DMZ) yakni pembuatan jaringan baru yang diperuntukan untuk server agar dapat bebas diakses publik, yang asalnya server dan perangkat-perangkat internal berada dalam satu jaringan kini dipisah menjadi dua jaringan berbeda. Sehingga *private network* tidak dapat dengan bebas diakses dari *Untrusted network*. Solusi lainnya adalah dengan menerapkan *Intrusion Prevention System* (IPS), yakni sebuah sistem yang mengawasi lalu lintas data pada jaringan dan mampu mengenali pola-pola usaha penyusupan yang bila berhasil terdeteksi IPS dapat segera mencegahnya dengan cara memblokir alamat menggunakan *blacklist firewall*. Selain itu, IPS akan memberikan peringatan berupa e-mail kepada administrator sehingga keamanan jaringan dapat selalu

terkontrol. Dipadukan dengan server berbasis linux ubuntu fitur dari sistem operasi pada PC Router Mikrotik, memungkinkan IPS dan DMZ untuk diterapkan bersama. Selain itu, dikarenakan kebutuhan minimum sistem dari Mikrotik RouterOS ini sangat rendah, dengan demikian komputer yang sudah yang tidak terpakai dapat difungsikan kembali.

Dengan diterapkannya sistem keamanan ini diharapkan dapat ancaman, atau bahkan upaya serangan yang dilancarkan pada server dapat dicegah dengan segera secara otomatis, dan juga memberikan pertahanan berlapis bagi perangkat yang berada di *private network*. Selain itu administrator dapat segera diberitahu jika terdeteksi adanya sebuah upaya penyusupan pada jaringan.

1.2 Maksud dan Tujuan

Maksud dari penelitian ini adalah melakukan perancangan sistem keamanan menggunakan metode DMZ dan IPS untuk melindungi server berbasis Linux Ubuntu. Sedangkan tujuan yang ingin dicapai dari penelitian ini adalah:

1. Menerapkan DMZ pada jaringan untuk memisahkan server dari private network.
2. Menerapkan IPS pada sistem untuk mendeteksi, mencatat, upaya penyerangan pada server dan mengirim email peringatan kepada administrator.
3. Menerapkan IPS menggunakan teknik pemblokiran alamat IP untuk merespon serangan pada server.

1.3 Batasan Masalah

Untuk mengerucutkan bahasan dari penelitian sistem keamanan jaringan ini maka dibuatlah beberapa batasan, diantaranya:

1. Sistem operasi yang digunakan pada PC Router adalah Mikrotik RouterOS 5.20.
2. Sistem keamanan ini dimplementasikan pada server dengan sistem operasi LINUX Ubuntu Server 14.04.3 LTS.
3. Perangkat lunak IPS yang digunakan adalah snort 2.9.9.0.
4. Jenis serangan yang akan diujikan adalah serangan dari *untrusted network.*

5. Teknik yang akan digunakan untuk pengujian adalah *port scanning, IP spoofing, Ping of Death Attack, dan Apache Range Header Attack*.

1.4 Metodologi Penelitian

Metode penelitian yang akan digunakan dalam penelitian ini. yaitu studi pustaka, perancangan, implementasi, pengujian dan analisa. Setiap kegiatan diuraikan sebagaimana berikut ini.

1. Studi Pustaka

   Kegiatan ini meliputi pengkajian literatur tentang komponen perangkat pembentuk sistem keamanan yang akan dibangun. Materi yang dikumpulkan berasal dari jurnal, buku-buku teks, dan konten Internet yang berkaitan dengan sistem keamanan jaringan. Hasil dari kegiatan ini adalah referensi teoritis untuk menunjang perancangan dari sistem keamanan ini.

2. Perancangan

   Pada tahap ini dibuatlah desain dari sistem keamanan ini termasuk membuat topologi jaringan, menetapkan fungsi sistem, dan menyiapkan perangkat lunak inti maupun pendukung. Seluruh kegiatan pada tahap ini mengacu pada referensi yang telah dikumpulkan ditahap sebelumnya dengan harapan sistem keamanan ini dapat berjalan sebagaimana mestinya.

3. Implementasi

   Pada tahap ini desain, topologi, dan fungsi yang sudah dirancang disimulasikan pada *virtual machine*. Kegiatan ini dimaksudkan untuk menguji rancangan sistem yang sudah dibangun dengan bebas. Jika terdapat kekurangan atau kesalahan pada perancangan sistem dapat dilakukan perancangan ulang untuk kemudian dilakukan simulasi kembali hingga sistem keamanan ini sesuai dengan yang diharapkan. Setelah simulasi berhasil dilakukan penerapan sistem ke *physical machine*. Spesifikasi, desain sistem, topologi jaringan, perangkat lunak yang digunakan dibuat sama dengan hasil simulasi terbaik.

4. Pengujian

   Pada tahap ini dilakukan pengujian akhir apakah sistem keamanan ini berjalan sebagaimana mestinya. Selain itu di tahap ini dilakukan uji penetrasi

keamanan pada server sebelum dan sesudah sistem keamanan ini diimplementasi.

5. Analisa

Analisa dilakukan pada hasil pengujian penetrasi sebelum dan sesudah sistem keamanan diimplementasi. Hasil yang didapat dari tahap ini salah satunya adalah data keberhasilan sistem keamanan ini mengenali, menangani, mempersulit usaha penyusupan yang dilakukan dari *untrusted network*.

1.5 Sistematika Penulisan

Sistematika penulisan dari laporan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini mencakup latar belakang masalah, maksud dan tujuan, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan dasar-dasar teori tentang topik yang akan dibahas berdasarkan studi literatur yang berhubungan dengan tugas akhir ini seperti: Mikrotik RouterOS, Firewall, Packet Sniffer, DMZ, IPS dan perangkat lain yang digunakan dalam perancangan sistem keamanan ini.

BAB III PERANCANGAN SISTEM

Bab ini menjelaskan tentang perancangan sistem, membahas tentang bentuk diagram sistem, topologi jaringan yang digunakan, serta konfigurasi tiap perangkat sehingga menjadi sebuah sistem keamanan yang dapat bekerja dengan baik.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini berisi cara pengujian serta analisis data yang didapat dari hasil pengujian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi simpulan berdasarkan penelitian dan saran yang kemungkinan dapat dikembangkan untuk penelitian lanjutan