BAB 1

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan semakin penting di masa sekarang ini, baik di dunia pekerjaan maupun pendidikan. Dengan banyaknya *device* yang terhubung terhadap masing-masing, maka akan semakin banyak celah kejahatan yang bisa dilakukan oleh orang tidak bertanggung jawab. Misalkan, adanya pencurian data yang dilakukan pada jaringan PT. ADLINK SINEMEDIA ataupun yang bertujuan untuk mematikan sumber daya jaringan di perusahaan tersebut. Oleh karena itu dibutuhkan suatu upaya yang bisa menjamin keamanan di *server* tersebut.

PT Adlink Sinemedia adalah perusahaan yang bergerak di bidang periklanan digital. Perusahaan ini mempunyai berbagai kontrak ekslusif dengan stasiun-stasiun televisi terkemuka sehingga bisa menjadi satu-satunya pilihan bagi klien produk apabila ingin memasarkan produk barunya. Contoh salah satu jenis periklanan yang digunakan kantor ini yaitu *Built In*, dimana produk klien diiklankan didalam suatu program televisi. sebeelum iklan tersebut ditayangkan maka akan diteliti terlebih dahulu data rating yang diinformasikan oleh perusahaan yang bergerak di rating televisi kepada Adlink. Salah satu cara yang diberikan oleh perusahaan rating tersebut adalah melalui *server* terpusat di kantor PT Adlink Sinemedia. Oleh karena itu dibutuhkan suatu pengamanan terhadap data yang disimpan di *server* pada PT. Adlink Sinemedia.

Dengan banyaknya cara yang bisa dilakukan untuk memperkecil kemungkinan terjadinya kejahatan yang bisa dilakukan pada *server* PT. Adlink Sinemedia. Beberapa cara yang bisa diimplementasikan untuk mengamankan *server* yaitu dengan menggunakan *Honeypot* dan *Intrusion Prevention System*. *Honeypot* adalah sebuah sistem umpan palsu yang dibuat mirip dengan sistem yang asli yang bertujuan untuk diserang sehingga sistem yang asli tetap aman dari serangan (Spitzner 2012: 12). Trafik jaringan dari luar akan diarahkan ke

sistem *Honeypot*, sehingga trafik ke *Honeypot* menjadi trafik yang berpotensi akan melakukan serangan atau bisa juga trafik normal. *Intrusion Prevention System* yang akan digunakan pada penelitian ini yaitu *Snort* dimana *IPS* ini akan digabungkan dengan *Honeypot* dalam melacak dan mencegah penyerang masuk ke *server*.

Snort pada intinya berfungsi sebagai pendeteksian terhadap trafik tersebut, dengan cara mengawasi trafik. Perangkat lunak *Snort* yang akan digunakan untuk pengamanan *server* yaitu Snort, Snort adalah perangkat lunak berlisensi terbuka atau *open source*. *Intrusion Prevention System* yang akan digunakan pada penelitian ini yaitu Snort, Snort adalah perangkat lunak *Intrusion Prevention System*. Snort pada intinya akan digabungkan dengan *Honeypot* yang berguna sebagai pencegahan dan melihat jejak aktivitas penyerang. Penelitian ini bertujuan untuk mengimplementasi *Snort* ke *server* dan mencegahnya berdasarkan jejak aktivitas penyerang menggunakan *Snort rules* dengan harapan bisa menambah tingkat keamanan yang ada pada *server* dan memantau *traffic* yang masuk ke *server*.

Pada penelitian ini penulis merancang dan mengimplementasikan sistem IPS dan menggabungkan nya dengan *Honeypot* dengan harapan agar dapat menangani suatu penyerangan yang terjadi yang ditampung didalam *log file* dan memberikan informasi jika ada jenis penyerangan baru yang belum diketahui oleh sistem IPS itu sendiri.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas oleh kerena itu diperlukan rumusan masalah yang berkaitan dengan penilitian ini dan permasalahan keamanan pada PT. Adlink Sinemedia :

a. Apa saja lapisan keamanan yang akan diterapkan terhadap *server* pada PT. Adlink Sinemedia

b. Bagaimana *Intrusion Prevention System* akan mengamankan *server* yang ada di PT Adlink Sinemedia?
c. Bagaimana proses implementasi *Honeypot* dan *Intrusion Prevention System* pada *server* di PT. Adlink Sinemedia?

1.3 Ruang Lingkup

Implementasi keamanan pada *server* menggunakan *Honeypot* dan *Intrusion Prevention System* sebagai berikut :

a. Serangan dilakukan terhadap *server* dan *user* pada jaringan dengan skala kecil. Terdiri dari 1 komputer *server* dan 1 *webapp* virtual sebagai *decoy*. Sistem operasi yang digunakan oleh *server* adalah Windows 10 dan *WebApp virtual* yang digunakan adalah HoneyPy. Implementasi *Honeypot* sendiri akan menggunakan *HoneyPy* yang bersistem WebApp.
b. Simulasi serangan akan menggunakan metode *port scanning nmap* melalui terhadap IP Public pada jaringan di PT Adlink Sinemedia
c. Ketika implementasi *server* hanya terhubung dengan internet selama beberapa saat untuk dilakukan pengujian kemudian dimatikan kembali akses ke IP Public untuk sementara.

1.4 Tujuan dan Manfaat Penulisan

1.41 Tujuan Penulisan

Menerapkan sistem keamanan *Honeypot* untuk mendeteksi trafik yang mencoba masuk ke dalam jaringan pada PT Adlink Sinemedia dan Menerapkan *Intrusion Prevention System* untuk mencegah serangan yang mungkin akan terjadi kepada *server*.

1.42 Manfaat Penulisan

Adapun manfaat penulisan yang diharapkan bisa muncul dari penelitian pada PT. Adlink Sinemedia yaitu :

a. *Server* yang digunakan pada PT. Adlink Sinemedia menjadi lebih aman dari serangan jaringan maupun serangan lainnya.
b. Dapat melacak percobaan serangan yang terjadi terhadap *server* di PT. Adlink Sinemedia.
c. Mengurangi celah keamanan yang ada pada *server* di PT. Adlink Sinemedia dengan *Intrusion Prevention System.*

1.5 Luaran yang Diharapkan

Luaran yang diharapkan dari pembuatan penelitian yang penulis lakukan yaitu ketika terjadi serangan terhadap *server* di PT Adlink Sinemedia, *Honeypot akan* mampu mendeteksi dan melacak serangan yang terjadi kemudian *Intrusion Prevention System* akan mencoba untuk mencegah serangan yang terjadi kepada *server*.

1.6 Sistematika Penulisan

Untuk memperoleh gambaran akan penelitian ini, oleh karena itu penulis membuat garis besar sistematika penulisan sebagai berikut :

BAB 1 : PENDAHULUAN

Bab ini berisi tentang latar belakang penulisan dan permasalahannya, tujuan penulisan, manfaat penulisan, luaran yang diharapkan serta sistematika penulisan.

BAB 2 : LANDASAN TEORI

Bab ini berisi tentang teori-teori mengenai konsep dasar jaringan, konsep dasar *server*, konsep dasar keamanan jaringan, konsep dasar *Honeypot*, konsep dasar *Intrusion Prevention System*, alat perangkat lunak yang digunakan serta referensi jurnal yang digunakan sebagai acuan.

BAB 3 : METODOLOGI PENELITIAN

Bab ini berisi tentang langkah-langkah sistematis penelitian, metode pengumpulan data, teknis analisis data dan komponen keamanan jaringan yang akan diterapkan

BAB 4 : ANALISIS DAN PEMBAHASAN

Bab ini berisi tentang profil organisasi, analisa sistem (analisa proses bisnis, analisa masukan dan keluaran, analisa masalah identifikasi kebutuhan), dan perancangan sistem (rancangan sistem, rancangan *server*, rancangan keluaran) serta pemecahan masalah dan pembuatan solusi.

BAB 5 : PENUTUP

Bab ini menjelaskan tentang kesimpulan yang didapat dari penelitian yang dibuat oleh penulis dan juga saran yang berhubungan dengan sistem yang akan dipakai pada penelitian ini.