BAB 1
PENDAHULUAN

1.1 Latar Belakang

Di dalam perkembangan dunia teknologi informasi, jaringan internet telah berkembang secara pesat, sehingga dapat dilakukan komunikasi data antar pengguna dengan mudah, baik mengakses data yang bersifat pribadi maupun tidak. Namun hal ini menimbulkan permasalahan baru dimana adanya pengguna internet yang memanfaatkan data-data tersebut untuk mencari keuntungan pribadi melalui cara yang illegal *(Cybercrime)*. Oleh karena itu, suatu sistem keamanan pada sebuah *server* pada jaringan komputer sangat penting, baik dalam konteks untuk menghindari serangan atau keselamatan data dari pada jaringan tersebut.

Tingkat keamanan di dalam sebuah jaringan komputer sangat berpengaruh terhadap eksistensi sebuah jaringan, dikarenakan jika tingkat keamanan sebuah jaringan lemah maka rentanlah terhadap serangan-serangan yang mengancam layanan yang terdapat pada jaringan tersebut. Oleh karena itu, sebuah jaringan komputer tidak boleh berada pada kondisi yang rentan terhadap serangan, banyak teknik intrusi yang dapat mengancam keamanan jaringan, seperti *port scanning, exploitation, Denial Of Service* (DoS), dan berbagai teknik serangan lain. Karena hal tersebut akan menyebabkan kerugian nantinya pada jaringan komputer. OSSIM (*Open Source Security Information Management*) adalah sebuah sistem kompleks yang melakukan pengawasan dan dapat menampilkan kondisi sebuah jaringan. OSSIM dapat menampilkan log dari yang digunakan untuk mengamankan suatu *server*.

Pada Proyek Akhir yang berjudul "Sistem Penanganan Serangan (*IPS-Intrusion Prevention System*) Berbasis OSSIM (*Open Source Security Information Management*)" ini akan dibahas tentang bagaimana membangun sebuah aksi penanganan serangan terhadap *server* atau jaringan komputer dengan menerapkan IPS (*Intrusion Prevention System*). Dikenal juga dengan *Intrusion Detection Prevention System* (IDPS), merupakan perangkat keamanan jaringan yang mengawasi jaringan dari berbagai ancaman berbahaya. Penanganan dan

pencegahan serangan terhadap *server* akan dilakukan dengan menerapkan IPS (*Intrusion Prevention Sysytem*). Pengujian dengan melakukan penyerangan dan aksi penanganan menggunakan Alienvault OSSIM sebagai perangkat lunak yang menjadi sistem keamanan server (IPS-*Intrusion Prevention System*) yang dapat menampilkan aktivitas dan manajemen log dari sensor yang dipasang pada jaringan.

1.2 Rumusan Masalah

Beberapa rumusan masalah dalam penyusunan Proyek Akhir ini adalah sebagai berikut.

1. Bagaimana cara mengimplementasikan sistem IPS (*Intrusion Prevention System*) pada Alienvault OSSIM ke dalam sebuah jaringan komputer?
2. Bagaimana cara kerja Alienvault OSSIM dalam melindungi sebuah jaringan komputer dan menampilkan log data manajemennya?

1.3 Tujuan

Berdasarkan rumusan masalah diatas maka diambil beberapa tujuan dari penyusunan Proyek Akhir ini sebagai berikut.

1. Membangun dan mengimplementasikan sistem keamanan Alienvault OSSIM (IPS-*Intrusion Prevention System*) ke dalam sebuah jaringan komputer.
2. Mengetahui cara kerja Alienvault OSSIM dalam melindungi sebuah jaringan pada sebuah jaringan komputer.

1.4 Batasan Masalah

Adapun batasan masalah dari Proyek Akhir ini adalah.

1. Menggunakan media modem *wifi* sebagai penghubung dalam jaringan.
2. Menggunakan IP versi 4 dalam pengimplementasiannya.
3. Pengalamatan yang digunakan pada *server* dan *client* adalah *static*.
4. Implementasi pada jaringan lokal.

5. Jenis serangan yang digunakan dalam pengujian adalah *Port Scanning,* dan *Denial of Service (DoS),* dan *Brute Force Attack.*
6. Tidak membahas tentang serangan *malware* maupun *virus.*
7. Dalam pengujian serangan menggunakan Sistem Operasi *Kali Linux*.

1.5 Definisi Operasional

Adapun definisi operasional pada proyek akhir ini adalah sebagai berikut :

1. Keamanan *server* atau jaringan, sebuah komunikasi data dalam dunia Teknologi Informasi selalu terdapat hubungan *server* dan *client*. Sebuah server yang berfungsi sebagai penyedia layanan harus selalu berada dalam keadaan aman dan optimal dalam kinerjanya. Berbagai serangan yang dapat muncul, harus dapat diwaspadai dan diantisipasi dengan menggunakan berbagai aturan pada jaringan.

2. Sistem keamanan *Open Source Alienvault SIEM* (OSSIM), yang merupakan sistem keamanan yang komprehensif mencakup *open source*. Alienvault adalah produk keamanan jaringan yang memungkinkan untuk mengintegrasikan ke dalam satu konsol, semua perangkat keamanan dan alat yang dimiliki di jaringan, dan pemasangan *tools open source* seperti *Snort, Openvas, ntop, dan OSSEC* [1].

3. *Intrusion Detection System* (IDS) adalah sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan) [2].

4. *Intrusion Prevention System* (IPS), merupakan sistem pencegahan atau penanganan terhadap serangan pada jaringan. Dikenal juga sebagai *Intrusion Detection Prevention System* (IDPS) yaitu perangkat keamanan jaringan yang berfungsi untuk mengawasi dan mencegah jaringan dari aktivitas yang berbahaya. Diharapkan dapat memberikan laporan kepada *administrator* mengenai usaha penyerangan terhadap sistem, melalui catatan atau log

yang dihasilkan oleh aplikasi, menjadi laporan dari aplikasi sebagai bukti digital yang mencatat segala usaha penyerangan ke dalam suatu sistem *server* [3].

1.6 Metode Pengerjaan

Metode yang digunakan dalam menyusun Proyek Akhir yang berjudul "Sistem Penanganan Serangan (IPS-*Intrusion Prevention System*) Berbasis OSSIM (*Open Source Security Information and Event Management*)" adalah dengan menerapkan metode SDLC (*System Developmet Life Cycle*) yaitu dengan tahapan :

1) Tahap Perencanaan

   Melakukan Studi Pustaka dengan menghimpun referensi dari berbagai sumber seperti buku-buku, artikel-artikel, modul-modul, internet, serta bahan referensi lain yang bisa dijadikan sumber informasi yang berhubungan dengan pembahasan Proyek Akhir ini.

2) Tahap Analisis

   a. Melakukan Analisis dalam pemasangan perangkat keamanan pada sebuah sistem jaringan dan konfigurasi pada aplikasi Alienvault OSSIM yang akan diimplementasikan pada sistem *server* atau pada jaringan.

   b. Melakukan Analisis terhadap informasi yang dihasilkan oleh perangkat Alienvault OSSIM.

3) Tahap Perancangan (Konfigurasi)

   Pada tahapan perancangan sistem untuk mengimplementasikan OSSIM untuk keamanan jaringan dibutuhkan setiap aspek yang mendukung untuk proses terbentuknya sistem keamanan, yaitu hardware, software, serta menentukan perangkat yang akan dipasang dan dikonfigurasi pada sistem keamanan sebuah server, seperti instalasi perangkat lunak, konfigurasi jaringan, serta konfigurasi layanan.

4) Tahap Pengujian

Tahap Pengujian Implementasi Alientvault OSSIM

Tahap pengujian dilakukan untuk mengetahui dan mendapatkan informasi dalam penerapan sistem keamanan menggunakan Alienvault OSSIM. Keamanan pada sisi *server* dihasilkan oleh berbagai aplikasi atau perangkat dalam jaringan. Setiap kejadian ini dikumpulkan dan dibakukan oleh sensor Alientvault, yang juga bertanggung jawab untuk mengirimkan data tersebut ke *server*.

1.7 Jadwal Pengerjaan

Tabel 1. 1 Jadwal Pengerjaan

No.	Kegiatan	Tahun 2017																			
		Maret				April				Mei				Juni				Juli			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Tahap Perencanaan																				
2	Tahap Analisis																				
3	Tahap Perancangan																				
4	Tahap Pengujian																				
5	Penyusunan dan Pembuatan Laporan																				