BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan jaringan internet dewasa ini sangatlah pesat, terbukti dengan banyaknya masyarakat yang sudah bisa mengakses internet. Dalam satu tahun terakhir tercatat lebih dari 3.000.000.000 pengguna aktif internet [1]. Seiring dengan pesatnya internet menjadikan keamanan dari data atau informasi yang berada di internet publik sangatlah penting. Pada tahun 2015, kejahatan internet meningkat 38% dari kejahatan internet yang terjadi pada tahun 2014 [2]. Dengan peningkatan ini, banyak dampak yang terjadi seperti kehilangan data atau informasi penting, penghancuran data-data penting, penguasaan mesin secara penuh, memanipulasi data dan kerusakan pada jaringan. Selain dari itu terdapat juga beberapa serangan yang sering terjadi pada jaringan di antaranya *Denial of Service, Unauthorized Access, Phising* dan *DNS Spoofing.* Berdasarkan hasil analisa McAfee Labs [3], jenis serangan yang sering terjadi ialah *Denial of Service, Brute Force, Browser, Shellshock, SSL, Backdoor, Botnet*. Untuk mengatasi masalah tersebut, sistem keamanan harus mampu mendeteksi dan memberikan respon terhadap serangan secara otomatis.

Untangle merupakan suatu sistem operasi berbasis linux yang berperan penting dalam pengamanan jaringan. Untangle memiliki fungsi *Intrusion Prevention System* (IPS) untuk mencegah dan memblokir secara otomatis dan cepat serta bisa diketahui secara cepat oleh admin jaringan dan fitur *report* yang berguna untuk memberikan informasi melalui *email* baik itu harian, mingguan atau bulanan serta memberikan notifikasi ketika terjadi serangan *hacker*.

Dalam Proyek Akhir ini dibangun sistem *Intrusion Prevention system* (IPS) menggunakan *Untangle* yang bertujuan memberikan pengamanan jaringan yang kompleks dari serangan *hacker* serta mengurangi pencurian dan kerusakan data atau informasi penting.

1.2 Rumusan Masalah

Perumusan masalah berdasarkan latar belakang yang telah diuraikan dapat dirumuskan sebagai berikut:

1. Bagaimana membangun sistem keamanan jaringan dengan *untangle*?
2. Bagaimana penanganan *untangle* terhadap serangan *Denial of Service, Exploit, Port Scanning* dan *Phishing*?
3. Bagaimana *untangle* memberikan informasi *source address, destination address* dan *port* penyerang kepada admin?

1.3 Tujuan

Adapun tujuan dari proyek akhir ini yang diharapkan tercapai ialah sebagai berikut:

1. Membangun sistem keamanan dengan *Intrusion Prevention System* menggunakan *Untangle.*
2. Mendeteksi menghentikan dan memblokir paket dari lalu lintas jaringan penyerang.
3. Memberi notifikasi dan *report* serangan jaringan pada admin.

1.4 Batasan Masalah

Agar dalam pengerjaan proyek akhir ini mendapatkan hasil yang optimal, maka masalah akan dibatasi sebagai berikut:

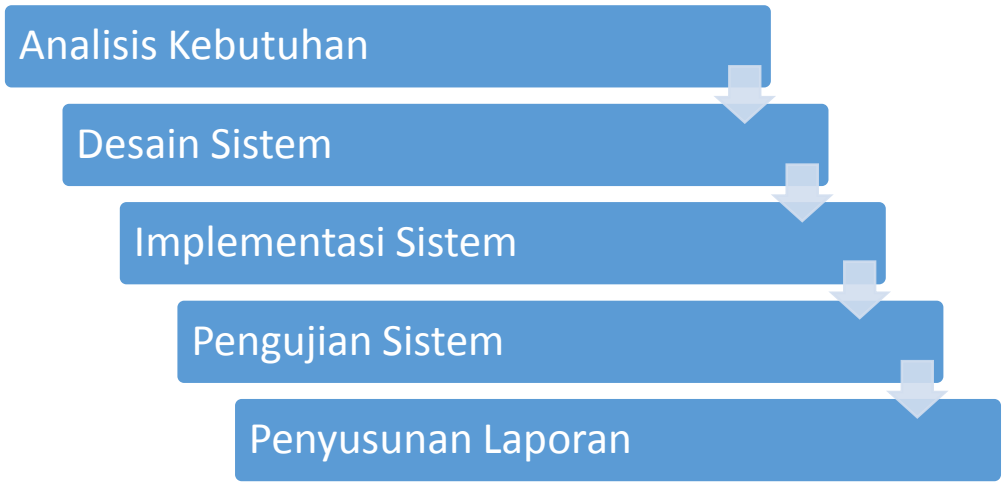
1. Sistem yang dibuat berfokus pada IPS.
2. Sistem keamanan jaringan ini menggunakan *Untangle* sebagai sistem operasi yang di dalamnya terdapat fungsi IPS.
3. Dalam sistem ini, informasi serangan dikirim ke admin jaringan berupa *email notification.*
4. Sistem IPS ini menggunakan *signature-based* untuk mendeteksi serangan.
5. Penyerangan dilakukan pada jaringan lokal.
6. Sistem ini tidak menangani serangan *malware*.
7. Tidak membahas konfigurasi *router*.

1.5 Definisi Operasional

1. *Intrusion Prevention System* (IPS) adalah sistem *Intrusion Prevention* yang dapat mendeteksi dan mencegah aktivitas berbahaya yang dilakukan oleh *hacker* [4].
2. *Untangle* merupakan aplikasi yang digunakan pada jaringan komputer yang memiliki fitur *Intrusion Prevention. Untangle* dapat memberikan perlindungan dan pemblokiran terhadap aktivitas berbhaya dari *hacker*. Perlindungan yang diberikan seperti ancaman terhadap serangan jaringan [5].

1.6 Metode Pengerjaan

Metode pengerjaan yang digunakan dalam pembuatan sistem IPS ini adalah analisis kebutuhan, desain sistem, implementasi sistem, pengujian sistem dan penyusunan laporan.



Gambar 1-1 Tahapan Metode Pengerjaan

1. ANALISIS KEBUTUHAN

   Analisis kebutuhan ialah tahap awal dalam pembuatan sistem keamanan jaringan dengan IPS. Pada tahap ini dilakukan analisis mengenai *software* dan *hardware* yang diperlukan, sistem operasi dan *tools* yang digunakan untuk sistem IPS.

2. DESAIN SISTEM

   Pada tahap ini dilakukan perencanaan dan desain topologi mengenai sistem yang diimplementasikan pada sistem IPS.

3. IMPLEMENTASI SISTEM

   Pada tahap ini dilakukan pembuatan sistem yang telah dirancang, seperti konfigurasi sistem. Serta pada tahap ini juga dilakukan instalasi perangkat keras dan lunak atau penggantian sistem yang lama dengan sistem yang baru.

4. PENGUJIAN SISTEM

   Pada tahap ini dilakukan pengujian terhadap sistem yang telah dibuat. Pengujian sistem dapat berupa penyerangan terhadap server pada jaringan lokal.

5. PENYUSUNAN LAPORAN

   Pada tahap ini dilakukan dokumentasi dan penyusunan laporan dari semua tahap yang telah dilakukan.

1.7 Jadwal Pengerjaan

Tabel 1-1 Jadwal Pengerjaan

No	Kegiatan	Jadwal Pelaksanaan Tahun 2016																			
		Januari				Februari				Maret				April				Mei			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Analisis kebutuhan																				
2	Desain Sistem																				
3	Implementasi Sistem																				
4	Pengujian Sistem																				
5	Penyusunan Laporan																				