BAB 1
PENDAHULUAN

1.1 Latar Belakang

Kebutuhan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui internet pula kegiatan komunitas komersial menjadi bagian terbesar dan pertumbuhannya menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar di dunia bisa diketahui selama 24 jam. Segi positif dari dunia maya ini tentu saja menambah *trend* perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Namun dampak negatif pun tidak bisa dihindari. Hingga saat ini serangan ke *server* mulai banyak terjadi, salah satunya adalah penyerangan terhadap SSH (*Secure Shell*) untuk melakukan *remote server*. Pemanfaatan SSH merupakan hal yang sangat penting untuk mengatur atau mengijinkan terjadinya komunikasi, hubungan, dan perpindahan data antara *server* dengan komputer. Pengamanan pada SSH harus dilakukan agar tidak sembarang orang bisa melakukan *remote server* dan mencuri data-data penting pada *server*. Tidak hanya pengamanan, pengawasan terhadap SSH juga menjadi hal penting demi menjaga keamanan pada *server*. Bahkan ketika keluar dari ruang lingkup *server* pun sistem pengawasan pada SSH sangat diperlukan.

Dari permasalahan tersebut, tentunya diperlukan pengamanan terhadap SSH. Salah satunya adalah menggunakan *Fail2ban*. *Fail2ban* adalah *package* keamanan yang digunakan untuk mencegah serangan *brute force* dan *dictionary attack* pada *linux* yang ditulis menggunakan *Python*. *Fail2ban* bekerja dengan cara membaca *log file* dari SSH, *apache* dan lainnya kemudian secara otomatis menerapkannya pada *IPtables* untuk memblok serangan. Pada *Fail2ban* ini terdapat konfigurasi untuk mengatur *IP Address* yang ingin diabaikan, waktu blok akses, dan jumlah maksimum *user* dapat mencoba *login*. Selain itu, diperlukan juga *monitoring* pada SSH agar *user* tidak perlu berada 24 jam di depan *server* untuk mengawasi *port* SSH. Dengan menambahkan fitur notifikasi berbasis *Telegram Messenger*, maka akan sangat memudahkan *user* pada saat melakukan *monitoring*.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, ada beberapa hal yang menjadi rumusan masalah, yaitu sebagai berikut:

1. Bagaimana mengamankan *port* SSH pada *server* dengan menggunakan *Fail2ban*?
2. Bagaimana mengimplementasikan fitur notifikasi berbasis *Telegram Messenger* sebagai media *monitoring* ketika *user* tidak dapat melakukan *monitoring* langsung?

1.3 Tujuan

Adapun tujuan dari proyek akhir ini adalah:

1. Mengimplementasikan *Fail2ban* untuk mengamankan *port* SSH pada *server*.
2. Mengintegrasikan SSH dengan *Telegram Messenger* sebagai media notifikasi ketika *user* berhasil *login*.

1.4 Batasan Masalah

Adapun batasan-batasan masalah pada proyek akhir ini adalah sebagai berikut:

1. *Server* menggunakan sistem operasi *Ubuntu Server*.
2. Implementasi dilakukan pada jaringan lokal.
3. Menggunakan *software Fail2ban* untuk mengamankan *port* SSH pada *server* yang berfungsi memblokir serangan.
4. Memblokir jenis serangan *brute force attack* dan *dictionary attack*.
5. Hanya melakukan pemblokiran berdasarkan IP yang terdeteksi sebagai *alert* dengan *ban time* yang telah ditentukan.
6. Mengirimkan notifikasi ke *Telegram Messenger* jika terdapat *user* yang berhasil *login* SSH dengan perantara *Telegram bot*.

7. Menggunakan *Shell Scripts* untuk menghubungkan SSH dengan *Telegram Messenger*.

1.5 Definisi Operasional

1. *Fail2ban*

   Fail2ban adalah *package* keamanan yang digunakan untuk mencegah serangan *brute force* dan *dictionary attack* pada *linux*. *Software* ini bekerja dengan melakukan *monitoring* jumlah kegagalan *login* dan selanjutnya ditindaklanjuti dengan memblokir IP dari *login* yang gagal tersebut.

2. SSH (*Secure Shell*)

   SSH atau *Secure Shell* adalah protokol jaringan yang mengatur atau mengijinkan terjadinya pertukaran data melalui saluran aman antara dua perangkat jaringan.

3. *Shell Scripts*

   Shell Scripts adalah beberapa perintah yang ditulis dengan *plaint text file* yang kemudian akan dieksekusi oleh *shell.*

4. *Telegram Messenger*

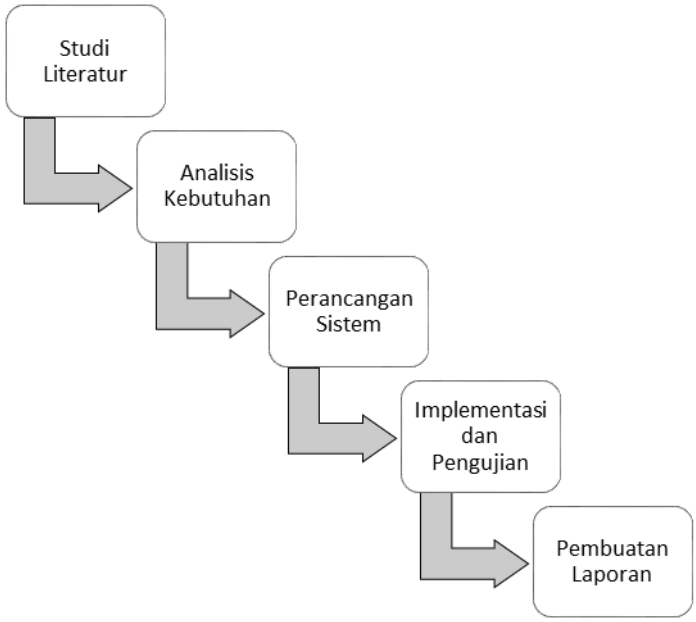
   Telegram Messenger adalah aplikasi pesan *chatting* yang memungkinkan pengguna untuk mengirimkan pesan *chatting* rahasia yang dienkripsi *end-to-end* sebagai keamanan tambahan.

5. *Telegram Bot*

   Telegram bot adalah sebuah *bot* dari *Telegram* yang dioperasikan oleh perangkat lunak dan memiliki banyak fitur. Aplikasi ini bisa terhubung dengan layanan lainnya.

1.6 Metode Pengerjaan

Metode yang akan digunakan dalam menyelesaikan proyek akhir ini adalah dengan metode yang ditunjukan pada gambar 1.1.



Gambar 1.1 Diagram

1. Studi Literatur

   Dilakukan pengumpulan data-data atau sumber-sumber yang berhubungan dengan topik yang akan dibahas dalam proyek akhir. Studi literatur bisa didapat dari berbagai sumber, jurnal, buku dokumentasi, internet dan pustaka.

2. Analisis Kebutuhan

   Pada tahapan ini dilakukan penentuan perangkat keras dan perangkat lunak yang akan digunakan dalam kebutuhan proyek akhir ini.

3. Perancangan Sistem

   Proses pembuatan rancangan sistem terdapat penggambaran rancangan topologi yang akan diimplementasikan.

4. Implementasi dan Pengujian

   Pada tahap ini dilakukan konfigurasi secara bertahap hingga selesai berdasarkan rancangan yang telah dibuat dan dilakukan pengujian agar meminimalisir terjadinya *error* terhadap perangkat yang dibuat.

5. Pembuatan Laporan

   Mencatat dan menyusun laporan tentang proyek akhir yang dikerjakan selama pengerjaan proyek akhir tersebut.

1.7 Jadwal Pengerjaan

Tabel 1.1 Jadwal Pengerjaan

No	Kegiatan	Waktu Pelaksanaan Tahun 2016																							
		Januari				Februari				Maret				April				Mei				Juni			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																								
2	Analisis Kebutuhan																								
3	Perancangan Sistem																								
4	Implementasi dan Pengujian																								
5	Pembuatan Laporan																								