BAB 1
PENDAHULUAN

Bab ini berisi uraian singkat mengenai latar belakang tugas akhir, identifikasi masalah dari tugas akhir, tujuan dan maksud dari tugas akhir, lingkup tugas akhir serta metode dan sistematika pembahasan tugas akhir.

1.1 Latar Belakang Tugas Akhir

Perkembangan internet yang semakin cepat dengan berbagai macam fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan webserver. Terutama dengan semakin terbukanya pengetahuan hacking dan cracking, didukung dengan banyaknya tools yang tersedia dengan mudah dan kebanyakan free, semakin mempermudah para intruder dan attacker untuk melakukan aksi penyusupan ataupun serangan. Terjadi nya penyusupan atau serangan dapat mengakibatkan masalah pada keberlangsungan sistem yang diserang oleh attacker .

Pencegahaan yang paling sering dilakukan untuk masalah ini adalah dengan menempatkan seorang administrator. Masalah timbul ketika sang administrator sedang tidak berada pada posisi siap sedia, misalnya sakit, berada di luar jam kerja, atau adanya kepentingan mendadak.Sedangkan serangan terhadap server bisa terjadi kapan saja.

Maka, dari permasalahan tersebut, administrator membutuhkan suatu sistem yang dapat membantu kerjanya. Sebuah sistem yang dapat membantu administrator jika sedang tidak berada di tempat, sebuah sistem yang dapat memberikan hasil laporan apa yang terjadi pada sistem apakah itu sebuah serangan atau penyusupan. Dengan hasil laporan yang di dapat ,administrator akan bertindak lebih jauh untuk mencegah terjadinya serangan di masa yang akan datang.

1.2 Identifikasi Masalah

Dari latar belakang di atas, perumusan masalah yakni bagaimana membangun sebuah sistem yang dapat memberikan notifikasi kepada admin jika terjadi serangan terhadap server.

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian Tugas Akhir ini adalah :

1. Sistem yang dibuat hanya menangani serangan bruteforce
2. Sistem hanya memberikan notifikasi berupa email kepada Admin jika terjadi serangan.
3. Sistem hanya akan dibuat di lingkungan sistem operasi berbasis Linux.
4. Sistem hanya akan menangani protocol SSH.

1.4 Tujuan Tugas Akhir

Adapun tujuan dan maksud tugas akhir ini adalah sebagai berikut :

1. Mencegah serangan bruteforce.
2. Memberikan informasi ke Administrator dari serangan yang terjadi.

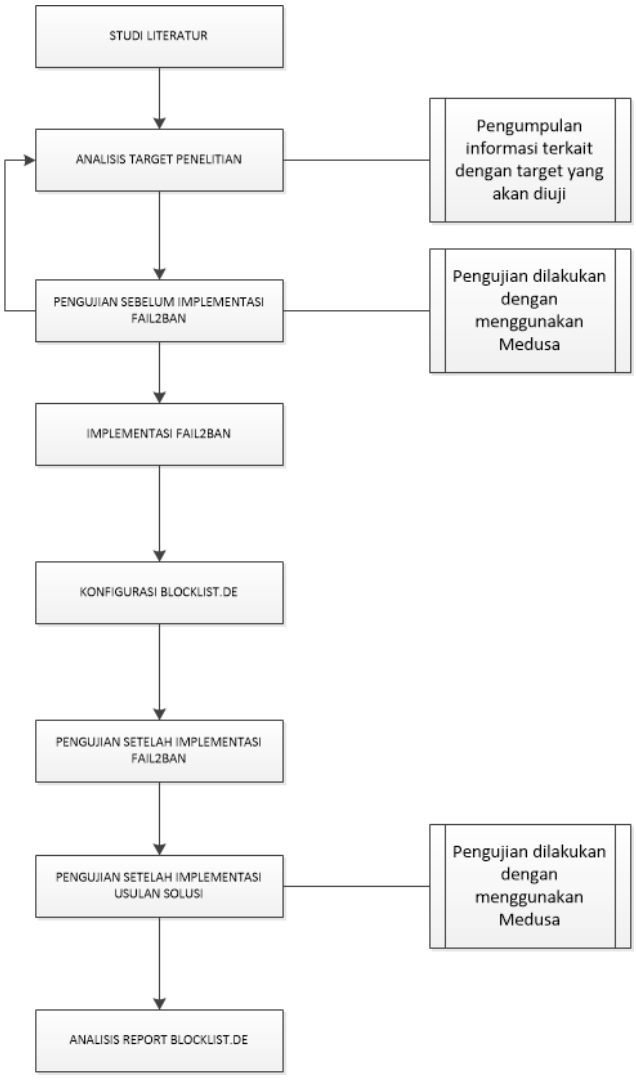
1.5 Lingkup Tugas Akhir

Adapun lingkup masalah pada penelitian Tugas Akhir adalah sebagai berikut :

1. Sistem operasi yang digunakan penyerang adalah Backtrack R3.
2. Aplikasi yang digunakan sebagai *defender* adalah **Fail2ban**.
3. Aplikasi yang digunakan penyerang adalah **Medusa**
4. Aplikasi reporting yang digunakan adalah web Blocklist.de

1.6 Metodologi Tugas Akhir

Pada pembuatan tugas akhir ini penulis menggunakan metode penelitian sebagai berikut berdasarkan pada gambar 1.1 :



Gambar 1-1 Metodologi Tugas Akhir

Berikut ini merupakan penjelasan pada gambar 1.1 :

1. Studi Literatur

   Pada tahap ini penulis melakukan pengumpulan fakta-fakta terkait dengan serangan *Bruteforce*

2. Tahap Analisis Lingkungan Penelitian

   Tahap ini adalah tahap dimana peneliti melakukan analisis terkait lingkungan penelitian, yaitu *Ubuntu server*.

3. Tahap Pengujian Sebelum Implementasi Fail2ban

   Tahap ini adalah tahap dimana dilakukan nya serangan *Bruteforce* terhadap target yang sudah ditentukan yang belum di implementasi Fail2ban.

4. Implementasi Fail2ban

   Tahap ini adalah tahap pengimplementasian Fail2ban sebagai bentuk solusi dari pencegahan serangan *Bruteforce*.

5. Konfigurasi Blocklist.de

   Tahap ini adalah tahap dimana *web reporting* di konfigurasi dengan mengisi data dari server yang di implementasi Fail2ban

6. Tahap Pengujian Setelah Implementasi Fail2ban

   Tahap ini adalah tahap dimana dilakukan nya pengujian yang sama dengan tahap sebelumnya dengan target yang sudah di implementasi Fail2ban.

7. Analisis Report Blocklist.de

   Tahap ini adalah tahap dimana menganalisa hasil *report* yang diterima oleh Blocklist.de dari Ubuntu Server.

1.7 Sistematika Penulisan Tugas Akhir

Secara umum keseluruhan laporan tugas akhir ini terdiri dari lima bab serta terdapat daftar pustaka, penjelasan mengenai tiap babnya adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini berisi uraian singkat mengenai latar belakang tugas akhir, identifikasi masalah dari tugas akhir, tujuan dan maksud dari tugas akhir, lingkup tugas akhir serta metode dan sistematika pembahasan tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini berisi penjelasan tentang dasar – dasar teori mengenai SSL, OpenSSL, Serangan Heartbleed dan cara penanggulangannya.

BAB 3 ANALISIS DAN PENGUJIAN

Bab ini berisi penjelasan tentang pengujian sebelum di implmentasi Fail2ban.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi *Fail2ban* dan pengujian ulang dengan metode yang sama sebelum pengimplementasian Fail2ban.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan beserta dengan saran selama pelaksanaan dan pengerjaan tugas akhir yang dilakukan,

DAFTAR PUSTAKA

Daftar pustaka berisi sumber penjelasan di dalam pelaksanaan tugas akhir.