BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi dan sistem pertahanan siber saat ini berkembang begitu pesat dengan kemajuan teknologi pada bidang siber khususnya pada *web server* dan *database* dapat menjadi suatu ancaman dalam dalam pencurian data dan informasi sehingga perlu adanya penilaian keamanan untuk menanggulangi terjadinya pencurian data[1]. Dampak positif dunia maya saat ini tentu saja mempermudah manusia dalam melakukan perkembangan teknologi dunia dengan segala bentuk kreatifitas. Namun dampak negatif pun tidak bisa dihindari[2]. *web server* dan aplikasi berbasis *web* sekarang banyak digunakan digunakan di berbagai organisasi dan pelaku usaha, dan mereka sering menjadi sasaran berbagai serangan dari yang dapat menyebabkan kerusakan pada sistem yang ada. Untuk mengurangi risiko penyerangan pada *web*, *web developer* perlu mengembangkan aplikasi yang aman untuk mencegah serangan. Deteksi serangan sangat penting untuk merespons insiden, membatasi kerusakan dari serangan, mencegah serangan, dan mencegah serangan di hari yang akan datang.

Menurut sebuah laporan oleh Badan Siber Sandi Negara (BSSN), selama 2019 hingga 2022, menurut pengamatan mereka ada 96 juta serangan siber (intrusi) ke jaringan internet di indonesia. Serangan yang terbesar adalah serangan *bruteforce attack*, diikuti dengan serangan menggunakan metode *malware*[3]. Dan juga pada laporan *top 10 OWASP web application security risk misconfigurasi* dari *web administrator* berada pada posisi enam, dengan begitu para *attacker* dapat mencari misconfigurasi tersebut menggunakan metode bruteforce directory maka dari itu pengujian metode *directory bruteforce* masih sangat efektif untuk mencari misconfigurasi tersebut[4].

Intrusi dapat didefinisikan sebagai kumpulan peristiwa dan ancaman yang mengancam kerahasiaan dan integritas informasi atau data pada sumber daya yang

ada diinternet seperti data pengguna, data perusahaan, data rahasia negara. Serangan pada jaringan komputer adalah ancaman radikal karena mereka diancam setiap jam sepanjang hari dan dengan penemuan celah keamanan yang sangat cepat. Masalah dalam pendeteksian serangan meningkat dikarenakan penggunaan *botnet* oleh *attacker*. Dua serangan jaringan yang umum adalah *Denial of Service* (DoS) dan *Bruteforce*[5]. Untuk menangani intrusi pada *server*, diperlukan *Intrusion Detection System* (IDS) yang diinstal pada *server*. IDS akan melacak serangan dan aktivitas yang mencurigakan pada *server* kemudian mengirimkan laporan ke keamanan *system administrator* [6]. Dalam deteksi intrusi, aplikasi berbasis *web* biasanya menggunakan: *web log* dari *web server* untuk mendeteksi intrusi. Sangat berguna untuk *web adminitrator* agar untuk dapat mencari tahu penyebabnya dari serangan di *web server*. Dengan menganalisis *file log* ini, *web adminitrator* mampu mengklasifikasi beberapa pola serangan pada *web* [7].

Pada penelitian ini, Penulis menggunakan perangkat lunak yang berbeda, yaitu Teler. Teler adalah alat deteksi intrusi *Realtime* dan peringatan berbasis *log web* yang berjalan di terminal. Teler dirancang untuk menjadi penganalisis ancaman berbasis terminal yang cepat. Inti Idenya adalah dengan cepat menganalisis dan mengklasifikasi ancaman untuk mencegah bahaya yang akan datang lebih cepat [8]. Penggunaan *web log* untuk mendeteksi penyusupan juga dilakukan. Dalam penelitian Seyyar dkk[9]., mereka mempelajari deteksi pemindaian kerentanan *web* melalui akses *file log web server Apache* selain deteksi serangan *XSS* dan *SQLI* menggunakan aturan berbasis metodologi . Devi dan Kumar [10] telah melakukan penelitian dengan menganalisis kerentanan aplikasi berbasis *web* menggunakan *Ethical Hacking*. Tujuan utama melakukan analisis kerentanan adalah untuk mengidentifikasi kesenjangan dan kelemahan dalam jaringan dan *web* aplikasi yang menggunakan pengujian penetrasi untuk melindungi berbagai pihak dari ancaman di *attacker* di dunia maya.

Dari penelitian sebelumnya, banyak yang belum mengulas Teler untuk mendeteksi intrusi pada *HTTP* di *web server* karena *tools* ini ada masih tergolong baru. Oleh karena itu, penulis mencoba menerapkan penggunaan Teler dalam

mendeteksi *HTTP* intrusi pada *web server* berbasis *Web log*. Intrusi adalah dilakukan dalam serangan yang biasa digunakan oleh penyerang, untuk contoh, pemindaian *port* dan *brute force* direktori menggunakan *Dirsearch.* Tujuan dari penelitian ini adalah untuk menguji apakah Teler dapat mendeteksi penyerangan dan kemudian melaporkannya peringatan serangan secara *real-time* ke *bot telegram,slack,discord*.

1.2 Rumusan Masalah

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

1. Bagaimana penerapan Teler sebagai *intrusion detection system* pada *web server*?
2. Bagaimana performa teler dalam mendeteksi serangan terhadap serangan *directory bruteforce* ?
3. Bagaimana perfoma teler dalam mengirimkan informasi ketika terjadi insiden serangan?

1.3 Batasan Masalah

Untuk mewujudkan penelitian yang sesuai dengan masalah yang ada diperoleh batasan-batasan masalah penelitian ini hanya berfokus pada :

1. Peneliti hanya menggunakan 1 *web server* sebagai uji coba dan 1 aplikasi Teler.
2. Peneliti melakukan implementasi ini pada *web server* uji coba(*blackbox*).
3. Peneliti hanya menggunakan 3 media penerima informasi *threat alert* yaitu Telegram , Discord dan Slack
4. Peneliti memfokuskan pada pendeteksian serangan *directory bruteforce* pada *webserver* yang diuji.
5. Peneliti hanya menggunakan dirsearch sebagai aplikasi untuk menguji *web server* yang sudah di konfigurasi teler.
6. Peneliti hanya menghitung detik jeda dari deteksi serangan dan pengiriman informasi serangan.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang ada maka dapat diketahui tujuan dari penelitian ini bahwa:

1. Mengimplementasikan Teler sebagai *intrusion detection system* pada *web server*.
2. Mengidentifikasi serangan *directory bruteforce* sebuah *website* ketika insiden penyerangan sedang berlangsung.
3. Mengindentifikasi rentang waktu laporan penyerangan pada media penerima informasi yang sudah dikonfigurasi.

1.5 Manfaat Penelitian

Dari penelitian ini, manfaat yang dapat diambil yaitu :

1. Diharapkan dapat memberikan gambaran mengenai unjuk kerja *software* Teler sebagai *intrusion detection system* pada *webserver* dalam mendeteksi serangan *directory bruteforce*.
2. Dengan mengetahui pengaruh penggunaan *software Teler* sebagai *intrusion detection system* pada *web server* diharapkan dalam implementasinya dapat meningkatkan memberikan peringatan pertama ketika terjadi insiden penyerangan pada *web server*.