BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah

Server merupakan sistem komputer yang menyediakan berbagai layanan dalam jaringan komputer[19]. Server terdiri dari berbagai jenis, diantaranya *web* server yang berfungsi untuk memberikan konten *web* kepada pengguna, *application* server yang digunakan untuk menjalankan dan mengelola aplikasi, *database* server yang digunakan untuk menyimpan dan mengelola data , email server yang digunakan untuk mengelola pengiriman dan penerimaan pesan, dan masih banyak lagi[18] . Saat ini, server berperan penting dalam keberlangsungan teknologi pada kehidupan sehari – hari.

Dengan semakin banyaknya penggunaan server dalam kehidupan sehari-hari di kalangan perusahaan, organisasi dan individu, risiko serangan *cyber* pada server semakin meningkat. Kompleksitas masalah dalam keamanan server terletak pada serangan *cyber* seperti pencurian data, peretasan, serangan kerentanan terhadap *malware* dan serangan lainnya yang berkelanjutan. Maka, keamanan server menjadi salah satu hal yang perlu diperhatikan dan ditingkatkan untuk melindungi data pengguna serta memastikan kelangsungan layanan pada server tersebut berjalan dengan baik.

1.2 Analisis Masalah

Pada bagian ini merupakan analisa masalah yang dituangkan berupa aspek – aspek diantarnya aspek keamanan, aspek teknis dan aspek lingkungan. Adapun analisis aspek aspek tersebut yaitu :

1.2.1 Aspek Keamanan

Server merupakan target utama dari berbagai serangan keamanan yang dapat membahayakan integritas, ketersediaan data, dan kerahasian. Ancaman – ancaman ini diantaranya *SQL injection* yang merupakan salah satu serangan umum yang terjadi pada server, dimana penyerang menyisipkan kode berbahaya untuk mengakses dan merusak basis data, selain itu ancaman *Cross-site Scripting*, serangan *brute force*, tidak ada implementasi enkripsi seperti SSL/TLS yang dapat membuat data yang dikirim antara server dan klien rentan terhadap penyadapan dan serangan *Distributed Denial of Service* (DDoS) yang dapat memenuhi server dengan lalu lintas palsu [2].

1.2.2 Aspek Teknis

Pada sebuah server, penting untuk memastikan server tersebut bebas dari celah keamanan yang dapat dimanfaatkan oleh penyerang. Dengan melakukan evaluasi keamanan secara berkala dan menyeluruh maka keamanan data pengguna, 5 mekanisme enkripsi data, kelemahan teknis dan fitur-fitur keamanan pada *Website* dapat didentifikasi dan diperbaiki keamanannya sehingga membantu aplikasi tetap berjalan dengan lancar[11].

1.2.3 Aspek Lingkungan

Keamanan pada server tidak hanya berdampak terhadap kualitas layanan dari server tersebut tetapi juga berdampak pada para pengguna. Server yang aman dan terpercaya memberikan kenyamanan pada pengguna, mengurangi adanya risiko kebocoran data yang akan meningkatkan kepercayaan pengguna[5]. Selain itu, adanya evaluasi keamanan yang dilakukan secara berkala juga turut berkontribusi untuk menangani insiden pada keamanan sehingga mendukung teknologi yang semakin ramah lingkungan.

1.3 Analisis Solusi yang Ada

Dalam konteks keamanan pada server dengan adanya tantangan serangan *cyber* berupa peretasan, pencurian data dan serangan *malware*. Maka, penyedia layanan diharapkan untuk mendeteksi, mencengah dan mengurangi risiko keamanan seperti menerapkan teknik autentikasi dan enkripsi yang baik serta melakukan pengecekan secara berkala guna memastikan bahwa fitur-fitur keamanan yang ada di penyedia layanan telah berfungsi dengan baik sehingga tidak ada celah yang dapat dimanfaatkan oleh penyerang.

1.4 Tujuan Tugas Akhir

Tujuan dari *capstone design* ini adalah untuk merancang dan mengembangkan solusi yang mampu mengatasi masalah keamanan *cyber* yang semakin mengingkat. Maka, pada *capstone design* ini menawarkan sebuah *platform* yang berisi *tools* yang dapat digunakan untuk pengujian keamanan server. *Platform* ini bertujuan untuk mengetahui celah keamanan pada suatu server sehingga *administrator* server dapat melakukan perbaikan terhadap temuan temuan celah keamanan sebelum dimanfaatkan oleh pihak yang tidak berwenang. *Platform* ini dikembangkan sebagai solusi keamanan server berbasis *Website* yang dapat diakses dengan mudah, sehingga mampu melayani berbagai kalangan, mulai dari pemilik bisnis kecil hingga perusahaan besar.

1.5 Batasan Tugas Akhir

Berikut merupakan batasan – batasan yang perlu diperhatikan dalam pengembangan *platform* ini :

- Solusi yang dikembangkan tidak mencakup pembuatan *tools* pengujian keamanan dari awal, melainkan mengembangkan sebuah *platform* berbasis *Website* yang mengintegrasikan *tools open source* yang sudah ada, dengan fokus utamanya adalah *tools* Nmap dan Nikto.
- Fitur pemindaian kerentanan yang disediakan *platform* ini terbatas pada identifikasi sistem operasi, pemindaian *port*, dan deteksi layanan atau aplikasi spesifik pada server target.
- *Platform* hanya berfungsi untuk mendeteksi, melaporkan temuan, dan memberikan rekomendasi perbaikan berbasis *generative* AI terhadap celah keamanan. Tindakan perbaikan atau mitigasi kerentanan tidak termasuk dalam ruang lingkup tugas akhir ini.
- Pengujian keamanan pada *platform* ini hanya terbatas pada keamanan server sebagai target utama. *Platform* ini tidak memeriksa keamanan seluruh perangkat dalam jaringan seperti router*, firewall*, atau komputer lainnya.
- Interaksi dengan sistem dibatasi hanya pada dua peran pengguna, yaitu "*user*" yang dapat menggunakan fitur pemindaian dan "*admin*" yang dapat mengelola data hasil pemindaian dan profil pengguna.