BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era konektivitas digital sekarang, teknologi informasi berkembang begitu cepat serta maju, salah satunya merupakan internet. Internet merupakan bagian dari teknologi data yang keberadaannya terus tumbuh dari tahun ketahun. Dalam pemanfaatannya, pengguna internet terus bertambah. Memandang luasnya cakupan daerah yang dijangkau oleh jaringan internet buat mencari data.

Pertumbuhan internet yang pesat ini diiringi dengan peningkatan jumlah pengguna dan cakupan wilayah yang dijangkau. Hal ini membuka peluang bagi para penjahat siber untuk melakukan serangan, termasuk serangan terhadap web server. Sebagai salah satu layanan informasi, website perlu membuat website yang dapat menangani permintaan banyak pengguna dengan baik.

Web server merupakan perangkat lunak yang memungkinkan pengguna mengakses website melalui internet. Serangan terhadap web server dapat mengakibatkan berbagai kerugian, seperti pencurian data, kerusakan infrastruktur, dan kerugian finansial [1].

Web server mempunyai tiga fungsi utama, Host beberapa situs web atau aplikasi web. Menangani permintaan FTP (File Transfer Protocol). Kirim dan terima email. Web server berfungsi sebagai menerima permintaan berupa halaman web memalui HTTP atau HTTPS dari web browser dan mengirimkan kembali hasilnya dalam bentuk halaman-halaman website yang berbentuk dokumen HTML [2].

Berdasarkan hasil survei penggunaan *web server* yang dilakukan *Netcraft* pada bulan januari 2024, menunjukkan bahwa *apache* dan *nginx* menjadi *web server open source* yang paling banyak digunakan menurut data dari *Netcraft*. Seperti yang terlihat pada tabel 1.1 berikut

Tabel 1. 1 *Penggunaan Web Server Aktif (sumber:Netcraft)*

Developer	Januari 2024	Persentasi
Apache2	39,401,334	20.48%
nginx	35,591,558	18.50%
Cloudflare	25,731,404	13.38%
Google	20,010,860	10.40%

Berdasarkan penggunaan web server yang semakin banyak, maka perlu untuk dilakukan keamanan, karena dalam web server menyimpan data pengguna seperti informasi pribadi atau data sensitif yang lain, kerahasian informasi web, keandalam layanan yang dapat mengganggu ketersediaan web dan membuat tidak dapat diakses oleh pengguna, dan untuk menjaga reputasi dan kepercayaan.

Saat ini, serangan terhadap web server semakin beragam dan kompleks, seperti serangan Distributed Denial of Service (DDoS), serangan Brute Force, dan injeksi SQL (SQL Injection). Serangan-serangan ini dapat menyebabkan gangguan layanan, pencurian data, dan akses tidak sah ke sistem. Untuk mendeteksi dan merespons serangan tersebut, penggunaan honeypot menjadi salah satu pendekatan yang efektif. Honeypot adalah sistem keamanan yang dirancang untuk menarik serangan dan mencatat aktivitas penyerang. Dalam konteks ini, terdapat tiga tipe utama honeypot: honeypot interaksi rendah, sedang, dan tinggi, yang masing-masing menawarkan tingkat kompleksitas dan interaksi yang berbeda dengan penyerang.

Meskipun honeypot telah terbukti efektif untuk mendeteksi serangan, masih ada perdebatan mengenai efektivitas masing-masing jenis honeypot dalam mengatasi ancaman terhadap web server. Untuk itu, penting bagi komunitas keamanan siber dan organisasi yang mengandalkan keamanan web server untuk memahami perbedaan dan manfaat dari setiap jenis honeypot. Melalui penelitian ini, penulis berharap dapat lebih memahami cara kerja ketiga jenis honeypot ini dan bagaimana mereka dapat membantu organisasi dalam melindungi infrastruktur web server dari serangan siber. Dengan demikian, penelitian ini dapat menjadi panduan

untuk mengembangkan strategi keamanan siber yang lebih efektif dalam menghadapi ancaman saat ini dan di masa depan.

1.2 Permasalahan

Web server memiliki peran vital sebagai pusat aktivitas berbagai layanan di internet, memproses ribuan koneksi dan transaksi setiap detik. Namun, di balik fungsinya yang esensial ini, web server menjadi target utama berbagai serangan siber yang terus berkembang, dengan tujuan untuk merusak, mencuri, atau bahkan menghancurkan data berharga. Serangan-serangan ini dapat datang dalam berbagai bentuk, seperti DDoS, Brute Force, dan injeksi SQL, yang semuanya berpotensi menyebabkan gangguan layanan dan kerugian besar bagi organisasi.

Dengan meningkatnya kompleksitas dan frekuensi serangan, para pengelola sistem menghadapi tantangan besar dalam memastikan keamanan web server mereka. Salah satu solusi yang sering dipertimbangkan adalah penggunaan honeypot. Namun, dalam memilih jenis honeypot yang tepat, pengelola harus mempertimbangkan berbagai faktor, seperti tingkat interaksi yang diinginkan, risiko yang dapat ditoleransi, dan efektivitas deteksi serangan.

Honeypot interaksi rendah menawarkan keamanan dasar dengan risiko minimal, tetapi mungkin tidak cukup efektif dalam mendeteksi serangan yang lebih canggih. Di sisi lain, honeypot interaksi tinggi dapat memberikan informasi yang lebih mendalam tentang teknik penyerang, tetapi dengan risiko yang lebih besar karena keterlibatan yang lebih kompleks. Honeypot interaksi sedang menawarkan keseimbangan di antara keduanya, namun efektivitasnya dalam berbagai situasi masih menjadi pertanyaan.

Permasalahan utama yang dihadapi dalam penelitian ini adalah menentukan jenis honeypot yang paling efektif dan efisien untuk mendeteksi serangan terhadap web server tanpa mengganggu operasionalnya. Bagaimana memilih honeypot yang tepat berdasarkan kebutuhan spesifik organisasi? Bagaimana mengintegrasikan honeypot ini ke dalam infrastruktur yang ada tanpa meningkatkan risiko? Dan yang terpenting, apakah mungkin untuk mengkombinasikan ketiga jenis honeypot ini untuk menciptakan solusi keamanan yang lebih komprehensif?

1.3 Tujuan

Tujuan dari penelitian ini adalah:

1. Menganalisis mekanisme kerja *honeypot*.
2. Membandingkan tingkat keakuratan deteksi.
3. Memberikan rekomendasi untuk implementasi *honeypot*.
4. Menjadi panduan bagi penelitian dan Implementasi di Masa Depan.

1.4 Manfaat

Manfaat dari penelitian ini adalah :

1. Pemahaman yang lebih baik tentang *Honeypot*.
2. Membantu mengambil keputusan pada organisasi atau instansi dalam melindungi *web server* dari serangan siber dengan lebih efisien, sesuai dengan sumber daya dan kebutuhan spesifik.
3. Sumber referensi untuk penelitian di Masa depan.

1.5 Sistematika Penulisan

Bab 1 Pendahuluan

Bab 1 menjelesakan tentang Latar Belakang Masalah, Permasalahan, Tujuan, Manfaat, dan Sistematika Penulisan.

Bab 2 Kajian Pustaka

Berisi penjelasan tentang teori-teori, konsep dan Penelitian Terkait yang berkaitan dengan penelitian ini.

Bab 3 Desain Sistem

Dalam bab III ini penulis membahas tentang Deskripsi Solusi, Desain Sistem dan Daftar Pustaka.

Bab 4 Eksperimen dan Analisis

Dalam bab IV ini penulis membahas tentang Metodologi Eksperimen, Pelaksanaan Eksperimen dan Analisis Hasil.

Bab 5 Penutup

Jelaskan tentang apa saja yang dibahas pada Bab 5. Penjelasan memuat bagian-bagian penting pada Penutup.