BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital ini, sistem informasi telah menjadi tulang punggung bagi banyak organisasi dan perusahaan. Sistem informasi digunakan untuk mengelola data, memfasilitasi komunikasi internal dan eksternal, menjalankan proses bisnis, dan menyediakan layanan kepada pengguna. namun penggunaan sistem informasi tidak terlepas terhadap serangan siber yang merugikan.

Data statistik dari Badan Siber dan Sandi Negara (BSSN) mencatat telah terjadi 370,02 juta serangan siber di Indonesia pada tahun 2022 Dibandigkan dengan tahun 2021 terjadi 266,74 juta serangan siber, yang dimana jumlah ini meningkat sebesar 38,72% [1]. ketika suatu badan organisasi, perusahaan , badan pemerintahaan dan lain sebagainya, terkena serangan siber tentunya akan menyebapkan berbagai masalah seperti, Gangguan operasional, Kerusakan reputasi, Hilangnya data pelanggan, Hilangnya data rahasia, Kehilangan bisnis, Kerugian material,Bocornya informasi perusahaan dan lain sebagainya. Berdasarkan *website* kompas, data Otoritas Jasa Keuangan (OJK), selama periode Semester I-2020 hingga Semester I-2021 saja, serangan siber membuat perbankan mengalami kerugian senilai Rp 246,5 miliar. Bahkan, secara global, Dana Moneter Internasional atau International Monetary Fund (IMF) memperkirakan angkanya mencapai Rp 1.420 triliun per tahun [2].

Agar terhindar dari kerugian materiil dan kerugian immateriil yang diakibatkan oleh serangan siber ,organisasi, perusahaan , badan pemerintahaan dan lain diharukan memiliki suatu sistem yang dapat memantau, menganalisis kerentanan, dan mencegah terhadap serangan siber.sistem pemantauan, analisis kerentanan, dan mencegah terhapat serangan siber ini dapat berupa *Intrusion Detection System (IDS)* yang dapat mendeteksi dan mencegah serangan siber.

Wazuh merupakan platform open source yang berperan sebagai *Intrusion Detection System (IDS)* atau sebagai sistem deteksi ancaman, pemantauan keamanan dan respons insiden. Mengimplementasikan wazuh dapat menjadi tembok pertahanan dalam sebuah badan organisasi, perusahaan , badan pemerintahaan dan lain sebagainya dalam mengatasi serangan siber. Implementasi wazuh memiliki fungsi untuk Threat prevention , Integrity monitoring ,Incident response ,Compliance dalam server, Deteksi ancaman ,Log Event Management dan Deteksi Celah dyang dapat meminimalisir terjadinya serangan siber.

1.2 Rumusan Masalah dan Solusi

Berdasarkan lantar belakang masalah yang telah dijelaskan di atas maka rumusan masalah dalam laporan magang ini adalah:

1. Bagaimana cara minimalisasir serangan siber?
2. Bagaimana membuat sistem pemantauan, analisis kerentanan, dan pencegahan terhadap serangan siber?

Dari rumusan masalah di atas kita dapatkan Solusi dalam menghadapi masalah-masalah tersebut seperti berikut:

1. Untuk meminimalisir serangan siber perlu dibuatnya sistem pemantauan, analisis kerentanan dan pencegahan terhadap serangan siber.
2. Implementasi Wazuh sebagai *Intrusion Detection System (IDS)* dapat berperan sebagai sistem pemantauan dan analisis kerentanan.
3. Membuat sistem blokir *brute force attack* pada wazuh.

1.3 Tujuan

Adapun tujuan dari penulisan laporan magang ini, sebagai berikut.

1. Membuat tembok pertahanan terhadap serangan siber.
2. Implementasi wazuh sebagai *Intrusion Detection System (IDS)* yang dapat berperan sebagai sistem pemantauan dan analisis kerentanan.
3. meminimalisir serangan siber dengan membuat sistem blokir brute force attack pada wazuh.

1.4 Batasan Masalah

Batasan malasah merupakan Batasan-batasan pembahasan yang akan penulis masukan di dalam laporan magang. Batasan masalah yang ada adalah sebagai berikut:

1. Implementasi wazuh hanya berperan sebagai sebagai *Intrusion Detection System (IDS)* yang berperan sebagai sistem pemantauan ,analisis kerentanan dan akan memblokir *brute force attack*.
2. Wazuh hanya akan memblokir *brute force attack SSH.*
3. Pencegahan serangan siber hanya dengan wazuh.
4. Pengimplementasi wazuh pada sistem operasi linux.

1.5 Penjadwalan Kerja

Selama melaksanakan magang di PT.INDO TRANS TEKNOLOGI penulis mendapatkan jadwal untuk magang di hari senin sampai jumat dengan ketentuan

senin dan kamis WFO dan untuk selasa, rabu, jumat WFH. Penulis mengerjakan tugas implementasi wazuh sebagai *intrusion detection system* secara bertahap mulai dari riset hinga uji efektifitas. Untuk lebih jelasnya berikut penulis membuat tabel pelaksanaan kerja di bawah.

Tabel 1. 1 Tabel Pelaksanaan Kerja

No	Deskripsi Kerja	Maret				April				Mei				Juni			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Riset wazuh																
2	Deploy wazuh server																
3	Penambahan agent wazuh																
4	Implementasi wazuh sebagai vulnerability scanner																
5	Costume dasboard wazuh																
6	Implementasi wazuh untuk blokir *burp force attack*																
7	Uji coba efektifitas wazuh dalam mengatasi serangan siber																