BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah mendorong banyak organisasi dan institusi untuk memanfaatkan sistem digital dalam operasional sehari-hari. Seiring dengan hal tersebut, ancaman terhadap keamanan siber juga mengalami peningkatan, baik dari segi jumlah, kompleksitas, maupun dampaknya. Salah satu jenis serangan yang umum terjadi adalah *brute force attack*, yaitu metode percobaan login berulang dengan menebak kombinasi *username* dan *password* untuk memperoleh akses ilegal ke dalam sistem.

Layanan SSH (*Secure Shell*) merupakan salah satu target utama dari serangan *brute force* karena fungsinya yang vital dalam pengelolaan server secara jarak jauh. Tanpa adanya sistem pemantauan dan deteksi yang memadai, serangan ini dapat berakibat pada kebocoran data, gangguan sistem, bahkan pengambil alihan kontrol oleh pihak yang tidak berwenang.

Dalam upaya memperkuat pertahanan terhadap ancaman tersebut, dibutuhkan sistem deteksi dini yang andal, *real-time*, dan mudah dikonfigurasi. Salah satu solusi yang digunakan adalah *Wazuh, platform open source* yang dirancang untuk memantau aktivitas keamanan melalui *analisis log*, deteksi ancaman, dan korelasi data berdasarkan aturan (*rules*) yang telah ditetapkan. *Wazuh* mendukung integrasi dengan berbagai komponen lain seperti *Filebeat* dan *Kibana*, sehingga memungkinkan visualisasi data dan pelaporan yang lebih informatif.

Untuk membuktikan efektivitas *Wazuh* dalam mendeteksi serangan *brute force*, dilakukan implementasi *Proof of Concept (PoC)* yang melibatkan simulasi serangan menggunakan *tools* seperti *Hydra*. Dua mesin virtual berbasis *Ubuntu* digunakan, dengan satu mesin bertindak sebagai *attacker* dan sekaligus *Wazuh Manager*, sementara mesin lainnya berfungsi sebagai target dengan peran sebagai *Wazuh Agent* dan *SSH Server*. Melalui

simulasi ini, dilakukan pengujian terhadap skenario *login* menggunakan *username* tidak valid dan percobaan akses menggunakan daftar *password* secara otomatis.

Hasil implementasi menunjukkan bahwa *Wazuh* mampu menghasilkan *alert* secara *real-time*, seperti indikasi kegagalan *login* melalui *PAM (Pluggable Authentication Module)* dan percobaan *login* menggunakan user yang tidak dikenal. Aktivitas ini terdeteksi dalam modul *Security Events*, serta diklasifikasikan ke dalam taktik *MITRE ATT&CK* seperti *Credential Access* dan *Privilege Escalation*. Hal ini menunjukkan bahwa sistem mampu mengidentifikasi pola serangan yang mencurigakan secara tepat dan terstruktur.

Melalui proses ini, dapat ditarik kesimpulan bahwa *Wazuh* merupakan solusi monitoring keamanan yang efektif dan layak untuk diimplementasikan dalam skala luas, baik pada institusi pendidikan, sektor industri, maupun pemerintahan. Optimalisasi monitoring serangan *brute force* berbasis *open source* seperti ini menjadi salah satu langkah penting dalam membangun sistem keamanan yang adaptif dan berkelanjutan di era transformasi digital.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam laporan Praktek Kerja Lapangan ini difokuskan pada bagaimana proses monitoring serangan *brute-force* pada layanan *SSH* dapat dilakukan menggunakan *platform Wazuh* berbasis *open source*, serta apa saja kendala yang ditemui selama tahapan instalasi, konfigurasi, dan pengoperasian sistem dalam mendukung deteksi dan pemantauan aktivitas mencurigakan secara *real-time*.

1.3 Tujuan PKL

Tujuan pelaksanaan Praktek Kerja Lapangan ini adalah:

1. Mengidentifikasi kendala-kendala yang dihadapi selama proses instalasi, konfigurasi, dan pengoperasian *Wazuh* dalam konteks deteksi serangan *brute-force* pada *SSH.*

2. Mengoptimalkan konfigurasi dan pemanfaatan *Wazuh* agar dmeningkatkan efektivitas monitoring serta pencegahan serangan *brute-force* pada layanan *SSH*.

1.4 Manfaat PKL

Adapun manfaat yang diperoleh dari implementasi sistem deteksi serangan *brute-force* menggunakan *Wazuh* ini adalah untuk membantu administrator sistem dalam memantau dan mengidentifikasi upaya serangan secara cepat dan akurat, sehingga dapat meningkatkan keamanan layanan *SSH* dan mengurangi risiko akses tidak sah yang berpotensi membahayakan sistem.