BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi yang pesat dalam beberapa dekade terakhir telah membawa banyak manfaat bagi berbagai sektor industri. Namun, hal ini juga memunculkan tantangan besar dalam hal keamanan siber. Seiring semakin kompleksnya ancaman yang dihadapi, organisasi dan perusahaan perlu beradaptasi dengan solusi yang efektif untuk melindungi sistem dan data dari potensi serangan siber. Salah satu ancaman yang paling umum adalah *Denial of Service* (*DoS*) dan *brute force attack* yang dapat mengeksploitasi kerentanannya pada sistem atau aplikasi, termasuk pada Windows Server.

PT. Dua Empat Tujuh (Solusi247) adalah perusahaan teknologi informasi di Indonesia yang memiliki lebih dari 20 tahun pengalaman dalam pengolahan data besar dan pengembangan solusi keamanan siber. Perusahaan ini berkomitmen untuk membantu kliennya dalam menghadapi ancaman siber melalui pengembangan produk *open source* yang handal dan efektif. Salah satunya dengan memanfaatkan Wazuh, sebuah *platform* keamanan berbasis *open source* yang dilengkapi dengan berbagai fitur penting, seperti deteksi anomali, pemantauan integritas file, serta analisis log secara *real-time*.

Dengan kemampuannya dalam mendeteksi ancaman siber secara cepat, Wazuh memiliki potensi besar untuk mendukung upaya mitigasi serangan *DoS* dan *brute force* pada Windows Server, yang kerap menjadi sasaran utama serangan. Meskipun Wazuh menawarkan berbagai fitur unggul dalam monitoring dan deteksi ancaman, implementasi dan pengujian efektivitasnya dalam menghadapi ancaman tersebut perlu diuji lebih lanjut.

Oleh karena itu, penelitian ini bertujuan untuk menguji dan mengevaluasi kemampuan Wazuh dalam mendeteksi serangan *DoS* dan *brute force* pada Windows Server. Penelitian ini juga diharapkan dapat memberikan gambaran yang jelas mengenai efektivitas Wazuh sebagai solusi keamanan siber yang dapat diandalkan dalam melindungi perusahaan dari ancaman yang semakin kompleks.

1.2 Deskripsi Pekerjaan

Sebagai bagian dari magang di PT. Dua Empat Tujuh, saya diberi tugas untuk menguji dan mengevaluasi Wazuh dalam mendeteksi serangan *DoS* dan *brute force* pada Windows Server. Pekerjaan ini mencakup beberapa tahapan, mulai dari pengumpulan informasi dan pemahaman sistem, instalasi Wazuh, simulasi dan pengujian serangan, hingga evaluasi dan penyusunan rekomendasi perbaikan.

Pada tahap awal, kegiatan berfokus pada pemahaman arsitektur dan konfigurasi sistem Wazuh, termasuk fungsi utama *Wazuh Server* dan *Wazuh Agent*, serta mempelajari jenis serangan seperti *DoS* dan *brute force*. Selanjutnya, dilakukan instalasi *Wazuh Server* di lingkungan pengujian dan *Wazuh Agent* pada *endpoint* Windows Server yang menjadi target pengujian, serta integrasi Wazuh dengan bot Telegram untuk pengiriman notifikasi *alert* secara *real-time*.

Setelah instalasi, dilakukan simulasi serangan *DoS* dan *brute force* menggunakan alat seperti *Hping3* dan *Hydra*. Simulasi ini bertujuan untuk menguji kemampuan Wazuh dalam mendeteksi serangan tersebut melalui analisis *log* dan aturan deteksi yang ada. Berdasarkan hasil pengujian tersebut, disusun rekomendasi perbaikan untuk meningkatkan keamanan dalam menghadapi ancaman *DoS* dan *brute force*.

Rekomendasi ini disampaikan kepada PT. Dua Empat Tujuh untuk mendukung penerapan dan pengaturan optimal Wazuh dalam lingkungan perusahaan. Kegiatan ini memberikan pengalaman praktis dalam pengujian keamanan siber sekaligus berkontribusi pada pengembangan solusi keamanan yang lebih baik.

1.3 Tujuan

Tujuan dari kegiatan magang ini adalah sebagai berikut:

1. **Menguji kemampuan Wazuh dalam mendeteksi serangan *DoS* dan *Brute Force*:**
    - Mengidentifikasi bagaimana Wazuh dapat mendeteksi serangan *DoS* dan *brute force* pada Windows Server.

2. **Mengembangkan keterampilan dalam pengujian keamanan siber:**
    - Meningkatkan kemampuan dalam merancang dan melaksanakan uji coba keamanan serta menganalisis efektivitas solusi keamanan yang diterapkan.
3. **Memberikan pemahaman tentang teknologi Wazuh dan integrasinya:**
    - Menyediakan wawasan mengenai penggunaan dan implementasi Wazuh dalam konteks perlindungan *endpoint* dan integrasinya dengan sistem lain.
4. **Memberikan kontribusi terhadap pengembangan keamanan siber di PT. Dua Empat Tujuh:**
    - Memberikan hasil uji coba yang dapat digunakan untuk meningkatkan pengaturan dan penerapan Wazuh dalam menghadapi ancaman *DoS* dan *brute force*.

1.4 Manfaat

Kegiatan magang ini memberikan berbagai manfaat bagi mahasiswa, perusahaan, dan universitas, yaitu:

1. **Bagi Mahasiswa**: Magang ini memberikan kesempatan bagi mahasiswa untuk mengembangkan keterampilan praktis dalam bidang teknologi informasi, khususnya dalam implementasi dan pengujian sistem keamanan. Selain itu, pengalaman magang ini memperkuat kemampuan teknis, riset, dan pemecahan masalah yang sangat dibutuhkan dalam karir profesional di bidang teknologi dan keamanan informasi.
2. **Bagi Perusahaan**: PT. Dua Empat Tujuh memperoleh hasil pengujian yang komprehensif mengenai efektivitas Wazuh dalam mendeteksi serangan *DoS* dan *brute force* pada *Windows Server*. Hasil penelitian ini memberikan wawasan berharga bagi perusahaan untuk mengevaluasi dan meningkatkan penerapan Wazuh dalam sistem keamanan yang ada.
3. **Bagi Universitas**: Magang ini memperkuat hubungan universitas dengan industri, memberikan wawasan tentang kebutuhan dan tren terkini yang dapat diintegrasikan ke dalam kurikulum. Selain itu, pengalaman magang

membantu universitas mengevaluasi kesesuaian kompetensi mahasiswa dengan kebutuhan pasar kerja, serta membuka peluang kerjasama lebih lanjut dengan perusahaan.