ABSTRAK

Docker merupakan proyek open source yang menyediakan platform terbuka bagi pengembang dan administrator untuk membangun, mengemas, dan menjalankan aplikasi dalam container di berbagai lingkungan. Container memungkinkan isolasi aplikasi dan ketergantungan lingkungan, namun juga membuka potensi risiko keamanan jika tidak dikelola dengan baik. Dalam konteks keamanan sistem, penting untuk mengetahui dan mengantisipasi berbagai kerentanan yang mungkin muncul pada image Docker.

Seiring meningkatnya penggunaan container dalam lingkungan produksi, ancaman keamanan terhadap teknologi ini juga semakin berkembang. Pemindaian kerentanan menjadi langkah krusial untuk memastikan bahwa image yang digunakan bebas dari komponen berbahaya atau celah keamanan. Namun, tidak semua alat pemindai memiliki efektivitas yang sama dalam mengidentifikasi risiko tersebut. Oleh karena itu, perlu dilakukan evaluasi terhadap kinerja alat pemindai kerentanan yang umum digunakan.

Penelitian ini menganalisis dan membandingkan dua alat pemindai kerentanan, yaitu OpenVAS dan Docker Scout, dalam mendeteksi celah keamanan pada image Docker. Proses pemindaian mengacu pada standar PTES (Penetration Testing Execution Standard) sebagai pedoman pelaksanaan pengujian keamanan. Setiap alat diuji pada beberapa image Docker untuk mengetahui jenis dan jumlah kerentanan yang terdeteksi.

Hasil penelitian menunjukkan bahwa masing-masing alat memiliki keunggulan dalam mendeteksi jenis kerentanan tertentu. OpenVAS lebih unggul dalam deteksi sistem secara menyeluruh, sedangkan Docker Scout lebih fokus pada kerentanan spesifik image. Rekomendasi keamanan yang dihasilkan dari kedua alat dapat digunakan untuk menyusun strategi mitigasi guna meningkatkan keamanan container Docker secara efektif.

Kata Kunci: Docker, PTES, OpenVAS, Docker Scout, Kerentanan