BAB 1 PENDAHULUAN

1.1. Latar Belakang

Teknologi merupakan hal yang sangat penting dalam kehidupan, terutama untuk mempermudah pekerjaan guna memenuhi kebutuhan sehari-hari, salah satunya internet. Di masa sekarang yang serba digital, jaringan internet banyak dimanfaatkan sebagai alat komunikasi yang dapat mempermudah seseorang individu maupun kelompok dalam pertukaran informasi jarak jauh yang saling berhubungan antara satu pengguna dengan pengguna lain.[1]

Seiring berjalannya waktu, teknologi juga mengalami kemajuan pesat. Hal ini secara tidak langsung memandu organisasi untuk mempromosikan bisnisnya. Hampir semua pelaku usaha baik besar maupun kecil menggunakan teknologi informasi untuk meningkatkan layanan bisnisnya guna meningkatkan efisiensi operasional. Untuk mencapai kinerja yang baik, bisnis memerlukan teknologi seperti server dan komputer dengan spesifikasi tinggi.[1] Namun, hal ini menimbulkan masalah bagi usaha kecil seperti startup atau *software development* karena biaya yang harus dikeluarkan cukup besar.Untuk mengatasi permasalahan tersebut dapat digunakan teknologi virtualisasi. Teknologi virtualisasi memungkinkan terciptanya perangkat virtual seperti sistem operasi, media penyimpanan data, dan perangkat keras pada sistem komputer yang sedang berjalan.Selain itu, teknologi ini mengurangi biaya yang diperlukan untuk pembelian infrastruktur dan meningkatkan efisiensi infrastruktur perangkat keras. .[1]

Dengan diterapkannya sistem virtualisasi server berbasis container, diharapkan dapat meningkatkan kinerja sebuah server dan memudahkan *deployment* (penyebaran) aplikasi web server, database server, dll ke server.[2] Sebagai container virtualizer, Docker menempati posisi yang lebih unggul dibandingkan teknologi virtualisasi container lainnya.[1] Meskipun container di Docker menawarkan banyak kemudahan, namun ada banyak hal yang perlu dipertimbangkan, termasuk masalah keamanan dan kerentanan yang ada pada

Docker. Keamanan sistem dapat ditingkatkan dengan melakukan uji kerentanan dan mendeteksi kerentanan sistem sebelum serangan terjadi. Pemindai kerentanan dapat digunakan untuk mendeteksi kerentanan dan mengambil tindakan terhadap kerentanan yang teridentifikasi. Adapun data yang sangat berharga untuk diamankan seperti data pelanggan, data keuangan, atau data bisnis strategi. Melindungi data-datanya dengan teknologi keamanan yang tepat seperti enkripsi, system firewall, dan control akses yang ketat, sangatlah penting bagi kelangsungan bisnis.

Pada penelitian ini, analisis kerentanan Docker dilakukan dengan menggunakan tools OpenVAS dan Docker Scout sebagai pemindai kerentanan dan menggunakan PTES sebagai acuan standar. Penggunaan kedua alat ini memungkinkan identifikasi kerentanan yang lebih lengkap, baik dari sisi aplikasi dan system secara keseluruhan, maupun dari sisi image Docker yang lebih spesifik. Pilihan standar PTES didasarkan pada fakta bahwa metodologi mencakup tahapan yang membantu melakukan analisis kerentanan dan penyerangan secara nyata. Fase-fase ini meliputi *pre-engagement intercations*, *intelligence gathering*, *thread modelling*, *vulnerable analisis*, *exploitation*, *post exploitation*, dan *reporting*.[3] Selain itu, jenis serangan seperti SQL injection untuk menguji celah keamanan pada image docker. Setelah itu hasil dari pengujian akan dianalisis kemudian di bandingkan seberapa efisien dalam penelitian ini dengan penelitian sebelumnya.

1.2. Rumusan Masalah

Bagaimana efektivitas alat pemindai kerentanan OpenVAS dan Docker Scout dalam mendeteksi celah keamanan pada Docker Container dan Docker Image yang rentan, serta bagaimana standar PTES dapat digunakan sebagai acuan sistematis dalam proses pengujian penetrasi tersebut?.

1.3. Tujuan dan Manfaat

Penelitian ini bertujuan untuk:

1. Mengevaluasi kerentanan Docker Container dan Docker ImageMenggunakan OpenVAS dan Docker scout. Docker Container dan Docker Image berdasarkan jumlah, jenis, dan Tingkat keparahan kerentanannya.

2. Mengimplementasikan tahapan *Penetration Testing Execution Standart* (PTES) dalam proses pengujian keamanan untuk menghasilkan pendekatan sistematis dan terstandar.
3. Menyusun rekomendasi strategi mitigasi keamanan yang berbasis hasil pemindaian untuk meningkatkan perlindungan system container di lingkungan DevSecOps.

Manfaat yang diharapkan dari penelitian ini meliputi:

1. Menjadi referensi dalam memilih alat pemindai kerentanan yang efektif untuk Docker container.
2. Memberikan wawasan mengenai penggunaan standar PTES dalam proses uji penetrasi terhadap container.
3. Membantu praktisi keamanan dan pengembang sistem dalam meningkatkan pertahanan terhadap ancaman siber pada lingkungan virtualisasi Docker.
4. Menunjukkan pentingnya pemindaian kerentanan sebagai bagian dari proses DevSecOps pada pengembangan aplikasi berbasis container.

1.4. Batasan Masalah

Untuk memfokuskan penelitian agar lebih terarah, maka ditetapkan batasan-batasan sebagai berikut:

1. Analisis kerentanan hanya dilakukan pada Docker image yang diketahui memiliki celah keamanan (vulnerable Docker).
2. Pemindaian kerentanan hanya menggunakan dua alat, yaitu OpenVAS dan Docker Scout.
3. Standar yang digunakan sebagai acuan dalam pengujian adalah PTES (*Penetration Testing Execution Standard*), tidak membandingkan dengan metode lain secara mendalam (hanya sebagai pembanding umum).
4. Jenis serangan yang digunakan dalam pengujian terbatas pada teknik SQL Injection.
5. Fokus pada perbandingan efektivitas deteksi, bukan perbaikan atau patching kerentanan.

1.5. Metode Penelitian

Penelitian ini menggunakan metode *prototyping* yang diterapkan untuk merancang dan mengembangkan sistem analisis kerentanan pada Docker Container secara bertahap dan iteratif. Metode ini dipilih karena memungkinkan peneliti untuk mengidentifikasi kebutuhan, mengembangkan prototipe sistem analisis, menguji efektivitas tools, dan melakukan perbaikan secara berulang hingga mencapai hasil yang optimal. Tahapan metode penelitian yang dilakukan meliputi:

1. Kajian Pustaka: Mengidentifikasi penelitian sebelumnya yang relevan untuk memahami kelebihan dan kekurangan metode yang telah ada. Dalam penelitian ini menggunakan tools OpenVAS dan Docker Scout sebagai alat untuk analisis kerentanan serta menggunakan metode PTES.
2. Pengumpulan data: Pada penelitian ini, data yang akan muncul yaitu data kuantitatif, dikarenakan berupa jumlah kerentanan yang ditemukan, tingkat keparahan (low,medium,high).
3. Rancangan Penelitian:
    a. Prosedur Penelitian:
        1) Menyiapkan lingkungan pengujian, termasuk instalansi OpenVAS dan Docker Scout pada sistem.
        2) Membuat atau mengunduh image docker yang telah diketahui rentan (vulnerable docker).
        3) Melakukan penyerangan dengan tools attack yang sudah di persiapkan seperti SQL Injection.
        4) Melakukan pemindaian kerentanan menggunakan OpenVAS dan Docker Scout secara terpisah.
        5) Membandingkan hasil pemindaian dari kedua tools berdasarkan jumlah kerentanan.
    b. Perancangan Sistem: Merancang system analisis yang mendokumentasikan hasil pemindaian, membandingkan performa OpenVAS dan Docker Scout, dan menghasilkan laporan yang sesuai dengan standar PTES.
4. Pengujian Hasil Penelitian: Menafsirkan data hasil pemindaian untuk keunggulan dan kelemahan dari OpenVAS dan Docker Scout dalam

mendeteksi kerentanan. Selanjutnya membandingkan hasil analisis dari alat OpenVAS dan Docker Scout dengan standar PTES yang digunakan untuk mengetahui seberapa efektiv dalam penggunaan alat tersebut. Selanjutnya memberikan rekomendasi praktis untuk penggunaan OpenVAS dan Docker Scout dalam pengamanan Container Docker.