BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi merupakan hal yang sangat penting dalam kehidupan, terutama untuk kelangsungan dan kenyamanan hidup manusia. Teknologi juga digunakan untuk mempermudah suatu pekerjaan guna memenuhi kebutuhan sehari-hari, salah satunya yaitu Internet. Di masa pandemi seperti sekarang ini, jaringan internet banyak dimanfaatkan sebagai alat komunikasi yang dapat mempermudah seorang individu maupun organisasi untuk pertukaran informasi jarak jauh yang saling menghubungan antara satu pengguna dengan pengguna lain.

Dengan mengikuti berkembangnya zaman, tentunya teknologi juga semakin berkembang. Hal ini secara tidak langsung juga menuntut sebuah organisasi dalam memajukan perkembangan perusahaanya, tentunya hampir semua perusahaan baik skala besar maupun kecil menggunakan teknologi informasi untuk meningkatkan layanan bisnis yang di kelolanya dalam meningkatkan perfoma perusahaan.

Peningkatan perfoma yang baik bagi perusahaan dibutuhkan suatu teknologi seperti *server* maupun *computer* dengan spesifikasi yang bagus, akan tetapi hal tersebut yang menjadi masalah bagi perusahaan terutama untuk perusahaan yang masih beskala kecil dikarenakan memerlukan biaya yang besar. Untuk mengatasi masalah itu dapat digunakan teknologi virtualisasi. Teknologi virtualisasi adalah teknologi mampu menciptakan suatu perangkatt virtual seperti sistem operasi, media penyimpanan data dan *hardware* pada sebuah sistem *computer* yang sedang berjalan, selain itu teknologi ini dapat mampu menekan biaya untuk membeli infrastruktur yang diperlukan dan peningkatan efektivitas infrastruktur *hardware*.

Salah satu jenis teknologi virtualisasi yaitu virtualisasi server. Virtualisasi server merupakan sebuah server yang di bangun pada *computer* atau laptop dengan menggunakan media *machineware*. Dalam membangun *virtual machine* juga membutuhkan *resource* yang banyak seperti *storage, memory,* maupun *bandwidth.*Tak dipungkiri sangat diperlukannya efisiensi penggunaan *resource*

hardware jika ingin menjalakan aplikasi yang lebih banyak lagi, hal tersebut dapat diatasi dengan metode *containerization. Container* dirasa lebih hemat dalam menkonsumsi *resource* serta menyediakan metode *isolation* yang juga disediakan oleh teknologi virtualisasi berbasis *virtual machine.*

Teknologi terbaru dari *container* yang dikembangkan oleh Solommon Hykes di dotCloud adalah Docker. Salah satu *platform* yang dibangun berdasarkan teknologi *container* . Docker sebagai virtualisasi kontainer memiliki kedudukan yang lebih unggul dibandingkan dengan teknologi virtualisasi *container* lainnya, Adanya sebuah *container* di docker memberikan banyak kemudahan, akan tetapi banyak hal yang harus diperhatikan salah satunya mengenai masalah keamanan/ kerentanan yang ada pada Docker. Oleh karena itu penelitian ini bertujuan untuk menganalisis kerentanan yang ada pada Docker, Penelitian ini dilakukan dengan menggunakan *Vulnerable Docker* yang merupakan sebuah *Virtual Machine* berisi Docker yang rentan yang dibuat oleh perusahaan *NotSoSecure*.

Pencegahan dalam meningkatkan keamanan sebuah sistem dapat di lakukan dengan melakukan uji kerentanan guna membantu dalam proses identifikasi kelemahan pada sistem sebelum adanya serangan. Untuk mendeteksi adanya kerentanan dan melakukan penanggangan terhadap kerentanan yang sudah teridentifikasi dapat dilakukakan menggunakan *Vulnerability scanner.* Pada penelitian ini *vulnerbility scanner* yang digunakan yaitu OpenVAS dan Docker Scan serta menggunakan standar NIST 800-115. Pemilihan standar NIST 800-115 di karenakan mempunyai tahapan yang cukup lengkap, meliputi tahap *planning, discovery, attack,* dan *Reporting.* Dari empat tahapan tersebut yang nantinya akan digunakan dalam melakukan pengujian pada penelitian ini. Oleh karena itu, analisis kerentanan pada Docker dilakukan berdasarkan *vulnerability* dan *threat.* Hasil dari analisis tersebut dapat digunakan untuk menjalankan beberapa *walkthrough* yang nantinya akan mendapatkan hasil eksploitasi dan total *attack threat* yang akan digunakan pada analisis risiko. Hasil analisis risiko tersebut dapat digunakan untuk membantu memperkuat sistem Docker untuk kedepanya.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang diberikan, maka dari itu rumasan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana memodelkan serangan yang akan diuji cobakan pada *Vulnerable Docker*?
2. Bagaimana menganalisis kerentanan yang ditemukan ?
3. Bagaimana menentukan tingkat kerentanan dari data hasil v*ulnerabily scanner*?

I.3 Tujuan Penelian

Bedasarkan rumusan masalah yang sudah dijabarkan. Maka tujuan dari penelitian ini, sebagai berikut:

a. Mengetahui permodelan serangan yang diuji cobakan pada *Vulnerable Docker*.
b. Mengetahui cara untuk menganalisis kerentanan yang ditemukan.
c. Mengetahui tingkat kerentanan dari data hasil *Vulnerability Scanner*.

I.4 Batasan Penelitian

Adapun batasan masalah pada penelitian ini adalah:

1. Penelitian dibatasi pada lingkungan sistem *Vulnerable Docker*.
2. Pembahasan risiko berdasarkan kerentanan dan threat pada sistem aplikasi dan Docker.
3. Penelitian hanya memberikan hasil dari analisis kerentanan pada Docker sesuai dengan standar NIST 800-115.

I.5 Manfaat Penelitian

Manfaat dari penelitian ini sebagai berikut:

1. Secara Teoritis, penelitian ini memberikan analisa risiko berdasarkan kerentanan dan eksploitasi yang akan dideteksi melalui *vulnerability scanner*.
2. Secara Praktis, mendapatkan cara penentuan penguatan pada kerentanan Docker

I.6 Sistematika Penulisan

Tugas akhir ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Pada bab ini berisi mengenai uraian latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batsan masalah dan sistematika penelitian.

Bab II Tinjauan Pustaka

Bab ini berisi literatur yang relevan dengan masalah yang sedang di teliti dan mempunyai keterkaitan dengan penelitian terdahulu.

Bab III Metodologi Penyelesaian Masalah

Bab ini berisi penjelasan mengenai konseptual model untuk merumuskan solusi dari permasalahan yang ada.Selain itu untuk menjawab rumusan masalah yang telah disusun yang bertujuan untuk memilih metode yang tepat dengan penelitian yang dilakukan.

Bab IV Perancangan dan *Scenario* Pengujian

Bab ini berisi tentang perancangan perangkat keras dan perangkat lunak yang akan digunakan untuk *Scenario* pengujian dan penelitian terhadap target.

Bab V Analisa Hasil dan Evaluasi

Pada bab ini berisi mengenai analisis dari perumusan masalah yang ada. Hasil yang di peroleh meliputi *Scenario* pada Bab IV serta gambaran dari tujuan penelian.

Bab VI Kesimpulan dan Saran

Pada bab ini berisikan penjelasan kesimpulan daru penelitian yang telah dilakukan, rancangan sistem dan *Scenario* pengujian, serta saran yang diberikan untuk penelitian selanjutnya.