BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi adalah tantangan yang tidak bisa dihindari dalam kehidupan manusia. Dalam hal ini perkembangan teknologi tersebut bisa dimanfaatkan dengan cara yang cermat [1]. Salah satu teknologi dalam *deployment* yaitu *docker*. *Docker* adalah open source project yang dirancang untuk membantu *application deployment* dengan menggunakan *software containers*. *Docker* menambahkan *application deployment engine* di atas *container execution environment* tervirtualisasi serta dirancang agar ringan dan cepat untuk menjalankan kode [2]. Dengan adanya *container* pada *Docker*, serta kelebihan didalamnya maka perlu ditinjau dari segi kerentanan dan keamanan pada *Docker* tersebut. Risiko keamanan terjadi karena adanya kerentanan atau *vulnerability* suatu sistem [3]. Menurut Jian yang telah mencari metode *defense* terhadap *escape attack*, *Docker* dihadapi dengan risiko serangan yang mengeksploitasi *kernel vulnerabiltiy* dari *malicious user*, setelah melakukan eksploitasi program *container* kemudian diluncurkan *escape attack* yang efektif sehingga dapat memperoleh hak akses *root* dari *host* dan akan mempengaruhi reabilitas *container* lain serta seluruh sistem [4].

Dengan adanya container dalam *Docker*, tentu juga memiliki resiko keamanan, salah satu resiko yaitu adanya kerentanan atau *vulnerability* pada sistem *Docker*. *Vulnerable docker* adalah *Virtual Machine* dengan *Docker* yang*vulnerable* diproduksi oleh perusahaan *NotSoSecure* pada tahun 2017, sebuah perusahaan memiliki fokus pada keamanan komputer [3]. Dalam memperkuat keamanan dalam sistem perlu dilakukannya uji kerentanan dalam proses analisa kelemahan pada suatu sistem sebelum adanya serangan yang terjadi. Dalam mendeteksi adanya kerentanan serta melakukan penangganan terhadap kerentanan yang teridentifikasi dapat digunakan metode *Vulnerability scanner* [5].

Vulnerability scanning adalah proses mendapatkan informasi *vulnerability* atau kerentanan pada network dengan menggunakan *tools network scanning* serta *vulnerability scanner*, dalam menemukan kerentanan seperti port terbuka, *bugs* pada aplikasi dan untuk mengetahui serangan yang mungkin terjadi pada website,

sehingga akan berdampak buruk apabila terjadi serangan [6]. *Vulnerability scanning* termasuk dalam automated *scanning* dimana kelebihan yang dimiliki yaitu efisien waktu serta biaya yang dikeluarkan lebih sedikit dibandingkan dengan *manual scanning*. *Penetration Testing* adalah metode Pengujian penetrasi, atau pentesting merupakan simulasi serangan oleh *attacker* dengan tujuan untuk melihat risiko potensi yang menyerang keamanan sistem [7], tidak cukup dengan mencari kerentanan yang dapat digunakan oleh *attacker* kemudian dilakukan eksploitasi pada kerentanan [8]. Dengan menggunakan standar NIST 800-115 yang merupakan panduan teknis untuk pengujian dan penilaian keamanan Informasi, standar yang dikhususkan untuk membantu organisasi dalam melakukan perencanaan tes keamanan Informasi, standar tersebut dinilai efisien dalam menangani kerentanan karena tahapan yang meliputi *planning, discovery, attack*, dan *report*-ing.

Menurut peneilitan oleh Tika Astriani tahun 2021, menggunakan *tools* OpenVas dan *Docker* Scan pada *vulnerable docker* dengan metode NIST 800- 115 diperoleh 7 *Vulnerability*, sedangkan hasil *vulnerability* dengan *Docker Scan* diperoleh 8 *Vulnerability* dengan kategori threat level *High, Medium* dan *Low* [5]. Hasil tersebut diperoleh melalui pengunaan frekuensi tiap walktrough, kemudian *vulnerability* yang memiliki nilai resiko tertinggi berada pada *Wordpress* User IDs and User.

Menurut penelitian oleh Fatin Hanifah tahun 2021, menganalisa *vulnerability* pada objek *vulnerable docker* menggunakan *AlienVault* dan *Docker Bench* dengan *framework CIS Control.* Melalui penelitian dengan mengumpulan data yang diperlukan, kemudian dilakukan analisa pada hasil eksploitasi *Vulnerable docker*. *Tools vulnerability scanner* pada penelitian tersebut adalah *AlienVault OSSIM* dengan *Docker* Bench for Security. Hasil yang diperoleh yaitu risiko tertinggi yang berada di aplikasi adalah *vulnerability* berupa *Wordpress User IDs* and *User Names Disclosure tools* yang digunakan yaitu *AlienVault*. Pada sistem ditemukan *vulnerability Enable User Namespace Support* [3]. Dari penelitian tersebut menggunakan 6 kontrol pada *CIS Control* V8.

Dalam penelitian ini, peneliti akan menggunakan *tools* Trivy dan Nessus sebagai *vulnerability scanner* untuk mendeteksi potensi kerentanan pada *vulnerable docker*. Dengan menggunakan standar NIST 800-115, hasil *report*ing digunakan

untuk analisa serangan *cyber* yang mungkin bisa dilakukan oleh *attacker* terhadap *vulnerable Docker*. Hasil tersebut diharapkan memberikan Informasi tambahan terkait serangan-serangan yang dilakukan oleh *attack*er dan kedepannyasebagai *report* untuk membantu memperkuat sistem *Docker*.

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas,maka rumusan masalah ditentukan sebagai berikut :

1. "Kerentanan apa yang dihasilkan oleh *tools* dalam *vulnerability scanning* pada *Continer vulnerable Docker* ?"
2. "Bagaimana *Vulnerability scanning* dengan *Penetration Testing* akan berjalan optimal dalam mencari kerentanan pada *Container vulnerable Docker* ?"

1.3. Tujuan Penelitian

Dari rumusan masalah yang sudah ditentukan, tujuan peneliti sebagai berikut :

1. Untuk memperoleh kerentanan pada *Container vulnerable Docker* dengan *tools scanning*
2. Untuk menguji performa *tools* dalam mencari kerentanan
3. Untuk mengkombinasi *Vulnerability scanning* dengan *Penetration Testing* dalam mencari kerentanan pada *Continer vulnerable Docker*

1.4 Batasan Masalah

Pada penelitian ini agar fokus pada batasan masalah, maka dibatasi dengan batasan sebagai berikut:

1. Penelitian menggunakan 2 *tools* pada *Vulnerability Scanning* dan 1 *tools* pada *Penetration Testing*
2. Objek *scanning* yang diteliti yaitu *Container* pada *Vulnerable docker*
3. Penelitian menggunakan *Virtual Machine*
4. Standar yang digunakan kedua meotde mengacu pada NIST 800-115
5. Hasil akhir penelitian berupa analisis dan *report* dari *tools* yang digunakan
6. Peneliti memberikan beberapa solusi terhadap kerentanan yang ditemukan