ABSTRAK

Docker sebagai virtualisasi *container* 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. Pencegahan dalam meningkatkan keamanan sebuah sistem dapat di lakukan dengan melakukan uji kerentanan guna membantu dalam proses identifikasi kelemahan pada sistem sebelum adanya serangan. Upaya dalam mendeteksi sebuah kerentanan yang ada pada Docker dapat menggunakaan *vulnerability scanner* yaitu OpenVAS dan Docker Scan. Pada 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.* Pada saat melakukan pengujian tentunya harus terdapat suatu tahapan yang jelas, maka dari itu standar yang digunakan pada penelitian ini yaitu NIST 800-115, standar ini dilakukan untuk simulasi pengujian dengan tahapan yang dimulai dari tahap *planning, discovery, attack* dan *report*. 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 Analis risiko. Didapatkan hasil analisa risiko tertinggi menggunakan OpenVas sebesar 116 pada *WordPress User IDs and User Names Disclosure* dan hasil analisa risiko tertiggi menggunakan Docker Scan sebesar 88,5 pada *Information Exposure Improper Input Validation* dan *Improper Input Validation*

Kata kunci — ***docker, nist,OpenVAS,vulnerability***