ABSTRAK

ANALISIS *VULNERABILITY MANAGEMENT* PADA *VULNERABLE* DOCKER DAN DOCKER *IMAGES* MENGGUNAKAN DOCKER SCAN DAN OPENSCAP BERDASARKAN STANDAR NIST CSF

Oleh

Fitria Nikmatul Hidayah

NIM : 1202184160

Penelitian ini menganalisis proses pengelolaan kerentanan Docker dan Docker *Images* dengan menggunakan standar NIST CSF. Penelusuran kerentanan menggunakan dua *tools scanning* yaitu Docker scan dan OpenSCAP. Kerentanan pada docker dan docker images versi - 1, diatasi dengan membuat sistem baru yaitu versi – 2 yang meningkatkan versi *software* Docker dan Docker Images. Standar NIST (*National Institute of Technologies*) CSF (*Cybersecurity Framework*) dibatasi pada inti *Identify, Protect, Detect, Respond* , dan *Recover*. Skenario pengujian dijalankan dengan melakukan *scanning* kerentanan pada dua versi sistem percobaan. (menampilkana angka hasil *scanning* terbanyak) dan (hasil dari NIST). Dari hasil analisis data yang telah di kumpulkan, didapatkan hasil mengenai perbandingan total Anomali dan Peristiwa yaitu OpenSCAP lebih cepat menghasilkan data kerentanan dengan persentase sebanyak 33.33% pada versi – 1 dan 92.5% pada versi – 2, perbandingan total *vulnerabilities* dengan hasil versi-1 memiliki persentase total *vulnerability* lebih besar yaitu sebanyak 100% pada versi – 1 dan 7.62% pada vresi – 2, terdapat 6 kerentanan yang muncul kembali, terdapat 18 kerentanan yang tidak ditemukan kembali, berapa lama waktu untuk proses *Recover*, dan kategori remediasi untuk kerentanan yang ditemukan meliputi kritis dan non-kritis. Saran dari penelitian ini yaitu dapat menggunakan *software vulnerability tools scanning* yang lebih rinci, memperluas penelitian pada *vulnerability management life cycle*, dan menggunakan semua kategori dari lima inti kerangka NIST CSF.

Kata Kunci : Pengelolaan, Docker, *Vulnerability*, NIST CSF