ABSTRAK

Menentukan *vulnerability* dan menentukan *risk level* pada Docker yang memiliki keretanan akan menjadi suatu pembahasan. Untuk mendapatkan data *vulnerability* dan juga mengidentifikasi eksploitasi dari penyerang, digunakan *vulnerability scanner* yaitu Aquasec dan untuk eksploitasi dilakukan simulasi dalam melakukan eksploitasi. Aquasec mendeteksi *vulnerability* pada aset Docker. Data dari Aquasec dianalisis untuk mendapatkan hasil *risk* yang berkaitan erat antara *vulnerability* dan eksploitasi. Hasil analisis antara *vulnerability* dan eksploitasi, menghasilkan *risk* yang dikategorikan dalam serangan menyesuaikan *framework* STRIDE. Hasil yang sudah diberikan, memberikan *risk* dengan *vulnerability* tingkat *Medium* dan sering terjadi pada eksploitasi *vulnerability*. Besar *risk* yang didapat sebesar 32.5 terhadap *vulnerability* pada Docker. *Risk* tersbut merupakan serangan berupa *information disclosure*. Hal ini memerlukan penanganan pada *risk* yang sering terjadi selama eksploitasi pada macam-macam *walkthrough*. Akan lebih baik jika penelitian terhadap Docker lebih luas dengan melihat dari berbagai aspek pada Docker.

Kata kunci: **Docker, STRIDE, *Vulnerability*, *Risk*, Aquasec**