ABSTRAK

Docker merupakan sebuah *project open-source* yang menyediakan *platform* terbuka untuk *developer* maupun *sysadmin* untuk dapat membangun, mengemas, dan menjalankan aplikasi dimanapun sebagai sebuah kontainer yang ringan. Penelitian ini menggunakan *Vulnerable Docker* yang merupakan sebuah Virtual Machine berisi Docker yang rentan yang dibuat oleh perusahaan *NotSoSecure*, perusahaan yang berfokus pada keamanan komputer. Penelitian ini bertujuan untuk menguji secara empiris mengenai analisis kerentanan pada *Vulnerable Docker* menggunakan *vulnerability scanner* dengan mengacu pada *framework* CIS Control. Tujuan penelitian tersebut dapat dicapai dengan melakukan eksperimen berupa mengumpulkan data yang diperlukan, menganalisis hasil eksploitasi yang telah dilakukan pada *Vulnerable Docker* dan yang terakhir yaitu membuat kesimpulan berupa laporan yang disesuaikan dengan *framework* CIS Control. *Vulnerability Scanner* yang digunakan pada penelitian kali ini yaitu AlienVault OSSIM dan Docker Bench for Security. Pada penelitian kali ini ditemukan risiko tertinggi pada level aplikasi yaitu risiko yang diakibatkan oleh *vulnerability* jenis *WordPress User IDs and User Names Disclosure* melalui *scanning* AlienVault. Dan pada level sistem diakibatkan oleh *vulnerability* jenis *Enable User Namespace Support*. Terdapat 6 kontrol pada CIS Control V8 yang digunakan untuk mengurangi risiko yang terjadi pada penelitian ini.

Kata kunci — ***docker, vulnerability, alienvault, cis control***