

SARI

Vulnerability adalah kelemahan sebuah sistem akibat dari berbagai jenis pola serangan. Pada setiap sistem dan jaringan tentu akan mempunyai vulnerability (kerentanan) dan dapat mengakibatkan kerusakan pada sistem bahkan data perusahaan sehingga menimbulkan kerugian. Identifikasi kerentanan adalah salah satu cara yang efektif untuk meminimalisir resiko serangan dari pihak luar. Vulnerability assessment dilakukan melalui beberapa tahapan yaitu antara lain melakukan identifikasi kerentanan, menganalisis hasil identifikasi kerentanan kemudian memberikan hasil identifikasi serta dampak yang diakibatkan kerentanan tersebut. Identifikasi kerentanan yang dilakukan meliputi dari aplikasi, sistem operasi serta infrastruktur jaringan. Analisis kerentanan dibagi menjadi dua yaitu fase identifikasi dan validasi. Proses pencarian kerentanan adalah fase penting dalam identifikasi. Sedangkan validasi hanya mengurangi jumlah kerentanan yang ditelusuri. Penggunaan openvas versi 8 sebagai alat bantu uji kerentanan dapat memberikan hasil analisa kerentanan yang memadai. Hasil yang dicapai dalam analisis kerentanan adalah mengevaluasi hasil temuan kerentanan kemudian dikategorikan sesuai dengan tingkat resikonya yaitu tingkat tinggi, tingkat sedang dan tingkat rendah. Melakukan vulnerability assessment akan meningkatkan keamanan informasi serta terhindar dari resiko yang buruk dan dapat menimbulkan kerugian. Hasil yang dicapai dalam kegiatan vulnerability assessment adalah memberikan evaluasi terhadap resiko kerentanan yang ditemukan dan dampak yang dapat ditimbulkan serta sebagai langkah preventif untuk meningkatkan kesadaran keamanan informasi.

Kata kunci : *Vulnerability, Assessment*