ABSTRAK

ANALISIS KERENTANAN MENGGUNAKAN ALIENVAULT DAN QUALYS PADA *VULNERABILITY OPERATING SYSTEM* BERDASARKAN *FRAMEWORK* STRIDE

Oleh

VRESELIANA AYUNINGTYAS

1202160234

Perkembangan teknologi informasi yang semakin pesat mengakibatkan keamanan menjadi sangat penting. Di samping kemudahan akses, terdapat juga ancaman terhadap kerentanan pada teknologi informasi. Jumlah serangan siber tahun 2019 menunjukan peringkat ke lima dengan jumlah 1.494.281, data ini di dukung oleh statistik serangan siber yang dikeluarkan oleh Honeynet Project BSSN. Oleh karena itu dibutuhkan *software* analisis pada kerentanan. Kerentanan merupakan kelemahan pada sistem atau desain yang digunakan saat penyusup mengeksekusi perintah, mengakses data yang tidak sah dan melakukan serangan penolakan layanan. Analisis dilakukan dengan menggunakan salah satu fungsi dari *software* AlienVault dan Qualys yaitu *Vulnerability Assessment.* Hasil *Vulnerability Scanning* yang dilakukan dianalisis, kemudian dihitung dengan rumus *risk* = *vulnerability* x *threat*. *Threat* didapatkan dari analisis sample *walkthrough,* sebagai acuan eksploitasi yang sering dilakukan. Hasil estimasi risiko dengan jumlah 73 memiliki risiko tertinggi sebesar 75 sebanyak 5 risiko, kemudian estimasi risiko dianalisis kembali menggunkan *framework* STRIDE dengan hasil salah satu fungsi tidak mengakomodasi jenis risiko yang ada yaitu *Spoofing.*

Kata Kunci: *vulnerable machine,* kerentanan, ancaman, *framework STRIDE.*