ABSTRAK

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

Oleh

BOBBY ABDULLAH

NIM : 1202164334

Banyaknya pihak yang tidak bertanggung jawab melakukan pencurian data, memanipulasi data, dengan memanfaatkan vulnerability pada suatu sistem. Hasil riset yang dilakukan oleh *Federal Bureau of Investigation* (FBI) dan *Internet Crime Complaint Center* (IC3) pada tahun 2019 membawa kerugian akibat aktivitas *cybercrime global* yang mencapai 3,5 miliar USD. Studi ini membandingkan hasil *vulnerability scan* antara dua *tools* (AlienVault dan Qualys) dengan parameter uji untuk menunjukkan kerentanan. Penelitian ini menggunakan *framework CYBER KILL*. Simulasi dilakukan dengan menggunakan sistem operasi yang memiliki kerentanan (VulnOS2, Vulnix, dan DC-1) pada Virtual Box sebagai objek penelitian serta AlienVault dan Qualys sebagai *manager scan*. Skenario pengujian yang dijalankan adalah dengan melakukan *vulnerability scan* untuk tiga *vulnerability operating system* menggunakan AlienVault dan Qualys. Laporan yang dihasilkan dari *vulnerability scan* AlienVault dan Qualys yang berisi jumlah kerentanan, serta informasi dan deskripsi kerentanan. Dari hasil perhitungan risiko menggunakan rumus *Risk = Vulnerability x Threat* diperoleh hasil bahwa kerentanan *Drupal Core Multiple Security Vulnerabilities* (*SA-CORE-2016-001*) memiliki skor tertinggi dengan total skor risiko: 433,5, maka Analisis eksploitasi ancaman terhadap kerentanan berdasarkan framework *Cyber Kill Chain* dan hasilnya menunjukkan bahwa eksploitasi ancaman terhadap kerentanan adalah tipe *Drupal Core*.

Kata kunci : (*AlienVault, Qualys, Vulnerability, Open Source, Tools, Framework, Cyber Kill, Cyber*)