ABSTRAK

Penggunaan aktivitas komputer meningkat dari hari ke hari, sebagian besar sistem yang terkomputerisasi sekarang telah terhubung ke jaringan internet. Semua aktivitas ini meningkatkan kerentanan dalam sistem terutama dalam bidang jaringan yang menuntut meningkatnya suatu kebutuhan akan kualitas keamanan jaringan. Kerentanan adalah potensi resiko bagi sebuah sistem dan penyerang memanfaatkan sebuah kerentanan ini untuk mengeksploitasi sistem sehingga penyerang mendapatkan akses dan informasi yang tidak sah. Hampir tidak mungkin memiliki sistem bebas kerentanan 100%, namun dengan mengurangi kerentanan dalam sebuah sistem dan jaringan sebanyak mungkin dapat meningkatkan keamanan jaringan.

Dalam penelitian ini, melakukan optimalisasi keamanan jaringan dengan pemodelan penilaian kerentanan (vulnerability assessment) dan proses hardening pada sistem dan desain jaringan komputer untuk mengukur tingkat kerentanan dan mengkategorikan aset jaringan yang kritikal, yang selanjutnya dilakukan perbaikan pada sistem dan desain jaringan sesuai standar keamanan jaringan serta dari hasil penilaian tersebut menghasilkan panduan kebijakan prosedur keamanan jaringan pada perusahaan PT XYZ.

Dengan metode *vulnerability assessment* dapat mengidentifikasi *OS vulnerability* (JunOS, IOS, Debian, Microsoft), *Network vulnerability* (Mac-Address, IP Address), *Open port vulnerability* (TCP/UDP), *Engine application vulnerability* (HTTP, FTP, NTP, Telnet, SSH) dan mengkategorikan tingkat kerentanan yang terbagi 4 kategori, yaitu *Critical* (10–9), *High* (8–7), *Medium* (6–5), *Low* (4–2), sedangkan *hardening* dapat meminimalkan tingkat resiko kerentanan dengan melakukan penguatan terhadap sistem, konfigurasi, dan desain topologi pada infrastruktur jaringan computer.

Kata kunci : *Assessment, Keamanan Jaringan, Security, Vulnerability*