ABSTRAK

SECURITY AUDITING PADA VULNERABLE MACHINE MENGGUNAKAN OPEN SOURCE IDS DAN VULNERABILITY SCANNER BERDASARKAN NIST CYBERSECURITY FRAMEWORK

Oleh

HERI SULTAN FRANSISCUS SITINJAK

NIM : 1202164304

Penelitian ini bertujuan untuk menentukan profil resiko dari *vulnerable machine*. *Vulnerable machine* yang dipakai dalam penelitian ini yaitu Typhoon OS melalui proses *security auditing*. *Security Auditing* diperlukan untuk mengetahui seberapa besar resiko OS terkena serangan dan menyusun solusi untuk OS tersebut. *Framework* yang dipakai dalam penelitian ini yaitu NIST *cybersecurity framework*, karena NIST *cybersecurity framework* merupakan framework yang bersifat defensif dan cocok untuk penelitian ini. Aplikasi yang dipakai dalam menunjang proses *auditing* penelitian ini yaitu OpenVAS dan suricata. OpenVAS dipakai karena memiliki *database* kerentanan yang cukup lengkap serta hasil scan mudah untuk dibaca. Suricata dipakai karena memiliki tabel *rules* yang cukup lengkap dibanding IDS lain serta ukurannya aplikasi lebih kecil dibanding aplikasi IDS lain. Untuk itu dilakukan analisa kerentanan yang ada dalam OS. Dengan melakukan analisa kerentanan, dapat diketahui model serangan apa saja yang bisa dipakai untuk melakukan penyerangan. Setelah memodelkan serangan, dilakukan eksperimen penyerangan menggunakan literatur/*walkthrough.* Dari eksperimen akan dicari relasi antara *vulnerability* dan *threat.* Kemudian, dari hubungan antara *vulnerability* dan *threat*, akan diperoleh profil resiko. Dari hasil profil resiko, dapat diketahui seberapa besar bahaya dari setiap kerentanan yang ada pada OS. Hasil dari analisa profil resiko menunjukkan bahwa *vulnerability* "*GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabilities*" memiliki resiko terbesar atas serangan siber sebesar 85,71%, serta menunjukkan bahwa Typhoon OS 25,40% lebih beresiko dibanding dengan OS lain. Dari hasil profil resiko juga menunjukkan bahwa *vulnerable machine* memiliki resiko yang tinggi atas serangan siber.

Kata kunci : s*ecurity auditing, vulnerable machine, framework,* profil resiko, model serangan