ABSTRAK

SECURITY AUDITING PADA *VULNERABLE MACHINE* MENGGUNAKAN *SNORT INTRUISON DETECTION SYSTEM* DAN GREENBONE *OPENVAS* BERDASARKAN *NASIONAL INSTITUTE OF STANDART AND TECHNOLOGY CYBERSECURITY FRAMEWORK*

Oleh

KRISFIAN ADJI BRATA

NIM : 120164373

Penelitian ini bertujuan untuk menganalisa kerentanan dan threat dalam 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 pada penelitian ini. Aplikasi yang dipakai dalam menunjang proses auditing ini yaitu *OpenVAS* dan *Snort*. *OpenVAS* dipakai karena memiliki database kerentanan yang cukup lengkap serta hasil scan mudah untuk dibaca. *Snort* dipakai karena memiliki tabel rules yang cukup lengkap dibanding *IDS* lain serta untuk akurasi deteksi seperti scanning port snort lebih unggul dibanding *IDS* lainnya. 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.kemudian dilakukan juga eksperimen penyerangan menggunakan literatur/walkthrough. Dari eksperimen akan dicari relasi antara vulnerability dan threat, 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. Kemudian setelah dilakukan pemecahan masalah dapat dilihat hasil bahwa "*CUPS < 2.0.3 Multiple Vulnerabilities*" merupakan *vulnerability* dengan kerentanan yang terbesar dari beberapa vulnerability yang ada yaitu dengan skor 30(50 %) dengan Nmap sebagai tools yang paling banyak terdeteksi yaitu 6 kali dari enam walkthrough yang dicoba. Dari hasil profil resiko juga menunjukkan bahwa *vulnerable machine* khususnya Typhoon memiliki resiko yang tinggi atas serangan siber.

Kata kunci : security auditing, vulnerable machine, framework, profil resiko,modelserangan.