

ABSTRAK

Keamanan server sangat diperlukan untuk menghindari serangan yang akan terjadi. IPS (*Intrusion Prevention System*) merupakan salah satu contoh solusi yang tepat untuk pengamanan suatu sistem. IPS dapat mencegah suatu serangan dengan memanfaatkan fitur dari IDS (*Intrusion Detection System*) dan fitur *firewall* yang mampu menolak akses dari suatu koneksi.

Pada tugas akhir ini, dilakukan implementasi IPS (Snort dan Bro) pada server yang kemudian diuji dengan serangan yang meliputi DOS (*Denial of service*), *port scanning*, dan *FTP brute force* dengan tiga topologi yang berbeda. Dari serangan tersebut, dilakukan analisa *security metric* dengan metode *VEA-bility metric* dimana hasil dari *VEA-bility* yang berupa nilai akan menentukan seberapa aman suatu sistem yang dimiliki dengan rentang nilai dari 0 hingga 10 yang didapatkan berdasarkan perhitungan yang melibatkan nilai *vulnerability dimension*, *exploitability dimension* dan *attackability dimension*. Dari hasil percobaan, didapatkan nilai 3.07 untuk topologi tanpa *firewall*, 5.98 untuk topologi dengan *server* yang terpisah dan 6.81 untuk topologi *server* yang terpisah dan menggunakan *firewall*. Sementara itu, didapatkan nilai CVSS untuk masing masing serangan yaitu 1.83 untuk DOS, 0.27 untuk *port scanning* dan 4.27 untuk *FTP brute force*.

Kata Kunci : *Intrusion Prevention System* (IPS), Snort, Bro, *VEA-bility metric*.