

Abstrak

Distributed Denial of Service (DDoS) merupakan jenis serangan yang dapat menghabiskan sumber daya *server*. Serangan ini mengakibatkan penurunan kualitas *server* sehingga tidak bisa diakses oleh pengguna yang sah. *Server* yang biasa menjadi korban serangan ini adalah milik perusahaan dari berbagai sektor. PT Datacomm Diangraha menyediakan solusi dari permasalahan tersebut. Seperti yang akan dilakukan PT Datacomm Diangraha kepada Perusahaan X, yaitu mengimplementasikan perangkat *Intrusion Prevention System (IPS)* sebagai Anti-DDoS pada pelanggannya sesuai dengan kebutuhan pelanggan tersebut. Makalah ini akan melakukan pengujian perangkat IPS dalam mencegah serangan DDoS seperti *TCP Flood*, *UDP Flood*, dan *ICMP Flood*. Pengujian dilakukan dengan menghubungkan penyerang dan korban ke perangkat IPS dalam jaringan lokal. Analisis akan dilakukan dengan membandingkan lalu lintas jaringan serta *throughput* korban ketika dilakukan penyerangan saat dilindungi IPS, tidak ada perlindungan, serta saat lalu lintas normal. Eksperimen dilakukan dengan melakukan penyerangan selama satu menit. Hasil dari eksperimen menunjukkan bahwa lalu lintas ketika dilindungi IPS menunjukkan kesamaan dengan saat lalu lintas normal. Sebagai tambahan, dilakukan pengujian untuk mencegah *malware XSS* untuk membuktikan IPS dapat mencegah serangan lain selain DDoS. Dari hasil pengujian didapatkan bahwa IPS dapat mencegah serangan DDoS dengan akurasi 100%. Didapatkan data *throughput* ketika terjadi serangan DDoS tanpa perlindungan IPS sebesar 260978.9 - 1080732.32 bps. Data *throughput* ketika terjadi serangan DDoS dengan perlindungan IPS sebesar 42.55 – 49.95 bps, yang menunjukkan kemiripan nilai dengan *throughput* saat lalu lintas normal yaitu sebesar 43.43 bps.

Kata Kunci: DDoS; IPS; Anti-DDoS; *malware*; XSS