

ABSTRAK

Perkembangan teknologi masa kini telah mengalami perkembangan pesat, memudahkan dan mendukung aktivitas sehari-hari. Namun, pertumbuhan ini juga berimbas pada peningkatan lalu lintas jaringan dan penggunaan perangkat keras. Jaringan konvensional tidak mampu dengan cepat beradaptasi terhadap perubahan ini. Keterbatasan dalam pemrograman ulang dan kontrol perangkat menghambat jaringan tradisional. Oleh karena itu, solusi muncul dalam bentuk *Software Defined Network* (SDN). SDN memisahkan kontrol jaringan dari lapisan data, memberi ruang untuk pemrograman yang lebih sederhana dan fleksibilitas yang lebih tinggi. Namun, SDN juga memiliki kerentanan, terutama dalam serangan. Kelemahan ini dieksploitasi dalam serangan *Distributed Denial of Service* (DDoS), serangan yang membuat kontroler tidak responsif. Penelitian ini pada tahap pengujian dengan mencari jumlah *attacker* minimal yang menghambat komunikasi *host*, mengukur waktu dan jumlah paket hilang. Kinerja dinilai menggunakan *Quality of Service* dengan menghitung *packet loss* melalui perintah ping, dan dianalisis berdasarkan ETSI TIPHON. Tujuan utama mendapatkan waktu secepat mungkin hingga *destination host unreachable*. Hasil pengujian serangan di satu jaringan yang sama menunjukkan jumlah *attacker* 1 waktu tidak terbatas, *attacker* 3 durasi waktu 8 menit 53 detik, *attacker* 5 durasi waktu 6 menit 56 detik, *attacker* 7 durasi waktu 4 menit 34 detik, *attacker* 9 durasi waktu 2 menit 29 detik, *attacker* 11 durasi waktu 58 detik. Serangan berbeda jaringan menunjukkan jumlah *attacker* 1 waktu tidak terbatas, *attacker* 3 durasi waktu 12 menit 53 detik, *attacker* 5 durasi waktu 10 menit 35 detik, *attacker* 7 durasi waktu 9 menit 25 detik, *attacker* 9 durasi waktu 3 menit, *attacker* 11 durasi waktu, 1 menit 16 detik.

Kata Kunci: **DDoS; HPING3; SDN;**