

## RINGKASAN

**Implementasi Snort Untuk Mendeteksi Serangan DDoS Jaringan Web Server,**  
Putra Ahmad Mudakir, NIM. E32211894, Tahun 2024, Teknik Komputer, Jurusan  
Teknologi Informasi, Politeknik Negeri Jember, I Gede Wiryawan,S.Kom.,  
Mkom.(Pembimbing).

Serangan Distributed Denial-of-Service (DDoS) merupakan salah satu ancaman utama bagi jaringan web server. Serangan ini dapat melumpuhkan server dan membuat layanan web tidak dapat diakses oleh pengguna. Snort adalah alat open-source yang dapat digunakan untuk mendeteksi dan mencegah serangan DDoS.

Snort adalah Sistem Pencegahan Intrusi (IDS) Open Source terkemuka di dunia. Snort IDS menggunakan serangkaian aturan yang membantu menentukan aktivitas jaringan berbahaya dan menggunakan aturan tersebut untuk menemukan paket yang cocok dan menghasilkan peringatan bagi pengguna.

Penelitian ini bertujuan untuk mengetahui efektivitas Snort dalam mendeteksi serangan DDoS pada jaringan web server. Penelitian ini menggunakan simulasi serangan DDoS dengan menggunakan alat LOIC dan Hping3. Hasil penelitian menunjukkan bahwa Snort dapat mendeteksi berbagai jenis serangan DDoS dengan tingkat akurasi yang tinggi.

Penelitian ini memberikan kontribusi dalam hal evaluasi efektivitas Snort dalam mendeteksi serangan DDoS pada jaringan web server. Penelitian ini diharapkan dapat membantu para administrator jaringan dalam meningkatkan keamanan jaringan web server mereka dari serangan DDoS.