ABSTRAK

Reyhan Zovian Martin, 51423280
Analisis Deteksi Serangan *Denial of Service* (DoS) *Syn Flood* Menggunakan Algoritma *Random Forest*. Penulisan Ilmiah. Informatika. Fakultas Teknologi Industri. Universitas Gunadarma. 2026.
Kata kunci: *Denial of Service*, Deteksi Serangan, *Random Forest*, *SYN-Flood*
(xii + 74 + Lampiran)

Penelitian ini membahas deteksi serangan *Denial of Service* (DoS) jenis *SYN-Flood* pada jaringan *virtual* menggunakan algoritma *Random Forest*. Permasalahan yang diangkat adalah serangan *SYN-Flood* dapat membebani *server* melalui pengiriman paket SYN dalam jumlah besar sehingga layanan sulit diakses oleh pengguna yang sah. Tujuan penelitian ini adalah membangun dan mengevaluasi model klasifikasi untuk membedakan trafik normal dan trafik serangan berdasarkan karakteristik paket jaringan. Metode penelitian meliputi perancangan jaringan *virtual*, simulasi trafik normal dan serangan, *capture* paket menggunakan *tcpdump*, konversi file *pcap* ke CSV, pengolahan *dataset*, pelatihan model *Random Forest* menggunakan *Python* dan *Scikit-learn*, serta evaluasi menggunakan *confusion matrix*, akurasi, presisi, *recall*, *F1-score*, *cross validation*, dan *feature importance*. Hasil pengujian menunjukkan model memperoleh akurasi sebesar 99,99%, dengan 18.902 dari 18.904 data uji terklasifikasi dengan benar. Hasil deteksi kemudian divisualisasikan melalui aplikasi web berbasis *Streamlit* yang dapat diakses melalui tautan Aplikasi Deteksi SYN-Flood. Dengan demikian, *Random Forest* mampu mendeteksi pola serangan *SYN-Flood* secara efektif pada lingkungan pengujian terkontrol.

Daftar Pustaka (2020-2026)