PENGEMBANGAN SISTEM KLASIFIKASI SERANGAN SIBER BERBASIS *MACHINE LEARNING*

Nama Mahasiswa	:	Nor Nadiya
Nim	:	6304221438
Dosen Pembimbing	:	M. Asep Subandri, M. Kom

ABSTRAK

Meningkatnya risiko serangan siber pada aplikasi *web*, khususnya *SQL Injection* dan *Brute Force* pada proses *login* pengguna. Penelitian ini bertujuan mengembangkan sistem klasifikasi serangan siber berbasis *Machine learning* menggunakan algoritma *Random Forest* dengan dataset CIC-IDS-2018. Sistem menangkap trafik jaringan pada halaman *login* aplikasi *web* yang diimplementasikan pada *Virtual Private Server* (VPS). Pengujian dilakukan melalui tiga skenario, yaitu *login* normal (*benign*), serangan *SQL Injection* dan *Brute Force* dengan tiga pengguna untuk menguji sistem. Model *Random Forest* digunakan untuk mengklasifikasikan serangan secara *real-time* dan mengirimkan notifikasi melalui Bot Telegram. Hasil pengujian pada 104 data uji menunjukkan bahwa model mencapai akurasi sebesar 97% dengan nilai *precision, recall*, *dan f1-score* yang tinggi pada kelas *Benign, Brute_Force_Web,* dan *SQL_Injection*. Hasil penelitian menunjukkan bahwa sistem mampu mendeteksi dan mengklasifikasikan serangan sehingga dapat meningkatkan keamanan aplikasi *web*.

Kata kunci: keamanan aplikasi *web*, serangan siber, *Machine learning, Random Forest*, *SQL Injection, Brute Force.*

DEVELOPMENT OF A MACHINE LEARNING-BASED CYBER ATTACK CLASSIFICATION SYSTEM

Nama Mahasiswa	:	Nor Nadiya
Nim	:	6304221438
Dosen Pembimbing	:	M. Asep Subandri, M. Kom

ABSTRACT

The increasing use of web applications has led to a higher risk of cyberattacks, particularly targeting user authentication processes such as SQL Injection and Brute Force attacks. This study aims to develop a machine learning-based cyberattack classification system using the Random Forest algorithm and the CIC-IDS-2018 dataset. The system utilizes the Scapy package to capture network traffic on the face login of a web application implemented in a WSL Ubuntu environment. Testing was conducted under three scenarios: normal login activity until successfully accessing the dashboard as benign traffic, SQL Injection attacks performed on the login form, and Brute Force attacks simulated using a Python Script that repeatedly attempts login credentials. The Random Forest model classifies network traffic in real time and sends notifications via a Telegram Bot when an attack is detected. The results indicate that the system is capable of effectively detecting and classifying network traffic, thereby enhancing web application security.

Keywords**: **web application security, Cyber Attacks, Machine learning, Random Forest, SQL Injection, Brute Force.