Using Suricata and Fail2ban as an Intrusion Prevention System (IPS) to Mitigate Network Attacks Using Telegram Notifications (Case Study at the Bengkalis Population and Civil Registration Agency)

Student Name	:	Reza Saputro Dwi Prastyo Widodo
Student ID Number	:	6103230041
Supervisor	:	Eko Prayitno, M.Kom

ABSTRACT

Network security at the Bengkalis Population and Civil Registration Service is crucial because this institution manages sensitive population data. Based on router system log observations, more than 19,100 dynamic IP blocking records were identified due to port scanning and SSH brute force attacks, most of which originated from foreign IP addresses. These attacks indicate continuous intrusion attempts targeting network services and causing large numbers of blacklist entries on the firewall. The current problem lies in manual monitoring and passive detection systems that delay attack mitigation. This study implemented an Intrusion Prevention System (IPS) by integrating Suricata and Fail2Ban using the Security Policy Development Life Cycle (SPDLC) method. System testing was conducted through VirtualBox simulation and physical hardware implementation. The test scenarios included 14 complex attack types such as DoS Hulk, Slowloris, Heartbleed, SSH brute force, port scanning, and Infiltration attacks. The results showed that the system successfully detected and blocked malicious IP addresses automatically in real time and generated instant notifications through a Telegram bot. This implementation is expected to improve network protection, reduce service disruption risks, and increase the efficiency of security monitoring at the Bengkalis Population and Civil Registration Service.

Keywords: *Fail2Ban, IPS, Network Security, SPDLC, Suricata, Telegram Bot.*