ABSTRAK

ZACKY SANTOSO. Analisis Serangan *Fileless Malware* Pada Linux Berbasis *Linux Security Module* (LSM) (Studi Kasus Aplikasi Web Berbasis Php). Dibimbing oleh HENDRA KURNIAWAN dan BERTA ERWIN SLAM.

Serangan *fileless malware* merupakan ancaman keamanan yang semakin meningkat karena mampu menjalankan *payload* langsung di memori tanpa meninggalkan berkas pada sistem, sehingga sulit dideteksi oleh mekanisme keamanan tradisional. Penelitian ini bertujuan untuk menganalisis efektivitas dan efisiensi *Linux Security Module*, khususnya SELinux dan Landlock, dalam memitigasi serangan *fileless malware* pada aplikasi web berbasis PHP. Metode penelitian yang digunakan adalah metode eksperimental dengan menjalankan sepuluh skenario serangan *fileless malware* pada tiga kondisi sistem, yaitu *Baseline* tanpa LSM, SELinux, dan Landlock. Pengujian dilakukan menggunakan dua pola serangan, yaitu serangan berurutan dan serangan bersamaan, dengan parameter yang diamati meliputi tingkat keberhasilan pemblokiran serangan serta penggunaan CPU dan RAM. Hasil penelitian menunjukkan bahwa pada kondisi *Baseline* seluruh serangan berhasil dijalankan, sedangkan *Linux Security Module* (LSM) SELinux dan Landlock mampu memblokir 100% ruang lingkup serangan yang di uji. Dari sisi efisiensi, SELinux menghasilkan *overhead* CPU yang lebih tinggi, sementara Landlock menunjukkan penggunaan CPU yang lebih rendah dengan penggunaan RAM yang relatif stabil. Temuan ini menunjukkan bahwa Landlock memberikan keseimbangan yang lebih baik antara keamanan dan efisiensi sistem pada lingkungan server web Linux.

Kata kunci: Aplikasi web, *fileless malware*, *Linux Security Module*, SELinux, Landlock.

ABSTRACT

ZACKY SANTOSO. Analysis of *File*less Malware Attacks on Linux Based on Linux Security Module (LSM) (Case Study of PHP-Based Web Application). Supervised by HENDRA KURNIAWAN and BERTA ERWIN SLAM.

Fileless malware attacks are an emerging security threat as they execute malicious payloads directly in memory without creating files on the system, making them difficult to detect using traditional security mechanisms. This study aims to analyze the effectiveness and efficiency of Linux Security Modules, specifically SELinux and Landlock, in mitigating fileless malware attacks on PHP-based web applications. An experimental research method was employed by executing ten fileless malware attack scenarios under three system conditions: Baseline without LSM, SELinux, and Landlock. The experiments were conducted using both sequential attack and concurrent attack patterns. The observed parameters included attack prevention effectiveness as well as CPU and RAM usage. The results indicate that all attack scenarios were successfully executed under the Baseline condition, whereas both Linux Security Module (LSM) SELinux and Landlock were able to block 100% tested attack scope. In terms of efficiency, SELinux generated higher CPU overhead, while Landlock demonstrated lower CPU usage with relatively stable RAM consumption. These findings suggest that Landlock provides a better balance between security and system efficiency for Linux web server environments.

Keywords: Fileless malware, Linux Security Module, SELinux, Landlock, web application.