ABSTRAK

AZEL FAHREZI. Analisis Serangan *Fileless Malware* pada Sistem Operasi Linux Berbasis SELinux dan AppArmor (Studi Kasus Aplikasi Web Berbasis PHP). Dibimbing oleh HENDRA KURNIAWAN dan BERTA ERWIN SLAM.

Serangan *fileless malware* merupakan ancaman siber yang beroperasi langsung di memori tanpa meninggalkan berkas, sehingga sulit dideteksi oleh sistem keamanan konvensional. Penelitian ini bertujuan menganalisis efektivitas dan dampak performa dua mekanisme keamanan kernel berbasis *Mandatory Access Control* (MAC), yaitu *Security-Enhanced Linux* (SELinux) dan AppArmor, dalam mencegah serangan *fileless malware* pada sistem operasi Debian berbasis aplikasi web PHP. Pengujian dilakukan menggunakan sepuluh skenario serangan dengan pendekatan eksperimental pada lingkungan virtual. Efektivitas diukur berdasarkan persentase keberhasilan blokir, sementara performa diukur melalui penggunaan CPU dan memori. Hasil penelitian menunjukkan bahwa SELinux dan AppArmor mencapai tingkat efektivitas 100% dengan berhasil mendeteksi dan mencegah seluruh skenario serangan tanpa pengecualian. Namun, terdapat perbedaan signifikan pada dampak performa. Berdasarkan pengujian durasi 5 menit, AppArmor menunjukkan efisiensi sumber daya yang lebih baik dengan rata-rata penggunaan CPU yang sangat rendah (0,19% – 0,28%) dan penggunaan memori yang stabil (6,06% – 7,20%). Sebaliknya, SELinux mencatat penggunaan sumber daya lebih tinggi, dengan rata-rata CPU mencapai 0,46% – 1,84% dan memori 7,43% – 9,45% akibat mekanisme audit dan pelabelan yang kompleks. Temuan ini merekomendasikan AppArmor untuk lingkungan dengan keterbatasan sumber daya, sedangkan SELinux disarankan untuk sistem yang memprioritaskan keamanan dan pencatatan audit mendalam.

Kata kunci: AppArmor, *fileless malware*, Linux, *Mandatory Access Control*, SELinux.

ABSTRACT

AZEL FAHREZI. Implementaion of Power Consumption Monitoring System for Small Micro Enterprise Based on Internet of Things. Supervised by HENDRA KURNIAWAN and BERTA ERWIN SLAM.

Fileless malware attacks are cyber threats that operate directly in memory without leaving any files, making them difficult to detect using conventional security systems. This study aims to analyze the effectiveness and performance impact of two kernel-level security mechanisms based on Mandatory Access Control (MAC), namely Security-Enhanced Linux (SELinux) and AppArmor, in preventing fileless malware attacks on a Debian-based operating system running PHP web applications. The testing was carried out using ten attack scenarios through an experimental approach in a virtual environment. Effectiveness was measured based on the percentage of successful blocking, while performance was evaluated through CPU and memory usage. The results show that SELinux and AppArmor achieved 100% effectiveness by successfully detecting and preventing all attack scenarios without exception. However, there were significant differences in performance impact. Based on a 5-minute testing duration, AppArmor demonstrated better resource efficiency with very low average CPU usage (0.19%–0.28%) and stable memory usage (6.06%–7.20%). In contrast, SELinux recorded higher resource consumption, with average CPU usage reaching 0.46%–1.84% and memory usage of 7.43%–9.45% due to its complex auditing and labeling mechanisms. These findings recommend AppArmor for environments with limited resources, while SELinux is suggested for systems that prioritize security and in-depth auditing.

Keywords: AppArmor, fileless malware, Linux, Mandatory Access Control, SELinux.