BAB I
PENDAHULUAN

A. Latar Belakang

Pesatnya perkembangan teknologi informasi telah meningkatkan kompleksitas ancaman dunia siber. Keamanan *kernel* merupakan komponen fundamental dalam menjaga stabilitas dan ketahanan sistem operasi modern. *Kernel* berperan mengatur sumber daya sistem serta mengontrol komunikasi antara perangkat keras dan perangkat lunak. Karena perannya yang kritis, *kernel* menjadi target utama bagi serangan siber yang menembus batas sistem operasi. Kegagalan dalam melindungi *kernel* dapat menyebabkan eksekusi kode berbahaya dengan hak istimewa tertinggi, menyebabkan kebocoran data dan gangguan operasional pada sistem [1].

Dalam beberapa tahun terakhir, lanskap ancaman telah didominasi oleh *fileless malware*, sebuah evolusi serangan yang sangat berbahaya. Berbeda dengan *malware* konvensional, serangan jenis ini beroperasi sepenuhnya di memori (RAM) dan tidak meninggalkan artefak pada sistem *file*. Karakteristik ini membuat *fileless malware* mencapai tingkat keberhasilan yang tinggi dalam menghindari deteksi antivirus tradisional yang bergantung pada analisis berbasis tanda tangan (*signature-based*) atau pemindaian berkas statis [2].

Serangan *fileless malware* umumnya memanfaatkan teknik *living-off-the-land* (LOTL), yakni menjalankan instruksi berbahaya dengan memanfaatkan tools bawaan sistem operasi seperti *PowerShell*, *WMI*, atau pada Linux melalui *curl*, *bash*, dan *php-cli* untuk menjalankan instruksi berbahaya secara tersembunyi [3], [4]. Selain itu, *malware* modern juga diperkuat dengan teknik *obfuscation* (pengaburan), yang mengubah urutan kode atau menyisipkan data berlebihan, sehingga menghambat analisis *teks* atau *biner* oleh sistem deteksi statis. Keterbatasan dalam deteksi ini menyoroti pentingnya analisis memori (*memory forensics*) dan kebutuhan untuk membandingkan *snapshot* memori untuk mengidentifikasi perubahan anomali yang disebabkan oleh aktivitas berbahaya [5], [6], [7].

Meskipun awalnya banyak ditemukan pada ekosistem *Windows* (*PowerShell* dan *WMI*), kini ancaman serupa juga menargetkan lingkungan Linux,

khususnya server web. Penelitian terdahulu menemukan bahwa hampir seluruh serangan *fileless web-based* pada sisi server dijalankan melalui skrip PHP yang dikirim langsung ke layanan web dan dieksekusi tanpa menyimpan *file* ke *disk* [8]. Hasil ini diperkuat oleh penelitian terdahulu di mana injeksi *backdoor* dapat disisipkan ke aplikasi web tanpa meninggalkan jejak *file* fisik, sehingga sulit dideteksi oleh sistem keamanan berbasis tanda tangan [5]. Serangan semacam ini menunjukkan bahwa aplikasi web berbasis PHP menjadi vektor ideal bagi penyerang untuk melakukan eksekusi memori langsung (*in-memory execution*).

Untuk menghadapi ancaman tersebut, sistem operasi Linux menyediakan kerangka *Linux Security Modules* (LSM) yang memungkinkan pengawasan dan penerapan kontrol akses yang fleksibel. Dua modul utama yang menawarkan pendekatan berbeda adalah *Security-Enhanced Linux* (SELinux) dan Landlock. SELinux menerapkan kontrol akses berdasarkan kebijakan keamanan yang ketat dengan menggunakan label keamanan pada subjek dan objek sistem. Pendekatan ini terbukti efektif dalam membatasi akses sistem serta mencegah eskalasi hak istimewa, termasuk pada lingkungan dengan keterbatasan sumber daya seperti perangkat *Internet of Things* (IoT) [9]. Sebaliknya, Landlock merupakan LSM berbasis *sandboxing* di *user space* yang memungkinkan pengembang aplikasi membatasi akses aplikasi terhadap sumber daya sistem, khususnya sistem berkas, melalui pendekatan *whitelist* [10].

Meskipun LSM memberikan lapisan perlindungan yang kuat, penerapan LSM menghadapi dua tantangan yaitu, Pertama, kompleksitas konfigurasi kebijakan *Mandatory Access Control* (MAC) pada SELinux sering menjadi kendala karena dianggap cukup sulit dan rumit, terutama tanpa pelatihan teknis memadai, karena memerlukan kebijakan yang sangat spesifik. Kedua, aktivasi mekanisme LSM dapat menimbulkan dampak kinerja (*overhead*) pada sistem. Beberapa penelitian menunjukkan bahwa penerapan SELinux dapat menyebabkan penurunan kinerja pada operasi sistem tertentu, sehingga menjadi faktor penghambat dalam adopsi penuh mekanisme keamanan berbasis *kernel* [11].

Berdasarkan tantangan dan perbedaan mekanisme ini, terdapat kesenjangan penelitian yang signifikan belum banyak penelitian yang secara langsung menguji efektivitas dan efisiensi *Linux Security Modules* (LSM) khususnya SELinux

sebagai penerap *Mandatory Access Control* (MAC) dan Landlock sebagai *sandboxing* berbasis *whitelist* dalam menghadapi serangan *fileless malware* yang dieksekusi melalui kerentanan aplikasi web, seperti *command injection* pada PHP. Studi yang ada sebelumnya terbatas pada konteks perangkat IoT [9] atau lingkungan *container* (seperti Docker) [12].

Penelitian ini bertujuan untuk melakukan analisis komparatif guna menilai secara menyeluruh efektivitas (kemampuan mitigasi serangan) dan efisiensi (dampak kinerja sistem) dari *Linux Security Modules* (LSM) yaitu SELinux dan Landlock, pada aplikasi web berbasis PHP yang berjalan pada sistem operasi Linux.

B. Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana perbandingan efektivitas *Linux Security Modules* (LSM) antara SELinux dan Landlock dalam mencegah serta mendeteksi serangan *fileless malware* pada kerentanan aplikasi web PHP di sistem operasi Debian 13 ?
2. Bagaimana perbandingan efisiensi kinerja (penggunaan sumber daya CPU dan RAM) *Linux Security Modules* (LSM) antara SELinux dan Landlock saat menghadapi serangan *fileless malware* pada aplikasi web PHP ?

C. Batasan Penelitian

Dalam penelitian ini, ruang lingkup akan difokuskan pada aspek-aspek tertentu agar proses dapat dilakukan secara terarah dan mendalam. Mengingat kompleksitas sistem keamanan Linux dan beragamnya bentuk serangan *fileless malware*, maka penulis membatasi cakupan studi hanya pada skenario dan variabel yang relevan langsung dengan tujuan penelitian. Batasan ini ditetapkan untuk memastikan validitas eksperimen, terukur hasil, serta kesesuaian dengan sumber daya dan waktu yang tersedia. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Jenis Serangan yang dianalisis terbatas pada *fileless malware* yang dieksekusi melalui kerentanan aplikasi web PHP, tanpa melibatkan *malware* berbasis *file*.

2. Aplikasi Web yang digunakan adalah aplikasi web berbasis PHP, yang memiliki kerentanan berupa *command injection,* pengujian ini hanya berlaku pada kondisi ketika server memiliki celah kerentanan PHP.
3. Lingkungan uji dilakukan pada dua perangkat (dua laptop/PC) yang terhubung melalui jaringan pribadi.
4. Teknologi Keamanan yang diuji dibatasi pada dua mekanisme utama: *Linux Security Module* (LSM) yaitu, SELinux dan Landlock.
5. Parameter yang dievaluasi mencakup pencegahan eksekusi *malware*, pencatatan *log*, serta dampak performa sistem (CPU/RAM), tanpa menganalisis aspek kriptografi atau mitigasi jaringan secara mendalam.
6. Sumber *malware fileless* merupakan simulasi internal yang dirancang khusus untuk keperluan pengujian, script yang dirancang untuk *payload fileless* berbasis *curl* dengan berbagai karakteristik.

D. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk:

1. Menganalisis *Linux Security Module*s (LSM) antara SELinux dan Landlock dalam mencegah serta mendeteksi serangan *fileless malware* pada kerentanan aplikasi *web* PHP di sistem operasi Debian 13.
2. Membandingkan efisiensi kinerja (terkait *overhead* penggunaan sumber daya CPU dan RAM) *Linux Security Modules* (LSM) antara SELinux dan Landlock saat menghadapi serangan *fileless malware* pada aplikasi web PHP.

E. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat baik secara teoritis maupun, dengan beberapa hasil penelitian yang dapat diterapkan. Manfaat dari penelitian ini meliputi:

1. Bagi Administrator Sistem Linux, penelitian ini memberikan literatur mengenai penerapan *Linux Security Modules* (LSM) SELinux dan Landlock sebagai mekanisme pertahanan tambahan untuk membatasi dampak serangan *fileless malware* pada aplikasi web. Hasil penelitian ini dapat

digunakan sebagai dasar pertimbangan dalam menentukan strategi dan konfigurasi keamanan server.

2. Kontribusi terhadap kajian keamanan sistem operasi, dengan menyediakan analisis empiris mengenai efektivitas dan efisiensi *Linux Security Module* (LSM) SELinux dan Landlock dalam menghadapi serangan *fileless malware* pada aplikasi web berbasis PHP pada sistem operasi Linux.
3. Penelitian ini dapat dijadikan referensi teknis dalam mengimplementasikan dan mengevaluasi efektivitas *Linux Security Module* (LSM) SELinux dan Landlock, termasuk dalam hal pencatatan *log* keamanan dan analisis dampak penerapan mekanisme keamanan terhadap performa sistem (CPU dan RAM).
4. Dasar Penelitian Lanjutan: Penelitian ini menyajikan kerangka metodologi eksperimen yang dapat di replikasi dan dikembangkan lebih lanjut untuk menguji efektivitas mekanisme keamanan lain terhadap *fileless malware* atau jenis serangan siber canggih lainnya pada berbagai lingkungan sistem operasi.