BAB I
PENDAHULUAN

Dalam bab pendahuluan ini akan dijelaskan latar belakang, rumusan masalah, tujuan, dan sistematika penulisan dari skripsi ini.

1.1 Latar Belakang

Dalam era transformasi digital yang masif, Keamanan Siber (*Cybersecurity*) telah berkembang menjadi isu global yang krusial, melampaui sekadar perlindungan teknologi informasi konvensional [12]. Secara umum, *cybersecurity* mencakup segala upaya, mulai dari teknologi, kebijakan, hingga proses, untuk melindungi semua aset digital seperti sistem, jaringan, dan data dari ancaman, kerusakan, atau akses illegal [8]. Ancaman siber tidak hanya berupa serangan canggih *Advanced Persistent Threats* (APT) yang menargetkan kerahasiaan data (Confidentialy/C), tetapi juga *ransomware* dan *malware* yang mengancam integritas (Integrity/I) dan ketersediaan (Availability/A) sistem, yang dikenal sebagai triad CIA. Institusi, termasuk lembaga pendidikan, kini menjadi target utama karena menyimpan aset data sensitif dan sering kali memiliki infrastruktur yang rentan [2].

Mengingat kompleksitas ancaman yang menyasar hingga ke level endpoint dan server internal, strategi keamanan siber modern menuntut pendekatan proaktif dan berlapis *(Defense in Depth*) [18]. Dalam penerapannya, perlindungan tidak hanya ada pada perimeter seperti *firewall* atau antivirus tradisional, yang terbukti tidak memadai menghadapi malware, ransomware, atau zero day yang beroperasi di dalam system. Oleh karena itu, integritas file menjadi pilar vital. Log serangan, *backdoor*, atau *rootkit* sering kali disamarkan sebagai modifikasi pada file-file system kritikal. Kemampuan untuk mendeteksi perubahan tersebut secara *real time,* melalui File Integrity Monitoring (FIM), telah menjadi fungsi inti yang harus diintegrasikan dengan sistem Security Information and Event Management (SIEM) [13].

Implementasi Security Operations Center (SOC) berbasis ELK Stack dengan integrasi Wazuh dan File Integrity Monitoring (FIM) terbukti mampu memperkuat kemampuan organisasi dalam mendeteksi anomali dan serangan siber melalui sistem log terpusat dan alert otomatis [1]. Fungsi sistem pengawasan ini juga mencakup optimasi keamanan *web server* terhadap anomali dan serangan yang dapat mengganggu integritas konfigurasi dan ketersediaan layanan [16]. Sistem ini memungkinkan pengawasan terhadap aktivitas file penting di server secara real-time, sehingga setiap perubahan tidak sah dapat segera diidentifikasi. Pendekatan tersebut menunjukkan pentingnya integrasi FIM sebagai bagian dari kebijakan data loss prevention dan strategi defense-in-depth modern.

Ancaman keamanan siber pada era digital saat ini tidak lagi terbatas pada perlindungan perimeter jaringan seperti firewall, melainkan juga menyasar server dan endpoint internal yang menyimpan data penting [2]. Sektor pendidikan menjadi salah satu target utama serangan siber secara global, dengan rata-rata lebih dari 4.300 serangan per organisasi setiap minggu dan peningkatan sebesar 31% dibanding tahun sebelumnya [2]. Hal tersebut menunjukkan bahwa institusi pendidikan memiliki tingkat kerentanan yang tinggi terhadap ancaman keamanan informasi, terutama karena keterbatasan sumber daya dan sistem pemantauan yang belum terintegrasi secara menyeluruh.

Serangan siber sering kali meninggalkan jejak berupa modifikasi atau penghapusan file penting pada sistem server. Kondisi tersebut memperlihatkan bahwa antivirus dan firewall tradisional tidak lagi memadai untuk menghadapi ancaman canggih seperti malware [21], ransomware, maupun serangan zero-day yang dapat beroperasi tanpa terdeteksi di dalam sistem [17], [18]. Untuk mengatasi permasalahan ini, File Integrity Monitoring (FIM) berperan penting dalam mendeteksi setiap perubahan terhadap file kritikal, memberikan informasi rinci mengenai siapa, kapan, dan bagaimana perubahan tersebut terjadi. Platform open-source Wazuh SIEM merupakan salah satu solusi yang banyak digunakan untuk mengintegrasikan fitur FIM dengan log management, deteksi intrusi, serta sistem alerting yang terpusat [1], [24]. Dengan demikian, administrator dapat memperoleh visibilitas penuh terhadap aktivitas sistem dan mendeteksi potensi pelanggaran secara cepat.

Konteks lokal juga menunjukkan urgensi yang serupa. Berdasarkan laporan resmi dari Pusat Data dan Teknologi Informasi (Pusdatin) Kemendikdasmen, dari lebih dari 4.500 kampus di Indonesia, hanya sekitar dua puluh yang memiliki sistem keamanan yang memadai [14]. Tingginya angka ini menegaskan bahwa sektor pendidikan masih rentan dan memerlukan peningkatan ketahanan siber [3]. Di Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur, terdapat beberapa layanan web penting seperti sarpras.fasilkom.id, skp.fasilkom.id, dan fasilkom1.upnjatim.ac.id yang dihosting pada server fakultas dan berfungsi dalam mendukung kegiatan akademik serta administrasi. Layanan - layanan tersebut menyimpan berbagai data penting civitas akademika, sehingga keamanan integritas file pada server tempat layanan tersebut berjalan menjadi krusial dalam menjaga keandalan dan kepercayaan sistem informasi fakultas.

Saat ini, sistem keamanan pada server Fakultas Ilmu Komputer masih mengandalkan layanan eksternal seperti Cloudflare untuk melindungi dari serangan siber. Namun, mekanisme pengawasan terhadap perubahan file internal belum diterapkan secara optimal dan belum pernah dilakukan audit keamanan file secara menyeluruh. Dalam beberapa kasus, pernah terjadi gangguan pada layanan seperti kegagalan autentikasi SSL dan *redirect* domain [19] yang disebabkan oleh perubahan konfigurasi server. Pentingnya penanganan *misconfiguration* pada *web services* ini sangat krusial [20]. Hal ini menunjukkan pentingnya penerapan sistem pemantauan integritas file secara real-time agar potensi perubahan tidak sah dapat segera terdeteksi dan ditangani.

Selain tantangan dari sisi infrastruktur jaringan, aspek keamanan data di tingkat server juga memerlukan perhatian khusus. Hingga saat ini, belum pernah dilakukan audit keamanan file secara menyeluruh pada server Fakultas Ilmu Komputer. Padahal, server tersebut menampung sistem-sistem penting seperti sistem informasi sarana prasarana dan sistem penilaian kinerja dosen serta tenaga kependidikan. Dengan sumber daya perangkat keras yang memadai, seperti CPU, RAM, dan penyimpanan yang cukup, penerapan sistem monitoring berbasis Wazuh SIEM sangat memungkinkan dilakukan di lingkungan Fakultas Ilmu Komputer.

Ketiadaan sistem pemantauan file yang terintegrasi secara langsung memperlihatkan adanya celah dalam mekanisme deteksi dini terhadap ancaman keamanan. Ancaman tidak hanya berasal dari eksternal, tetapi juga dapat terjadi dari dalam sistem (insider threat) maupun akibat kesalahan konfigurasi (misconfiguration) [8], [20]. Hal ini menimbulkan research gap dalam penerapan sistem monitoring integritas file di lingkungan akademik. Berdasarkan permasalahan tersebut, penelitian ini dilakukan untuk menganalisis kinerja File Integrity Monitoring (FIM) berbasis Wazuh SIEM dalam mendeteksi perubahan file tidak sah secara langsung pada server Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur. Urgensi penerapan FIM diperkuat oleh insiden yang pernah terjadi pada layanan web fakultas, khususnya domain sarpras.fasilkom.id. Insiden ini terjadi sekitar awal tahun 2025. Efeknya adalah layanan web tersebut tidak dapat diakses secara normal oleh pengguna. Gangguan ini teridentifikasi disebabkan oleh perubahan file konfigurasi yang tidak terdeteksi pada *web server*, yang mengakibatkan kegagalan autentikasi SSL dan *redirect domain*.

Dengan sumber daya perangkat keras server yang dinilai memadai, penerapan solusi SIEM sangat memungkinkan. Wazuh SIEM dipilih sebagai platform utama karena alasan berikut: 1) Sifat *Open-Source* dan *Zero-Cost*: Ideal untuk lingkungan akademik dengan keterbatasan anggaran. sejalan dengan kebutuhan keamanan siber dengan anggaran terbatas [23]. 2) Fitur Terintegrasi (FIM dan SIEM): Wazuh menggabungkan fungsi penting *File Integrity Monitoring* (FIM) dan kapabilitas deteksi keamanan lain dalam satu platform terpusat, yang menjamin pemantauan secara *real-time*. Platform *open source* yang terintegrasi ini juga dapat ditingkatkan kemampuannya untuk *security monitoring* yang lebih canggih, seperti *log collection* berbasis AI [22]. 3) Dukungan Skalabilitas dan Komunitas Aktif: Kehadiran komunitas yang luas serta kemampuannya untuk mengelola sejumlah besar endpoint menjamin kemudahan implementasi dan pemeliharaan jangka Panjang. [12]

Berdasarkan permasalahan yang dihadapi, penelitian ini dilakukan untuk menganalisis kinerja *File Integrity Monitoring* (FIM) berbasis Wazuh SIEM. Metodologi yang digunakan adalah PPDIOO (*Prepare, Plan, Design, Implement, Operate, Optimize,* yang berfungsi untuk memastikan proses implementasi dan

pengoperasian sistem berjalan secara terstruktur dan berkesinambungan [15], terutama dalam proyek implementasi dan optimasi *Security Operation Center (SOC)* menggunakan alat *open-source* [26].

Dengan mempertimbangkan kompleksitas ancaman siber yang terus meningkat, tingginya kerentanan di sektor pendidikan, dan belum optimalnya sistem pengawasan integritas *file* secara *real-time* pada server Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur yang pernah menyebabkan gangguan layanan web krusial, maka penelitian ini menjadi sangat mendesak. Oleh karena itu, studi ini dilakukan untuk menganalisis kinerja File Integrity Monitoring (FIM) berbasis Wazuh SIEM, menggunakan metodologi PPDIOO (*Prepare, Plan, Design, Implement, Operate, Optimize*) yang terbukti efektif dalam memastikan proses implementasi dan optimasi *Security Operation Center* (SOC) berjalan secara terstruktur dan berkesinambungan [15], [26]. Luaran utama dari penelitian ini adalah (1) Implementasi fungsional dari platform Wazuh SIEM sebagai SOC sederhana di lingkungan fakultas, serta (2) Analisis kinerja yang terukur (meliputi latensi deteksi dan akurasi *alerting*) terhadap modifikasi *file* kritikal. Hasil akhir ini diharapkan dapat menutup *research gap* yang ada dan secara signifikan memperkuat ketahanan siber fakultas dalam menghadapi ancaman internal maupun eksternal.

1.2 Rumusan Masalah

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

1. Bagaimana penerapan File Integrity Monitoring (FIM) berbasis Wazuh SIEM pada server Fakultas Ilmu Komputer UPN “Veteran” Jawa Timur dalam memantau perubahan file kritikal?
2. Bagaimana kinerja FIM Wazuh dalam mendeteksi perubahan file tanpa otorisasi, ditinjau dari waktu deteksi, akurasi, dan efisiensi sistem, serta rekomendasi peningkatan konfigurasi yang dapat diberikan?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini mencakup beberapa aspek agar pembahasan tetap terarah dan sesuai dengan tujuan penelitian.

1.3.1 Objek Penelitian

Objek penelitian ini adalah server Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur yang menjalankan tiga layanan utama, yaitu sarpras.fasilkom.id, skp.fasilkom.id, dan fasilkom1.upnjatim.ac.id. Server tersebut dipilih karena memiliki infrastruktur yang aktif digunakan untuk mendukung kegiatan akademik dan administratif, serta dinilai relevan untuk implementasi sistem keamanan berbasis Wazuh.

1.3.2 Fokus Penelitian

Fokus penelitian terletak pada modul File Integrity Monitoring (FIM) yang terdapat pada platform Wazuh SIEM. Modul tersebut dianalisis untuk menilai sejauh mana kemampuan sistem dalam mendeteksi perubahan file yang terjadi pada server.

1.3.3 Parameter Analisis

Parameter yang digunakan dalam penelitian meliputi waktu deteksi perubahan file, akurasi alert yang dihasilkan oleh sistem, serta efisiensi kinerja FIM dalam proses monitoring integritas file.

1.3.4 Batasan Pembahasan

Penelitian hanya membahas modul FIM dan tidak mencakup modul Wazuh lainnya, seperti *Vulnerability Detection* dan *Log Data Analysis*. Selain itu, performa jaringan tidak menjadi bagian dari pembahasan karena jaringan Fakultas Ilmu Komputer telah dilindungi oleh layanan eksternal Cloudflare. Penelitian ini juga tidak membahas proses audit keamanan menyeluruh maupun pemulihan sistem pasca serangan.

1.3.5 Lingkup Pengujian

Lingkup pengujian dibatasi pada deteksi perubahan file serta pengukuran kinerja sistem FIM yang diterapkan pada server Fakultas Ilmu Komputer. Pengujian dilakukan pada lingkungan server dengan sumber daya perangkat keras yang memadai untuk mendukung implementasi Wazuh secara optima

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan sebelumnya, dibuat tujuan skripsi sebagai berikut :

1. Menerapkan File Integrity Monitoring (FIM) berbasis Wazuh pada server Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur.
2. Menganalisis kinerja FIM Wazuh dalam mendeteksi perubahan file tidak sah berdasarkan waktu deteksi, akurasi alert, dan efisiensi sistem.

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini, baik secara teoritis, praktis, maupun strategis adalah sebagai berikut:

1. Memperkaya literatur mengenai implementasi FIM berbasis SIEM di sektor pendidikan tinggi.
2. Memberikan petunjuk teknis bagi Fakultas Ilmu Komputer untuk meningkatkan keamanan file server.
3. Mendukung peningkatan ketahanan siber institusi pendidikan melalui pendekatan berbasis open-source dan deteksi dini.

1.6 Sistematika Penulisan

Sistematika Penulisan ini dibuat agar penyusunan skripsi memiliki kerangka yang jelas dan sesuai dengan rencana yang telah ditetapkan. Adapun susunan bab dalam skripsi ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Bab ini menjelaskan bagian pendahuluan yang memberikan gambaran umum mengenai penelitian yang dilakukan secara komprehensif. Di dalamnya mencakup uraian tentang latar belakang yang mendasari perlunya penelitian dilakukan, perumusan serta

pembatasan masalah yang menjadi fokus kajian, dan tujuan yang hendak dicapai sesuai dengan ruang lingkup penelitian. Selain itu, disajikan pula manfaat penelitian baik secara teoritis maupun praktis, serta sistematika penulisan yang menguraikan susunan bab dalam skripsi ini agar pembaca memperoleh pemahaman yang jelas mengenai arah, konteks, dan cakupan penelitian secara keseluruhan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tinjauan pustaka yang membahas teori-teori pendukung, konsep-konsep terkait, serta hasil penelitian terdahulu yang relevan dengan topik penelitian. Kajian ini bertujuan untuk memberikan landasan teoritis yang kuat, memperjelas posisi penelitian terhadap studi sebelumnya, serta menjadi acuan dalam penyusunan kerangka berpikir dan pelaksanaan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan metodologi penelitian yang digunakan sebagai dasar dalam pelaksanaan dan analisis penelitian. Di dalamnya mencakup model penelitian yang menggambarkan alur serta pendekatan yang digunakan untuk mencapai tujuan penelitian, tahapan penelitian yang menjelaskan langkah-langkah sistematis mulai dari perencanaan hingga evaluasi hasil, serta lingkungan penelitian yang mendeskripsikan kondisi, tempat, dan perangkat yang digunakan dalam proses penelitian. Keseluruhan bagian ini bertujuan untuk memberikan gambaran yang jelas dan terukur mengenai prosedur yang diterapkan dalam menganalisis kinerja sistem yang diteliti.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil dari pengembangan sistem informasi serta pembahasannya. Isi dari bab ini merupakan implementasi dari metodologi yang telah dijelaskan pada bab sebelumnya.

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian dan saran yang dapat diberikan. Kesimpulan dibuat untuk menjawab rumusan masalah yang ada pada bab sebelumnya.

DAFTAR PUSTAKA

Bagian ini memuat daftar referensi atau sumber literatur yang digunakan selama penyusunan skripsi.

LAMPIRAN

Bagian ini menyajikan dokumen-dokumen pendukung atau bukti yang berkaitan dengan proses penelitian dan penulisan skripsi.