BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi yang semakin pesat telah mendorong organisasi dan institusi untuk mengandalkan *website* sebagai pusat komunikasi, pelayanan, dan transaksi digital. *Website* tidak lagi sekadar berfungsi sebagai media publikasi, tetapi juga menjadi pintu akses utama bagi pengguna maupun sistem lainnya. Oleh karena itu, keamanan *website* menjadi faktor strategis yang berperan penting dalam menjaga keberlangsungan dan keandalan layanan digital. Meskipun demikian, ancaman siber terhadap *website* terus berkembang seiring dengan meningkatnya kompleksitas tekno*logi*. Teknik serangan semakin canggih, mulai dari pemindaian otomatis (*web scans*), injeksi dengan metode *obfuscation*, hingga serangan multi-vektor yang mengeksploitasi kelemahan konfigurasi maupun perilaku abnormal pada aplikasi. Dalam penelitian *In-Application Defense Against Evasive Web Scans through Behavioral Analysis* menunjukkan bahwa serangan pemindaian web yang bersifat menyamar (*evasive*) dapat dikenali melalui analisis perilaku secara *real-time* dalam aplikasi [1].

Salah satu pendekatan yang banyak digunakan untuk mengelola dan menganalisis data keamanan secara terpusat adalah *Security Information and Event Management*. SIEM merupakan sistem yang mengintegrasikan proses pengumpulan, normalisasi, korelasi, dan analisis data *log* serta *security event* dari berbagai sumber untuk memberikan visibilitas keamanan secara *real-time* maupun historis. SIEM menggabungkan fungsi *Security Information Management* yang berfokus pada pengelolaan *log* historis dengan *Security event Management* yang menitikberatkan pada deteksi kejadian keamanan secara langsung. Melalui mekanisme korelasi event dan analisis terintegrasi, SIEM mampu meningkatkan efektivitas pemantauan keamanan serta mendukung deteksi dini terhadap pola serangan yang kompleks dan berulang pada sistem berbasis web [2].

Untuk menghadapi kompleksitas data keamanan yang besar dan beragam, seperti *log* aktivitas, hasil pemindaian, maupun pola serangan, pendekatan visualisasi data melalui *dashboard* keamanan semakin dipandang penting. Asimiyu dalam *Visualizing Cyber Threats* menegaskan bahwa *dashboard* yang bersifat *actionable* mampu mengubah data ancaman yang kompleks menjadi bentuk visualisasi yang intuitif, sehingga mendukung tim keamanan dalam mendeteksi dan merespons ancaman dengan lebih cepat [3]. Hal serupa juga dikemukakan oleh [4], melalui penelitian *Evaluating Cyber Security Dashboards for Smart Cities*, yang mengevaluasi efektivitas *dashboard* berbasis web dalam menyajikan informasi keamanan secara komprehensif serta memberikan wawasan mengenai desain *dashboard* yang efektif bagi berbagai domain pengguna.

Lebih jauh lagi, kemampuan untuk memprediksi potensi ancaman keamanan menjadi perhatian penting dalam berbagai penelitian terkini. Dalam karya *Enhancing Cyber Security through Predictive Analytics* menunjukkan bahwa analisis berbasis perkiraan dapat meningkatkan kemampuan sistem dalam mendeteksi ancaman secara *real-time*, yang kemudian dapat ditampilkan melalui *dashboard* sebagai informasi perkiraan untuk membantu pengambil Keputusan [5]. Sejalan dengan itu, dalam penelitian [6] mengusulkan integrasi antara teknik *data mining* dan visualisasi dengan memanfaatkan *Power* BI untuk menganalisis pola serangan serta memberikan representasi visual terhadap ancaman siber.

Selain aktivitas autentikasi dan akses sistem, website yang mengelola konten secara dinamis juga memiliki risiko terhadap penyisipan tautan eksternal mencurigakan. Salah satu bentuk ancaman tersebut adalah *Malicious Link Injection* atau dapat dikaitkan dengan *SEO Spam Injection*, yaitu penyisipan URL tidak sah ke dalam konten website untuk mengarahkan pengguna atau mesin pencari ke situs eksternal. Ancaman ini dapat terjadi melalui kompromi akun admin, kelemahan validasi input, *stored XSS, SQL Injection*, maupun akses tidak sah terhadap basis data atau file website. Penelitian [7] menunjukkan bahwa SEO spam injection pada website perguruan tinggi dapat menghasilkan redirect tersembunyi ke situs eksternal serta berdampak pada integritas sistem, reputasi institusi, dan kepercayaan pengguna. Oleh karena itu, mekanisme deteksi URL mencurigakan diperlukan

karena malicious URL merupakan salah satu komponen penting dalam berbagai ancaman web dan dapat dideteksi melalui pendekatan blacklist, analisis URL, maupun teknik deteksi otomatis lainnya [8].

Meskipun berbagai penelitian telah membahas integrasi visualisasi keamanan dan analisis data, masih sedikit kajian yang secara spesifik menitikberatkan pada pemanfaatan *application log* dan pemindaian konten untuk analisis keamanan website institusi pendidikan. Deteksi terhadap aktivitas login mencurigakan, akses route sensitif, lonjakan error, serta penyisipan tautan eksternal berbahaya perlu disajikan dalam satu *dashboard* keamanan agar administrator dapat melakukan pemantauan dan investigasi secara lebih cepat. Oleh karena itu, penelitian ini mengusulkan Analisis Keamanan *Application Log* Website Berbasis *Dashboard* Menggunakan Metode SIEM sebagai upaya untuk mencatat, menganalisis, mengorelasikan, dan memvisualisasikan event keamanan, termasuk deteksi *Malicious Link Injection* pada konten website, sehingga mendukung pengambilan keputusan keamanan secara cepat dan berbasis data.

1.2 Perumusan Masalah

Website Jurusan Teknik Informatika telah digunakan sebagai sarana informasi dan layanan bagi mahasiswa maupun pengunjung, namun hingga kini belum dilengkapi dengan sistem pemantauan keamanan yang mampu menyajikan *log* aktivitas dan event keamanan secara terstruktur. Hasil evaluasi kerentanan dan *log* aktivitas belum disajikan dalam bentuk yang mudah dipantau, sehingga pihak pengelola berpotensi mengalami kesulitan dalam mendeteksi ancaman secara cepat, mengidentifikasi pola serangan, serta melakukan audit atau investigasi apabila terjadi insiden. Kondisi ini dapat membuka peluang terjadinya serangan otomatis, akses tanpa izin, percobaan login gagal berulang, akses route sensitif, lonjakan *error HTTP*, serta aktivitas pengelolaan data yang mencurigakan. Selain ancaman berbasis autentikasi dan akses, konten website yang bersifat dinamis juga berpotensi mengalami penyisipan tautan eksternal mencurigakan atau *Malicious Link Injection*. Ancaman ini dapat terjadi ketika *URL* tidak sah tersimpan pada konten website, seperti pada isi berita, agenda, galeri, profil, akademik, program studi, atau kemahasiswaan, sehingga tautan tersebut tetap terbaca pada *source*

HTML halaman meskipun tidak selalu terlihat secara visual oleh pengguna. Kondisi tersebut dapat mengganggu integritas konten, menurunkan reputasi institusi, serta berpotensi mengarahkan pengguna atau mesin pencari ke situs tidak resmi. Oleh karena itu, diperlukan sistem analisis keamanan *application log* website berbasis dashboard menggunakan *metode Security Information and Event Management* (SIEM) untuk mengumpulkan, menormalisasi, mengorelasikan, menganalisis, dan memvisualisasikan event keamanan secara terstruktur. Sistem ini juga mengintegrasikan mekanisme deteksi *URL* mencurigakan melalui pemindaian konten, *domain rules*, *keyword rules*, dan *background scan*, sehingga aktivitas yang teridentifikasi dapat diklasifikasikan sebagai *suspicious event*, dicatat sebagai alert keamanan, ditampilkan pada dashboard, serta dikirimkan dalam bentuk notifikasi peringatan kepada super administrator sebagai fungsi monitoring dan *early warning system.*

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan sesuai dengan tujuan yang ditetapkan, maka batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian difokuskan pada analisis keamanan *application log website* Jurusan Teknik Informatika.
2. Pendekatan keamanan yang digunakan adalah SIEM berbasis analisis *log* pada level aplikasi web.
3. Aktivitas yang dianalisis meliputi *Login*, *logout*, percobaan *Login* gagal, akses halaman (*route*), serta aktivitas pengelolaan data oleh administrator.
4. Deteksi keamanan dibatasi pada aktivitas mencurigakan berbasis perilaku pengguna, seperti *brute force Login*, akses di luar jam operasional, lonjakan kesalahan HTTP (4xx/5xx), dan akses ke *route* sensitif.
5. Deteksi *Malicious Link Injection* dibatasi pada pemindaian URL mencurigakan yang terdapat pada konten dinamis website, seperti berita, agenda, galeri, profil, akademik, program studi, dan kemahasiswaan.
6. Mekanisme deteksi *URL* mencurigakan dilakukan berdasarkan *domain rules*, *keyword rules, dan background scan* yang digunakan untuk

mengklasifikasikan domain atau tautan sebagai *allow*, *block*, *review*, *keyword match*, atau *unknown external domain*.

7. Penelitian ini tidak membahas aspek keamanan jaringan, konfigurasi server fisik, maupun infrastruktur sistem secara menyeluruh di luar aplikasi web.
8. Sistem yang dikembangkan berfokus pada penyajian hasil analisis keamanan dalam bentuk dashboard interaktif dan notifikasi peringatan, tanpa melakukan tindakan mitigasi otomatis terhadap serangan.

1.4 Tujuan

Tujuan penelitian ini adalah untuk menganalisis keamanan *application log website* dengan menerapkan metode SIEM yang disajikan dalam bentuk *dashboard* keamanan. Analisis dilakukan melalui pengolahan dan korelasi data *log* aktivitas aplikasi web guna mendeteksi aktivitas mencurigakan serta mendukung proses pemantauan dan evaluasi keamanan *website*. Studi kasus *Website* Jurusan Teknik Informatika.

1.5 Manfaat

Adapun manfaat dari penelitian yang diharapkan adalah:

a) Meningkatkan keamanan *website* jurusan.

   Dengan adanya sistem analisis keamanan berbasis *dashboard*, setiap aktivitas dan potensi ancaman dapat dipantau secara *real-time*. Hal ini membantu jurusan mendeteksi serangan atau akses tidak sah lebih cepat sehingga risiko kebocoran data dapat diminimalkan.

b) Mendukung proses audit dan evaluasi sistem.

   Dashboard keamanan yang dirancang mampu menyediakan catatan hasil pemindaian dan aktivitas sistem secara terstruktur. Dengan adanya data tersebut, proses audit keamanan dan evaluasi kerentanan *website* dapat dilakukan lebih mudah dan akurat.

c) Meningkatkan kepercayaan pengguna.

   Dengan sistem keamanan yang lebih transparan dan terpantau, mahasiswa, dosen, maupun pengunjung *website* akan merasa lebih aman. Hal ini diharapkan dapat meningkatkan kepercayaan pengguna terhadap *website* Jurusan Teknik Informatika sebagai sumber informasi resmi.