BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

SMAN 1 Rancaekek, sebagai institusi pendidikan menengah, sangat bergantung pada infrastruktur jaringan dan layanan aplikasi web untuk mendukung seluruh proses belajar mengajar maupun kegiatan administrasi. Objek penelitian difokuskan pada layanan aplikasi web SMAN 1 Rancaekek dengan domain https://smanrancaekek.sch.id, yang berfungsi sebagai titik akses utama bagi seluruh warga sekolah untuk memperoleh informasi dan pengelolaan data, seperti informasi terkait kegiatan akademik, data kepegawaian, dan arsip administrasi. Tingginya frekuensi akses terhadap layanan web ini, ditambah dengan sifat sensitif data yang tersimpan, secara inheren menjadikan situs ini target potensial bagi serangan siber.

Namun, pertumbuhan pesat ketergantungan pada teknologi informasi dan konektivitas ini berbanding lurus dengan peningkatan kompleksitas dan frekuensi ancaman keamanan siber [1]. Serangan jaringan komputer didefinisikan sebagai upaya untuk mendapatkan akses tidak sah ke jaringan, dengan tujuan mencuri data atau melakukan tindakan destruktif lainnya. Intrusi, sebagai bentuk spesifik dari serangan, adalah upaya tidak sah dan melanggar hukum untuk mengakses, memodifikasi, atau mengendalikan sistem/jaringan informasi, yang berpotensi membuatnya tidak dapat diandalkan atau tidak dapat dioperasikan [2]. Fakta ini diperkuat dengan pengalaman pihak SMAN 1 Rancaekek yang sebelumnya pernah mengalami insiden keamanan siber, di mana seorang pihak luar berhasil mengeksploitasi kelemahan pada sistem untuk mengakses data dan mengancam akan menyebarkannya demi keuntungan

pribadi jika tidak diberikan imbalan sejumlah uang [3]. Modus operandi ini dikenal sebagai tindakan dari pelaku *gray hat*, yaitu individu yang memiliki kemampuan teknis seperti peretas, namun tidak memiliki izin atau mandat resmi untuk melakukan penetrasi terhadap sistem. Kejadian ini secara tegas menunjukkan bahwa keamanan sistem tidak dapat hanya mengandalkan kepercayaan atau pendekatan informal, melainkan harus didukung oleh sistem pertahanan yang kuat dan berlapis untuk menjaga integritas dan kerahasiaan data. Di antara berbagai jenis serangan, injection attack adalah salah satu metode yang paling umum dan berbahaya [4]. Serangan ini terjadi ketika peretas menyisipkan perintah atau kode berbahaya ke dalam aplikasi atau program yang kemudian diproses oleh sistem. Dampak dari serangan ini bisa sangat merugikan, termasuk pencurian data, gangguan layanan, kerusakan integritas data, atau bahkan berhasil melewati mekanisme otentikasi sistem. Dari sisi teknis, aplikasi web SMAN 1 Rancaekek teridentifikasi memiliki kerentanan, khususnya terhadap *SQL Injection*, web defacement penyusupan semacam ini umumnya terjadi melalui celah keamanan pada sistem, seperti kerentanan pada *Content Management System* (CMS), plugin, atau kurangnya pembaruan perangkat lunak. Dampak dari penyusupan ini sangat substansial, tidak hanya mencoreng reputasi dan kredibilitas instansi pemerintah di mata publik, tetapi juga membahayakan keamanan data pengunjung situs yang dapat terpapar konten atau risiko berbahaya lainnya.

Masalah krusial lainnya adalah ketiadaan sistem pemantauan aktif yang bekerja secara real-time untuk mengawasi aktivitas pada server web di SMAN 1 Rancaekek, yang secara signifikan menghambat deteksi dini terhadap aktivitas mencurigakan atau indikasi serangan, sehingga insiden keamanan seringkali baru disadari setelah dampak kerugian telah terjadi dan menyebar luas. Lebih lanjut, menurut Badan Siber dan Sandi Negara dalam Landskap Keamanan Siber 2024 bahwa institusi pendidikan seringkali

menjadi sasaran serangan siber akibat kurangnya pemahaman mengenai pentingnya keamanan jaringan dan data [5]. Hal ini juga diperburuk oleh keterbatasan sumber daya manusia (SDM) di lingkungan sekolah yang belum sepenuhnya memahami konsep *secure coding* untuk mengembangkan aplikasi yang tangguh dari serangan, serta belum familiar dengan penggunaan sistem *Intrusion Detection System* (IDS) atau *Security Information and Event Management* (SIEM) seperti Wazuh yang mungkin terlalu kompleks untuk diimplementasikan dan dikelola secara mandiri oleh tim IT sekolah.

Mengacu pada kondisi tersebut, terdapat kebutuhan mendesak akan sebuah sistem keamanan yang tidak hanya mampu memantau lalu lintas antara web dengan server secara berkelanjutan, tetapi juga memiliki kapabilitas untuk mendeteksi serta menanggulangi potensi serangan secara otomatis. *Intrusion Detection and Prevention System* (IDPS) adalah solusi relevan yang dirancang untuk memantau dan menganalisis jaringan atau sistem guna mengidentifikasi kerentanan, melaporkan aktivitas berbahaya, dan menerapkan langkah-langkah pencegahan guna mengatasi perkembangan ancaman terkait komputer [6]. Penelitian ini mengusulkan pengembangan dan implementasi aplikasi bernama Semont (Sentinel Monitoring) sebagai sistem IDPS berbasis signature-based. Metode signature-based ini bekerja dengan teknik pattern matching, yaitu mencocokkan pola paket data yang dikirimkan dari pengguna ke server dengan pola serangan yang telah terdaftar dalam basis data. Metode ini dikenal efisien dalam mendeteksi ancaman yang terdokumentasi dan terbukti mampu mengurangi tingkat kesalahan deteksi (false positive maupun false negative). Namun, kelemahan mendasarnya terletak pada ketidakmampuannya dalam mendeteksi serangan zero-day atau varian serangan baru yang belum memiliki signature dalam basis data. Meskipun demikian, pemilihan pendekatan ini didasarkan

pada efisiensi dan akurasi deteksi untuk serangan yang umum dan telah dikenal, serta pertimbangan kemudahan implementasi dan pengelolaan di lingkungan SMAN 1 Rancaekek.

Aplikasi Semont didesain untuk mendeteksi dan mencegah berbagai kategori serangan kerentanan seperti injection (termasuk XSS, SQL *Injection*, *Remote Code Execution* (RCE), *Local File Inclusion* (LFI), dan sejenisnya), serta serangan brute force. Selain itu, Semont juga akan memiliki kapabilitas untuk mendeteksi deface pada direktori web dan mampu melakukan penghapusan halaman yang ter-deface secara langsung. Sistem ini akan berfokus pada pemantauan lalu lintas antara web dengan server yang melewati Port 80 (HTTP) dan Port 443 (HTTPS) yang merupakan jalur utama akses ke layanan web sekolah, serta akan menghasilkan laporan komprehensif dari log yang dibuat, memudahkan tim IT sekolah dalam memantau dan menganalisis insiden. Tujuan utama dari implementasi sistem ini tidak hanya untuk mendeteksi serangan secara real-time dan mencegah kompromi terhadap data, tetapi juga untuk memperkuat infrastruktur keamanan siber sekolah secara menyeluruh, walaupun dengan adanya kemungkinan kode aplikasi web yang rentan. Pemilihan Semont juga didasarkan pada pertimbangan bahwa antarmuka pengguna (UI) yang intuitif dan mudah dipahami akan memudahkan tim IT sekolah dalam mengoperasikan dan mengelola sistem tanpa memerlukan keahlian mendalam di bidang keamanan siber yang kompleks. Dengan adanya aplikasi Semont ini, diharapkan keamanan data dan infrastruktur digital sekolah dapat terjaga secara signifikan, dan ini dapat menjadi model penerapan sistem keamanan yang efektif serta meningkatkan kesadaran akan pentingnya keamanan siber di lingkungan pendidikan lainnya.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, beberapa masalah utama terkait keamanan sistem informasi di SMAN 1 Rancaekek dapat diidentifikasi sebagai berikut:

1. **Kerentanan Aplikasi Web Terhadap *Injection Attacks***: Website SMAN 1 Rancaekek teridentifikasi memiliki kerentanan, khususnya terhadap *SQL Injection* dan jenis *injection* lainnya seperti XSS, RCE, dan LFI. Kerentanan ini memungkinkan penyerang menyisipkan kode atau perintah berbahaya melalui input pengguna, seperti parameter URL atau formulir, yang dapat berdampak pada pencurian atau modifikasi data.
2. **Eksposur Data Sensitif**: Adanya temuan eksposur data sensitif (informasi siswa, orang tua, dan staf) yang tersimpan pada sistem web SMAN 1 Rancaekek, menunjukkan risiko serius terhadap privasi dan keamanan data warga sekolah.
3. **Ancaman *Web Defacement* dan *Judi Online***: Situs web sekolah berisiko tinggi terhadap serangan *web defacement*, baik yang merusak tampilan maupun yang menyisipkan konten perjudian daring, yang dapat mencoreng reputasi dan membahayakan pengunjung.
4. **Insiden Keamanan yang Pernah Terjadi**: Website sekolah pernah mengalami insiden keamanan siber yang mengakibatkan akses tidak sah dan upaya pemerasan data oleh pihak luar (pelaku *gray hat*), yang menegaskan bahwa situs tersebut pernah berhasil dieksploitasi.

5. **Ketiadaan Sistem Pemantauan *Real-time***: Belum adanya sistem *monitoring* aktif yang bekerja secara *real-time* untuk mengawasi aktivitas pada server web SMAN 1 Rancaekek, menyebabkan deteksi dini terhadap aktivitas mencurigakan atau indikasi serangan menjadi sulit.

6. **Dampak Akibat Serangan yang Tertunda Deteksinya**: Kurangnya deteksi dini menyebabkan insiden keamanan seringkali baru disadari setelah dampak kerugian terjadi dan menyebar luas, berpotensi mengakibatkan pencurian data sensitif, gangguan layanan, dan kerusakan integritas data.

7. **Kebutuhan Sistem Pertahanan Proaktif Otomatis**: Adanya kebutuhan mendesak akan sebuah sistem keamanan yang tidak hanya mampu memantau lalu lintas jaringan secara berkelanjutan, tetapi juga memiliki kapabilitas untuk mendeteksi serta menanggulangi potensi serangan secara otomatis.

8. **Kebutuhan Deteksi *Brute Force* dan Pemulihan *Deface***: Sistem yang ada belum mampu secara spesifik mendeteksi serangan *brute force* dan secara otomatis mengatasi (*menghapus*) halaman web yang ter-*deface* pada direktori web.

9. **Keterbatasan Pemahaman Keamanan Siber di Lingkungan Pendidikan**: Institusi pendidikan seringkali menjadi sasaran serangan siber akibat kurangnya pemahaman mengenai pentingnya keamanan jaringan dan data, membuat mereka rentan terhadap serangan dari pihak tidak bertanggung jawab.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah dipaparkan, penelitian ini merumuskan permasalahan sebagai berikut:

1. Bagaimana merancang dan mengimplementasikan aplikasi Semont sebagai sistem Pendeteksi dan Pencegah Intrusi (IDPS) berbasis signature-based untuk mendeteksi dan mencegah berbagai kategori serangan vulnerability (seperti injection termasuk XSS, SQL Injection, RCE, LFI, dan sejenisnya) serta serangan brute force pada jaringan komputer SMAN 1 Rancaekek?
2. Bagaimana aplikasi Semont dapat secara efektif mendeteksi deface pada direktori web?
3. Bagaimana sistem Semont dapat memantau lalu lintas jaringan pada Port 80 (HTTP) dan Port 443 (HTTPS) untuk mengidentifikasi pola serangan yang telah ditentukan, serta menghasilkan laporan komprehensif dari log yang dibuat untuk memudahkan tim IT sekolah dalam memantau dan menganalisis insiden?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengembangkan dan mengevaluasi solusi keamanan siber yang dirancang khusus untuk mengatasi kerentanan pada infrastruktur digital SMAN 1 Rancaekek. Tujuan-tujuan tersebut secara spesifik mencakup:

1. **Perancangan Sistem Pertahanan Proaktif:** Merancang dan mengimplementasikan arsitektur aplikasi Semont (Sentinel Monitoring) sebagai *Intrusion Detection and Prevention System* (IDPS) yang terintegrasi secara modular dengan server web SMAN 1 Rancaekek.

2. **Deteksi dan Pencegahan Ancaman Berbasis *Signature*:** Mengembangkan algoritma deteksi berbasis *signature* yang efisien dan akurat untuk mengidentifikasi serta menanggulangi berbagai kategori serangan siber yang umum, seperti *injection attacks* (termasuk SQL Injection, XSS, RCE, LFI), *brute force attacks*, dan aktivitas *vulnerability scanning*.
3. **Penguatan Integritas Web dan Ketersediaan Layanan:** Menciptakan fungsionalitas untuk mendeteksi *web defacement* pada direktori web serta menyediakan kapabilitas remediasi langsung (penghapusan halaman ter-deface) untuk menjaga integritas visual dan ketersediaan layanan website.
4. **Sistem Pemantauan dan Notifikasi Cepat:** Mengimplementasikan sistem pemantauan lalu lintas pada Port 80 (HTTP) dan Port 443 (HTTPS) yang mampu mencatat insiden secara komprehensif, menghasilkan laporan analitis, dan mengirimkan notifikasi *real-time* ke administrator melalui Telegram untuk memungkinkan respons yang cepat dan tepat.

1.5 Ruang Lingkup

Untuk menjaga fokus dan batasan penelitian, ruang lingkup yang akan dibahas dalam Tugas Akhir ini mencakupi bidang informatika dan dibatasi pada hal-hal berikut:

1. Objek Penelitian: Objek penelitian adalah layanan aplikasi web SMAN 1 Rancaekek yang beralamat di domain https://smanrancaekek.sch.id.
2. Jenis Serangan yang Difokuskan: Penelitian ini akan berfokus pada deteksi dan pencegahan berbagai kategori vulnerability seperti injection attacks (termasuk

XSS, SQL Injection , RCE, LFI, dan sejenisnya), serangan brute force, serta deteksi aktivitas pemindaian kerentanan (vulnerability scanning).

3. Metode Deteksi dan Pencegahan: Sistem yang dikembangkan akan menggunakan pendekatan signature-based , di mana deteksi dilakukan dengan mencocokkan pola serangan yang telah diketahui dan terdaftar dalam basis data.

4. Protokol yang Dipantau: Pemantauan lalu lintas jaringan akan dilakukan pada Port 80 (HTTP) dan Port 443 (HTTPS), yang merupakan jalur utama akses ke layanan web sekolah.

5. Fungsi Aplikasi Semont : Aplikasi Semont akan dirancang untuk mendeteksi dan mencegah serangan, mendeteksi deface pada direktori web, menghasilkan laporan dari log yang dibuat, dan memberikan informasi terkait insiden.

6. Pengolahan dan Analisis Data: Penelitian ini mencakup pengolahan dan analisis data log yang dihasilkan oleh aplikasi Semont untuk mengidentifikasi pola serangan dan memberikan wawasan keamanan.

7. Kelayakan Teknologi: Penelitian ini juga akan mengevaluasi kelayakan teknologi IDPS berbasis signature-based

8. Tidak Mencakup: Penelitian ini tidak mencakup pengembangan metode deteksi anomali berbasis statistik atau rule-based secara mendalam, serta tidak membahas secara spesifik keamanan infrastruktur jaringan secara keseluruhan di luar cakupan aplikasi web