BAB I
PENDAHULUAN

1. 1. Latar Belakang

Perkembangan teknologi jaringan dan internet yang semakin pesat mendorong meningkatnya penggunaan sistem informasi berbasis jaringan di berbagai sektor, termasuk pendidikan. Kondisi ini menjadikan infrastruktur jaringan dan *server* sebagai komponen penting dalam mendukung layanan digital. Namun, peningkatan pemanfaatan teknologi jaringan juga diikuti oleh meningkatnya ancaman keamanan jaringan seperti *malware*, *brute force*, *Distributed Denial of Service* (DDoS) serta aktivitas *scanning*. Ancaman tersebut berpotensi mengganggu ketersediaan layanan, integritas sistem, dan kerahasiaan data. Analisis *log* keamanan server menunjukkan bahwa pola serangan dapat dikenali melalui *event log* dan lalu lintas jaringan yang tidak normal, sehingga ancaman keamanan jaringan dapat dideteksi sejak tahap awal [1].

Meskipun ancaman keamanan jaringan terus berkembang, pada penerapannya masih banyak sistem yang belum dilengkapi dengan mekanisme monitoring dan deteksi insiden keamanan yang memadai. *Monitoring* sering kali dilakukan secara manual atau tidak berjalan secara *real-time*. Selain itu, *log* keamanan yang tersebar di berbagai sistem dan perangkat jaringan menyulitkan *administrator* dalam melakukan analisis insiden secara cepat. Akibatnya, banyak insiden keamanan jaringan yang tidak terdeteksi sejak dini. Penerapan sistem *Security Information and Event Management* (SIEM) berbasis *Wazuh* dapat membantu mengelola dan menganalisis *log* keamanan secara terpusat, sehingga meningkatkan efektivitas *monitoring* dan deteksi ancaman keamanan jaringan [2].

Deteksi dini dan analisis insiden keamanan jaringan memiliki peran penting dalam mengurangi dampak serangan siber. Indikasi awal terjadinya serangan dapat dikenali lebih cepat dengan memantau log keamanan, sehingga tindakan pencegahan

dapat dilakukan sebelum serangan berkembang menjadi insiden yang lebih serius. Selain itu, analisis insiden membantu *administrator* memahami pola serangan dan celah keamanan yang ada. Penelitian menunjukkan bahwa analisis *log* keamanan efektif dalam mendukung proses deteksi dini ancaman keamanan jaringan [3].

Security Operations Center (SOC) merupakan pusat operasional keamanan siber yang berfungsi untuk melakukan *monitoring*, deteksi, analisis, dan respon terhadap insiden keamanan jaringan secara terpusat. Metode ini memungkinkan pengelolaan keamanan jaringan dilakukan secara lebih terstruktur dan responsif. Keberadaan SOC menjadi penting seiring meningkatnya kompleksitas ancaman siber yang membutuhkan sistem keamanan dengan kemampuan pemantauan dan respons secara *real-time* [4].

Namun, penerapan SOC konvensional umumnya membutuhkan biaya yang besar, infrastruktur yang kompleks, serta sumber daya manusia yang memadai. Hal ini membuat SOC konvensional kurang sesuai untuk diterapkan pada organisasi berskala kecil maupun lingkungan pendidikan. Oleh karena itu, konsep *Mini Security Operations Center* (SOC) dikembangkan sebagai solusi yang lebih sederhana dan terjangkau, namun tetap mempertahankan fungsi utama SOC. Penggunaan SIEM berbasis *open source* seperti *Wazuh* terbukti mampu mendukung *monitoring* dan analisis keamanan jaringan secara efektif pada lingkungan dengan keterbatasan sumber daya [5].

Dalam implementasi *Mini* SOC, pemilihan *tools* yang tepat menjadi hal yang penting. *Wazuh* digunakan sebagai SIEM dan *Host-based Intrusion Detection System* (HIDS) untuk menganalisis *log* dan memantau integritas sistem. *Suricata* berfungsi sebagai *Intrusion Detection System/Intrusion Prevention System* (IDS/IPS) untuk mendeteksi serangan jaringan melalui analisis lalu lintas jaringan. Sementara *Wazuh Dashboard* digunakan untuk menampilkan data *log* dan *alert* dalam bentuk *dashboard* yang mudah dipahami. Integrasi *Wazuh* dan *Suricata* mampu meningkatkan akurasi deteksi serta mempermudah analisis insiden keamanan jaringan secara terpusat [6].

Berdasarkan hasil wawancara dengan Pranata Laboratorium Jaringan Komputer Jurusan Teknik Informatika Politeknik Negeri Bengkalis, diketahui bahwa laboratorium jaringan sering digunakan oleh mahasiswa untuk kegiatan praktikum. Dalam kondisi tersebut, penggunaan jaringan cukup tinggi dan gangguan jaringan kerap terjadi. Pranata laboratorium jaringan komputer menyampaikan bahwa gangguan jaringan biasanya diketahui dari laporan mahasiswa, seperti koneksi yang melambat, tidak dapat mengakses jaringan, atau terputus saat praktikum berlangsung.

Selain itu, proses pemantauan jaringan masih dilakukan secara manual dan belum didukung oleh sistem monitoring keamanan jaringan yang terpusat. Hal ini menyebabkan aktivitas jaringan yang mencurigakan sulit terdeteksi sejak awal. Akibatnya, insiden keamanan baru diketahui setelah berdampak pada kinerja jaringan, seperti penurunan kualitas koneksi atau gangguan akses selama praktikum. Kondisi tersebut berpotensi menghambat kelancaran proses pembelajaran serta menurunkan keandalan jaringan di laboratorium.

Berdasarkan permasalahan tersebut, penelitian ini mengimplementasikan *Mini Security Operations Center* (SOC) berbasis *Wazuh* dan *Suricata* dan pada Laboratorium Jaringan Komputer Jurusan Teknik Informatika Politeknik Negeri Bengkalis dengan tujuan untuk membangun sistem *monitoring* keamanan jaringan secara terpusat, mendukung deteksi dini dan analisis insiden keamanan jaringan, serta respon aktif terhadap serangan siber. Diharapkan hasil penelitian ini dapat meningkatkan keamanan jaringan di lingkungan Jurusan Teknik Informatika Politeknik Negeri Bengkalis serta menjadi referensi penerapan Mini SOC pada skala kecil.

1. 2. Rumusan Masalah

Bagaimana mengimplementasikan *Mini Security Operations Center* (SOC) berbasis *Wazuh* dan *Suricata* pada Laboratoriom Jaringan Komputer di Politeknik Negeri Bengkalis, serta bagaimana kemampuan sistem tersebut dalam melakukan

deteksi dini, analisis, dan respon terhadap insiden keamanan jaringan di lingkungan Jurusan Teknik Informatika Politeknik Negeri Bengkalis.

1. 3. Batasan Masalah

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

1. Penelitian ini difokuskan pada implementasi *Mini Security Operations Center* (SOC) berbasis *Wazuh* dan *Suricata* pada Laboratorium Jaringan Komputer Jurusan Teknik Informatika Politeknik Negeri Bengkalis.
2. Implementasi *Mini Security Operations Center* (SOC) dilakukan pada lingkungan jaringan lokal Laboratorium Jaringan Komputer Jurusan Teknik Informatika Politeknik Negeri Bengkalis dengan mengintegrasikan *Wazuh*, Suricata, sistem notifikasi *Telegram*, dan *Wazuh Active Response*. Sistem menyediakan fitur monitoring keamanan jaringan secara terpusat, deteksi dan pencegahan intrusi, pengiriman notifikasi otomatis, serta visualisasi *alert* melalui *dashboard* keamanan untuk mendukung analisis insiden keamanan jaringan.
3. Jenis ancaman keamanan jaringan dibatasi pada serangan *Distributed Denial of Service* (DDoS), *brute force* SSH, *Port scanning* dan *SQL Injection*.
4. Objek uji coba pada penelitian ini berupa *web server* dan basis data uji dengan menggunakan aplikasi *Damn Vulnerable Web Application* (DVWA) yang dibangun di lingkungan laboratorium sebagai simulasi layanan jaringan dan digunakan sebagai target pengujian serangan.

1. 4. Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengimplementasikan *Mini Security Operations Center* (SOC) berbasis *Wazuh* dan *Suricata* pada Laboratorium Jaringan Komputer di Jurusan Teknik Informatika Politeknik Negeri Bengkalis.
2. Membangun sistem yang dapat memonitoring, deteksi dini insiden keamanan jaringan secara terpusat dan analisis insiden keamanan jaringan berdasarkan data *alert* yang dihasilkan oleh *Wazuh* dan *Suricata* di lingkungan Laboratorim Jaringan Komputer Jurusan Teknik Informatika Politeknik Negeri Bengkalis.

1. 5. Manfaat

b. Bagi Institusi

Penelitian ini dapat menjadi alternatif dalam meningkatkan keamanan jaringan pada Laboratorium Jaringan Komputer Jurusan teknik Informatika di Politeknik Negeri Bengkalis melalui penerapan sistem *monitoring* dan deteksi insiden keamanan jaringan secara terpusat.

c. Bagi Pengelola Laboratorium

Hasil penelitian ini dapat membantu *administrator* jaringan dalam memantau aktivitas jaringan, mendeteksi ancaman lebih awal, serta mempermudah penanganan gangguan atau insiden keamanan jaringan.

d. Bagi Mahasiswa

Penelitian ini dapat dijadikan sebagai media pembelajaran terkait implementasi dan pengelolaan sistem keamanan jaringan berbasis SOC menggunakan *tools open source*.