201910370311099
Fajrul Ikram Mantiri Usman
Prodi Informatika

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) adalah jaringan perangkat pintar yang terhubung melalui internet untuk saling berbagi data dan komunikasi. Teknologi ini memanfaatkan sensor, aktuator, dan sistem komputasi untuk memproses informasi secara real-time, memungkinkan otomatisasi dan efisiensi dalam berbagai aplikasi [1]. IoT terintegrasi oleh perangkat fisik dengan infrastruktur digital melalui komunikasi tanpa batas ruang dan waktu. IoT memegang peranan penting dalam membangun ekosistem yang cerdas, menciptakan peluang inovasi di berbagai sektor sekaligus menghadapi tantangan terkait keamanan, skalabilitas, dan interoperabilitas perangkat [2].

Celah keamanan dalam *Internet of Things* (IoT) merupakan isu yang semakin penting di tengah peningkatan perangkat IoT. Penelitian menunjukkan bahwa banyak perangkat IoT dirancang tanpa mempertimbangkan aspek keamanan yang memadai sehingga menciptakan berbagai kerentanan. Terutama pada bagian protokol komunikasi yang lemah dan tidak terenkripsi dapat memungkinkan penyerang untuk mengakses data sensitif yang ditransmisikan antara perangkat [3]. Berdasarkan hasil penelitian yang pernah dilakukan, perangkat IoT memiiki celah keamanan yang dapat rentan di eksploitasi. Seperti pada *bootloader* [4], *firmware* [4], *node sensor* [5], *dan memory* [6].

Perangkat IoT rentan terhadap serangan siber karena keterbatasan kapasitas pemrosesan, penyimpanan, dan keamanan bawaan, yang sering tidak dirancang untuk mengatasi ancaman keamanan. Serangan-serangan seperti *Denial of Service* (DoS) [7], serangan *Man-in-the-Middle* (MITM) [8], dan penyusupan data sensitif sering kali menargetkan perangkat IoT yang terhubung ke jaringan. Pada lingkungan yang melibatkan banyak perangkat IoT, setiap perangkat yang rentan dapat membuka jalan bagi serangan yang berpotensi

merusak jaringan atau mengakses data rahasia. Hal ini menyebabkan perusahaan harus memiliki strategi keamanan siber yang kuat, khususnya dalam mengamankan perangkat IoT yang rentan [9].

Salah satu cara untuk mengelola keamanan dan mempermudah dalam melakukan monitoring aktivitas yang terjadi dengan menggunakan *Security Information and Event Management* (SIEM). SIEM berfungsi dengan mengumpulkan, menganalisis, dan mengelola data keamanan dari berbagai sumber, termasuk log dari perangkat jaringan, aplikasi, dan sistem [10]. Hasil studi sebelumnya menunjukkan penggunaan Splunk SIEM pada sistem IoT sebagai solusi efektif untuk menghadapi ancaman DDoS dari botnet IoT. Splunk mampu mendeteksi dan mengurangi serangan DDoS dari botnet IoT dengan memantau paket seperti TCP SYN, ICMP, dan DNS dari perangkat IoT yang telah diserang [11]. Penelitian lain dilakukan integrasi IDS dan Wazuh pada perangkat GPS IoT, sistem ini digunakan untuk analisis data dari serangan seperti MITM dan DoS. Serangan MITM menggunakan ARP Spoofing dan Sniffing untuk menyusup pada lalu lintas jaringan. Serangan DoS mengirim banyak paket ACK pada perangkat GPS untuk mengganggu perangkat. Integrasi IDS dan Wazuh memberikan hasil peningkatan dalam mendeteksi serangan MITM sebesar 50% dan 96% dalam mendeteksi serangan DoS [12].

Penelitian ini bertujuan mengimplementasikan Wazuh sebagai sistem keamanan pada IoT dengan fokus pada kemampuan pemantauan dan visualisasi ancaman. Wazuh akan diintegrasikan untuk memonitor aktivitas perangkat IoT secara real-time serta memberikan respons otomatis terhadap potensi serangan yang telah disimulasikan. Penelitian ini akan mengevaluasi efektivitas Wazuh dalam mengidentifikasi pola ancaman yang kompleks melalui analisis log perangkat. Tujuan utama dari implementasi ini adalah meningkatkan kemampuan deteksi dini terhadap ancaman, mengurangi tingkat kerentanan perangkat IoT, serta meminimalkan dampak insiden keamanan siber pada jaringan yang terhubung.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, penelitian ini memiliki beberapa rumusan masalah sebagai berikut:

1. Bagaimana mengimplementasikan Wazuh untuk *monitoring* keamanan pada jaringan perangkat IoT?
2. Bagaimana kinerja Wazuh di dalam proses monitoring dan visualisasi data serangan pada jaringan perangkat IoT?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengimpementasikan Wazuh dalam monitoring keamanan jaringan pada jaringan perangkat IoT
2. Mengevaluasi kemampuan monitoring dan visualisasi yang dihasilkan oleh Wazuh untuk membantu pengguna dalam memahami pola serangan dan mengambil tindakan responsif secara *real time*.

1.4 Batasan Masalah

Untuk menjaga fokus dan keterukuran penelitian, beberapa batasan masalah ditetapkan sebagai berikut:

1. Penelitian ini hanya menganalisis kinerja Wazuh sebagai platform SIEM dalam konteks keamanan IoT pada perangkat Raspberry Pi yang terhubung ke jaringan, tanpa melibatkan platform SIEM lain.
2. Evaluasi dilakukan terhadap perangkat IoT yang menggunakan Raspberry Pi dan terhubung dengan jaringan internal, yang dikelola dengan Wazuh server yang berjalan di VirtualBox dengan OS Ubuntu, sehingga tidak mencakup perangkat IoT di luar jaringan tersebut.
3. Analisis akan dilakukan dalam periode waktu tertentu yang ditetapkan, sehingga hasil penelitian mencerminkan kondisi dalam kurun waktu tersebut.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan laporan ini, sebagai berikut :

BAB I PENDAHULUAN

Pada Bab ini membahas tentang latar belakang dari penelitian, rumusan masalah dari penelitian yang dilakukan, batasan masalah yang ada pada penelitian, tujuan dan manfaat dari penelitian yang dilakukan serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada Bab ini membahas tentang landasan teori yang berhubungan dengan topik penelitian dan penelitian terdahulu yang telah dilakukan berkaitan dengan topik yang dibahas.

BAB III RANCANGAN DAN REALISASI

Pada Bab ini membahas tentang rancangan penelitian, tahapan penelitian, objek penelitian, framework yang akan digunakan, serta teknik pengumpulan dan analisis data.

BAB IV HASIL DAN PEMBAHASAN

Pada Bab ini akan membahas mengenai hasil dan pembahasan dari pengujian terhadap sistem yang telah diimplementasikan pada penelitian yang telah dilakukan.

BAB V PENUTUP

Pada Bab ini akan membahas mengenai kesimpulan yang didapat dari penelitian yang telah dilakukan dan memberikan saran untuk pengembangan terhadap penelitian selanjutnya berdasarkan hasil dari penelitian.

DAFTAR PUSTAKA

Pada bagian ini berisi tentang referensi dalam pembentukan laporan ini.