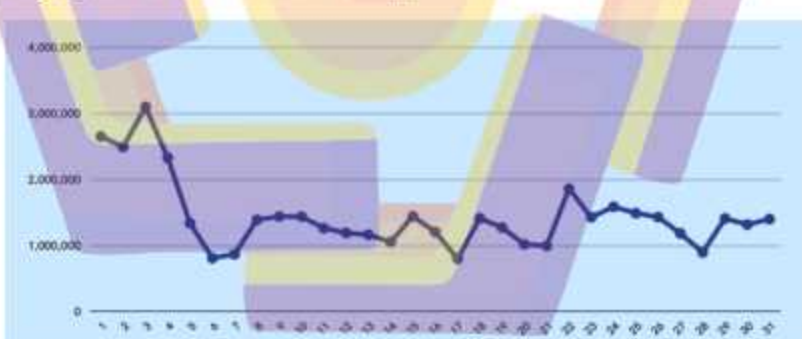
BAB I
PENDAHULUAN

1.1 Latar Belakang

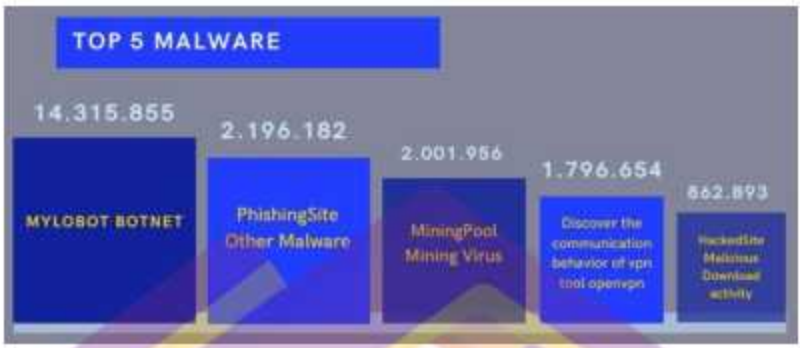
Kemajuan teknologi informasi dan komunikasi berkembang dengan cukup cepat dan pesat, dibalik cepat dan pesatnya kemajuan perkembanganya terdapat juga sisi negatif lain yang ikut berkembang yaitu kejahatan siber atau yang sering disebut dengan *cybercrime*. Dengan meningkat dan menjadi semakin majunya metode, aktivitas, dan modus dalam kejahatan siber sehingga keamanan siber atau *cyber security* harus ditingkatkan seiring berjalannya waktu agar tidak ketinggalan. Dari data laporan bulanan hasil monitoring keamanan siber Agustus 2022 yang dicatat oleh Badan Siber dan Sandi Negara (BSSN) yaitu terdapat 44.776.891 anomali trafik dan jumlah anomali tertinggi terdapat pada tanggal 3 Agustus 2022 dengan jumlah 3.103.770 anomali trafik[1].



Gambar 1.1 Sebaran kasus per sektor pada Agustus 2022[1].

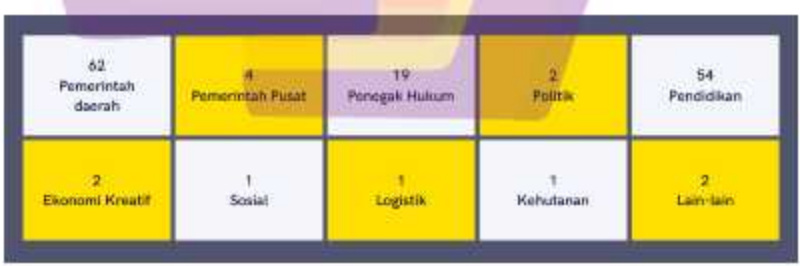
Dalam kurung waktu bulan Januari sampai 18 oktober 2022, terdapat 893.952.873 anomali trafik yang mencurigakan untuk menyerang keamanan di indonesia. Dari jumlah tersebut, didominasi oleh aktivitas serangan malware. Pelaksana tugas (Plt) Direktorat Keamanan Siber BSSN Andi Yusuf menyatakan, Dari keseluruhan anomali traffic, yang paling banyak berupa aktivitas serangan malware sebanyak 55,83%, kemudian information leak 14,99%, dan aktivitas trojan

10,45%[2].



Gambar 1.2 Top 5 Malware hasil monitoring keamanan siber Agustus 2022[1]

Dari hasil monitoring anomali trafik keamanan siber Agustus 2022 yang dilakukan oleh BSSN diketahui terdapat 5 malware dengan jumlah yang tinggi yaitu diantaranya Mylo Bot Botnet, Phishing Site, Mining Pool, Discover sensitive directory, dan Trojan Rat[1]. Dampak dari serangan tersebut tercatat pada data persebaran kasus per sektor yang dicatat oleh BSSN dimana dapat dilihat sektor Pemerintahan daerah dan Pendidikan adalah sektor tertinggi yang terdampak, ini mengungkapkan bahwa sektor Pemerintah daerah dan Pendidikan paling banyak terjadi peretasan selama bulan Agustus 2022. Namun, tidak menutup kemungkinan pada sektor lain untuk tetap perlu mendapatkan perhatian terkait keamanan yang dimiliki.



Gambar 1.3 Sebaran kasus per sektor pada Agustus 2022[1].

Dengan adanya penjabaran dan berita di atas dapat disimpulkan bahwa

meningkatkan penjaga keamanan jaringan, sistem, dan data aset sangatlah penting bagi sektor manapun baik perusahaan, pemerintah, dan lain-lainnya. Solusi yang bisa dilakukan adalah dengan monitoring secara real time dan menganalisis serangan yang terjadi baik dari sumbernya maupun tujuannya, yang dimana hal ini dapat dibaca dalam log aktivitas dari monitoring tersebut. Monitoring server berguna untuk memastikan aset-aset penting yang bersifat rahasia agar tetap aman seperti 3 aspek dalam keamanan informasi yaitu *Confidentiality*, *Integrity*, dan *Availability*. Maka diperlukan sebuah *Security Information and Event Management* (SIEM), dengan menggunakan SIEM dapat mengumpulkan informasi keamanan yang berisikan data *log* pada *hardware*, jaringan dan aplikasi. Teknologi SIEM berguna untuk mengumpulkan data dalam jumlah yang cukup besar dan bisa menganalisis serta menghubungkan peristiwa dari berbagai sumber. Dengan kata lain, SIEM adalah sistem informasi yang mencakup fungsi agregasi data, korelasi data, deteksi dan alert, reporting, serta penyimpanan data. Tools yang digunakan adalah wazuh, yang dimana wazuh adalah aplikasi berbasis *Open Source* yang berperan sebagai *Host-Based Intrusion Detection System* (HIDS). Wazuh juga terdapat beberapa fitur penting yaitu; *Intrusion Detection*, *Security Analytics*, *File Integrity Monitoring*, *Log Data Analysis*, dan lain-lain. Sehingga dapat meminimalkan serangan terhadap server dengan pendeteksi serangan.

Tentu untuk perusahaan-perusahaan terutama yang bergerak dalam jasa penanganan dan solusi jaringan baik dalam mendesain, mengimplementasikan dan juga memelihara perangkat jaringan sangat mustahil jika tidak memiliki keamanan yang kuat, dengan SIEM mampu meningkatkan lagi keamanan sistem, *hardware*, jaringan dan aset-aset berharga menjadi lebih aman dan terhindar dari serangan siber atau kejahatan internet. Terhubungnya dengan Telegram mampu menyampaikan atau memberitahu *alert* secara *realtime* ketika ada serangan terjadi sehingga insiden cepat direspon dan segera diselesaikan.

Berdasarkan uraian masalah yang terdapat diatas peneliti membuat sebuah topik penelitian yang berjudul **"IMPLEMENTASI *SECURITY INFORMATION* and *EVENT MANAGEMENT* (SIEM) MENGGUNAKAN**

WAZUH DENGAN NOTIFIKASI TELEGRAM". Judul tersebut dipilih dikarenakan masih banyak perusahaan terutama perusahaan yang bergerak dibidang jasa dan pembangunan infrastruktur jaringan ingin meningkatkan keamanan dalam mengamankan data-data dan aset berharga perusahaan sesuai dengan 3 aspek dalam keamanan informasi yaitu *Confidentiality, Integrity*, dan *Availability* (CIA). Untuk merancang dan mengimplementasikan SIEM sebagai monitoring sistem peneliti menggunakan metode PPDIOO yang terdiri dari *Prepare*, *Plan*, *Design*, *Implement*, *Operate*, *Optimize*. Yang dimana metode tersebut sesuai dan seirama dengan langkah-langkah dalam menerapkan wazuh.

1.2 Rumusan Masalah

Perumusan masalah ini bertujuan mengarahkan dan memperjelas arah dari penelitian ini agar sesuai dengan hasil yang diharapkan, maka masalah yang dapat dirumuskan adalah:

1. Bagaimana perancangan *security information and event management* (SIEM) berbasis wazuh?
2. Bagaimana mengetahui dan mengidentifikasi serangan *Brute force*, SQL *injection* dan *distributed denial of service* (DDOS) pada wazuh?
3. Apakah *security information and event management* (SIEM) berbasis wazuh dapat mempermudah mengetahui serangan?

1.3 Batasan Masalah

Dengan terbatasnya waktu dan kemampuan peneliti, maka peneliti menyadari perlu adanya pembatas masalah antara lain:

1. Penelitian ini menggunakan dua sistem operasi *ubuntu linux* sebagai wazuh *server dan agent*.
2. Penelitian ini menggunkan sistem operasi kali linux yang memiliki peran sebagai peyerang.
3. Penelitian ini hanya menjelaskan bagaimana cara melihat dan mengidentifikasi log serangan.
4. Endpoint protection menggunakan Wazuh, Deteksi Serangan Siber menggunakan Wazuh, dan Integrasi Wazuh dengan Telegram.
5. penelitian ini hanya melakukan serangan *Brute force*, SQL *injection* dan *distributed denial of service* (DDOS).
6. Penelitian ini hanya mensimulasi serangan tanpa adanya pemulihan sistem yang dilakukan oleh penyerangan.

1.4 Tujuan Penelitian

Tujuan serta maksud yang akan dicapai oleh peneliti dalam penelitian ini adalah:

1. Mengidentifikasi serangan serangan *Brute force*, SQL *injection* dan *distributed denial of service* (DDOS) yang terdeteksi oleh wazuh.
2. Melakukan konfigurasi untuk memperancangkan implementasi dan mensimulasikan monitoring jaringan secara realtime.
3. Mengetest seberapa responsif bot telegram mengirimkan notifikasi serangan.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini peneliti membagi menjadi beberapa yaitu manfaat bagi peneliti dan pembaca. Yang dimana lebih jelasnya sebagai berikut:

1. Bagi Peneliti
   a. Memperoleh gelar sarjana strata 1 sarjana komputer (S.Kom.) pada program pendidikan Informatika Universitas AMIKOM Yogyakarta
   b. Menambah pengetahuan dan wawasan seputar dunia keamanan jaringan.
   c. Menambah pengetahuan tentang cara kerja, kegunaan, dan performa wazuh dalam menghadapi serangan.
   d. Mengimplementasi ilmu dan teori yang didapatkan pada saat kuliah di Universitas Amikom Yogyakarta dan yang didapatkan di luar kampus.
2. Bagi Pembaca
   a. Menambah pengetahuan dan wawasan seputar dunia keamanan jaringan.
   b. Sebagai pertimbangan dalam menentukan keamanan jaringan menggunakan wazuh.

1.6 Sistematika Penulisan

Penelitian ini berisikan lima bab dengan sistematika penjelasan sebagi berikut:

BAB I PENDAHULUAN

Bab ini berisikan pembahasan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan pembahasan tentang tinjauan pustaka, dasar-dasar teori yang berhubungan, dan digunakan untuk mendukung penulisan penelitin ini.

BAB III METODE PENELITIAN

Bab ini berisikan pembahasan tentang jenis dan desain penelitian, objek penelitian, alat dan bahan yang digunakan, waktu dan tempat penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan pembahasan tentang tahapan yang peneliti lakukan dalam membuat sistem SIEM, pengimplementasi wazuh, pengujian dengan melakukan simulasi penyerangan, dan mengidentifikasi serangan yang terjadi.

BAB V PENUTUP

Bab ini berisikan pembahasan tentang kesimpulan hasil penelitian dan saran yang dapat peneliti rangkum selama proses penelitian.