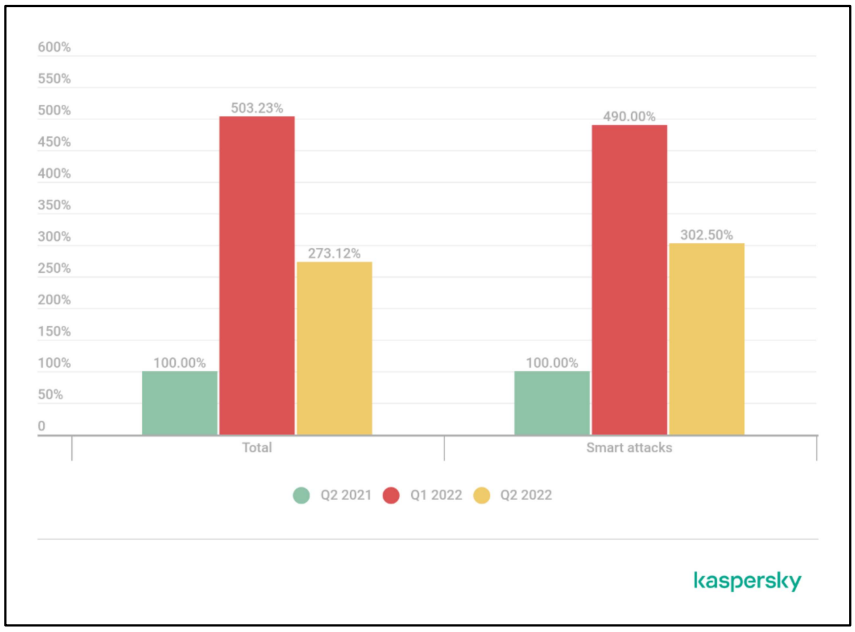
BAB I
PENDAHULUAN

1.1 Latar Belakang

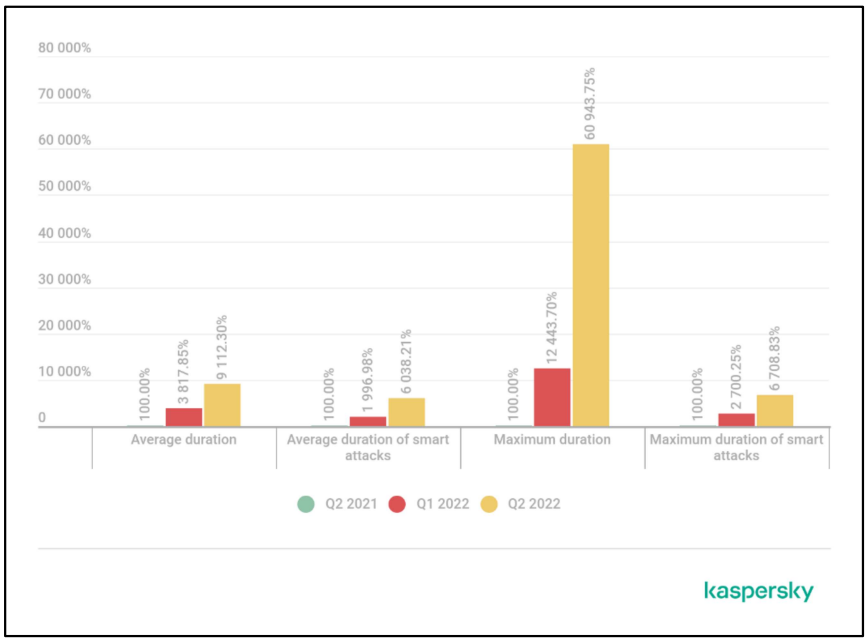
Penerapan teknologi pada kehidupan manusia tentunya mampu memberikan kemudahan pada berbagai macam sektor untuk menjalankan aktivitasnya sehari-hari, baik itu secara individu atupun organisasi. Pesatnya perkembangan teknologi di masa Sekarang tidak lepas dari meningkatnya kebutuhan manusia akan kecepatan, kemudahan, keakuratan serta keamanan. Saat ini, sektor Teknologi Informasi dan Komunikasi mengalami perkembangan yang pesat. Hal ini terlihat dari berbagai kemajuan teknologi informasi dan komunikasi yang sering kita jumpai dalam kehidupan sehari-hari, seperti Internet (Jaringan Terhubung).

Internet merupakan suatu sistem komunikasi yang memiliki kemampuan untuk menghubungkan banyak komputer maupun jaringan komputer secara global di semua penjuru dunia. Melalui internet berbagai individu maupun organisasi dapat saling bertukar informasi. Terus meningkatnya penggunaan internet sebagai media utama untuk bertukar informasi, tentu saja berbanding lurus dengan peningkatan jumlah data berharga yang beredar melalui jaringan internet. Namun, peningkatan tersebut juga berbanding lurus dengan munculnya berbagai macam celah keamanan yang seringkali dimanfaatkan oleh para penjahat elektronik untuk mendapatkan keuntungan finansial. Hal tersebut tentunya mengancam serta membahayakan banyak sekali pengguna internet. Di bawah ini disajikan beberapa contoh aksi serangan yang dapat terjadi melalui internet, termasuk namun tidak terbatas pada: eksposur data yang dapat menyebabkan kerugian finansial yang serius, pengiriman email phising berisi pesan penipuan atau tautan berbahaya, serta serangan *Denial of Service (DoS)* dan *Distributed Denial of Service (DDoS*).

Distribusi Serangan Denial of Service (DDoS) adalah upaya yang disengaja untuk menyebabkan server atau host kehabisan sumber daya dengan mengalirkan sejumlah besar permintaan atau data kepadanya. Hasilnya, host tersebut tidak dapat memberikan layanan kepada pengguna lain yang mencoba mengaksesnya karena sumber daya seperti memori, CPU, dan lalu lintas telah habis terpakai(Arman, 2020). *Distributed denial-of-service (DDoS)* adalah tipe serangan yang terus berkembang dalam kekuatan dan kompleksitasnya seiring dengan perkembangan organisasi yang menjadi targetnya. Serangan ini memiliki kapasitas dan biaya yang semakin meningkat untuk merespons dan menghadapinya. Berdasarkan Laporan DDoS Q2 2022 yang dikeluarkan oleh Kaspersky, Sistem Intelijen DDoS Kaspersky telah merekam 78.558 serangan DDoS.



Gambar 1. 1 Perbandingan jumlah serangan DDoS: Q2 2022 dan Q2 2021 serta Q1 2022 dikutip dari sumber : (*DDoS Attacks in Q2 2022* | *Securelist*, n.d.)



Gambar 1. 2 Perbandingan durasi serangan DDoS: Q2 2022 dan Q2 2021 serta Q1 2022 dikutip dari sumber : (DDoS Attacks in Q2 2022 | Securelist, n.d.)

Berdasarkan gambar 1.1 dan gambar 1.2 pada Q2 2022, serangan DDoS mengalami penurunan dibandingkan dengan periode pelaporan Q1 2022. Namun serangan yang terjadi telah berubah dari kuantitas menjadi kualitas, yang mana serangan menjadi lebih lama dan lebih rumit. Serangan *Distributed Denial of Service (DDoS)* pada Q2 2022 telah mencapai level baru karena jumlah serangan cerdas dan durasi rata-rata serangan melonjak tajam. Jika dibandingkan dengan tahun sebelumnya, rata-rata durasi serangan DDoS mengalami kenaikan hingga 100 kali lipat, mencapai 3.000 menit. Serangan DDOS ini kebanyakan menargetkan website-website Pemerintahan dan Infrastruktur Publik seperti perusahaan transportasi dan juga Kesehatan. (*DDoS Attacks in Q2 2022 | Securelist*, n.d.).

Serangan DDoS memiliki beberapa varian dan setiap varian mempunyai karakteristik yang berbeda dalam serangannya. Oleh sebab itu penanganan untuk setiap tipe varian juga akan berbeda tergantung karakteristiknya. Dalam

usaha menangani isu tersebut, penulis melakukan analisis pada Security Information and Event Management (SIEM).

SIEM adalah suatu metode yang digunakan untuk mengawasi, menganalisis, memberikan pemberitahuan, serta merespons insiden-insiden tertentu secara otomatis. Dengan penerapan SIEM, log dari beragam peristiwa dapat terkumpul secara instan dari berbagai sumber yang terhubung dengan server yang telah dikonfigurasi. (Tiara Sakinah, 2022). Hal ini dapat memudahkan proses pengawasan sistem oleh organisasi karena seluruh aktivitas yang terjadi pada sistem akan tercatat pada log.

Pada penelitian ini penulis akan menggunakan *tools* yang *open source*, yaitu Wazuh. Hal ini dikarenakan fitur-fitur yang disediakan Wazuh dapat terbilang cukup lengkap meskipun gratis. Aplikasi ini akan melakukan pengumpulan data keamanan, deteksi ancaman, perlindungan terhadap *endpoint* serta respons insiden sehingga dapat menyediakan visibilitas keamanan.

1.2 Identifikasi Masalah

Setelah memahami penjelasan sebelumnya mengenai latar belakang masalah, kita dapat mengidentifikasi permasalahan yang sedang dihadapi sebagai berikut :

1. Angka kejadian serangan DDoS pada instansi pemerintah dan infrastruktur publik sangat tinggi.

1.3 Rumusan Masalah

Setelah berhasil mengidentifikasi permasalahan sebelumnya, langkah selanjutnya adalah merumuskan masalahnya sebagai berikut:

1. Apa saja metode untuk mengidentifikasi serangan DDoS pada suatu sistem ?

2. Bagaimana kemampuan sistem SIEM dalam menganalisis isu terkait serangan DDoS ?
3. Apa Langkah yang tepat dalam mengatasi serangan DDoS dengan efektif ?

1.4 Batasan Masalah

Dengan berpegang pada perumusan masalah sebelumnya, kami membatasi masalah sebagai berikut:

1. Penelitian ini hanya akan menitikberatkan pada analisis syslog yang menunjukkan kemungkinan adanya serangan DDoS yang ditujukan ke situs web.
2. Kami akan menggunakan Sistem Operasi CentOS 8, Ubuntu Server 22.04, Wazuh 4.3, dan suricata sebagai alat uji dalam penelitian ini.
3. Untuk memantau manajemen log, kami akan menggunakan aplikasi Wazuh.
4. Penelitian ini akan dilakukan di lingkungan Lab Fakultas Ilmu Komputer UPN Veteran Jakarta sebagai tempat pelaksanaan percobaan.

1.5 Tujuan Penelitian

Dengan mempertimbangkan batasan masalah sebelumnya, penelitian ini bertujuan untuk :

1. Menemukan dan mengenali serangan DDoS yang terjadi pada sistem.
2. Menganalisis efektivitas SIEM dalam menghadapi serangan DDoS.
3. Menyajikan hasil pengujian, analisis, dan solusi terkait dengan masalah serangan DDoS.

1.6 Manfaat Penelitian

Berikut adalah beberapa manfaat yang diperoleh melalui penelitian ini :

1. **Bagi Penulis:**
    a. Menyelesaikan salah satu persyaratan untuk lulus dari program Strata Satu (S1) di Fakultas Ilmu Komputer Universitas Pembangunan Veteran Jakarta.
    b. Memperoleh pengetahuan dan pemahaman tentang serangan DDoS serta cara untuk mendeteksi serangan tersebut.

2. **Bagi Universitas:**
    a. Menyumbangkan karya ilmiah dalam bidang ilmu Informatika.
    b. Menjadi referensi untuk penelitian terkait keamanan siber.

3. **Bagi Masyarakat:**
    a. Meningkatkan pemahaman tentang keamanan siber.
    b. Menjadi tambahan referensi untuk penelitian dengan topik yang sama.
    c. Memberikan saran kepada organisasi terkait pengawasan keamanan siber.

1.7 Sistematika Penulisan.

Dalam penulisan tugas akhir ini, struktur yang digunakan mengikuti aturan penulisan yang terdiri dari beberapa bagian, antara lain:

BAB 1 PENDAHULUAN

Pada bab ini, dijelaskan tentang asal-usul dan alasan dilakukannya penelitian, pertanyaan-pertanyaan yang ingin dijawab dalam penelitian, tujuan dari penelitian, manfaat dari hasil penelitian, cakupan atau batasan

masalah yang diteliti, hasil yang diharapkan, dan bagaimana penulisan akan disusun secara sistematik.

BAB 2 TINJAUAN PUSTAKA

Bab ini mencakup penjelasan rinci mengenai berbagai teori yang menjadi dasar dari penelitian ini. Kontennya meliputi berbagai elemen seperti metode, teknik, konsep, prosedur, dan definisi yang relevan dengan topik penelitian yang sedang dilakukan.

BAB 3 METODOLOGI PENELITIAN

Dalam bab ini, akan dijelaskan proses penelitian yang meliputi langkah-langkah, tinjauan teoritis, perancangan eksperimen, batasan area penelitian, sumber data, metode pengumpulan data, pengolahan data, dan analisis data yang digunakan untuk mencapai tujuan penelitian. Setiap langkah yang diambil akan dijelaskan dengan dasar yang relevan.

BAB 4 HASIL DAN PEMBAHASAN

Pada bagian ini, dijelaskan prosedur yang harus diikuti dalam melakukan penelitian terhadap masalah yang relevan, dengan tujuan mencapai hasil yang diinginkan.

BAB 5 PENUTUP

Pada bagian ini, akan diuraikan ringkasan mengenai hasil penelitian yang terdapat pada bab 4, beserta rekomendasi untuk meningkatkan sistem agar menjadi lebih efisien dan fleksibel di penelitian mendatang..

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN