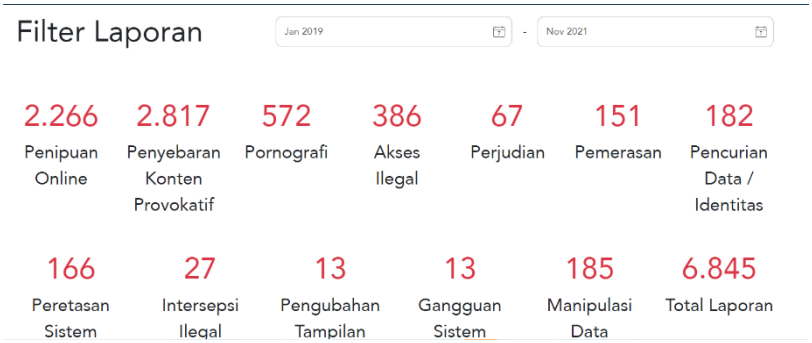
BAB I

PENDAHULUAN

1.1.Latar Belakang

Teknologi merupakan hal yang paling dekat dengan manusia saat ini. Penggunaan teknologi sangat membantu manusia baik tiap individu maupun organisasi di berbagai sektor. Teknologi dianggap memberi kemudahan dalam memberi dan menerima informasi, mempermudah banyak aktivitas sehari-hari, memberi efisiensi pada setiap aktivitas seperti waktu yang relative lebih cepat, biaya yang lebih murah, dan sumber daya manusia yang jika tanpa adanya teknologi maka semua dilakukan dengan manual dengan waktu yang lebih lama, biaya yang tinggi, dan banyak memerlukan sumber daya manusia untuk mengerjakannya. Teknologi sangat erat kaitannya dengan data. Keberadaan teknologi adalah untuk menyampaikan kumpulan informasi dengan mudah dan efisien.

Data adalah sekumpulan fakta yang dapat diolah menjadi sebuah informasi, nantinya informasi tesebut akan berguna bagi orang lain. Setiap individu maupun organisasi bertukar informasi dengan tujuan tertentu, dan banyak dari informasi tersebut yang memiliki tingkat keamanan yang tinggi. Pentingnya pengawasan pada setiap informasi merupakan aturan yang tidak bisa dilewatkan oleh setiap individu maupun organisasi. Organisasi harus memperhatikan atau melakukan *monitoring* pada data mereka. Menurut statistik Polisi Siber, terhitung sejak Januari 2019 hingga November 2021 terdapat 182 kasus pencurian data dan 185 kasus manipulasi data.



Gambar 1. 1 Hasil statistik Polisi Siber per Januari 2019 - November 2021

Kurangnya *awareness* pada keamanan data seperti memanggil orang-orang yang tidak bertanggung jawab untuk melakukan kejahatan dengan mencuri data tersebut atau biasa disebut *data exfiltration.* Beberapa kasus yang terjadi dapat teridentifikasi oleh tim keamanan organisasi tersebut, namun banyak diantaranya tidak teridentifikasi sampai saat dilakukan audit sistem keamanan barulah teridenifikasi terjadinya masalah tersebut atau biasa disebut *Zero Day Attack*. Menurut penelitian yang dilakukan oleh HelpNet pada tahun 2021, sekitar 74% serangan pada organisasi baik besar maupun kecil merupakan serangan *Zero Day Attack.* Hal ini tentu sangat membahayakan integritas data pada setiap organisasi. Kesalahan yang biasa dilakukan sampai terjadi data exfiltration adalah, tidak melakukan *update* sistem dan manajemen *patch* secara berkala, kurang melakukan monitoring dan analisis keamanan, serta kurangnya pengetahuan mengenai *data exfiltration* tersebut.

Banyak pintu masuk untuk penyerang agar dapat melakukan *data exfiltration*, seperti melalui layanan *Secure Shell (SSH), Domain Name System (DNS),* serta layanan *Control and Command (C2)* lainnya. Untuk itu, setiap organisasi harus melakukan pemantauan pada lalu lintas jaringan, memantau *behaviour* yang mencurigakan, serta dapat memberikan solusi jika sewaktu-waktu terjadi *data exfiltration* tersebut.

Untuk mengatasi hal tersebut diatas, penulis melakukan analisis pada *Security Information and Event Management* atau disingkat SIEM. SIEM merupakan metode untuk mengumpulkan, menganalisa, memberi *alert* memberi laporan, serta melakukan automatisasi respon pada sebuah insiden. SIEM akan mengumpulkan *log* secara *real-time* dari berbagai sumber yang terhubung dengan server. Hal ini tentu akan mempermudah organisasi dalam melakukan pemantauan terhadap sistem. Setiap aktivitas akan tercatat pada *log* dan dapat langsung dianalisa oleh organisasi. *Tools* yang akan digunakan oleh penulis adalah Wazuh, karena dianggap lengkap walapun gratis dan merupakan *tools* yang *open-source*. Aplikasi ini akan memberi kelas pada kerentanan atau hal yang dianggap mengancam sistem yang sedang dipantau. Menurut Catescu (2018) perusahaan dengan usaha kecil menengah tidak mampu membeli peralatan keamanan siber yang lengkap dikarenakan harganya yang tidak murah, sistem pemantauan seperti SIEM tools lain juga memiliki harga yang mahal. Oleh karena itu, penulis memberikan hasil analisis melakukan pemantauan sistem dengan perangkat yang *open-source* dan dapat digunakan oleh usaha kecil menengah.

1.2.Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka identifikasi masalah adalah sebagai berikut :

1. Banyaknya kasus *data exfiltration* pada organisasi
2. Kurangnya analisa dan *monitoring* terhadap sistem dengan SIEM

1.3.Rumusan Masalah

Berdasarkan identifikasi masalah yang telah dijelaskan sebelumnya, maka diperoleh rumusan masalah:

1. Bagaimana mengetahui sebuah sistem yang mengalami *data exfiltration* ?
2. Bagaimana kemampuan SIEM dalam melakukan analisa terkait masalah *data exfiltration ?*
3. Apakah solusi yang baik untuk mengatasi *data exfiltration* ?

1.4.Batasan Masalah

Berdasarkan rumusan masalah yang telah dijelaskan sebelumnya, maka diperoleh Batasan masalah:

1. Penelitian hanya difokuskan pada sys*log* yang mencirikan terjadinya *data exfiltration*.
2. Penelitian ini menggunakan Sistem Operasi Windows 10, Ubuntu Debian, Wazuh.ova, dan Kali Linux dalam pengujiannya.
3. Penelitian ini menggunakan laboratorium dengan environment pribadi.
4. Penelitian ini menggunakan aplikasi Wazuh untuk melakukan pemantauan *log management*.

1.5.Tujuan Penelitian

Berdasarkan Batasan masalah yang telah dijelaskan sebelumnya, tujuan penulis melakukan penelitian ini adalah sebagai berikut :

1. Mengidentifikasi *data exfiltration* pada sistem.
2. Melakukan analasis kemampuan SIEM dalam mengatasi masalah *data exfiltration*.

3. Menjabarkan hasil pengujian dan analisis serta memberikan rekomendasi solusi yang dapat dilakukan untuk mengatasi *data exfiltration*.

1.6.Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah sebagai berikut :

1. **Bagi Penulis**
   a. Untuk memenuhi salah satu syarat kelulusan Strata Satu (S1), Informatika Fakultas Ilmu Komputer Universitas Pembangunan Veteran Jakarta.
   b. Mendapatkan pengetahuan dan pemahaman mengenai *data exfiltration* serta cara untuk mencegah hal tesebut.
2. **Bagi Universitas**
   a. Sebagai kontribusi karya ilmiah dalam disiplin ilmu Informatika.
   b. Sebagai tambahan referensi terhadap penelitian di bidang keamanan siber.
3. **Bagi Masyarakat**
   a. Menambah pengetahuan mengenai keamanan siber.
   b. Sebagai acuan untuk referensi terhadap penelitian dengan topik serupa.
   c. Membantu Organisasi untuk memberi saran terkait pengawasan keamanan siber

1.7.Sistematika Penulisan

Sistematika penulisan skripsi ini dengan menggunakan metode tertentu sebagai berikut :

BAB 1 : PENDAHULUAN

Pada Bab ini berisi Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Batasan Masalah, Luaran yang Diharapkan, dan Sistematika Penulisan.

BAB 2 : LANDASAN TEORI

Pada Bab II Landasan Teori berisi tentang teori-teori mendasar, referensi jurnal, dan metode yang digunakan dalam penelitian ini.

BAB 3 : METODOLOGI PENELITIAN

Pada Bab III Metodologi Penelitian berisi tentang kerangka pikir, alur metode dalam memproses penelitian ini, serta segala metode yang terdapat dalam penelitian ini.

BAB 4 : HASIL DAN PEMBAHASAN

Pada Bab IV Hasil dan Pembahasan berisi tentang penjelasan mengenai proses pengolahan data dan pembuatan model untuk sistem, lalu pembahasan tentang analisis hasil pengujian dari data yang sudah diolah pada penelitian ini.

BAB 5 : PENUTUP

Pada Bab V Penutup berisi tentang kesimpulan dari hasil dari penelitian yang dilakukan pada bab 4 (empat) dan juga saran yang dapat digunakan sebagai acuan agar sistem dapat diperbaharui lebih baik dan lebih dinamis.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN