BAB I PENDAHULUAN

I.1 Latar Belakang

Dalam era *digital* yang semakin maju, pengetahuan mengenai ancaman siber menjadi hal yang penting dalam menghadapi kemajuan teknologi. Ancaman siber merupakan serangan yang dapat mengganggu, merusak, atau mencuri data dalam dunia siber, dapat menimbulkan dampak serius pada individu, organisasi, dan masyarakat secara luas. Menunjukkan bahwa motivasi serangan siber pada infrastruktur kritis bervariasi, dari tujuan finansial hingga politik. Oleh karena itu, penting bagi organisasi untuk mengantisipasi berbagai ancaman dan mengembangkan strategi keamanan komprehensif untuk melindungi aset penting dan memastikan kontinuitas layanan yang vital bagi masyarakat (Alqudhaibi et al., 2023).

Dalam upaya untuk menjaga tingkat keamanan yang optimal, organisasi telah mengimplementasikan berbagai perangkat keamanan, termasuk *Security Information and Event Management* (SIEM). SIEM merupakan sistem yang digunakan untuk mencegah, mendeteksi, dan bereaksi terhadap serangan siber (González-Granadillo et al., 2021). Pada penelitian ini akan menggunakan salah satu aplikasi SIEM *open source*, yaitu IBM QRadar karena terdapat banyak fitur yang membuat aplikasi ini menjadi sangat *powerful* dan juga dokumentasi yang tersedia pada *website* IBM.

Threat Intelligence memberikan wawasan tentang ancaman yang potensial, sementara *Threat Behavior* memungkinkan deteksi pola perilaku yang mencurigakan yang mungkin menjadi indikasi terjadinya serangan. Penelitian ini akan menggunakan *Threat intelligence* dan *Threat Behavior* sebagai acuan mengidentifikasian eksploitasi yang dilakukan.

Fungsi kontrol keamanan mencakup empat komponen utama yaitu *Identification*, *Authentication*, *Authorization*, dan *Accounting* (IAAA). *Identification* adalah proses mengidentifikasi entitas yang mencoba mengakses sistem atau jaringan. *Authentication* memastikan bahwa identitas yang telah diidentifikasi adalah valid. *Authorization* menentukan hak akses apa yang dimiliki entitas yang telah

diautentikasi dalam sistem, dan *Accounting* mencatat semua aktivitas yang dilakukan oleh entitas dalam sistem, termasuk akses dan tindakan yang diambil. Dengan menerapkan fungsi kontrol ini, organisasi dapat membangun pertahanan yang kuat terhadap ancaman siber dan memastikan integritas, kerahasiaan, serta ketersediaan sistem (Martín et al., 2021).

Penelitian ini bertujuan untuk melakukan identifikasi dan *profiling* IBM QRadar dalam menunjukkan kemampuan deteksi terhadap berbagai jenis serangan siber. Proses identifikasi dan *profiling* ini menggunakan platform eksperimen yang terdiri dari tiga server virtualisasi yaitu Kali Linux sebagai pengujian keamanan jaringan, IBM QRadar sebagai SIEM untuk mendeteksi dan menganalisis ancaman keamanan dalam jaringan, serta CentOS sebagai *target* penyerangan. Menggunakan tiga kategori teknik serangan siber, yaitu *Port Scanning*, *Brute Force*, dan DDoS. Pemilihan ketiga teknik serangan untuk menguji kemampuan deteksi dan analisis serangan siber oleh IBM QRadar.

Hasil dari pengujian eksperimen diolah menjadi sebuah analisa fungsi kontrol keamanan. Kemudian data tersebut digunakan sebagai dasar untuk analisis *profiling Threat intelligence dan Threat Behavior* yang lebih mendalam terhadap serangan siber. Dengan begitu, *profiling* dapat digunakan untuk meningkatkan keamanan TI dan merespons ancaman siber dengan lebih efektif.

I.2 Perumusan Masalah

Berdasarkan uraian masalah yang telah dijelaskan pada latar belakang, maka permasalahan yang akan dikaji pada penelitian ini adalah sebagai berikut:

1. Bagaimana mengenali fungsi SIEM IBM QRadar sebagai kontrol keamanan?
2. Bagaimana fungsi kontrol SIEM IBM QRadar memiliki rincian data?
3. Bagaimana fungsi kontrol keamanan dengan rincian data SIEM IBM QRadar dapat berfungsi mendeteksi serangan pada jaringan?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah yang ada, tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Mengenali fungsi *Threat Intelligence* pada SIEM IBM QRadar yaitu berupa fungsi kontrol utama menggunakan aspek *Identification*, *Authentication*, *Authorization*, dan *Accounting log*.
2. Mengenali metrik-metrik yang merinci fungsi kontrol utama pada SIEM IBM QRadar.
3. *Profiling* metrik fungsi kontrol IBM QRadar sebagai SIEM berdasarkan variasi serangan pada jaringan.

I.4 Batasan Penelitian

Adapun batasan dalam melakukan penelitian ini, sebagai berikut:

1. Lingkup pengenalan fungsi kontrol berupa serangan dan pendeteksian serangan dalam bentuk simulasi dan eksperimen.
2. Kategori serangan berupa *Port Scanning, Brute Force,* dan DDoS dengan 3 *softtware* berbeda untuk kategori *Port Scanning*, *Brute Force*, dan DDoS. Setiap *software* ini digunakan dengan perilaku yang berbeda untuk mendapatkan gambaran *Profiling* SIEM IBM QRadar dalam mendeteksi dan merespons berbagai jenis serangan siber.
3. Eksperimen menggunakan pendekatan sistem *blackbox* dan analisa tidak membahas aspek internal *software* yang digunakan.

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut:

1. Secara teoritis
   a. Dapat menambah pengetahuan terkait fungsi kontrol utama pada SIEM IBM QRadar menggunakan *Identification, Authentication, Authorization, dan Accounting.*
   b. Dapat mengenali metrik-metrik dari *Threat Intelligence* dan *Threat Behavior* berdasarkan hasil eksperimen serangan.
2. Secara praktis

a. Sistem SIEM IBM QRadar pada jaringan membantu praktik keamanan dalam mengimplementasikan indikator *rules* sesuai dengan berbagai jenis serangan siber.
b. Mengenali serangan yang digunakan berdasarkan pada praktik konfigurasi *rules* untuk *Port Scanning*, *Brute Force*, dan DDoS.