BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan semakin pesatnya perkembangan teknologi informasi, kebutuhan akan keamanan jaringan menjadi semakin penting, terutama dalam mengelola sistem informasi yang kompleks. Setiap aktivitas yang berlangsung dalam sistem jaringan umumnya terekam dalam bentuk *log file*, yang dapat digunakan untuk menelusuri jejak aktivitas pengguna maupun sistem. Log ini menyimpan informasi yang sangat berharga dan bisa dimanfaatkan untuk mendeteksi pola-pola yang tidak biasa atau bahkan serangan siber.

Namun, seiring meningkatnya volume *log* yang dihasilkan oleh perangkat jaringan, proses analisisnya menjadi semakin menantang, terutama jika dilakukan secara manual. Salah satu pendekatan yang kini banyak digunakan untuk mengatasi tantangan ini adalah penerapan *machine learning*, khususnya metode *unsupervised learning* seperti *Autoencoder* dan *One-Class SVM*. Kedua metode ini dapat digunakan untuk mendeteksi aktivitas mencurigakan tanpa perlu data yang sudah diberi label sebelumnya (*Zhang et al., 2022*).

PT. XYZ, yang bergerak di bidang keamanan siber, memiliki tanggung jawab untuk memantau serta menyusun laporan aktivitas jaringan dari para kliennya secara rutin. Salah satu tugas dari *security analyst* di perusahaan ini adalah

menganalisis *file log* yang dihasilkan oleh perangkat seperti *Fortigate*. *Log* tersebut secara otomatis diarsip oleh sistem *Wazuh* dalam format *plaintext*. Format ini seringkali menyulitkan proses analisis karena tidak langsung dapat diolah sebagai data terstruktur.

Selain volume data yang besar, format log yang tidak langsung siap diproses menyebabkan proses identifikasi anomali menjadi memakan waktu dan rentan terhadap kesalahan. Keterbatasan ini tentunya dapat menghambat efektivitas dalam menjaga keamanan jaringan, terutama dalam proses penyusunan laporan keamanan bulanan.

Oleh karena itu, diperlukan sebuah sistem yang mampu mengotomatisasi proses deteksi anomali pada *log* Fortigate. Penelitian ini mengusulkan pengembangan sistem tersebut dengan membandingkan dua pendekatan *unsupervised learning*: *Autoencoder*, yang bekerja berdasarkan *reconstruction error*, dan *One-Class SVM*, yang bekerja berdasarkan *boundary*. Sistem ini diharapkan dapat membantu *security analyst* di PT. XYZ dalam menganalisis *log* secara lebih cepat dan akurat, sehingga dapat meningkatkan efektivitas pemantauan keamanan jaringan. (*Xu et al., 2021*).

Hasil dari proses ini diharapkan berupa file .csv yang memuat daftar aktivitas jaringan yang terdeteksi sebagai anomali. Output ini nantinya akan menjadi bahan utama dalam penyusunan laporan keamanan bulanan, sekaligus mempercepat proses kerja dari tim analis keamanan jaringan.

1.2 Identifikasi Masalah

XYZ saat ini menghadapi tantangan dalam proses penyusunan laporan keamanan bulanan yang sangat bergantung pada analisis manual log akses Fortigate. Proses manual ini tidak hanya memakan waktu dan sumber daya secara signifikan, tetapi juga memiliki risiko tinggi untuk melewatkan deteksi aktivitas mencurigakan yang krusial bagi keamanan jaringan. Oleh karena itu, dapat diidentifikasi bahwa masalah utama adalah tidak adanya sistem otomatis yang mampu memproses log secara efisien dan mendeteksi anomali menggunakan pendekatan *machine learning* untuk mendukung kebutuhan pelaporan keamanan di PT XYZ.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mengubah log Fortigate berformat .txt menjadi data tabular yang siap dianalisis?
2. Bagaimana membangun dan menerapkan model deteksi anomali menggunakan *Autoencoder* dan *One-Class SVM* terhadap data akses dari *log* Fortigate?
3. Bagaimana performa kedua model dalam mengidentifikasi akses mencurigakan berdasarkan metrik evaluasi seperti *precision*, *recall*, *F1-score*, dan *ROC AUC*?

1.4 Batasan Masalah

Penelitian ini hanya akan berfokus pada pengolahan data log dari perangkat Fortigate yang disimpan dalam format .txt hasil arsip Wazuh. Metode deteksi yang digunakan terbatas pada *Autoencoder* dan *One-Class SVM*, dan data yang dianalisis hanya mencakup periode tertentu sesuai kebutuhan laporan bulanan.

1.5 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah:

1. Mengembangkan sebuah metode untuk melakukan *parsing* dan pra-pemrosesan pada *log* syslog Fortigate dari format *plaintext* menjadi *dataset* tabular yang terstruktur dan siap untuk dianalisis oleh model *machine learning*.
2. Membangun, melatih, dan menerapkan model deteksi anomali berbasis *Autoencoder* dan *One-Class SVM* menggunakan *dataset log* Fortigate yang telah diproses.
3. Menganalisis dan membandingkan performa kedua model (*Autoencoder* dan *One-Class SVM*) dalam mendeteksi aktivitas mencurigakan, serta menyajikan hasilnya menggunakan metrik evaluasi yang relevan.

1.6 Manfaat Penelitian

Secara teoritis, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan studi terkait deteksi anomali berbasis log menggunakan

pendekatan *unsupervised learning*. Secara praktis, penelitian ini dapat menjadi solusi untuk membantu *security analyst* dalam melakukan analisis log secara lebih efisien dan akurat, sekaligus mempercepat proses penyusunan laporan keamanan yang berbasis data.

1.7 Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metodologi CRISP-DM (Cross-Industry Standard Process for Data Mining). Tahapan dalam metodologi ini meliputi Business Understanding, Data Understanding, Data Preparation, Modeling, Evaluation, dan Deployment. Pendekatan ini dipilih karena sifatnya yang terstruktur dan iteratif, sangat cocok untuk proyek data mining seperti ini.

1.7.1 Metode Pengumpulan Data

Data yang digunakan dalam penelitian ini diambil dari file log Fortigate yang telah diarsipkan oleh sistem Wazuh. Data mentah tersebut akan melalui beberapa tahap seperti parsing, pembersihan, dan transformasi ke dalam bentuk tabular sebelum digunakan untuk pelatihan model.

1.8 Sistematika Penulisan Laporan Skripsi

Sistematika penulisan laporan skripsi ini disusun untuk memberikan gambaran yang jelas mengenai struktur isi dan komponen laporan yang berkaitan dengan penelitian berjudul *"Deteksi Anomali Jaringan pada Sistem Log Fortigate*

Firewall dengan Menggunakan Autoencoder dan One-Class SVM untuk Analisis Syslog Fortigate di PT. XYZ".

1.8.1 Komponen Awal Laporan

1. Hard Cover
2. Halaman Cover
3. Pembatas masing-masing bab dan bagian
4. Lembar Monitoring Bimbingan
5. Lembar Perbaikan/Revisi yang telah ditandatangani penguji
6. Lembar Pernyataan
7. Lembar Penguji
8. Lembar Keterangan dari Perusahaan atau Tempat Penelitian
9. Lembar Pengesahan

1.8.2 Bagian Pendahuluan dan Abstrak

1. Kata Pengantar
2. Abstrak, yang berisi ringkasan penelitian termasuk tujuan, metode, hasil, serta kesimpulan penelitian.

1.8.3 Struktur Isi Laporan

1. Daftar Isi
2. Daftar Tabel
3. Daftar Gambar

4. Daftar Lampiran
5. Bab I Pendahuluan. Memuat latar belakang, rumusan masalah, tujuan, manfaat, serta metode penelitian dalam konteks deteksi anomali jaringan menggunakan data Syslog Fortigate.
6. Bab II Landasan Teori. Menguraikan teori yang mendukung deteksi anomali, autoencoder sebagai metode pembelajaran mesin, serta studi terdahulu yang relevan.
7. Bab III Metodologi. Menjelaskan tahapan metodologi penelitian, desain sistem deteksi anomali, serta proses pelatihan dan evaluasi autoencoder dan one-class SVM.
8. Bab IV Hasil dan Pembahasan. Menyajikan hasil implementasi sistem, analisis deteksi anomali pada Syslog Fortigate, serta evaluasi performa model Autoencoder dan One-Class SVM yang digunakan.
9. Bab V Penutup. Berisi kesimpulan dari penelitian dan saran pengembangan lanjutan terkait sistem deteksi anomali jaringan berbasis Wazuh di PT. XYZ.
10. Daftar Pustaka
11. Lampiran, yang terdiri dari dokumen pendukung seperti surat keterangan bebas plagiat, hasil Turnitin dan source code implementasi.