BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Keamanan jaringan menjadi salah satu aspek krusial dalam operasional perusahaan yang bergantung pada teknologi informasi, termasuk PT PLN Batam. Dengan meningkatnya intensitas serangan siber, sistem *firewall* telah menjadi elemen penting untuk melindungi infrastruktur jaringan(Purba dan Efendi, 2021). *Firewall* mencatat log serangan sebagai data mentah yang berisi informasi penting tentang aktivitas jaringan, termasuk potensi ancaman(Sholihan *et al*., 2023). Namun, log serangan yang dihasilkan sering kali sangat besar dan memerlukan analisis lebih lanjut untuk memahami tingkat ancaman yang terkandung di dalamnya.

Klasifikasi tingkat ancaman berdasarkan log serangan *firewall* dapat membantu tim keamanan jaringan untuk memprioritaskan respons terhadap ancaman yang lebih kritis. Salah satu metode yang efektif untuk tugas ini adalah algoritma *Naive Bayes*, yang mampu memberikan hasil klasifikasi berdasarkan pola data historis(Churcher *et al.*, 2021). Dalam konteks PT PLN Batam, analisis log serangan dengan pendekatan ini dapat meningkatkan efisiensi deteksi ancaman, meminimalkan risiko gangguan operasional, dan meningkatkan keamanan jaringan perusahaan.

Oleh karena itu, penelitian ini berfokus pada klasifikasi tingkat ancaman pada log serangan *firewall* menggunakan algoritma *Naive Bayes* di

PT PLN Batam. Hasil penelitian diharapkan dapat memberikan solusi yang efektif untuk mendukung pengelolaan keamanan jaringan perusahaan.

B. Perumusan Masalah

Berdasarkan uraian latar belakang diatas maka dapat diambil perumusan masalah dalam penelitian ini adalah :

1. Bagaimana cara mengolah dan menganalisis data log serangan *firewall* di PT PLN Batam agar dapat digunakan untuk klasifikasi tingkat ancaman?
2. Bagaimana performa algoritma *Naive Bayes* dalam mengklasifikasikan tingkat ancaman berdasarkan log serangan *firewall*?

C. Batasan Masalah

Agar fokus penelitian tetap terjaga dan tidak meluas dari inti pembahasan, penelitian ini diberi batasan-batasan berikut.

1. Penelitian hanya berfokus pada log serangan yang tercatat oleh *firewall* di PT PLN Batam.
2. Algoritma yang digunakan dalam penelitian ini adalah *Naive Bayes* tanpa membandingkan dengan algoritma lain.
3. Data log serangan yang digunakan adalah data historis dari periode tertentu yang tersedia selama penelitian.
4. Hasil klasifikasi dibatasi pada tiga tingkat ancaman: *High, Medium*, dan *Low*

D. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengklasifikasi tingkat ancaman pada log serangan *firewall* di PT PLN Batam menggunakan algoritma *Naive Bayes*, sehingga dapat membantu tim keamanan jaringan dalam mendeteksi dan memprioritaskan ancaman secara lebih efisien.

E. Manfaat Penelitian

Untuk memahami pentingnya penelitian ini perlu dijelaskan manfaat yang diharapkan dapat dicapai. Adapun manfaat dari penelitian ini antara lain :

1. Bagi Perusahaan: Memberikan solusi yang dapat meningkatkan efisiensi deteksi ancaman dan respons keamanan jaringan di PT PLN Batam.
2. Bagi Peneliti Lain: Menambah referensi mengenai penggunaan algoritma *Naive Bayes* untuk analisis log serangan *firewall*.
3. Bagi Akademisi: Memberikan kontribusi terhadap perkembangan studi di bidang keamanan jaringan dan pembelajaran mesin.