BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Keamanan jaringan adalah faktor penting dalam era digital pada saat ini, terutama pada pengamanan informasi yang ada pada jaringan. Salah satu faktor penting dalam bidang teknologi informasi yaitu keamanan jaringan komputer, hal tersebut berguna untuk melindungi data suatu organisasi yang dianggap penting. Jaringan komputer harus bisa memberikan keamanan bagi pengguna untuk menjaga informasi data pribadi dari penyusup. Meningkatnya pertumbuhan internet dapat menyebabkan peningkatan serangan yang mengeksploitasi protokol dan aplikasi internet yang rentan. Indonesia pada tahun 2019 menduduki peringkat ke-9 dari 157 negara berdasarkan data ancaman keamanan internet yang dirilis oleh Symantec, dengan ancaman kejahatan *cyber* yang paling banyak terdeteksi pada tahun 2018 (Navirgo & Habibbullah, 2019).

Intrusion Detection System (IDS) merupakan suatu sistem yang berguna untuk mendeteksi pola dan aktivitas mencurigakan yang memungkinkan terjadinya serangan melalui proses pemantauan lalu lintas jaringan (Jupriyadi, 2018). Sistem deteksi intrusi bisa dimanfaatkan untuk membaca dan mendeteksi aktivitas mencurigakan yang dapat memasuki jaringan dan menemukan celah pada komputer untuk melakukan serangan atau eksperimen dan menganalisis situasi intrusi. Untuk mendeteksi aktivitas mencurigakan pada jaringan, diperlukan bantuan IDS. IDS memberikan garis pertahanan pertama yang sangat penting terhadap intrusi (Baraas *et al* ., 2019). IDS adalah fungsi atau kemampuan perangkat keras untuk mencari, menganalisis, dan mendeteksi aktivitas mencurigakan pada komputer yang umumnya terdapat pada jaringan.

Data mining merupakan proses yang dapat dimanfaatkan dalam menciptakan hubungan antar data untuk menarik kesimpulan dari data tersebut. Data yang digunakan untuk penelitian, dapat diolah menjadi pengetahuan, informasi, dan data serangan pada IDS dapat diklasifikasikan. Teknik pengenalan

pola dengan menggunakan matematika untuk penyelesaian merupakan teknik yang digunakan dalam *data mining*. Data serangan pada IDS terlalu banyak dan perlu dilakukan analisa di kemudian hari. Hal tersebut dapat mengakibatkan kehilangan waktu dan biaya yang besar. Teknik *data mining* digunakan sebagai solusi untuk melakukan analisa terhadap data IDS, yang akan membantu dalam mengklasifikasikan data serangan seperti serangan *denial of services, probe, user to root,* dan *r2l* serta aktivitas jaringan normal. Algoritma C4.5 merupakan algoritma yang sering digunakan untuk klasifikasi. Algoritma tersebut dapat membuat pohon keputusan serta menyajikan aturan pada pohon keputusan yang dapat digunakan untuk membantu menemukan hubungan dan pola dalam data yang tersembunyi (Baraas *et al* ., 2019).

Berdasarkan masalah di atas, penelitian akan dilakukan untuk mengklasifikasikan serangan jaringan dengan menggunakan algoritma *data mining* C4.5 pada data *intrusion detection system*.

1.2 PERUMUSAN MASALAH

Rumusan masalah pada penelitian ini berdasarkan latar belakang adalah efektivitas klasifikasi serangan pada sistem deteksi intrusi yang masih rendah dan belum terstruktur. Oleh karena itu, perlu dilakukan klasifikasi serangan jaringan dengan menerapkan *data mining* menggunakan algoritma C4.5 untuk meningkatkan klasifikasi serangan yang terdapat pada *intrusion detection system* dan sejauh mana perbaikan tersebut dapat memberikan kontribusi dalam meningkatkan keamanan jaringan.

1.3 PERTANYAAN PENELITIAN

1. Bagaimana model pohon keputusan *(decision tree)* yang dibangun dengan algoritma C4.5 untuk klasifikasi serangan pada *intrusion detection system*?
2. Bagaimana tingkat akurasi dari metode algoritma C4.5 untuk klasifikasi serangan jaringan?

1.4 TUJUAN PENELITIAN

Adapun tujuan yang ingin dicapai pada penelitian ini adalah menerapkan algoritma *data mining* C4.5 untuk klasifikasi serangan pada *Intrusion Detection System* (IDS) dengan mengetahui anomali pada jaringan.

1.5 MANFAAT HASIL PENELITIAN

Manfaat yang diharapkan dari penelitian ini antara lain:

1. Memberi pengetahuan mengenai penggunaan *data mining* dengan menerapkan algoritma C4.5 untuk klasifikasi serangan jaringan.
2. Membantu mengklasifikasikan jaringan supaya dapat meminimalisir serangan pada jaringan internet, hasil deteksi serangan dapat digunakan sebagai bahan evaluasi sistem pada aktivitas jaringan anomali guna penanganan oleh sysadmin.