BAB I
PENDAHULUAN

1.1 Latar Belakang

Sebuah Keamanan jaringan komputer saat ini menghadapi tantangan besar akibat meningkatnya volume data dan kompleksitas ancaman siber [8]. Salah satu ancaman yang sulit diidentifikasi adalah serangan pemindaian jaringan atau *Ipsweep*. Aktivitas ini bertujuan memetakan alamat IP aktif sebelum melakukan serangan yang lebih besar [14]. Masalah muncul karena serangan ini sering dilakukan secara perlahan guna menghindari deteksi sistem keamanan konvensional yang kaku [1].

Kenyataan di lapangan menunjukkan sistem keamanan sering mengalami kesulitan membedakan aktivitas pengguna sah dengan serangan *Ipsweep*. Karakteristik serangan ini sengaja dirancang meniru pola lalu lintas data normal sehingga sering lolos dari pemantauan administrator [4]. Jika tahap pemindaian tidak dideteksi sejak dini, risiko penyusupan dan pencurian data pada infrastruktur jaringan akan meningkat [19]. Kondisi ini menuntut adanya metode deteksi yang lebih responsif.

Peneliti menemukan bahwa pendekatan berbasis aturan statis sudah tidak lagi optimal dalam menangani data jaringan yang sangat besar dan dinamis. Penggunaan teknologi *Machine Learning* menjadi relevan karena mampu mengolah ribuan baris data secara otomatis [2]. Meskipun beberapa metode lain telah dikembangkan untuk mengoptimalkan fitur deteksi [15], pemilihan algoritma tunggal yang efisien dalam mengenali pola kepadatan tetap menjadi kunci utama akurasi deteksi anomali [10].

Peneliti berupaya mengatasi permasalahan tersebut dengan menerapkan algoritma *clustering* DBSCAN. Algoritma ini dipilih karena memiliki keunggulan dalam mendeteksi data yang tidak memenuhi syarat kepadatan sebagai anomali atau *noise* [3]. Gagasan ini muncul untuk melihat sejauh mana algoritma berbasis kepadatan mampu mengisolasi serangan *Ipsweep* pada dataset NSL-KDD [6]

melalui validasi *Silhouette Score* [5]. Penelitian ini diharapkan memberikan solusi deteksi dini yang efektif bagi keamanan jaringan

1.2 Rumusan Masalah

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

1. Bagaimana kemampuan algoritma DBSCAN dalam mengidentifikasi serangan *Ipsweep* sebagai anomali pada dataset NSL-KDD?
2. Seberapa efektif penggunaan metrik *Silhouette Score* dan visualisasi *scatter plot* dalam mengevaluasi hasil pemisahan antara serangan *Ipsweep* dan lalu lintas jaringan normal yang memiliki karakteristik fitur serupa?

1.3 Batasan Masalah

Agar penelitian ini tetap terfokus dan tidak menyimpang dari tujuan utama, maka ditetapkan batasan masalah sebagai berikut:

1. Data yang digunakan adalah dataset publik NSL-KDD yang diperoleh dari *UCI Machine Learning Repository*.
2. Penelitian difokuskan pada deteksi serangan jenis *Ipsweep* yang termasuk dalam kategori serangan *Probing*.
3. Algoritma yang digunakan dalam proses identifikasi anomali hanya terbatas pada metode *Density-Based Spatial Clustering of Applications with Noise* (DBSCAN).
4. Parameter yang akan diuji dan dioptimalkan dalam penelitian ini adalah nilai *epsilon* (eps) dan *minimum samples* (min_samples).
5. Evaluasi hasil pengelompokan hanya menggunakan metrik *Silhouette Score* dan visualisasi *scatter plot* dua dimensi.
6. Penelitian ini dilakukan dalam lingkungan simulasi menggunakan bahasa pemrograman Python dan tidak diujikan pada lalu lintas jaringan secara langsung (*real-time*).

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai oleh peneliti dalam penelitian ini adalah sebagai berikut:

1. Untuk mengimplementasikan algoritma DBSCAN dalam mengidentifikasi serangan *Ipsweep* sebagai anomali pada dataset NSL-KDD.
2. Untuk mengevaluasi efektivitas penggunaan metrik *Silhouette Score* dan visualisasi *scatter plot* dalam memvalidasi hasil pemisahan antara data serangan dan data normal yang memiliki karakteristik fitur serupa.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan kegunaan baik secara teknis maupun non-teknis bagi berbagai pihak, yaitu:

1. **Manfaat Teoritis (Bagi Peneliti Selanjutnya)** Memberikan kontribusi bagi pengembangan literatur mengenai penerapan algoritma *Density-Based Spatial Clustering of Applications with Noise* (DBSCAN) dalam bidang keamanan jaringan. Penelitian ini juga dapat menjadi referensi bagi peneliti selanjutnya dalam mengkaji penggunaan metrik evaluasi seperti *Silhouette Score* pada dataset yang memiliki tingkat kerapatan fitur yang tinggi antara data normal dan serangan.
2. **Manfaat Praktis (Bagi Administrator Jaringan atau Organisasi)** Memberikan gambaran teknis mengenai efektivitas algoritma berbasis kepadatan dalam mengidentifikasi pola serangan *Ipsweep* secara otomatis. Hasil analisis ini dapat dimanfaatkan oleh administrator jaringan sebagai dasar dalam merancang sistem pendeteksi gangguan yang lebih responsif, sehingga mampu meminimalisir risiko penyusupan yang dilakukan melalui tahap pemindaian jaringan (*scanning*).

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun secara sistematis untuk memberikan gambaran menyeluruh mengenai alur penelitian, yang terbagi ke dalam bab-bab sebagai berikut:

BAB I: PENDAHULUAN Bab ini menguraikan latar belakang pemilihan topik, rumusan masalah yang menjadi fokus penelitian, batasan masalah agar penelitian tetap terarah, tujuan yang ingin dicapai, manfaat penelitian, serta sistematika penulisan secara keseluruhan.

BAB II: TINJAUAN PUSTAKA Bab ini berisi landasan teori dan tinjauan pustaka yang relevan dengan objek penelitian. Materi yang dibahas meliputi konsep dasar keamanan jaringan, karakteristik serangan *Ipsweep*, penjelasan teknis mengenai dataset NSL-KDD, serta prinsip kerja algoritma *Density-Based Spatial Clustering of Applications with Noise* (DBSCAN).

BAB III: METODOLOGI PENELITIAN Bab ini menjelaskan tahapan yang dilakukan dalam penelitian, mulai dari pengumpulan data, prosedur *preprocessing* data seperti *scaling* dan *encoding*, hingga alur kerja penerapan algoritma DBSCAN dalam mendeteksi anomali. Selain itu, bagian ini juga memuat rancangan pengujian menggunakan metrik *Silhouette Score*.

BAB IV: HASIL DAN PEMBAHASAN Bab ini merupakan bagian utama yang menyajikan hasil implementasi algoritma pada dataset. Di dalamnya terdapat analisis terhadap hasil *clustering*, visualisasi sebaran data menggunakan *scatter plot*, serta evaluasi terhadap efektivitas algoritma dalam mengidentifikasi serangan *Ipsweep* sebagai anomali.

BAB V: PENUTUP Bab ini menyajikan kesimpulan yang ditarik dari hasil penelitian dan pengujian yang telah dilakukan. Selain itu, bab ini juga memuat saran-saran dari peneliti untuk pengembangan penelitian selanjutnya agar hasil deteksi anomali dapat lebih optimal.