

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi yang semakin pesat membawa dampak besar dalam berbagai bidang terutama dalam pengelolaan jaringan komputer [1]. Berbagai instansi dan perusahaan bergantung pada jaringan yang aman dan stabil untuk menunjang operasionalnya. Namun dengan meningkatnya ketergantungan terhadap sistem berbasis jaringan risiko serangan siber pun semakin tinggi [2]. Salah satu ancaman yang sering terjadi adalah serangan *brute force* yaitu metode serangan yang dilakukan dengan mencoba berbagai kombinasi *username* dan *password* secara otomatis hingga menemukan kredensial yang benar [3].

Serangan *brute force* berpotensi menimbulkan berbagai ancaman, seperti pengambilalihan akun, akses tidak sah ke sistem, serta pencurian data sensitif. Dalam lingkungan perusahaan terutama yang menggunakan perangkat jaringan seperti Mikrotik, serangan ini dapat berdampak pada gangguan operasional dan menurunkan tingkat keamanan sistem [4]. PT Pelindo Daya Sejahtera sebagai perusahaan yang memiliki infrastruktur jaringan berbasis Mikrotik, juga menghadapi tantangan serupa. Berdasarkan hasil observasi selama 2 bulan di PT Pelindo Daya Sejahtera, ditemukan bahwa terdapat banyak percobaan *login* gagal dalam *log autentikasi* Mikrotik, yang berpotensi mengindikasikan adanya upaya *brute force attack*.

Untuk mengatasi serangan *brute force*, umumnya perusahaan menerapkan metode berbasis aturan (*rule-based detection*) dengan *firewall* Mikrotik yang secara otomatis memblokir IP yang gagal *login* berulang kali dalam waktu singkat [5]. Meskipun metode ini cukup efektif, namun memiliki beberapa keterbatasan, seperti tidak dapat mengenali pola serangan yang lebih kompleks, serta rentan terhadap *false positive*, di mana pengguna sah bisa saja terblokir akibat kesalahan *login* yang tidak disengaja [6]. Oleh karena itu diperlukan pendekatan yang lebih adaptif dalam mendeteksi serangan *brute force* dengan tingkat akurasi yang lebih baik.

Salah satu solusi yang dapat meningkatkan efektivitas deteksi serangan *brute force* adalah menggunakan *machine learning*. Pendekatan ini memungkinkan

sistem untuk belajar dari pola trafik *autentikasi* dan membedakan antara akses sah dan serangan. *Random Forest*, sebagai salah satu algoritma *machine learning* yang handal dalam klasifikasi data, dapat digunakan untuk menganalisis fitur seperti jumlah percobaan *login*, *IP* sumber, *username*, *protocol*, serta status *autentikasi* [7]. Keunggulan algoritma ini terletak pada kemampuannya dalam menangani dataset yang kompleks serta menghasilkan prediksi yang lebih akurat dibandingkan metode *rule base* [8].

Pada penelitian yang dilakukan oleh Khazin Mubarak dan Moh. Ali Romli, yang berjudul “Implementasi Metode *Rule Based* dalam Mendeteksi Serangan *Brute force* pada *Owncloud*”, metode *rule-based detection* digunakan untuk mengidentifikasi pola serangan *brute force* dengan menetapkan aturan tetap, seperti memblokir IP yang melakukan sejumlah percobaan *login* gagal dalam periode tertentu. Pendekatan ini cukup efektif dalam mendeteksi serangan sederhana, namun memiliki keterbatasan dalam mengenali pola serangan yang lebih kompleks dan dapat beradaptasi dengan perubahan teknik penyerang. Selain itu, metode *rule-based* sering kali menghasilkan *false positive*, di mana pengguna sah dapat terblokir akibat kesalahan *login* yang tidak disengaja. Hingga saat ini belum ditemukan penelitian yang secara khusus menerapkan algoritma *Random Forest* untuk mendeteksi serangan *brute force* berdasarkan *log autentikasi* Mikrotik, terutama dalam lingkungan jaringan di PT Pelindo Daya Sejahtera. Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan mengembangkan sistem deteksi serangan *brute force* berbasis *machine learning* yang lebih akurat dan adaptif dibandingkan dengan metode *rule-based* yang telah ada[6].

Penelitian ini akan berfokus pada deteksi serangan *brute force* dengan menggunakan algoritma *random forest* berdasarkan studi kasus di PT Pelindo Daya Sejahtera. Data *log autentikasi* Mikrotik dari perusahaan ini akan digunakan sebagai dataset utama dalam proses pengujian model. Dengan memanfaatkan data nyata, penelitian ini diharapkan dapat memberikan solusi yang lebih aplikatif dalam meningkatkan keamanan jaringan di lingkungan perusahaan. Model yang dikembangkan akan menganalisis pola percobaan *login* untuk mengidentifikasi apakah suatu aktivitas mencurigakan merupakan serangan *brute force* atau bukan,

sehingga *administrator* jaringan dapat mengambil tindakan yang lebih cepat dan akurat [9].

Tujuan utama dari penelitian ini adalah untuk mengembangkan sistem deteksi otomatis terhadap serangan *brute force* menggunakan *machine learning*, yang dapat menganalisis *log autentikasi* secara *real-time* dan memberikan hasil klasifikasi yang akurat. Dengan pendekatan ini sistem keamanan jaringan dapat lebih adaptif dalam mengenali pola serangan dan meminimalkan *false positive*. Hasil yang diharapkan adalah model deteksi serangan *brute force* yang efektif, dengan tingkat akurasi yang tinggi, serta mampu diterapkan dalam lingkungan operasional PT Pelindo Daya Sejahtera dan perusahaan lainnya yang menggunakan mikrotik sebagai perangkat jaringan.

Berdasarkan paparan di atas, dapat disimpulkan bahwa serangan *brute force* merupakan ancaman yang nyata bagi keamanan jaringan perusahaan [10], termasuk di PT Pelindo Daya Sejahtera. Pendekatan berbasis aturan memiliki keterbatasan dalam mengenali pola serangan yang semakin kompleks, sehingga penerapan *Machine learning*, khususnya dengan algoritma *Random Forest*, menjadi solusi yang lebih adaptif dan akurat. Dengan adanya model deteksi otomatis berbasis *Machine learning*, perusahaan dapat meningkatkan sistem keamanannya dengan lebih efisien. Oleh karena itu, penelitian ini memiliki signifikansi yang tinggi dalam mendukung pengembangan sistem keamanan jaringan yang lebih tangguh di lingkungan industri.

1.2. Perumusan Masalah

Dalam penguraian masalah ini, terdapat tiga poin yang perlu dijelaskan: permasalahan yang ada, solusi/metode yang diusulkan, dan pertanyaan penelitian yang hendak dijawab dalam penelitian ini.

1.2.1. Permasalahan

Serangan *brute force* merupakan salah satu ancaman keamanan yang sering terjadi dalam sistem jaringan perusahaan, termasuk di PT Pelindo Daya Sejahtera. Serangan ini dilakukan dengan mencoba berbagai kombinasi *username* dan *password* secara berulang hingga mendapatkan akses yang sah. Jika tidak terdeteksi

dengan baik, serangan ini dapat menyebabkan akses tidak sah, pencurian data, serta potensi eksploitasi lebih lanjut terhadap sistem jaringan.

1.2.2. Metode Usulan

Penelitian ini akan menggunakan pendekatan *machine learning*, khususnya algoritma *Random Forest*, untuk mendeteksi serangan *brute force* berdasarkan *log autentikasi* Mikrotik di PT Pelindo Daya Sejahtera. Model ini akan dikembangkan dengan menganalisis pola *autentikasi* pengguna, sehingga dapat membedakan antara aktivitas *login* yang sah dan percobaan serangan *brute force*.

1.2.3. Pertanyaan Penelitian

Pertanyaan Penelitian yang dijawab dalam penelitian ini meliputi :

1. Bagaimana penerapan algoritma *Random Forest* dalam membangun model deteksi serangan *brute force* pada *log autentikasi* Mikrotik?
2. Sejauh mana tingkat akurasi model yang dihasilkan menggunakan metode *Random Forest* pada data *log autentikasi* Mikrotik PT Pelindo Daya Sejahtera?

1.3. Tujuan dan Manfaat

1.3.1. Tujuan Penelitian

Tujuan utama dalam penelitian ini adalah untuk :

1. Mendeteksi serangan *brute force* pada sistem autentikasi Router MikroTik dengan memanfaatkan algoritma *Random Forest* sebagai metode klasifikasi terhadap *log autentikasi*.
2. Mengevaluasi performa model yang dihasilkan, dengan mengukur tingkat akurasi, *precision*, *recall*, dan *F1-score* pada *Log autentikasi* mikrotik PT Pelindo Daya Sejahtera.

1.3.2. Manfaat Penelitian

Manfaat dalam penelitian ini adalah :

1. Memberikan solusi dalam mendeteksi serangan *brute force* secara otomatis berdasarkan *log autentikasi*, sehingga membantu *administrator* jaringan dalam mencegah akses tidak sah secara lebih cepat dan akurat.

2. Meningkatkan pemahaman dan penerapan *machine learning*, khususnya algoritma *Random Forest*, dalam konteks keamanan jaringan berbasis analisis *log*.
3. Menjadi referensi bagi peneliti selanjutnya yang berfokus pada deteksi intruksi dan sistem keamanan berbasis *log* analisis.

1.4. Batasan-batasan

Adapun batasan-batasan dalam penelitian ini meliputi :

1. Objek penelitian ini terbatas pada *log autentikasi* mikrotik yang digunakan di PT Pelindo Daya Sejahtera, sehingga hasil penelitian ini lebih spesifik untuk lingkungan jaringan yang menggunakan perangkat tersebut.
2. Jenis serangan yang dideteksi dalam penelitian ini hanya serangan *brute force*, yang ditandai dengan percobaan *login* berulang dalam periode tertentu menggunakan kombinasi *username* dan *password* yang berbeda.
3. Data yang digunakan dalam penelitian ini diperoleh dari *log autentikasi* Mikrotik, yang mencakup informasi seperti IP sumber, username, login, protocol, waktu percobaan, dan status *autentikasi* (sukses/gagal).
4. Metode *machine learning* yang digunakan dalam penelitian ini adalah *random forest*, tanpa melakukan perbandingan dengan metode lain seperti SVM atau *deep learning*.

1.5. Sistematika Penelitian

BAB I : PENDAHULUAN

Menjelaskan mengenai latar belakang, perumusan masalah, permasalahan, metode penelitian, pertanyaan penelitian, tujuan dan manfaat penelitian, batasan masalah, serta sistematika penulisan terkait penelitian.

BAB II : KAJIAN PUSTAKA

Kajian Pustaka berisi landasan teori berkaitan dengan Keamanan Jaringan *Brute force*, Mikrotik, *Machine learning*, *Random Forest* serta evaluasi model dan penelitian terkait.

BAB III : METODE PENELITIAN

Menjelaskan perancangan sistem yang mencakup dataset *log autentikasi mikrotik*, arsitektur sistem metode algoritma, *preprocessing* data, modeling dan skenario pengujian sistem.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini berisi penyajian hasil implementasi dan evaluasi dari sistem deteksi *brute force login* menggunakan algoritma *Random Forest*. Di dalamnya dijelaskan performa model berdasarkan akurasi, visualisasi *heatmap* parameter, *confusion matrix*, serta laporan klasifikasi yang menggambarkan kemampuan model dalam membedakan aktivitas *login* normal dan serangan. Selain itu, ditampilkan pula integrasi sistem ke *router MikroTik* dan hasil pengujian di lingkungan nyata.

BAB V : KESIMPULAN

Bab ini memuat kesimpulan dari hasil penelitian yang telah dilakukan, yang menjawab pertanyaan penelitian terkait efektivitas metode *Random Forest* dalam mendeteksi serangan *brute force* pada *router MikroTik*. Selain itu, disampaikan pula saran yang dapat dijadikan pertimbangan untuk pengembangan sistem atau arah penelitian selanjutnya.