BAB I

PENDAHULUAN

1.1 Latar Belakang

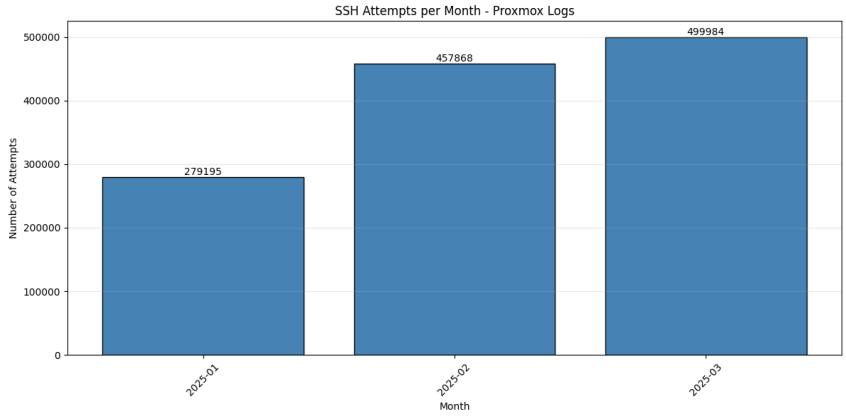
Keamanan akses jarak jauh merupakan aspek krusial dalam pengelolaan infrastruktur server. Salah satu protokol yang paling umum digunakan adalah *Secure Shell* (SSH) karena kemampuannya dalam menyediakan komunikasi terenkripsi dan akses administratif penuh terhadap sistem. Banyaknya tingkat adopsi SSH menjadikan vektor serangan yang paling sering dieksploitasi oleh pelaku ancaman siber, khususnya melalui serangan *brute force* terhadap mekanisme autentikasi SSH. Serangan *brute force* sendiri telah menyumbang kerugian ekonomi global hingga $2,5 miliar per tahun [1].

Dalam menjalankan operasional bisnis, PT Maro Anugrah Jaya bergantung pada infrastruktur server berbasis Proxmox [2]. Proxmox adalah platform virtualisasi *open-source* untuk mengelola mesin virtual dan kontainer secara terpusat [3]. Infrastruktur server perusahaan terdiri atas dua server Proxmox, yaitu satu server utama dan satu server cadangan. Server utama mengoperasikan 1 mesin virtual dan 12 kontainer yang menangani berbagai layanan bisnis penting seperti *website*, *database*, serta aplikasi internal perusahaan [2]. Layanan tersebut mencakup beberapa unit usaha dan sub-merek, termasuk Bowbo Xpress, Bowbo Munchies, Bowbo Dimsum, serta platform administratif milik anak perusahaan, PT Maro Kuliner Nusantara dan PT Wadah Berkah Nusantara Jaya [2]. Dengan rencana ekspansi ke sektor bisnis lainnya, kebutuhan akan keamanan infrastruktur server menjadi semakin krusial.

Sebagai upaya mitigasi awal terhadap ancaman akses tidak sah, PT Maro Anugrah Jaya telah menerapkan mekanisme keamanan berbasis aturan dengan memasang Fail2Ban pada server Proxmox. Fail2Ban digunakan untuk memantau log autentikasi sistem dan secara otomatis memblokir alamat IP yang melakukan percobaan login gagal secara berulang dalam rentang waktu tertentu [4]. Pendekatan ini bertujuan untuk menekan serangan *brute force*.

Namun, meskipun Fail2Ban telah diterapkan, aktivitas serangan terhadap layanan SSH menunjukkan bahwa tidak seluruh percobaan serangan dapat ditangani secara efektif. Hal ini disebabkan oleh karakteristik sistem keamanan berbasis aturan yang sangat bergantung pada ambang batas statis, seperti jumlah kegagalan login dan jendela waktu tertentu. Penyerang yang memahami pola kerja mekanisme ini dapat menyesuaikan strategi serangan agar tetap berada di bawah ambang deteksi, sehingga aktivitas berbahaya tidak memicu pemblokiran otomatis.

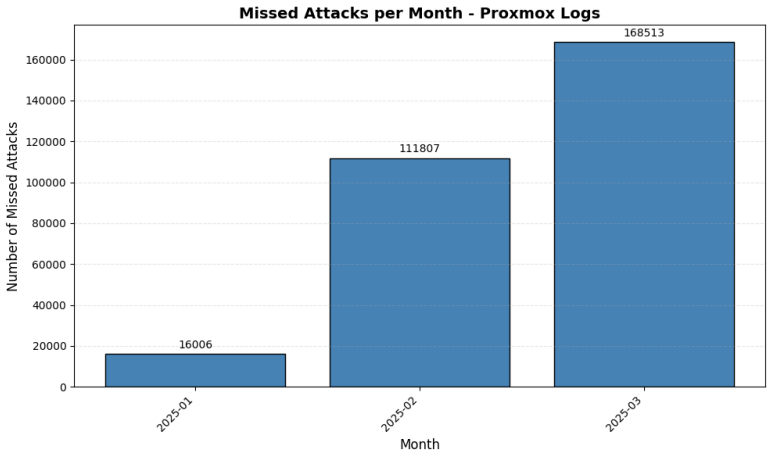
Analisis awal terhadap log autentikasi SSH selama tiga bulan terakhir mengindikasikan adanya perbedaan pola aktivitas percobaan login. Sebagian percobaan menunjukkan karakteristik frekuensi tinggi dalam waktu singkat yang umumnya dapat ditangani oleh mekanisme Fail2Ban. Di sisi lain, adapun percobaan login gagal dengan frekuensi rendah dan interval waktu yang lebih panjang, serta berasal dari alamat IP yang bervariasi. Aktivitas dengan karakteristik tersebut tidak memicu pemblokiran otomatis oleh Fail2Ban. Berbeda dengan *brute force* cepat, serangan dengan interval panjang dan volume serangan rendah diklasifikasikan sebagai *slow-rate* [7]. Teknik ini memanfaatkan *botnet* terdistribusi dan rotasi alamat IP, membuatnya menyerupai aktivitas pengguna normal dan sulit diidentifikasi oleh sistem deteksi berbasis aturan [8].



Gambar 1.1 Grafik Percobaan Serangan SSH

Berdasarkan gambar 1.1, jumlah percobaan serangan SSH terhadap server PT Maro Anugrah Jaya menunjukkan peningkatan signifikan dari Januari hingga Maret 2025. Pada Januari 2025, tercatat sebanyak 279.185 ribu kali

percobaan login gagal. Angka ini meningkat tajam pada Februari 2025 menjadi 457.868 kali percobaan, dan kembali naik pada Maret 2025 hingga mencapai 499.984 kali percobaan. Peningkatan dari bulan ke bulan ini menunjukkan adanya eskalasi aktivitas serangan SSH yang bersifat agresif. Tren ini mengindikasikan bahwa infrastruktur perusahaan menjadi target utama bagi pelaku serangan otomatis yang terus mencoba mengeksploitasi kredensial login server secara paksa.



Gambar 2.2 Grafik Percobaan Serangan SSH yang dilewatkan Fail2Ban

Dengan menerapkan Fail2Ban, berdasarkan gambar 1.2, jumlah *missed attacks* mengalami peningkatan signifikan dari bulan ke bulan. Pada Januari 2025 tercatat sebanyak 16.006 percobaan login yang tidak terdeteksi oleh Fail2Ban. Jumlah ini meningkat tajam pada Februari 2025 menjadi 111.807 percobaan, dan kembali meningkat pada Maret 2025 hingga mencapai 168.513 percobaan. Tren ini menunjukkan bahwa meskipun jumlah total percobaan login dapat ditekan melalui mekanisme berbasis aturan, sebagian aktivitas serangan tetap berlangsung secara persisten tanpa menghasilkan peringatan atau pemblokiran otomatis.

Masalah yang dihadapi PT Maro Anugrah Jaya adalah cerminan dari tren ancaman siber yang lebih luas, baik di tingkat nasional maupun global. Laporan Badan Siber dan Sandi Negara (BSSN) tahun 2024 mencatat bahwa Indonesia mengalami lebih dari 360 juta insiden serangan siber sepanjang tahun 2024, menjadikannya salah satu target utama secara global [4]. Kondisi ini diperburuk oleh meningkatnya layanan akses jarak jauh akibat transformasi digital dan

kebijakan *work from home* pasca pandemi COVID-19, yang memperluas permukaan serangan dan membuat pertahanan jaringan semakin kompleks [6].

Pada PT Maro Anugrah Jaya, mekanisme *public key* atau penggunaan kunci SSH belum seluruhnya diadopsi secara menyeluruh. Akses SSH pada infrastruktur server perusahaan saat ini masih bergantung pada autentikasi berbasis *username* dan *password* yang dikelola secara terpusat.

Penerapan autentikasi berbasis kunci, meskipun secara teoritis lebih aman, perusahaan menghadapi tantangan dalam pengelolaan kunci apabila harus didistribusikan kepada banyak pengguna atau pihak ketiga, terutama tanpa mekanisme manajemen kunci, rotasi, dan pencabutan akses yang terstandarisasi, sehingga berpotensi menimbulkan risiko kebocoran atau penyalahgunaan. Selain itu, pemfilteran akses berbasis alamat IP menjadi kurang fleksibel untuk diterapkan mengingat pola kerja yang dinamis dan adanya kebutuhan akses jarak jauh dari lokasi yang beragam, termasuk skema kerja jarak jauh (*work from home*).

Meskipun Fail2Ban mampu menekan serangan *brute force* berintensitas tinggi, ancaman utama yang dihadapi PT Maro Anugrah Jaya bukan hanya tingginya jumlah percobaan login, tetapi ketidakmampuan sistem keamanan yang ada dalam mendeteksi upaya akses tidak sah yang bersifat persisten dan tersembunyi. Ancaman ini berpotensi memberikan akses administratif ke server Proxmox, yang dapat berdampak pada pencurian data, perubahan konfigurasi sistem, hingga gangguan layanan bisnis perusahaan. PT Maro Anugrah Jaya membutuhkan mekanisme deteksi dini yang mampu mengidentifikasi pola serangan secara proaktif, dengan target menurunkan tingkat *False Negative* (serangan yang tidak terdeteksi) terhadap pola *slow-rate* yang selama ini lolos dari pemantauan sistem berbasis aturan.

Teknologi pembelajaran mesin, khususnya dengan algoritma *Long Short-Term Memory* (LSTM), menawarkan pendekatan yang lebih adaptif dalam mendeteksi anomali temporal [9]. Berbeda dengan sistem berbasis aturan yang bergantung pada variabel statis, LSTM dapat mempelajari pola perilaku normal dan abnormal dalam suatu jendela waktu [10]. Kemampuan LSTM dalam mempertahankan informasi jangka panjang diharapkan menjadikan LSTM

sebagai algoritma yang relevan untuk mendeteksi pola serangan *slow-rate* [11]. Pendekatan ini diharapkan mampu menjawab kebutuhan akan sistem deteksi intrusi yang lebih proaktif, aplikatif, sekaligus memberikan kontribusi dalam meningkatkan keamanan infrastruktur server PT Maro Anugrah Jaya.

1.2 Pertanyaan Penelitian

Berdasarkan latar belakang yang sudah dipaparkan, rumusan masalah pada penelitian ini terdiri dari beberapa poin, yaitu:

RQ1 Sejauh mana efektivitas model LSTM dalam mendeteksi ragam serangan SSH berdasarkan log autentikasi, diukur menggunakan metrik akurasi, presisi, *recall*, dan *F1-score*?

RQ2 Bagaimana karakteristik serangan SSH *slow-rate* dapat dianalisis dan dibedakan dari *brute force* cepat untuk mendukung proses deteksi?

RQ3 Bagaimana performa sistem deteksi intrusi berbasis pembelajaran mesin ketika diimplementasikan dalam skenario nyata, ditinjau dari aspek tingkat deteksi?

1.3 Batasan Penelitian

Berdasarkan identifikasi masalah yang sudah disebutkan, berikut batasan masalah dari penelitian ini:

1.3.1 Jenis serangan SSH yang diteliti mengutamakan fokus pada serangan SSH *brute force* dengan teknik *slow-rate*.

1.3.2 Sistem deteksi intrusi yang dikembangkan belum diimplementasikan dan diuji secara penuh pada lingkungan produksi nyata, melainkan diuji secara eksperimental menggunakan data log SSH eksternal berdasarkan skenario pengujian yang dijelaskan pada bab analisis dan perancangan sistem.

1.3.3 Model pembelajaran mesin yang digunakan terbatas pada arsitektur *Long Short-Term Memory* (LSTM) dengan parameter dan hyperparameter yang ditentukan berdasarkan eksperimen awal.

1.3.4 Data yang digunakan dalam penelitian ini terbatas pada log SSH yang telah dikumpulkan, alamat login IP yang telah dianonimisasi dan tidak mengandung informasi sensitif perusahaan, serta telah mendapatkan persetujuan resmi dari PT Maro Anugrah Jaya untuk keperluan penelitian akademik.

1.3.5 Evaluasi kinerja sistem dibatasi pada perbandingan dengan sistem deteksi berbasis aturan yaitu Fail2Ban, tanpa mencakup perbandingan dengan solusi pembelajaran mesin lainnya atau implementasi pada skala perusahaan yang lebih besar.

1.4 Tujuan Penelitian

Berikut beberapa tujuan dari penelitian ini, yaitu:

1.4.1 Mengidentifikasi dan menganalisis ancaman akses tidak sah pada layanan SSH, khususnya serangan *brute force* dengan karakteristik *slow-rate*, yang tidak dapat dideteksi secara efektif oleh mekanisme keamanan berbasis aturan yang digunakan oleh PT Maro Anugrah Jaya.

1.4.2 Mengembangkan sistem deteksi intrusi berbasis algoritma *Long Short-Term Memory* (LSTM) untuk meningkatkan kemampuan deteksi dini terhadap serangan *slow-rate*, sehingga memberikan visibilitas ancaman yang lebih baik bagi perusahaan.

1.4.3 Menganalisa dan membandingkan kinerja model deteksi intrusi berbasis LSTM dengan mekanisme deteksi berbasis aturan (Fail2Ban) dalam mendeteksi serangan SSH *slow-rate* menggunakan metrik akurasi, presisi, *recall*, dan *F1-score*.

1.4.4 Menilai tingkat deteksi (*detection rate*) sistem yang diusulkan pada skenario pengujian berbasis data historis, dengan target capaian tingkat deteksi yang memadai untuk mendukung pengambilan keputusan keamanan, serta membandingkannya dengan kinerja mekanisme deteksi berbasis aturan (Fail2Ban).

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1.5.1 Memberikan solusi keamanan bagi PT Maro Anugrah Jaya dalam menghadapi ancaman SSH *brute force* dengan teknik *slow-rate*, sekaligus meningkatkan kemampuan pemantauan dan respons terhadap insiden keamanan siber di lingkungan perusahaan.

1.5.2 Menyediakan solusi alternatif yang lebih adaptif dan aplikatif untuk mengatasi keterbatasan sistem keamanan berbasis aturan dalam mendeteksi serangan *slow-rate* pada protokol SSH.

1.5.3 Memberikan kontribusi pada pengembangan ilmu pengetahuan di bidang keamanan siber dan pembelajaran mesin, khususnya dalam deteksi serangan *slow-rate* pada SSH menggunakan algoritma LSTM, serta memperkaya literatur penelitian untuk referensi akademik selanjutnya.

1.6 Sistematika Penulisan

Laporan penelitian ini disusun dengan beberapa bagian untuk mempermudah pembacaan dan pemahaman.

1.6.1 Bab 1 Pendahuluan

Pada bab ini pembahasan mencakup tentang latar belakang, rumusan masalah, batasan penelitian, tujuan penelitian, dan manfaat penelitian dari penelitian yang dilakukan.

1.6.2 Bab 2 Tinjauan Pustaka

Bab ini membahas penelitian terdahulu terkait teori deteksi sarangan SSH menggunakan pembelajaran mesin, metode penelitian yang akan digunakan sebagai referensi penelitian, serta landasan teori mengenai tipe Proxmox, protokol SSH, serangan *brute force*, algoritma LSTM, dan teori lainnya yang digunakan selama penelitian.

1.6.3 Bab 3 Metodologi Penelitian

Bab ini membahas tentang metodologi perancangan model pembelajaran mesin dan perancangan aplikasi, lalu metrik evaluasi baik dari model pembelajaran mesin dan perancangan aplikasi, serta skenario pengujian.

1.6.4 Bab 4 Implementasi dan Pengujian Sistem

Bab ini membahas tentang implementasi sistem, performa hasil pengujian, analisis komparatif dengan sistem deteksi intrusi berbasis aturan, serta evaluasi efektifitas deteksi terhadap serangan *slow-rate*, kendala solusi terhadap masalah yang ditemukan saat melakukan perancangan dan implementasi, serta limitasinya.

1.6.5 Bab 5 Kesimpulan dan Saran

Bab ini membahas kesimpulan hasil penelitian dan saran untuk pengembangan penelitian selanjutnya.