BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Di tengah kemajuan zaman digital yang terus berlanjut, jaringan komputer menjadi bagian penting yang membentuk landasan bagi berbagai aspek kehidupan modern. Keterhubungan yang semakin mendalam antar perangkat dan infrastruktur digital menciptakan ekosistem yang aktif dan penting bagi aktivitas sehari-hari, termasuk komunikasi, perdagangan, serta penyimpanan dan akses data sensitif. Salah satu ancaman utama dalam ekosistem jaringan ini adalah serangan pola trafik, termasuk serangan anomali. Anomali dalam lalu lintas jaringan dapat berupa lonjakan tak terduga dalam volume data, aktivitas akses yang tidak sah, atau perubahan pola yang mencurigakan. Anomali dengan tujuan mencuri informasi sensitif atau kredensial pengguna. Serangan seperti ini dapat memiliki dampak serius pada keamanan informasi dan operasional jaringan. Oleh karena itu, pemahaman yang mendalam tentang serangan pola trafik dan kemampuan untuk mendeteksinya dengan cepat dan efisien menjadi sangat penting bagi administrator jaringan dan profesional keamanan informasi.

Dengan meningkatnya ancaman kejahatan melalui lalu lintas jaringan yang bersifat bolak-balik, institusi perlu memperkuat langkah-langkah preventif dalam strategi keamanan jaringan yang digunakan. Penggunaan perangkat MikroTik Router menjadi langkah penting dalam menghadapi tantangan ini, karena perangkat tersebut dilengkapi dengan fitur-fitur keamanan yang kuat seperti *firewall*, VPN, dan *IDS/IPS* untuk memonitor dan mengelola lalu lintas jaringan dengan lebih efektif. Selain itu, pengelolaan log yang efektif juga diperlukan untuk merekam dan menganalisis aktivitas jaringan yang mencurigakan atau berpotensi berbahaya, sehingga dapat memberikan tanggapan yang cepat dan akurat terhadap ancaman yang muncul.

Penggunaan jaringan internet negatif sering kali mencakup aktivitas seperti hacking untuk meretas sistem, penyebaran malware yang merusak, dan pencarian

anomali dalam infrastruktur jaringan yang dapat menjadi tanda adanya serangan atau kegiatan yang mencurigakan. Namun, melalui analisis perangkat log MikroTik, para administrator jaringan dapat memperoleh wawasan yang lebih dalam tentang pola aktivitas yang tidak biasa atau aneh dalam jaringan mereka. Dengan memantau log MikroTik secara cermat dan menggunakan teknik analisis yang tepat, seperti deteksi pola, identifikasi perilaku yang tidak normal, dan pencarian tanda-tanda serangan, maka dapat lebih mudah untuk menemukan dan menanggapi anomali sebelum mereka menjadi masalah yang lebih besar.

Dalam situasi saat ini yang menuntut keamanan jaringan yang lebih kuat dan pengendalian yang lebih cermat terhadap penggunaan jaringan Wi-Fi, penggunaan MikroTik menjadi suatu keharusan. MikroTik telah menjadi sangat akrab di kalangan pengguna internet di Indonesia, diakui sebagai sistem operasi dan perangkat lunak yang mampu mengubah perangkat komputer biasa menjadi router jaringan yang handal.

Ketidak mampuan untuk merespons insiden dengan cepat dan tepat merupakan masalah lain yang timbul dari keterbatasan akses ini. Tim yang membutuhkan informasi mungkin tidak dapat merespons dengan cepat karena mereka harus menunggu data yang disaring dan disampaikan oleh pengelola utama. Selain itu, ketergantungan pada pengelola utama untuk menyaring dan menyampaikan informasi dapat mengakibatkan interpretasi yang kurang tepat atau informasi yang tidak lengkap, yang dapat mempengaruhi kualitas analisis dan keputusan yang diambil berdasarkan data tersebut.

Implementasi kebijakan akses yang jelas, penggunaan alat anonimisasi data, dan penyediaan laporan yang sesuai dapat menjadi solusi untuk mengatasi masalah ini tanpa mengorbankan aspek keamanan jaringan.

Dengan demikian, penelitian ini berfokus untuk mempelajari cara analisis log MikroTik sebagai bagian dari strategi keamanan jaringan. Untuk menemukan anomali log dari log yang diperoleh dari perangkat mikrotik.Topik penelitian ini yaitu analisis log MikroTik sebagai langkah kunci dalam mendeteksi dan merespons serangan serta pola serangan yang berpotensi berbahaya. Oleh karena itu, penelitian ini akan mengambil bahan mengenai keamanan jaringan, dengan

judul skripsi yang diusulkan adalah “Analisis Log Mikrotik Untuk Mendeteksi Serangan Dan Trafik Anomali Di Jaringan Laboratorium Jaringan Prodi Teknologi Informasi”.

1.1.1 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, penelitian ini terkait analisis log MikroTik untuk mendeteksi adanya aktivitas yang tidak biasa atau tidak sah, seperti anomali trafik, lonjakan dalam lalu lintas jaringan yang berpotensi menjadi ancaman pada jaringan Laboratorium Teknologi Informasi.

1.1.2 Manfaat Hasil Penelitian

Penelitian ini dapat membantu mendeteksi pola serangan, termasuk serangan anomali yang melibatkan lonjakan tak terduga dalam *volume* data, aktivitas akses yang tidak sah, atau perubahan pola yang mencurigakan. Selain itu, penelitian ini juga dapat menjadi landasan bagi implementasi praktis dalam meningkatkan keamanan jaringan di berbagai lingkungan, terutama dalam pencegahan dan deteksi serangan jaringan. Dengan demikian Manfaatnya dapat dirasakan oleh pengguna jaringan di Unjaya seperti, pengelola jaringan, dosen, staff, mahasiswa dan entitas lainnya yang bergantung pada keamanan jaringan untuk menjaga integritas dan ketersediaan data serta layanan mereka.

1.1.3 Perrtanyaan Penelitian

1. Bagaimana kinerja penggunaan perangkat MikroTik Router dan *tools* pihak ketiga seperti Splunk dalam meningkatkan keamanan jaringan dengan memperkuat langkah-langkah pencegahan serta mendeteksi serangan pola trafik dan anomali dalam lalu lintas jaringan?
2. Bagaimana efektivitas penggunaan *tools* pihak ketiga seperti Splunk dalam analisis log jaringan untuk mendeteksi pola atau anomali yang mencurigakan, serta memberikan respons yang cepat terhadap ancaman keamanan?

1.2 TUJUAN PENELITIAN

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Melakukan analisis log jaringan yang dihasilkan oleh perangkat MikroTik guna untuk mendeteksi pola trafik atau anomali yang mencurigakan pada jaringan Laboratorium Prodi Teknologi Informasi.
2. Memahami serangan pola trafik dan anomali dalam lalu lintas jaringan serta dampaknya pada keamanan informasi dan operasional jaringan.