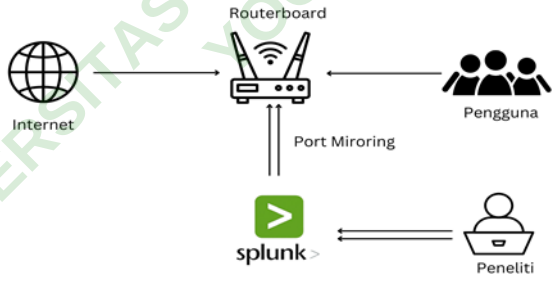
BAB 3
METODE PENELITIAN

Penelitian ini dikosentrasikan untuk menemukan anomali dari sebuah log, Pada penelitian ini juga akan membahas bagaimana menggunakan Splunk untuk melakukan analisis log dari perangkat mikrotik, untuk melancarkan analisis ini penulis akan melakukan port mirroring dan mengatasi tentang penerapan Splunk terhadap analisis file log anomali keamanan. Penelitian ini berfokus pada pendeteksian anomali dari log yang diperoleh dengan cara *port mirroring* dari splunk ke mikrotik, Untuk mencapainya, penelitian ini memerlukan pemeriksaan lebih dalam dengan cara analisis log mikrotik menggunakan Splunk. File *log* yang di kumpulkan dari mikrotik dan di analisis menggunakan Splunk digunakan untuk mendeteksi anomali atau perilaku yang tidak biasa dalam jaringan. Karena utilitas penting ini, penelitian ini akan berusaha menemukan cara yang cepat dan efektif untuk menemukan anomali sistem komputer melalui analisis catatan *log*.



Gambar 3.1 Proses *Port Mirroring*

Dalam upaya untuk memahami dan menganalisis serangan flooding pada jaringan, diperlukan simulasi yang dapat memberikan gambaran nyata tentang bagaimana serangan tersebut terjadi dan berdampak pada sistem jaringan. *Low Orbit Ion Cannon* (LOIC) adalah salah satu alat yang dapat digunakan untuk tujuan ini. LOIC adalah alat sumber terbuka yang sering digunakan untuk melakukan serangan Denial of Service (DoS) dengan mengirimkan sejumlah besar paket ke target

tertentu, sehingga mengakibatkan gangguan pada layanan yang disediakan oleh target tersebut.

Rules mikrotik yang di aktifkan untuk mendapatkan log yaitu aturan floding diantaranya yaitu DNS flood , SSh flood,Telnet flood, SMB flood , SNPP/backdoor flood , Metasploit indication dan *Abnormal Traffic logging.* Alasan pemilihan *rules* MikroTik yang berfokus pada *flooding* adalah karena serangan *flooding* merupakan salah satu jenis serangan yang paling umum dan berbahaya dalam jaringan. Serangan ini dapat menyebabkan penurunan kinerja jaringan, *downtime*, dan bahkan kegagalan total sistem jika tidak terdeteksi dan dimitigasi dengan cepat. Dengan menerapkan *rules* untuk mendeteksi serangan *flooding*, MikroTik dapat memberikan data log yang rinci tentang sumber dan karakteristik serangan, sehingga pengelola jaringan untuk mengambil tindakan yang tepat dan cepat dalam menangani ancaman tersebut.

Penelitian ini berfokus pada kapabilitas dan kapasitas mikrotik sebagai node yang mengirimkan data log ke pihak ketiga**,** dengan fitur logging dan manajemen lalu lintas jaringannya yang lengkap,Mikrotik berperan penting dalam mengumpulkan dan mengirimkan data log yang mendetail tentang aktivitas jaringan.

3.1 ALAT PENELITIAN

Untuk mencapai tujuan penelitian ini, dibutuhkan beberapa alat, berikut adalah penjelasan singkatnya.

3.1.1 Router Mikrotik

Router, juga dikenal sebagai *Router Board*, adalah perangkat keras yang dirancang, diproduksi, dan menggunakan *RouterOS* sebagai sistem operasinya oleh Mikrotik. Perangkat yang menyerupai PC dari segi komponennya, namun memiliki dimensi yang lebih kecil, seperti prosesor, RAM, ROM, dan *Memori Flash*. Sistem operasinya satu - satunya adalah *RouterOS* yang khusus digunakan oleh Mikrotik. *Router Board* memiliki berbagai jangkauan luas jenis arsitektur, model, tipe, dan jumlah antarmuka yang berbeda satu sama lain, sehingga memudahkan kita dalam memilih perangkat ini untuk memenuhi kebutuhan kita. Dari tipe arsitektur, model,

dan jumlah antarmuka yang berbeda satu sama lain, memudahkan kita dalam memilih perangkat ini untuk memenuhi kebutuhan kita.

RouterOS adalah sistem operasi berbasis unix yang memungkinkan PC untuk bertindak sebagai server dan melakukan hampir semua tugas jaringan. *RouterOS* berbeda dari sistem operasi lainnya karena mendukung berbagai jenis *driver hardware*. Jadi, jika *hardware* Mikrotik *RouterOS* tidak mendukung *driver* tertentu, tidak dapat menambah atau menginstal *driver* tambahan, seperti halnya Sistem Operasi. Jika menemukan bahwa perangkat yang dipasangkan Mikrotik *RouterOS* tidak dapat dikenali, maka harus mengirimkan file yang disebut *soppout.rif* ke web Mikrotik untuk mendapatkan file update Mikrotik *RouterOS* terbaru. Setelah dipasang, perangkat akan dapat dikenali oleh Mikrotik *RouterOS.* Ini adalah keunggulan Mikrotik yang selalu terinstall pada semua jenis *RouterBoard* Arfan et al., (2019)

3.1.2 Splunk

Sebuah platform perangkat lunak yang memungkinkan pemantauan, pencarian, analisis, dan visualisasi data yang dihasilkan mesin. Splunk menangkap, mengindeks, dan menghubungkan data secara real-time ke dalam wadah yang dapat dicari, serta menghasilkan dashboard, peringatan, grafik, dan visualisasi yang membuat data mudah dibaca dan dianalisis Ahfaz et al., (2023).

Adapun bebrapa fitur yang di gunakan untuk melancarkan penelitian sebagai berikut:

1. *Server Syslog*: Alat *server syslog* seperti *rsyslog* atau *syslog-ng* untuk menerima log dari perangkat MikroTik dan mengirimkannya ke Splunk untuk analisis lebih lanjut.
2. Skrip dan *Query* Splunk: Skrip dan *query* Splunk yang disesuaikan digunakan untuk melakukan analisis yang lebih mendalam terhadap log MikroTik.
3. Dashboard dan Visualisasi: fitur pembuatan dashboard dan visualisasi data yang digunakan untuk memonitor secara *real-time*

aktivitas jaringan, mendeteksi serangan, dan melihat pola lalu lintas dengan lebih jelas.

3.1.3 *Low Orbit Ion Cannon* (LOIC)

LOIC (*Low Orbit Ion Cannon*)adalah salah satu alat untuk melakukan serangan *DoS* yang ampuh dan tersedia secara gratis. LOIC pada awalnya dikembangkan oleh perusahaan *Praetox Technologies* sebagai alat *testing* sebelum dirilis ke *public*. Alat ini dapat melakukan serangan *DoS* sederhana dengan mengirim paket data dalam jumlah banyak berupa paket UDP, TCP, atau permintaan HTTP ke target yang diserang. Keunggulan dari alat LOIC, selain dapat digunakan secara gratis, cara penggunaannya juga mudah.

Namun LOIC memiliki kelemahan yaitu apabila menggunakan aplikasi ini akan sangat mudah untuk melacak penyerang, karena setiap melakukan penyerangan, IP dari penyerang tidak disamarkan dan terekspos ke pihak korban atau target Aprianto (2023).

3.1.4 Hping3

Merupakan alat jaringan yang dapat mengirim paket TCP/IP secara custom dan mampu menampilkan jawaban dari target. Alat ini tersedia di Kali Linux secara *pre-installed*. Beberapa hal yang dapat dilakukan menggunakan hping3 adalah menguji aturan *firewall*, melakukan *port scanning*, dan menguji performa jaringan. Hping3 dapat juga digunakan untuk mengirim paket secepat mungkin, yakni dengan menggunakan opsi *flood* (Nida & Adrian, 2023).

3.2 JALAN PENELITIAN

Gambar 3.2 Proses Jalanya Penelitian

Gambar 3.1 menunjukkan bahwa penelitian ini dibagi menjadi beberapa tahapan untuk menyelesaikannya. Tahapan jalan penelitian tersebut adalah sebagai berikut:

1. Sebelum memulai tahap awal penelitian, penulis menyiapkan semua referensi yang tersedia sebagai literatur, dalam penelitian ini penulis beracuan pada jurnal dan artikel sebagai referensi dengan tujuan mendukung pelaksanaan penelitian.
2. Penulis menyiapkan semua kebutuhan *software* dan *hardware* yang dibutuhkan dalam pelaksanaan penelitian.
3. Penulis mengidentifikasi masalah dan merancang solusi terkait dengan deteksi anomali pada jaringan, serta menguraikan alat dan teknologi yang akan diperlukan.
4. Dalam pengambilan data, penulis mengumpulkan informasi yang diperlukan untuk analisis. Data diperoleh dari *log* mikrotik yang terpasang pada jaringan Unjaya. Dalam penelitian ini, log yang akan digunakan yaitu *log firewall*. Pengumpulan data melibatkan mengumpulkan log dari perangkat MikroTik, seperti *log firewall*, sebelum pengambilan log tersebut penulis membuat aturan – aturan yang sesuai dengan jenis serangan yang kemudian nantinya aturan pada ip firewall itu akan terisi oleh berbagi log serangan yang sesuai, yang kemudian akan dilakukan analisis lebih lanjut karena yang akan dideteksi adalah anomali pada jaringan pada unjaya.
5. Pada tahap implementasi penulis akan menerapkan rencana dan langkah- langkah yang telah dipersiapkan dan direncanakan sebelumnya. Proses implementasi ini melibatkan berbagai langkah-langkah yang terdiri dari hal-hal berikut. Pada setiap tahap perlu dijelaskan secara *explisit* kegiatan yang dilakukan serta metodologinya. Penentuan software, aturan ip firewall, desain *interface* dan koneksi, pemodelan dashboard, atau pemodelan lainnya dapat dituliskan setelah sub-bab ini.

a. Instalasi Splunk

Penelitian ini menggunakan versi *trial Splunk Enterprise* selama 60 hari dengan kebutuhan sistem sebagaimana tercantum dalam Tabel 3.1.

Tabel 3.1 Kebutuhan Sistem Splunk

Operating System	Windows / Mac OS / Linux
Processor	Minimal 2-core 64-bit CPU 2GHz
Memory	Minimal 4GB
Web Browser	Versi terbaru dari Chrome / Firefox / Safari
Port Splunk Web	8000

b. Memasukan Data

Dalam pengambilan data pada *log* mikrotik dengan aturan ip firewall pada tahun 2024 kemudian di upload pada Splunk. Karena versi *trial* ini hanya memiliki kapasitas 500 MB dalam studi literatur perencanaan pengumpulan data implementasi analisis sekali unggah.

c. Pencarian

Setelah data yang sesuai telah disiapkan, langkah selanjutnya adalah mengolah data, yang dilakukan dengan membuat aturan pada Splunk untuk mencari dan menampilkan data. Menu "*Search & Reporting*" di Splunk memungkinkan pencarian untuk menemukan informasi dari data yang di dapatkan melalui aturan pada mikrotik.

d. Dasbor Visualisasi Data

Setelah pencarian dan pengolahan data selesai, hasilnya akan disimpan dalam "Dashboard Panel" dan dapat dilihat didashboard Splunk.

6. Pemeriksaan / Melakukan Analisis

Penulis memeriksa data yang telah dikumpulkan untuk mendapatkan informasi yang berguna. Dalam analisis melibatkan penggunaan fitur dan alat analisis Splunk untuk mengidentifikasi serangan, pola lalu lintas mencurigakan, atau anomali dalam log MikroTik yang menggangu kinerja pada mikrotik sehingga memberatkan kinerja mikrotik. Selain itu, analisis dilakukan untuk menentukan apakah penelitian yang dilakukan sudah sesuai dengan tujuan dan sebagai dasar untuk membuat kesimpulan.

7. Laporan Hasil

Setelah melakukan analisis, langkah terakhir adalah menyusun laporan hasil penelitian, melakukan evaluasi terhadap kinerja sistem deteksi anomali, memberikan saran untuk peningkatan keamanan jaringan, dan menarik kesimpulan keseluruhan dari penelitian penulis.