1 Pendahuluan

Penggunaan Internet memiliki pertumbuhan yang cepat selama dekade terakhir[1]. *Software defined network* (SDN) sebagai pengaturan lalu lintas jaringan menjadi faktor penting untuk mendukung layanan pada Internet. SDN merupakan arsitektur jaringan yang digunakan untuk komunikasi jaringan dan mengontrol beberapa perangkat sekaligus. Arsitektur pada jaringan SDN terdiri dari tiga lapisan; Lapisan Aplikasi, Lapisan Kontrol, dan Lapisan Data atau Infrastruktur. Lapisan Aplikasi menyediakan layanan inti seperti virtualisasi jaringan *could* dan optimasi jaringan pusat data. Lapisan Kontrol terdiri dari logika kontrol SDN yang disebut *controller*, platform perangkat lunak yang memiliki tampilan lengkap dari jaringan seperti topologi, lalu lintas, dan status port. Kemudian Lapisan Data atau Infrastruktur terdiri dari perangkat penerusan data seperti *switch* dan *router*. Setiap lapisan dihubungkan oleh *Application Programming Interface* (API) yang merupakan sebuah *interface* yang dapat menghubungkan aplikasi satu dengan aplikasi lainnya. Pada jaringan SDN terdapat *Northbound* API dan *Southbound* API. *Northbound* API digunakan untuk komunikasi antara Lapisan Kontrol dengan Lapisan Aplikasi. Sedangkan *Southbound* API digunakan untuk komunikasi antara Lapisan Kontrol dengan Lapisan Data. *Southbound* API memiliki beberapa protokol standar seperti VXLAN, GRE atau MPLS[1], dan OpenFlow sebagai protokol paling terkenal yang dikelola oleh *Open Networking Foundation* (ONF) yang sedang diteliti dan dikembangkan secara intensif oleh para peneliti dan industri.

Arsitektur SDN menawarkan keuntungan *programable* dan manajemen jaringan menjadi lebih fleksibel dan terskala. Penggunaan SDN OpenFlow semakin populer pada infrastruktur modern. Semakin banyak jaringan SDN yang diimplementasikan, maka perlu memerthatikan masalah keamanan. Kekuatan pada SDN OpenFlow adalah karena lapisan kontrol yang terpusat, namun sentralisasi menyebabkan masalah keamanan[1]. Masalah keamanan berfokus pada kejahatan yang dilakukan oleh *hacker* dengan sasaran pada pengontrol terpusat, rentan terhadap serangan pada *switch* dengan memanipulaasi aturan aliran atau memanipulasi host. Kejahatan tersebut berupa serangan seperti; DoS, *Table Overflow*, Pembajakan Lokasi Host, dan *Link Fabrication*. Disebutkan pada penelitian sebelumnya[19], DoS merupakan serangan paling umum yang paling sering dijumpai diantara serangan-serangan lainnya, sudah banyak peneliti yang menangani kasus tersebut. Pada tugas akhir ini penulis berfokus untuk Serangan Pembajakan Lokasi Host, karena merupakan jenis serangan baru di SDN yang belum banyak dijumpai dan dibahas oleh peneliti dibandingkan dengan serangan lainnya[20].

Pembajakan Lokasi Host merupakan serangan di jaringan SDN OpenFlow yang berfokus pada penipuan lokasi host dengan sasaran mengelabui controller untuk membelokan paket ke penyerang. Serangan ini dapat menyebabkan terjadinya perpindahan lokasi host, duplikasi paket atau layanan palsu, dan pemutusan layanan. Untuk mengetahui serangan tersebut, Forensik Jaringan berperan sebagai alat untuk penyelidikan dalam mencari bukti. Bukti tersebut terdapat pada *log file* yang ada pada jaringan, namun saat ini pembacaan *log file* masih dilakukan secara manual[16]. Maka diperlukan sistem untuk dapat melakukan analisis log secara otomatis, agar dapat meningkatkan efisiensi dalam proses penyelidikan. Proses otomatisasi dapat dilakukan dengan Metode *Clustering*, dimana serangan akan diklasifikasi ke dalam beberapa *cluster* dan akan diketahui ada berapa banyak serangan yang terdeteksi pada *cluster* tersebut. Algoritma yang digunakan adalah *K-Means Clustering*, dimana data akan dikategorikan berdasarkan identitas dari jenis serangan. *K-Means* dipilih karena pada algoritma ini memiliki waktu komputasi yang cepat dan efisien dengan jumlah data yang cukup besar[10]. Oleh karena itu, pada penelitian ini akan membuat sebuah sistem yang dapat mendeteksi serangan dengan melakukan analisis log secara otomatis menggunakan metode *K-Means Clustering.*

Topik dan Batasannya

Berdasarkan latar belakang masalah penelitian ini, dapat disimpulkan bahwa topik permasalahan yang diselesaikan yaitu membuat sebuah sistem yang dapat mendeteksi Serangan Pembajakan Lokasi Host melalui proses analisis log yang dilakukan secara otomatis menggunakan metode *K-Means Clustering*. Dataset yang digunakan diambil dari data simulasi log di jaringan SDN OpenFlow yang telah dibuat dengan serangan Pembajakan Lokasi Host. Penelitian ini dilakukan secara offline, sehingga log file sudah tersedia dan tidak dilakukan saat sistem telah berjalan. Penelitian ini hanya dilakukan pada jaringan SDN yang menggunakan OpenFlow. Versi OpenFlow yang digunakan adalah 1.3. Berfokus pada Controller dan menggunakan Single Controller. Modul berjalan menggunakan RYU Controller 4.2.

Tujuan

Implementasi dan analisis hasil akurasi dari pengujian sistem dalam mendeteksi serangan berdasarkan analisis log pada serangan Pembajakan Lokasi Host di jaringan SDN OpenFlow, sehingga dapat digunakan untuk mempermudah proses forensik jaringan dalam penyelidikan bukti serangan.

Organisasi Tulisan

Tahapan selanjutnya yang akan dilakuakan adalah pada bagian 2 sebagai Studi Terkait, bagian 3 sebagai perancangan dan implementasi alat yang dibangun, bagian 4 sebagai hasil pengujian, dan pada bagian 5 terdapat kesimpulan dan saran.