1. LATAR BELAKANG

1.1. PENDAHULUAN

Software Define Network adalah arsitektur jaringan dan komunikasi yang dapat digunakan untuk merancang, mengelola dan mengimplementasikan jaringan [5]. Salah satu standar yang digunakan pada SDN adalah *OpenFlow* sebagai pengontrol SDN untuk berkomunikasi antara lapisan *controller* dengan lapisan *forwarding* untuk menyesuaikan jaringan yang ada pada *Software Define Network*. Sejak kemunculannya arsitektur SDN tidak terfokus pada keamanan jaringan sehingga memiliki kekurangan pada keamanan jaringan[3], Dalam pengontrol *OpenFlow* memiliki keterbatasan dalam menyimpan *flow enties* sehingga dapat menyebabkan Flow Table pada OpenFlow, kekurangan ini dapat dieksploitasi oleh hacker untuk melakukan pembajakan. Dengan adanya sisi negatif pada penggunaan jaringan komputer ini diperlukan pengembangan pada forensik jaringan untuk dapat melakukan identifikasi penyelidikan.

Dalam penyelidikan Forensik Jaringan diperlukan informasi serangan, *firewall,* penyerang, dan korban yang disimpan pada log file. Namun, saat ini pembacaan log file masih dilakukan secara manual[1]. Untuk meningkatkan efisiensi dalam proses investigasi diperlukan analisis agar file log dapat dilakukan secara otomatis. Otomatisasi analisis log file ini dapat dilakukan dengan memanfaatkan metode *Clustering.* Metode *Clustering* dipilih karena dapat menangani *noise* dan dapat melakukan clustering pada dimensi data (atribut) yang tinggi[10] dan algoritma *clustering* yang digunakan adalah *K-Mean Clustering*, dimana data akan dikategorikan berdasarkan karakteristik serangan[2]. *K-Mean Clustering* dipilih karena pada algoritma ini memiliki waktu komputasi yang cepat dan efisien dengan jumlah data yang cukup besar[10].

Pada penelitian sebelumnya yang berjudul *"An Evidence-Based Technical Process For OpenFlow-Based Software Define Network Forensics",* menyatakan bahwa analisis file log belum tersedia pada arsitektur jaringan untuk setiap serangan. Oleh karena itu penelitian ini akan melakukan otomasi analisis log file untuk pencarian penyerang dan mencari akurasi *K-Means Clustering* dalam menganalisis file log agar dapat menghasilkan otomasi analisis file log dengan serangan *Table OverFlow* dengan menggunakan Controller Ryu.

1.2. RUMUSAN MASALAH

Berdasarkan Latar belakang yang telah disampaikan, dapat dirumuskan masalah pada tugas akhir ini adalah:

1. Bagaimana memproses log file yang ada dengan metode *K-Means Clustering* agar dapat digunakan untuk keperluan forensik terutama pada serangan *Flow Table OverFlow* ?
2. Bagaimana hasil *K-Means Clustering* dapat menghasilkan akurasi analisis file log ?

Berdasarkan rumusan masalah yang ada, berikut batasan masalah pada penelitian ini[3]:

a. Log Analisis pada jaringan SDN hanya menggunakan *OpenFlow.*
b. Versi *OpenFlow* yang digunakan adalah 1.3.
c. Serangan yang ada pada *OpenFlow* adalah *Flow Table OverFLow.*
d. Berfokus pada Controller dan menggunakan Single Controller.
e. Modul berjalan menggunakan RYU Controller 4.2.
f. Pengklasifikasian File Log Analisis sehingga dapat mengetahui serangan dengan otomatis.
g. Dalam penelitian ini, dilakukan secara offline, sehingga file log sudah tersedia dan bukan dilakukan saat sistem telah berjalan.

1.3. TUJUAN

Berdasarkan perumusan masalah, maka tujuan pembuatan tugas akhir ini adalah :

1. Klasifikasi dan analisis *K-Means Clustering* dalam mendeteksi serangan Flow Table pada OverFlow pada File Log.
2. Menganalisis akurasi arsitektur *K-Means Clustering* dalam mendeteksi serangan Flow Table pada OverFlow pada File Log.

1.4. RANGKAIAN KEGIATAN

Kegiatan	Bulan								
	Jan	Feb	Mar	Apr	Mei	Sep	Oct	Nov	Des
Studi Literatur									
Pengumpulan data									
Identifikasi Sistem									
Analisis dan Perancangan Sistem									
Tahap Pembuatan Sistem									
Tahap Pengujian Sistem									