Analisa Performa *Elastic’s Logstash, Sys-ng* dan *Barnyard* Sebagai Metode *Log Stash* Mata Garuda

Oleh Dimas Rizky H.P. – 2110141011 – 3 D4 IT A

Overview

Network Intrusion Detection System (NIDS) merupakan sistem yang dipasang pada jaringan untuk memanajemen keamanan dari jaringan tersebut. Sistem ini dipasang pada lokasi yang spesifik contohnya pada server yang terhubung dengan jaringan di luar segmen jaringan internal yang ingin dilindungi. NIDS bekerja dengan cara mengumpulkan paket yang melalui sistem deteksinya, sehingga jika ada paket yang mencurigakan, NIDS akan memberitahu network administrator mengenai kejadian ini.

Konsep kerjanya sama dengan metode penyadapan jaringan telepon. Petugas keamanan akan menempatkan alat penyadap diantara dua koneksi telepon, setelah alat penyadap diletakkan, maka petugas keamanan akan dapat mendengarkan percakapan diantara koneksi telepon tersebut. Jika ada sesuatu yang mencurigakan, seperti peprcakapan dua orang yang merencanakan pembunuhan, rencana pengeboman dan aksi aksi terorisme lainnya, petugas keamanan akan segera memberi info ini ke pihak berwenang agar pihak yang berwenang dapat melakukan sesuatu untuk mengatasi hal tersebut.

Sebelum pihak yang berwenang mendapatkan informasi percakapan dari petugas keamanan tersebut, tentunya petugas kemanan harus memberitahukan informasi ini ke pihak yang berwenang melalui beberapa tahap, ada tahap dimana petugas keamanan melakukan pembuatan laporan terlebih dahulu, lalu mengantarkan laporan tersebut ke pihak yang berwenang atau bisa juga agen tersebut melakukan kontak dengan pihak yang berwenang melalui surat elektronik untuk mempercepat terjalinnya komunikasi.

NIDS akan menuliskan serangkaian kejadian yang terjadi pada jaringan yang ditumpanginya, NIDS menuliskannya ke dalam file yang dinamakan *log file*. Log file ini nantinya akan dikumpulkan oleh sistem dalam rentang waktu yang spesifik untuk diproses data dan informasinya.

Mata Garuda dikenal sebagai NIDS berbasis snort yang handal dan dipercaya untuk memantau aktivitas jaringan internet di Indonesia dan di beberapa negara di ASEAN. Sampai dengan saat ini, Mata Garuda menerima puluhan ribu bahkan jutaan paket perharinya. Hal ini tentu membutuhkan kecepatan pemrosesan yang tinggi oleh sistem mata garuda untuk memenuhi fungsinya sebagai NIDS. Namun, hingga sampai saat ini, Mata Garuda masih memperlukan kurang lebih 15 menit jeda waktu untuk mengumpulkan laporan dari informasi dan kejadian yang terjadi pada jaringan internet yang ada. Hal ini tentunya akan menjadi masalah serius jika tidak segera ditangani, melihat jika laporan mengenai serangan tidak segera diberitahukan kepada network administrator. Hal ini dapat terjadi karena metode *Log Stashing* dari Mata Garuda masih dinilai kurang dikembangkan, sehingga untuk menyelesaikan permasalahan tersebut perlu diaplikasikannya metode lain untuk melakukan stashing.

Pada analisa performa ini, metode yang akan di analisa adalah log stashing menggunakan Barnyard2, Elastic Logstash, dan Syslog-ng