Performance Analysis of Mata Garuda’s Log Stash Method Using Elastic’s Logstash, Sys-ng and Barnyard2

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

Introduction

Network intrusion detection system (NIDS) is methods of security management for networks. This system is installed at specific points such as servers that interface between the outside environment and the network segment to be protected. NIDS works by collecting network packet that passed its system, so if there’re malicious network packet passes its point, NIDS will notice it and report it to the network administrator.

How it works is same as phone wiretapping works, security agent place the device between two phone line connection, and then the security agent who place the wiretap device can hear the conversation that happening between those phone, if there’s something suspicious e.g. bombing plan, or terrorist attack plan, the security agent will tell police that there are some event that will happen. And then police can act to overcome this event.

Before police officer receive the report from the security agent, security agent have to reach the police station first. They have to create the report document and then take those document to the police station. How long it’ll take from create the document and take it to police station is determined by the method security officer take, would they write it by hand and then bring it by car to police station or write it on digital document and then send it to police station by email. In this case the line-connection between two phone is the network, wiretap device is NIDS itself, police is network administrator, and the security agent is the one that’ll tell police that there are this recent event. The method that security agent use to create report and bring that report to police station refer to what log stashing method will be used to bring the information to the network administrator.

Network intrusion system collects network packet traffic by write down the occurred events to the log file. This log file then collected every x-time by stashing it with specific method and then process the stashed data so it can provide the information about the events that are happening at that time. Event means the network packet data that received by the NIDS.

Mata Garuda is well-known snort-based network intrusion detection system, that monitor whole network traffic on Indonesia and some ASEAN country. Mata Garuda received thousands to millions network packet per day. It means that it needs blazing processing speed of packet data to be able to fulfill its purposes. To date, Mata Garuda needs moreover, fifteen-minutes to process or refresh the information that being displayed on the monitor. This happened because Mata Garuda log stash method hasn’t developed optimally. This would become a serious problem if the malicious event is a huge security risk that will become catastrophe if network administrator didn’t do anything to solve it in time. Just imagine, that there is bombing plan in 13.00 that intercepted by security agent and then they report it to the police station at 13.15. It’ll become serious problem for the Mata Garuda.

There are many method out there to stashing the log data that produced by NIDS. This research is about doing a performance analysis for each log stashing method that Mata Garuda can implement to. The performance analysis will be done to three method, using Barnyard2, Elastic’s Logstash, and Sys-ng. This research would help Mata Garuda team to determine which method is best to imSplemented as the stashing method in Mata Garuda log file.

Barnyard2

Barnyard2 is an open source interpreter for snort unified2 binary output files. Its primary use is allowing snort to write to disk in an efficient manner and leaving the task of parsing binary data into various formats to a separate process that will not cause Snort to miss network traffic.

Elastic Logstash

Logstash is an open source, server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it and then sends it to the local storage/stash

Syslog-ng

Syslog-ng allows network intrusion detection system to flexibly collect, parse, classify, and correlate logs from across system infrastructure and store or route them to log analysis tools