Log Analyzer for Dummies

GIAC GCIH Gold Certification

Author: Emilio Valente
evalente@sdsc.edu

April 2008

Road map

- Objective
- Introduction
- Brief description of a Syslogger
- What companies offer
- Components
- Case study
- Summary - Demo

The Objective

- The goal is to put together an architecture that allows, in any environment, quick detection of an incident occurring (presently going on) or that already happened (a few hours ago) during the “Identification” phase of the Incident Handling procedure.

Introduction

- Syslogging is an important aspect of troubleshooting
- Enables a person to:
  - **(1) see what is happening on the network**
  - **(2) reconstruct what already happened (forensic analysis) on the network**

Brief description of a Syslogger

- Syslogger collects and stores Syslog messages
- Each configured device on the network (LAN and WAN)
- Many devices in the network (end-systems, network devices, appliances)
- Large amount of information which is difficult to monitor in real-time or in archives

What companies offer

- A self-contained package can be very expensive, sometimes exceeding $ 100,000.
- I have tested three (3) companies' products and the prices have ranged from $ 35,000 to $ 60,000
- "Intelligence"- has the ability to correlate events and execute actions appropriately. For example: shut down a switch port against a DoS attack

Components

- Relational Database
- Centralized Syslogger
- Web Interface
- Reports

Relational Database

- First you install the kind of database you wish to use (MySQL, Postgress, etc.)
- I used Microsoft SQL because we already had a commercial license for it
- Logs accumulate in your database faster than you realize
- Keep only the last 3 months of running logs
- Backup and store logs older than 3 months

Centralized Syslogger

- Kiwi Syslogger is the only expense needed to build the Network Log Analyzer.
- The commercial version (about $159.00) allows the possibility to Log to an ODBC database
- Support: Access/SQL/Oracle/MySQL/Informix; (The free edition does not have that necessary feature)
- Syslogger Daemon runs on: Windows 98/ME, NT4/2000/2003, XP/Vista

Database & Syslogger Security

- Use Kiwi Syslogger with ONLY-READ account when logging messages into the database
- Disable the default “public” account
- Keep the restrictions on privileges for new database accounts on this database
- Encrypt the logs across the network using one of the many utilities offered by vendors. “*Kiwi Secure Tunnel”* is free.

Web Interface

- The web Interface is where the Network Log Analyzer takes form
- I named it “Syslog Manager” in the demo
- In PHP: friendly and fast interface, to query the database and to find any small piece of information in the huge amount of logging data efficiently and quickly

Web Interface 2

- It is divided into two panels:
- upper panel
  - **select one** networking device or **“All devices”**
  - **Date/Time** automatically goes back to the last two hours of activity
  - **Four different keywords** combined with the **date search**
- The bottom part
  - **Last ID:** generated into the database
  - **Total Number of Records:** the amount of messages stored as records
  - **“Print Results”** button: The results listed and ordered by date and time (latest on the top).

Reports

- The day-to-day activity starts with an analysis of the Kiwi midnight reports
  - Archived Status Report
  - Daily Syslog Statistics
- The first notifies that the file containing the entire day activity has been successfully archived and also shows other useful information
- The second needs to be analyzed in detail to understand and investigate possible abnormal activities
  - “Identification” phase of the Incident Handling “Signs of an incident” is the starting point of the investigation. A precise analysis of logs has to be done before declaring that an incident occurred

Case Study

- Abnormal number of messages for the devices called Brazil showed in the reports
- Common event that appears in several devices using my Syslog Manager (one click)
- I was able to identify account name “SColbert” logged in successfully through ssh on systems
- Account has been disabled because Colbert is an employee that is currently on a leave of absence >>>> INCIDENT

Summary - Demo & Questions

- Timing is everything: This tool provides powerful correlation which is an immense advantage in terms of time and precision that can be invaluable for any sysadmin at the identification phase of an incident handling procedure.
- Demo
- Questions