VIEHGROUP

Log analysis In Ethical hacking

B.SHARATH.RAJ

Log analysis is the process of reviewing, translating and understanding computer-generated records called logs. Logs are produced by a range of structured technologies, including network devices, operating systems, applications, and more. A log contains a series of contextual messages describing the ongoing activities within the system. Log files may be distributed to the log collector via an active network, or they may be stored in files for later updating. In any case, log analysis is a soft art of reviewing and translating these messages to gain insight into the internal functioning of the system.

How to Perform Log Analysis

Logs provide health visibility and performance of the application stack and infrastructure, allowing teams of engineers and system administrators to easily identify and fix problems. Here is our basic five-step log management process for log analysis software:

Tool & Collection - install a collector to collect data from any part of your stack

Include and index - combine data from all log sources into one place to simplify the search and analysis process. Reference makes logs checked, so security and IT staff can quickly find the information they need

Search and Analyze - Analytical techniques such as pattern recognition, simplification, marking and correlation analysis can be applied by making or using a traditional reading machine.

Monitor and alert - With machine learning and statistics, IT organizations can use real-time, log-based monitoring that generates alerts when certain conditions are met. Automation can enable continuous monitoring of large volumes of logs that integrate a variety of programs and applications.

Report and dashboard - Simple reports and dashboard are important features of log analysis software. Customizable dashboards can also be used to ensure that access to private security logs and metrics is provided to employees on a need-to-know basis.

Tasks and Methods of Log Analysis

Log analysis functions cheat data to help users edit and extract information from the log. Here are a few of the most common methods of log analysis.

Familiarity - familiarity is the way data is handled when parts of a message are converted to the same format. The process of combining log data and index should include a custom step where attributes from log entries in all applications are set up and displayed in the same format.

Pattern Recognition - machine learning applications can now be used with log analysis software to compare incoming messages with a pattern book and distinguish between "interesting" and "unsatisfactory" log messages. Such a system may discard the normal log entries, but send a warning when you receive an abnormal installation.

Editing and Tagging - as part of our log analysis, we may want to integrate log entries of the same type. We may want to track every type of error in all applications, or we may want to filter the data in different ways.

Relationship Analysis - when an event occurs, it may appear in logs from many different sources. Relative analysis is the process of analyzing log information from various systems and obtaining log entries for each system linked to a known event.

Log Analysis for Cyber Security

Organizations wishing to improve their online security skills must develop log analysis skills that can help them identify and respond to online threats. Organizations that successfully monitor their online safety through log analysis can make their network assets more vulnerable to attack. Cyber security monitoring can reduce the frequency and intensity of cyber attacks, promote early response to threats and help organizations meet cyber security compliance requirements, including:

ISO / IEC 27002: 2013 Information technology - Security methods - Information security management code

PCI DSS V3.1 (Sections 10 and 11)

NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

The first step in an effective online security monitoring system is to identify business applications and technical infrastructure where event logging should be allowed. Use this list as a starting point to decide what types of logs your organization should employ:

System logs

System activity logs

Last point logs

App logs

Verification logs

Physical safety logs

Network logs

Email logs

Firewall logs

VPN logs

Netflow logs

Timber logs

HTTP proxy logs

Logs for DNS, DHCP and FTP

Appflow logs

Web Server Logs and SQL

Cyber security monitoring logs

Logs to protect malware program software

Login system access logs (NIDS).

Login system block logs (NIPS) logs.

Data loss logs (DLP).

Event logging for all of these programs and applications can generate huge amounts of data, at great cost and resources needed to successfully manage logs. Cyber security experts should determine the most important logs for consistent monitoring and use automated or software-based analytics methods to save time and resources.

Conclusion

This project proposes the mission of Log analysis .) is a natural, yet unique, branch of the problemdetermination toolbox. In annalogy to the work of aphysician, the goal is to detect the problem as it occurs,foresee the upcoming symptoms, and provide some remedybefore problems escalate. By building on machine-learningtechnology, MELODY provides the means to automatethe process of detection–prediction–action. Throughintegration with IBM ILOG rules engine, it also providesa means to encode and incorporate the knowledge fromsubject matter experts.From a knowledge management perspective, our approachto information summarization is lossless, in whichBnoninteresting[data is preserved, although it will get lowrelevance scores. We successfully address the nontrivialchallenge of devising an information extraction mechanismthat solely utilizes data stemming from faulty machines.Our analysis includes the incorporation of clusteringtechniques that enable analysis not only at the level ofindividual log messages but also automatic constructionof metastates, which carry information at a higher