Using Security Logs for Collecting and Reporting Technical Security Metrics

Title	Using Security Logs for Collecting and Reporting Technical Security Metrics
Publication Type	Conference Paper
Year of Publication	2014
Authors	Vaarandi, R., Pihelgas, M.
Conference Name	Military Communications Conference (MILCOM), 2014 IEEE
Date Published	Oct
Keywords	Big Data, computer network security, Correlation, Internet, log analysis methods, log analysis techniques, Measurement, Monitoring, open source technology, Peer-to-peer computing, security, security log analysis, security logs, security metrics, technical security metric collection, technical security metric reporting, Workstations

Abstract

During recent years, establishing proper metrics for measuring system security has received increasing attention. Security logs contain vast amounts of information which are essential for creating many security metrics. Unfortunately, security logs are known to be very large, making their analysis a difficult task. Furthermore, recent security metrics research has focused on generic concepts, and the issue of collecting security metrics with log analysis methods has not been well studied. In this paper, we will first focus on using log analysis techniques for collecting technical security metrics from security logs of common types (e.g., Network IDS alarm logs, workstation logs, and Net flow data sets). We will also describe a production framework for collecting and reporting technical security metrics which is based on novel open-source technologies for big data.

URL https://ieeexplore.ieee.org/document/6956774/
DOI 10.1109/MILCOM.2014.53
Citation Key 6956774

Big Data computer network security Correlation internet log analysis methods log analysis techniques Measurement Monitoring open source technology Peer-to-peer computing security security log analysis security logs Security Metrics technical security metric collection technical security metric reporting Workstations