JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

IMPLEMENTATION OF CENTRALIZED INFORMATION SYSTEMS LOGS SERVER

BACHELOR OF COMPUTER SECURITY AND FORENSICS

KAMITA PAUL KINUTHIA

I132/0863/2013

ODHIAMBO RODGERS OKOTH

I132/3146/2013

**SUPERVISOR:** MR. PAUL ABUONJI

# ABSTRACT

Log management and analysis is a vital part of organization’s network management and system information that refers to different security events, which occur within the system. Logs are used for different security events which occur within the system such as recording user activities, track authentication attempts and other security events. Due to increasing number of threats against networks and systems, the number of security logs increases. However, many organizations that work in a distributed environment face the following problems: log generation and storage, log protection and log analysis. Moreover, ensuring that security, system and network administrators analyze log data in an effective way is another issue. In this project we implement a centralized information systems log server. This allows real time detection and alert of all log transactions from different client machines to one centralized server.

The overall objective of this project is to implement a centralized information system log server from which keystrokes directory changes and windows open will reveal activities and program run by the user and directory changes on the system user machine. The methodology chosen for this project is agile methodology, scrum software development model.

The project was implemented focusing on development of sprints which involved of new release functionality, requirements, quality, cost and competition, results of the implementation were positive describing the success of our project, the system therefore achieved its goals meeting our objectives, however we recommend future work on our project to be done to ensuring it runs in a variety of operating systems.