**OPEN SOURCE IDS FOR A RESOURE CONSTRAINED SET-UP**

BSC. COMPUTER SECURITY AND FORENSICS

BY

ROSE WAMBUI WANJOHI

I132/0873/2013

MICHAEL GITAU MBUGUAH

I132/0889/2013

SUPERVISOR: MR CASTRO YOGA.

# ABSTRACT

Intrusion detection system(IDS) is a devices or software that monitor the network systems for any malicious activity or policy violation. Firms and organizations which are resource constrained are not able to implement these network security systems since most of them are very expensive. There is always a question of whether the amount they will use to implement these systems is relatively equal or less than the amount used after a security breach has occurred. This research project was conducted in a virtualized environment which simulated a typical network. The two intrusion detection systems, bro and snort were implemented and tests run against them. The main objective of this project was to identify, implement and recommend a suitable open source IDS for a resource constrained environment/set-up. After running the test bro appeared to be the best IDS. It had a higher speed, less time to analyze traffic and detected more exploits than snort. Therefore, we recommend that the resource constrained firms to implement the Bro intrusion detection system.

*Keywords:* open source, IDS, resource constrained