MICIE: A Model for Identifying and Collecting Intrusion Evidences

Abdulghani Ali Ahmed, Yee Wai Kit

Faculty of Computer Systems & Software Engineering
University Malaysia Pahang, Pahang, Malaysia

abdulghani@ump.edu.my, pokemania2008@hotmail.com

***Abstract* - Today it is very important to maintain an intermediary level of security to ensure safe and trusted communication for daily usage. Secured data communication over internet and any other network is hard to achieve due to the threat of intrusions and misuse. Unfortunately, none of the existing systems have proved to be flawless, though various approaches have been used to thwart network intrusion activities. This paper proposes an investigation Model for Identifying and Collecting Intrusion Evidences (*MICIE*). In particular, the proposed model *MICIE* comprises three main features, SNORT as IDS, MySQL as database and BASE for result viewing. These features were installed on Raspberry Pi, which was used to aid the data collection process. The results demonstrated that the proposed model is promising for identifying and collecting evidence of network intrusions in real time.**

Index Terms* - *Intrusion evidence. Cloud computing. Forensic investigation. Raspberry Pi.

978-1-5090-5698-9/16 $31.00 © 2016 IEEE
DOI 10.1109/SITIS.2016.54