Campus Hybrid Intrusion Detection System using SNORT and C4.5 Algorithm

Slamet 1 Izzeldin I. Mohamed 2 , Fahmi Samsuri 2

1 Faculty of Technology and Information, 1Department of Information Systems, Institut Bisnis &
Informatika Stikom Surabaya, Indonesia
slamet@stikom.edu

2 Faculty of Electrical and Electronics Engineering University Malaysia Pahang, Malaysia
izzeldin@ump.edu.my , fahmi@ump.edu.my

Abstract:
The rapid development of internet greatly helps human work. However, the number of information system security incidents has risen sharply, so that in fact the sides of human life are threatened. Detection techniques against attacks on computer networks must be continuously developed so that integrity, availability and confidentiality on a computer network become more secure. Most of current intrusion detection systems only use one of the two detection methods, misused detection or anomaly detection, both of them have their own limitations. In this paper, the authors built Hybrid Intrusion Detecting System combines misuse detection system with anomaly detection system. The basis of misused detection module is snort, and anomaly detection module is constructed by using Algorithm C4.5 detectors. This system works by creating alerts built from an engine that reads the parameters in the attacker's IP address. Webmin is used to simplify rule management. Whereas for analyzing logs (attack history), an ACID (Analysis Console for Intrusion Databases) is used. Attack and detection testing is carried out in the campus network of Institut Bisnis dan Informatika Stikom Surabaya. The system implementation uses a PC Router with the Ubuntu 18.04 Linux as operating system. As a result of implementing this system: misused detection module uses the signature of attacks to detection the known attacks; anomaly detection module can detect the unknown attacks; signature generation module extracts the signature of attacks that are detected by Anomaly Detection System module, and maps the signatures into snort rules.

Keywords: Intrusion Detection; Attack; Snort; C4.5

Acknowledgement

This research is funded by University Malaysia Pahang, UMP Lab2Market Research Fund (UIC170901). This acknowledgment also goes to Faculty of Electrical and Electronics Engineering for providing us with facilities to conduct this research