IMPLEMENTATION OF RULE-BASED METHOD IN DETECTING BRUTE FORCE ATTACKS ON OWNCLOUD

KHAZIN MUBAROK
Informatics Study Program, Faculty of Science & Technology, Y
ogyakarta University of Technology
Jl. North Ringroad Jombor Sleman Yogyakarta
E-mail: khazinnismo@gmail.com

ABSTRACT

Owncloud is an open-source cloud storage media. It is regarded as the most effective server for storing data. However, data security remains a primary concern for users of the Owncloud server media. Owncloud server managers cannot guarantee the security of data on the Owncloud servers they manage. To ensure the protection and detection of Owncloud attacks, network analysis is essential for observing brute-force attack patterns on the server. Forensic analysis is also necessary to identify any potential attackers. The analysis process necessitates the use of Snort software as a sniffing packet and Wireshark as a capturing packet based on the Intrusion Detection System (IDS) during testing attacks. The rule-based method is used to test brute-force attacks. The implementation of the rule-based method involves the use of predetermined scenario rules to identify suspicious attack patterns. This setup includes examining login activity patterns, such as the number of failed login attempts from the same IP over a specific period.