ABSTRACT

The development of computer networking technology is growing rapidly. This adds to the technological advancement of technological development as a new trend to express creativity. But there are some certain impacts that cannot be avoided. One of which is case of server attack that often happens recently in the form of SSH attack, which is used to remote server. Therefore, it needs efforts to achieve security towards SSH, one of them is using Fail2ban. Fail2ban is used to handle brute force attack and dictionary attack to linux by detecting log file from SSH, Apache, and other logs, then automatically apply it to iptables to block the attack. Fail2ban can be configured to set time of access block, and maximum number of times a user can try to login. The other advantage of applying Fail2ban is the SSH server can be monitored remotely so that administrators do not need 24 hours overseeing the SSH server. In the monitoring, there are notifications when users log in to server which will be sent to Telegram Messenger. Notifications are sent in the form of the date, time entry, Host IP address, IP users, as well as information such as ISP, city, and country of the user. The test results showed that Fail2ban can prevent attacks from Hydra and Metasploit.

Keywords: Fail2ban, SSH, Telegram Messenger