ABSTRACT

More and more server attacks will cause the server to experience operating system corruption. Examples of attacks that occur such as DDoS and brute force attacks. In preventing such attacks, security is required on the server. This study discusses system attacks on servers by combining mock servers and implementing firewall systems to secure servers from attackers. The mock server was created using a honeypot cowrie and installed a web server. Honeypot cowrie interacts with the SSH (secure shell) medium, and can record brute force attacks. The results of brute force attacks are recorded in cowrie honeypot logs and can be seen on the kippo graph using a browser. This research uses quantitative method because this research analyzes the performance and performance of the server in case of attack. Testing was conducted in two scenarios, namely the first scenario of attacking port 80 and obtained a very large percentage of CPU and memory on Mikrotik RouterOS that impacted the performance of Mikrotik RouterOS such as difficulty to control Mikrotik RouterOS and slow traffic. Logs in the first scenario obtained an average of 515.542 attacks. While in the second scenario attack port 22 and obtained the percentage of CPU and memory increased on the honeypot server, because the attack directly impacted the honeypot instead of to Mikrotik RouterOS. Logs in the second scenario obtained 7.727 usernames and 273 passwords and a total of 568 activities occurred.

Keyword : *Honeypot*, *Cowrie*, SSH, *Brute force*, Mikrotik *Router*OS