ABSTRACT

The internet is a medium used by users to access services, such as web services. On a web has a server known as a web server that serves to serve requests and accommodate important information on the web. Because the web server is a container of important information on the web, making a web server a major consideration for safekeeping from attacks that can harm information systems. Because of this, security on the web server is needed to prevent attackers from carrying out attacks. Port knocking and honeypot are methods used to secure web servers from attack attempts. Port knocking prevents by closing the specified logic port. However, the port can still be accessed by administrators or those who have access rights by tapping on the port according to the predefined parameter stages. Then, when the attacker tries to enter through a logical port that has been port knocked and does not have access rights, the attacker will be refused entry and be redirected to the honeypot. In the honeypot method, it is used as a fake or fake server where the attacker will think that the honeypot server is the real server. In addition to being a mock server, the honeypot can also see the activities carried out by attackers while on the honeypot server. This test requires two computers, one as a client computer used to attack and one as a server computer. The combination method of port knocking and honeypot will be enabled on the server computer. Parameter testing is done by using port scanning and brute force attacks to test the success of the combination of port knocking and honeypot methods. The test results by reviewing the literature on port knocking and honeypots work well. Port knocking can provide port rules, while honeypots can create shadow servers and can log attacker activities.

Keywords: Brute force, Honeypot, Network Security, Port Knocking, Port scanning.