ABSTRACT

The faster the development of information technology, the more ways or tricks to break into digital security systems that are very vulnerable, according to kompas.com in March 2020, Tokopedia experienced a data leak that affected 15 million users. The importance of building a security system so that it is not misused by irresponsible people who can harm many people, so we need a security system that can secure servers from various attacks. Honeypot is a fake server that can be a solution to protect the server from hacker attacks. When hackers manage to gain access to the main server, all important data can be misused, therefore switching the main server into an artificial server on SSH, webserver and wordpress is one solution to protect the main server. In this study, a honeypot system was built using 3 honeypots, namely cowrie to secure SSH, snare to secure the webserver and a plugin to secure wordpress security method using signature-based. Signature-based basically every activity in the form of an attack will have its own footprint / footprint, from the footprint an analysis is carried out and the signature of the attack is obtained. Testing is done by displaying the results of attacks carried out live and being able to find out where the source of the attack came from. The test results get the attacker's ip address, the time and date of the attack and the tools used.

Keywords: Hacker,Honeypot,Cowrie,Snare,Wordpress