ABSTRACT

Digitalization in the industrial sector is growing rapidly, with digitalization the work process can be completed faster, in industries that have implemented this digitalization, servers are needed that can accommodate all work and have a strong security system. Servers are often targeted by hackers to carry out cyber attacks because attacking a server will result in paralysis of a company, one of the security on the server is Honeypot and Wazuh. Both security systems can be implemented on servers, especially servers that use Linux OS. Both can be used to identify and detect cyber attacks. Honeypot is a security system that creates a fake server, functions as a trap and wazuh is an open source cyber attack detection system platform. Therefore, a server must have a very strong security system, honeypot and Intrusion Detection System (IDS) are one solution to this problem. This study focuses on analyzing the security system on the server using Honeypot and combined with IDS. The IDS that will be used is Wazuh and the honeypot used is honeypot cowrie. The scenario in this study uses 2 devices, namely the server as the target and the laptop as the wazuh agent and the attacker uses the kali linux VM on the laptop, then installs the security system on the server computer. The attack process is carried out by the attacker using the Kali Linux OS on the VM to the server that has been configured with a security system, the attack is carried out using the Medusa, Metasploit and HPing3 tools, some of the attacks carried out are, Dos, bruteforce and malware (backdoor), the results of the attack test obtained that wazuh can detect attacks with a delay of 5 minutes after the attack was launched and entered the honeypot cowrie server not the original server. In testing the network quality when the server was attacked, the Qos results were obtained, namely Throughput: 393 kb/s, Packet loss: 7.2 %, Delay: 16.65 ms and Jitter: 16.66 ms.

Keyword : Honeypot, HIDS, Wazuh,