ABSTRAK

Sistem keamanan *server* menjadi sangat penting dalam menjaga sebuah data. Dinas komunikasi informatika persandian dan statistik kabupaten bekasi saat ini hanya menggunakan *firewall* sebagai sistem keamanan *server* nya. Untuk mengatasi hal tersebut, perlu dibangun sistem keamanan *server* untuk mencegah serangan yang dapat menyebabkan kerugian kehilangan data. Penelitian ini menggunakan sistem keamanan *server honeypot cowrie* dan *IDS snort*. Metode pengembangan sistem yang digunakan yaitu *Network Development Life Cycle (NDLC).* Pengujian penyerangan menggunakan teknik *port scanning,* teknik *brute force attack,* dan melakukan blok *ip address* peretas. Pengujian dengan teknik *port scanning* dapat menghasilkan informasi penting pada suatu jaringan dan mendeteksi *port* berapa saja yang terbuka, diantaranya port 22 yaitu *ssh (secure shell)*. Teknik serangan *bruteforce attack* dapat menghasilkan kombinasi *username* dan *password* yang ada pada sistem *server* secara ilegal. *IDS snort* dapat mendeteksi serangan yang masuk pada sistem *server*, kemudian *IDS snort* dapat memblokir *ip address* peretas yang melakukan serangan terhadap sistem *server*.

Kata Kunci : *cowrie, firewall*, *honeypot, IDS, NDLC, snort.*

ABSTRACK

Server security system is an imperative in maintaining data. Currently, Communication, Informatics, Code, and Statistics Office of Bekasi Regency only uses a firewall as its server security system. To solve the problem, that needed to build a server security system to prevent attacks that can cause data loss. This research used Cowrie Honeypot server security systems and IDS snort. The system development method used is the Network Development Life Cycle (NDLC). Testing attacks use Port Scanning techniques, Brute-force Attack techniques, and blocking hackers' IP addresses. Testing with port scanning techniques can generate the important information on a network and detect which ports open, including port 22, namely SSH (secure shell). The Brute force Attack technique can illegally produce username and password combination on the server system. IDS snort can detect incoming attacks on the server system then IDS snort can block the IP address of hackers who attack the server system.

Keywords: *cowrie, firewall, honeypot, IDS, NDLC, snort.*