

**IMPLEMENTASI HONEYPOT COWRIE UNTUK MENDETEKSI  
SERANGAN PROTOKOL SSH PADA SERVER BESERTA WEB  
MONITORING DAN NOTIFIKASI OTOMATIS  
(STUDI KASUS UPT TIK UNDIKSHA )**

Oleh

Putu Bayu Megawanta, NIM 1615051020

Program Studi Pendidikan Teknik Informatika

Jurusan Teknik Informatika

Fakultas Teknik dan Kejuruan

Universitas Pendidikan Ganesha

**ABSTRAK**

Perkembangan teknologi komunikasi saat ini semakin cepat berkembang. Salah satu contoh dari teknologi komunikasi yang biasa digunakan adalah internet. Internet saat ini menjadi sebuah kebutuhan untuk mempermudah berbagai pekerjaan. Dalam hal tersebut, terdapat perlakuan kriminalitas yang dilakukan oleh pihak yang tidak bertanggung jawab. Salah satunya adalah serangan pada sebuah jaringan yang memiliki protokol remote SSH (Secure Shell) ke komputer server. Dengan masalah tersebut, salah satu solusi yang dapat diterapkan adalah dengan menggunakan Cowrie Honeypot pada server Xyz UPT TIK. Honeypot tersebut dilengkapi dengan sistem monitoring berbasis web serta notifikasi dengan aplikasi Telegram yang bertujuan untuk notifikasi peringatan dini. Hasil pengujian pada Cowrie Honeypot terbentuk pada point CIA (Confident, Integrity, Availability). Confident serta integrity memperoleh hasil dari nilai confusion matrix pada akurasi 99.89%. Confusion matrix merupakan sebuah rangka penilaian pada sistem untuk menentukan sebuah integritas serta kepercayaan pada suatu sistem. Kemudian pada Availability mendapatkan hasil 99.92% dengan melakukan service restart pada Cowrie Honyepot serta 63.80% saat permasalahan perangkat.

**Kata Kunci :** Cowrie Honeypot, Protokol SSH (Secure Shell), Telegram, Server Xyz UPT TIK Undiksha, Confusion Matrix, CIA

**IMPLEMENTATION OF COWRIE HONEYPOT TO DETECT SSH  
PROTOCOL ATTACKS ON SERVERS ALONG WITH WEB  
MONITORING AND AUTOMATIC NOTIFICATIONS  
(CASE STUDY: UPT TIK UNDIKSHA)**

By

Putu Bayu Megawanta, NIM 1615051020

Informatics Engineering Education Study Program

Department of Informatics Engineering

Faculty of Engineering and Vocational

Ganesha University of Education

**ABSTRACT**

The development of communication technology is currently growing rapidly. One example of communication technology that is commonly used is the internet. The internet is currently a necessity to facilitate various jobs. In this case, there are criminal acts committed by irresponsible parties. One of them is an attack on a network that has a remote SSH (Secure Shell) connection to a server computer. With this problem, one solution that can be applied is to use Cowrie Honeypot on the Xyz UPT TIK server. The honeypot is equipped with a web-based monitoring system and notifications through the Telegram application, which aims for early warning notifications. The test results on Cowrie Honeypot are formed at the CIA (confidentiality, Integrity, and availability) point. Confidentiality and integrity were obtained from the confusion matrix value with 99.89% accuracy. A confusion matrix is an assessment framework for a system to determine its integrity and trustworthiness. Then on availability, get results of 99.92% by doing a service restart on Cowrie Honyepot and 63.80% when device problems occur.

**Keywords:** Cowrie Honeypot, SSH (Secure Shell) Protocol, Telegram, Undiksha ICT Xyz Server, Confusion Matrix, CIA