

**LAPORAN KOMPREHENSIF TUGAS BESAR  
IMPLEMENTASI HONEYPOT COWRIE SEBAGAI SISTEM  
PERTAHANAN DAN DETEKSI DINI PADA VIRTUAL  
PRIVATE SERVER (VPS)**



**OLEH**

<b>M.AKBAR JABIR</b>	<b>10584111323</b>
<b>ARFAN</b>	<b>10584111123</b>

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH MAKASSAR  
2026**

## A. PENDAHULUAN

Perkembangan layanan berbasis internet mendorong banyak organisasi dan individu untuk memanfaatkan Virtual Private Server (VPS) sebagai media penyimpanan data dan penyedia layanan secara online. VPS memberikan fleksibilitas dan kemudahan dalam pengelolaan sumber daya, namun di sisi lain memiliki kelemahan pada aspek keamanan, terutama terhadap serangan yang menyasar layanan jaringan seperti Secure Shell (SSH). Kondisi ini menuntut adanya mekanisme pendekripsi serangan yang efektif agar administrator dapat mengenali pola serangan sejak dulu dan melakukan tindakan pencegahan yang tepat.

Salah satu pendekatan yang banyak digunakan untuk mempelajari dan mendekripsi serangan adalah penggunaan honeypot. Honeypot merupakan sistem jebakan yang sengaja dibuat menyerupai server asli dengan tujuan menarik perhatian penyerang, sehingga seluruh aktivitas penyerang dapat dipantau dan direkam tanpa mengganggu layanan produksi. Data log yang dihasilkan honeypot dapat dimanfaatkan untuk menganalisis teknik, pola, serta intensitas serangan yang terjadi pada sebuah server.

Pada tugas besar ini diimplementasikan honeypot Cowrie pada lingkungan VPS atau simulasi VPS berbasis Ubuntu Server sebagai pendekripsi serangan terhadap layanan SSH. Cowrie dipilih karena mampu mensimulasikan layanan SSH secara interaktif dan mencatat detail aktivitas penyerang, mulai dari upaya login hingga perintah yang dijalankan. Pengujian dilakukan dengan tiga jenis serangan, yaitu port scanning menggunakan Nmap, brute force attack menggunakan Hydra, dan denial of service (DoS/DDoS) menggunakan LOIC. Hasil pengujian kemudian dianalisis untuk melihat kemampuan honeypot dalam mendekripsi serangan serta tingkat akurasi deteksi yang dihasilkan.

Tujuan dari laporan ini adalah mendeskripsikan proses konfigurasi honeypot Cowrie pada Ubuntu Server, menjelaskan langkah pelaksanaan tiga skenario serangan terhadap layanan SSH, serta menyajikan hasil dan analisis deteksi serangan oleh honeypot. Dengan demikian, diharapkan implementasi ini dapat menjadi referensi dalam meningkatkan keamanan layanan VPS

sekaligus sebagai sarana pembelajaran mengenai perilaku dan pola serangan pada sistem jaringan.

## B. KONFIGURASI LINGKUNGAN DAN HONEYPOT

1. Konfigurasi Server Asli (VPS)
2. Instalasi & Konfigurasi Honeypot Cowrie

## C. SKENARIO DAN LANGKAH PENYERANGAN

1. Pengujian Port Scanning (Nmap)
2. Pengujian Brute Force Attack (Hydra)
3. Pengujian Denial of Service / DDoS (LOIC)
4. Pengujian Pola Penyerangan
  - a. Individual
    - 1) port scanning
    - 2) brute force
    - 3) DoS
  - b. Double
    - 1) Port Scanning + Brute Force,
    - 2) Brute Force + DoS
    - 3) DoS + Port Scanning
  - c. Multiple

Melakukan tiga serangan sekaligus ke server.

## D. HASIL PENGUJIAN

No	Pola Serangan	Nama Pengujian	Kondisi Sebelum (%)	Kondisi Sesudah (%)	Hasil (Terdeteksi / Tidak)
1	Individual	Port Scanning	0%	100%	Terdeteksi
2	Individual	Bruteforce Attack	0%	100%	Terdeteksi
3	Individual	DDoS Attack	0%	100%	Terdeteksi
4	Double	Port Scanning & Bruteforce Attack	0%	100%	Terdeteksi
5	Double	Bruteforce Attack & DDoS Attack	0%	100%	Terdeteksi

6	Double	DDoS Attack & Port Scanning	0%	100%	Terdeteksi
7	Multiple	Port Scanning, Bruteforce Attack, & DDoS Attack	0%	100%	Terdeteksi

## E. KESIMPULAN