**Laporan Akhir Analisis Intelijen Ancaman Menggunakan Honeypot Cowrie**

**Tanggal Laporan** : 25 Agustus 2025

**Penerima** : Aditya (Mentor)

**Penyusun** : Rangga – Nanda

## 1. Ringkasan Eksekutif

Laporan ini merinci hasil dari implementasi sistem **honeypot interaktif Cowrie v2.6.1** pada server Ubuntu 20.04. Tujuannya adalah untuk secara pasif menangkap dan menganalisis aktivitas siber guna mengumpulkan intelijen ancaman. Selama periode observasi, honeypot berhasil merekam beberapa sesi serangan yang berasal dari satu sumber (10.10.11.1).

Sistem ini berhasil mencatat seluruh siklus serangan, mulai dari fase percobaan login (brute-force), infiltrasi (login berhasil) menggunakan kredensial lemah, pengintaian sistem (reconnaissance) pasca-eksploitasi, hingga upaya pengiriman *payload* (pengunduhan file). Analisis log menunjukkan Taktik, Teknik, dan Prosedur (TTP) yang jelas dari penyerang. Proyek ini membuktikan bahwa honeypot Cowrie adalah alat yang sangat efektif untuk memahami perilaku penyerang dan mengidentifikasi potensi kerentanan.

## 2. Metodologi dan Lingkungan Teknis

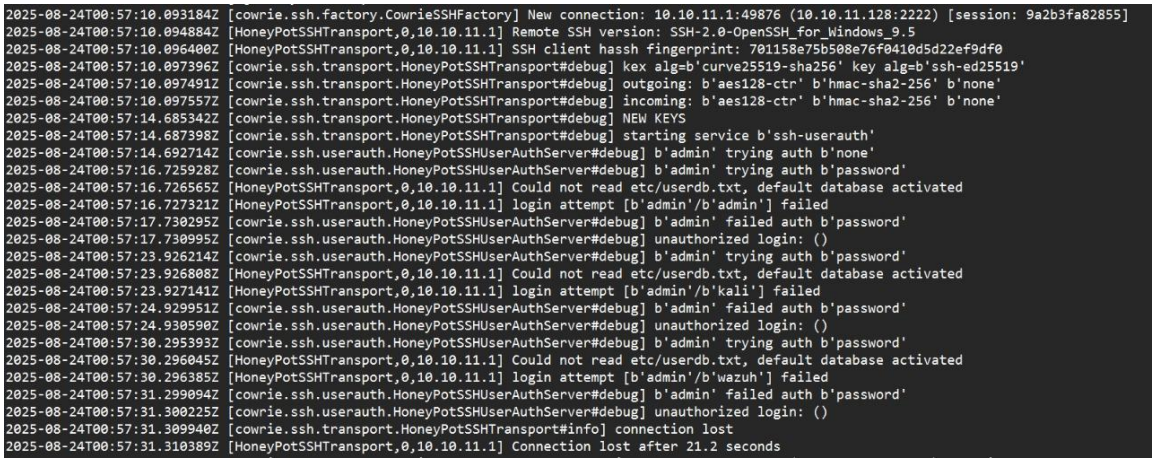
- **Perangkat Lunak Honeypot**: Cowrie v2.6.1 pada Python 3.10.12
- **Sistem Operasi Server**: Ubuntu Server 20.04
- **Alamat IP Honeypot**: 10.10.11.131
- **Konfigurasi Jaringan**: Aturan **iptables DNAT** diterapkan untuk meneruskan koneksi dari port standar SSH (TCP/22) ke port layanan Cowrie (TCP/2222), memastikan penangkapan serangan yang realistis sambil mempertahankan alamat IP asli penyerang.
- **Sumber Serangan Teridentifikasi**:
    - **Alamat IP**: 10.10.11.1
    - **Klien SSH**: SSH-2.0-OpenSSH_for_Windows_9.5

## 3. Analisis Hasil dan Perilaku Penyerang

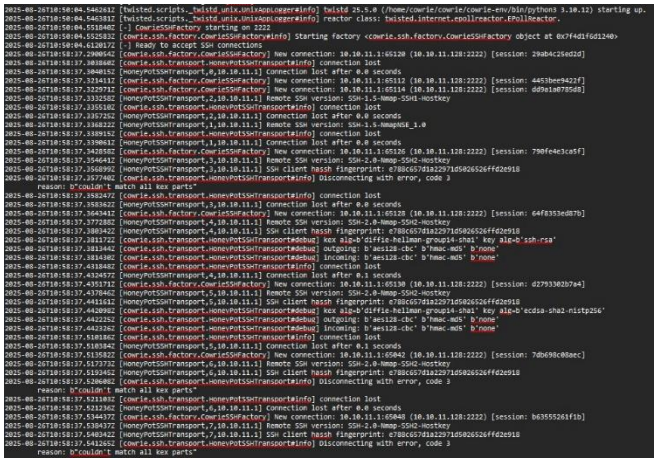
Aktivitas penyerang yang terekam dalam log dapat dianalisis dalam tiga fase utama.

### 3.1. Fase 1: Percobaan Login (Brute-Force)

Penyerang melakukan beberapa upaya untuk mendapatkan akses dengan menebak kombinasi *username* dan *password*. Honeypot berhasil mencatat semua upaya ini pada (Gambar 1.1).




Gambar 1.1

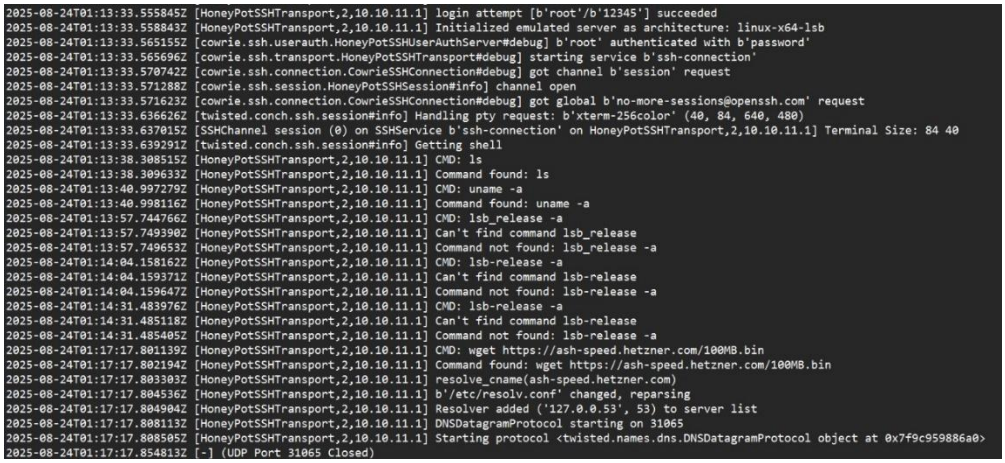


Gambar 1.2

Analisis Gambar 1.2: Pola ini menunjukkan penggunaan daftar kata sandi yang umum atau terkait dengan alat keamanan siber, yang mengindikasikan kemungkinan serangan otomatis. Selain itu, adanya aktivitas **Nmap** menegaskan bahwa penyerang melakukan *scanning* untuk mencari celah sebelum mencoba login.

### 3.2. Fase 2: Infiltrasi Berhasil

Setelah beberapa kali gagal, penyerang berhasil masuk ke sistem dengan menargetkan akun **root** menggunakan kredensial yang sangat lemah.




Gambar 1.3

Analisis Gambar 1.3: Keberhasilan ini menyoroti risiko keamanan yang signifikan dari penggunaan kata sandi yang lemah pada akun dengan hak akses tinggi.

### 3.3. Fase 3: Aktivitas Pasca-Eksploitasi

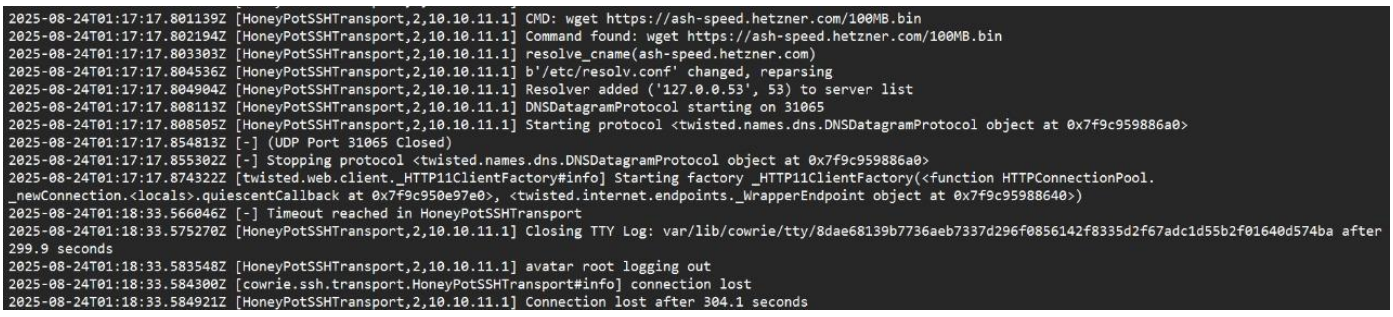
Ini adalah fase paling kritis di mana intelijen mengenai niat penyerang dapat dikumpulkan pada (Gambar 1.4).

**A. Pengintaian Sistem (Reconnaissance)**

Setelah masuk, penyerang segera menjalankan serangkaian perintah untuk mengidentifikasi lingkungan sistem, seperti **ls**, **uname -a**, serta **lsb_release -a**. Perilaku ini umum dalam fase pengintaian.

**B. Pengiriman Payload (Payload Delivery)**

Tujuan akhir penyerang terungkap saat ia mencoba mengunduh file biner dari URL https://ash-speed.hetzner.com/100MB.bin menggunakan perintah **wget**. Untungnya, honeypot berhasil mencegahnya.




Gambar 1.4

**4. Temuan Teknis dan Observasi**

- **Batas Emulasi Honeypot**: Kegagalan honeypot dalam merespons perintah **lsb_release** menunjukkan bahwa penyerang yang canggih mungkin dapat mendeteksi bahwa mereka berada dalam lingkungan palsu.
- **Potensi Bug Perangkat Lunak**: Pada pukul 01:34:50Z, log mencatat **Unhandled error in Deferred** dengan KeyError: 'S2'. Error internal ini mengindikasikan potensi bug dalam Cowrie saat menangani sesi tertentu.

**5. Kesimpulan**

Proyek implementasi honeypot ini dinilai berhasil. Sistem yang dibangun mampu menarik dan menipu penyerang, merekam intelijen berharga (TTP), dan mengumpulkan artefak serangan (file). Data yang terkumpul memberikan bukti nyata tentang metode yang digunakan oleh penyerang dan menegaskan kembali pentingnya kebijakan kata sandi yang kuat serta pemantauan keamanan proaktif.