IMPLEMENTASI DAN ANALISIS HONEYPOT BERBASIS COWRIE UNTUK MENDETEKSI SERANGAN SIBER

Dhafin Rizky Aulia[1] Wahyu Arief Rahman[2], Voully Abdullah Zhacque[3]

[1,2,3]Program Studi Informatika, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa,
Jl. Jenderal Sudirman Km 3, Cilegon, Banten, Indonesia

e-mail: [1]3337210045@untirta.ac.id

ABSTRACT

The use of the internet in Indonesia has grown rapidly. The Indonesian Internet Service Providers Association (APJII) reported that the number of internet users in Indonesia reached 221,563,479 people in 2024, out of the total population. However, as the number of internet users increases, so do the threats that endanger them. Cybersecurity threats continue to evolve alongside the complexity and sophistication of technologies employed by cybercriminals. In addition to building robust security systems, it is equally important to understand the methods used by attackers to design more effective defense strategies. This is where the concept of honeypots comes into play. A honeypot is a security system designed to mimic vulnerable targets, thereby attracting attackers and revealing the tactics, techniques, and procedures they use. One of the most widely used honeypots is Cowrie. This study utilizes Cowrie as an SSH honeypot to be tested against brute force attacks using Hydra. The results show that Hydra successfully identified 15 username and password combinations from the pre-configured Cowrie system.

Keywords: Honeypot, Cybersecurity, Cowrie, SSH

I. PENDAHULUAN

Penggunaan internet di Indonesia berkembang pesat. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) melaporkan bahwa jumlah pengguna internet di Indonesia pada tahun 2024 mencapai 221.563.479 orang, dari total populasi Indonesia yang mencapai 278.696.200 jiwa pada tahun 2023. Dengan demikian, sekitar 79,5 persen dari seluruh penduduk Indonesia menggunakan internet. Angka ini menunjukkan kenaikan sebesar 1,4 persen dibandingkan dengan periode sebelumnya, yang tercatat sebanyak 218,4 juta pengguna (Asosiasi Penyelenggara Jasa Internet Indonesia, 2024). Hal ini menunjukkan betapa pentingnya internet dalam kehidupan sehari-hari masyarakat Indonesia, baik dalam aspek sosial, ekonomi, pendidikan, maupun hiburan.

Adopsi internet yang semakin meluas ini dipengaruhi oleh berbagai faktor, seperti semakin terjangkaunya perangkat mobile, penetrasi jaringan 4G dan 5G yang semakin luas, serta kemudahan akses internet di berbagai daerah, baik perkotaan maupun pedesaan. Internet juga telah menjadi alat penting dalam mendukung berbagai sektor, mulai dari perdagangan elektronik (e-commerce), layanan kesehatan digital, pendidikan daring, hingga sektor pemerintahan yang semakin digital.

Namun, semakin bertambahnya pengguna internet, semakin banyak pula gangguan yang mengancam pengguna nya. Berdasarkan laporan hasil analisis terbaru AwanPintar.id, total seluruh serangan siber di Indonesia mencapai 2.499.486.085 selama semester pertama 2024 (Fikrie, 2024). Hal tersebut tentu mengkhawatirkan bagi banyak orang, terlebih berbagai ancaman yang menyerang server mulai dari port scanning, bruteforce dan denial of service dapat membuat server lumpuh sehingga tidak dapat melayani berbagai permintaan dari client. Ancaman terhadap keamanan siber ini semakin berkembang seiring dengan kompleksitas dan kecanggihan teknologi yang digunakan oleh para pelaku kejahatan siber. Dengan meningkatnya ketergantungan masyarakat terhadap internet untuk transaksi finansial, komunikasi pribadi, serta penyimpanan data penting, potensi ancaman semakin nyata.

Ancaman siber saat ini tidak hanya terbatas pada risiko terhadap data pribadi individu, tetapi juga memiliki potensi untuk merusak aspek yang jauh lebih luas, seperti keamanan nasional, stabilitas ekonomi, dan ketahanan global. Kejahatan siber yang semakin canggih dan meluas dapat menargetkan berbagai sektor penting, mulai dari lembaga pemerintah, perusahaan besar, hingga infrastruktur kritis negara. Serangan siber yang berhasil dapat menyebabkan kerusakan yang signifikan, termasuk kebocoran data sensitif, gangguan layanan publik, kerugian finansial, bahkan merusak reputasi dan kepercayaan publik terhadap sistem digital yang ada. Untuk menghadapi ancaman ini, banyak individu, organisasi, dan perusahaan yang mulai mengimplementasikan berbagai alat dan teknologi keamanan siber guna melindungi data dan sistem mereka dari potensi serangan.

Beberapa perangkat keamanan yang paling umum digunakan seperti antivirus, firewall, VPN (*Virtual Private Network*), IDS (*Intruder Detection System*), dll. Penggunaan alat-alat keamanan ini sangat penting untuk mengurangi risiko yang ditimbulkan oleh ancaman siber. Meskipun tidak ada sistem yang sepenuhnya kebal terhadap serangan, kombinasi dari berbagai alat dan kebijakan keamanan yang diterapkan

dengan baik dapat memperkuat perlindungan dan memastikan bahwa data serta sistem tetap aman dari potensi bahaya yang mengintai. (Natanegara et al., 2023)

Selain membangun sistem keamanan yang kuat, penting juga untuk memahami cara kerja para penyerang agar dapat merancang strategi pertahanan yang lebih efektif. Di sinilah konsep honeypot hadir. Honeypot adalah sebuah sistem keamanan yang dirancang untuk meniru target yang rentan, sehingga menarik perhatian penyerang untuk mengungkapkan taktik, teknik, dan prosedur yang mereka gunakan. Honeypot dapat menangkap penyusup dengan mengubah port yang bertindak sebagai jebakan/tempat di jaringan untuk menipu penyerang, mengumpulkan log, dan aktivitas serangan. Salah satu honeypot yang paling populer digunakan dalam riset keamanan adalah Cowrie.

Cowrie adalah honeypot SSH yang dirancang untuk mencatat aktivitas berbahaya dari penyerang, seperti percobaan login dan eksekusi perintah berbahaya. Ini memberikan wawasan yang lebih dalam tentang upaya kompromi terhadap sistem. Cowrie merekam setiap sesi serangan, membantu memahami lebih detail alat, metode, dan prosedur penyerang. Dengan Cowrie, kita bisa melihat secara langsung bagaimana penyerang berinteraksi dengan sistem, mencatat setiap perintah, file yang diunduh, hingga setiap tombol yang mereka tekan. Cowrie bekerja dengan cara mensimulasikan server asli, di mana penyerang yang berhasil masuk akan mengira mereka telah meretas server, padahal sebenarnya mereka sedang berinteraksi dengan sistem palsu yang secara cermat mencatat semua tindakan mereka.

Tujuan dari penelitian ini adalah untuk mengevaluasi sejauh mana Cowrie mendeteksi dan mengidentifikasi berbagai jenis serangan yang dapat terjadi pada server seperti upaya login brute-force, eksploitasi kerentanannya, atau percakapan yang dilakukan oleh penyerang setelah berhasil mengakses honeypot. Penelitian ini juga bertujuan untuk menganalisis taktik, teknik, dan prosedur (TTPs) yang digunakan oleh penyerang saat berinteraksi dengan honeypot Cowrie. Tujuan lainnya adalah untuk menguji kemampuan Cowrie dalam menyediakan data log serangan yang akurat dan relevan secara real-time. Penelitian ini akan menilai bagaimana Cowrie mencatat percakapan dan langkah-langkah yang diambil oleh penyerang, serta kemampuannya dalam menyediakan informasi yang dapat digunakan oleh tim keamanan untuk mengidentifikasi dan merespons serangan dengan cepat.

II. TINJAUAN PUSTAKA

2.1 **Jaringan Komputer**

Jaringan komputer merupakan suatu sistem yang terdiri dari dua komputer atau lebih yang terkoneksi melalui media transfer data atau media komunikasi tertentu, sehingga memungkinkan mereka untuk berbagi data, aplikasi, atau perangkat keras secara saling terhubung. Setiap pengguna di Internet memiliki alamat IP atau MAC. Alamat IP atau alamat MAC ini digunakan untuk mengidentifikasi alamat tertentu atau alamat pengiriman, Jaringan komputer memiliki banyak keuntungan, seperti kemampuan untuk berbagi sumber daya, meningkatkan efisiensi kerja, memfasilitasi komunikasi yang cepat, dan menyediakan akses ke informasi dan layanan yang luas. Namun, jaringan juga rentan terhadap risiko keamanan dan harus dilindungi dengan menggunakan langkah-langkah keamanan seperti firewall, enkripsi data, dan autentikasi pengguna.

2.2 **Internet**

Internet adalah jaringan global yang menghubungkan jutaan perangkat di seluruh dunia, memungkinkan pertukaran informasi secara cepat dan mudah. Internet memungkinkan kita untuk mengakses berbagai macam informasi, berkomunikasi, serta menjalankan berbagai layanan digital. Sebagai jaringan yang sangat luas, internet menggunakan protokol komunikasi, seperti HTTP dan HTTPS, yang memungkinkan pengiriman data di antara perangkat yang terhubung.

Internet berasal dari konsep jaringan komputer yang pertama kali dikembangkan oleh Departemen Pertahanan Amerika Serikat pada akhir 1960-an. Seiring perkembangan waktu, internet berubah menjadi jaringan global yang digunakan untuk berbagai keperluan, dari informasi hingga hiburan.

2.3 **Honeypot**

Honeypot adalah sistem keamanan server yang berfungsi dengan membuat replika layanan palsu dari server yang ingin dilindungi. Sistem ini telah dikembangkan sebagai perangkat open-source yang dapat diunduh secara gratis oleh pengguna yang berminat. Honeypot berperan sebagai garis pertahanan terakhir jika ada keterbatasan biaya dalam mengamankan server web. Terdapat tiga jenis honeypot yang dapat disesuaikan sesuai dengan tingkat potensi ancaman yang dihadapi oleh server, dan pengguna memiliki fleksibilitas untuk memilih salah satu dari ketiga layanan tersebut guna diimplementasikan pada sistem jaringan mereka. ketiga layanan tersebut sebagai berikut.

a. Low Interaction Honeypot

Low Interaction Honeypot adalah jenis layanan pertama dalam honeypot, di mana honeypot menciptakan replika server dan administrator jaringan. Dalam hal ini, pemilik server tetap memiliki kontrol penuh atas aktivitas intrusi yang terjadi.

b. Medium Interaction Honeypot

Medium Interaction Honeypot merupakan layanan lain yang disediakan oleh Honeypot yang menciptakan sistem operasi palsu untuk menarik perhatian penyerang. Dalam layanan ini, sistem mengarahkan beberapa perintah penyerang ke honeypot palsu, dan sebaliknya, semua informasi mengenai penyerang disimpan dan dapat dievaluasi oleh administrator

jaringan. Salah satu contoh penyedia layanan ini adalah Cowrie.

c. High Interaction Honeypot

High Interaction Honeypot merupakan layanan ketiga dalam honeypot, di mana administrator jaringan tidak perlu lagi secara aktif memantau aktivitas penyusupan. Pada layanan ini, server asli direplikasi sepenuhnya, sehingga penyerang dapat menyerang server replika yang berisi informasi palsu. Dengan demikian, penyerang akan merasa puas karena mengakses informasi secara ilegal, namun pada kenyataannya, server asli tetap aman tanpa terkena dampak apapun dari serangan tersebut.

2.4 **Cowrie**

Cowrie adalah perangkat lunak yang digunakan untuk menyamarkan layanan di server openssh. Perangkat lunak ini termasuk dalam kategori honeypot Medium Interaction yang digunakan untuk mendeteksi dan mencatat serangan brute force pada server SSH, Telnet, dan OpenSSH. Cowrie beroperasi dengan menggunakan konsep redirection, yang berarti setelah serangan openssh berhasil, Cowrie mengarahkan penyerang ke layanan honeypot palsu. Hal ini membuat penyerang mengira bahwa serangannya berhasil, padahal sebenarnya mereka hanya terperangkap dalam honeypot palsu. Fitur utama Cowrie adalah kemampuan untuk melakukan log atau pencatatan aktivitas. Dengan fitur logging ini, semua aktivitas penyerang tercatat dalam sistem palsu. Hal ini memungkinkan administrator jaringan untuk mengetahui secara detail apa yang dilakukan oleh penyerang pada sistem palsu tersebut. (Natanegara et al., 2023)

Hydra adalah sebuah cracker login jaringan yang dibangun di berbagai sistem operasi seperti Kali Linux, Parrot, dan lingkungan pengujian penetrasi utama lainnya. Hydra bekerja dengan menggunakan pendekatan yang berbeda untuk melakukan serangan brute force untuk menebak kombinasi nama pengguna dan kata sandi yang tepat. Hydra biasanya digunakan oleh penguji penetrasi bersama dengan satu set program seperti crunch, cupp, dan lain-lain, yang digunakan untuk menghasilkan daftar kata. Hydra kemudian digunakan untuk menguji serangan menggunakan daftar kata yang dibuat oleh program-program ini.

III. METODOLOGI PENELITIAN

3.1 **Desain Penelitian**

Penelitian ini berfokus pada analisis mendalam terhadap data log yang dihasilkan oleh Cowrie selama serangan. data log akan disimpan didalam file cowrie.log. Serangan akan dilakukan selama 30 menit menggunakan hydra, salah satu tools untuk melakukan brute force attack pada login suatu layanan. Setelah penyerang berinteraksi dengan honeypot Cowrie, peneliti akan menganalisis log yang terekam untuk memetakan aktivitas penyerang, mengidentifikasi pola serangan, dan memverifikasi efektivitas pencatatan oleh Cowrie. Analisis ini memungkinkan pemahaman yang lebih mendalam mengenai teknik dan prosedur yang digunakan oleh penyerang serta memberi wawasan mengenai titik lemah pada sistem yang perlu diperkuat.

3.2 **Instrumen Penelitian**

Untuk menunjang implementasi, berikut spesifikasi perangkat keras yang digunakan :

Perangkat Keras

1. Nama Unit : ASUS UX320LG
2. *Processor* : Intel i7 4500U
3. RAM : 8 GB
4. HDD : 1 TB

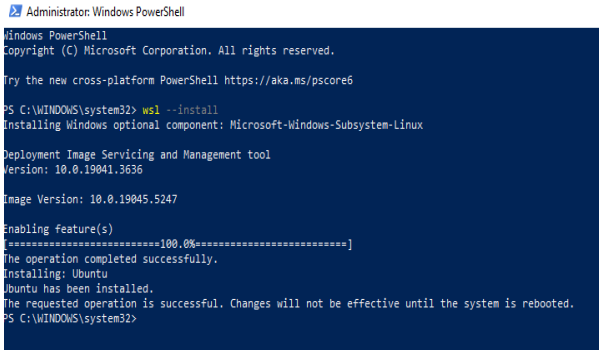
Perangkat Lunak

Berikut adalah beberapa *software* yang digunakan :

1. WSL 2
2. Ubuntu 24.04.01 LTS
3. Python 3.12.3
4. Cowrie 2.6.1
5. PIP (*Python Package Installer*) 24.3.1
6. Hydra v9.5

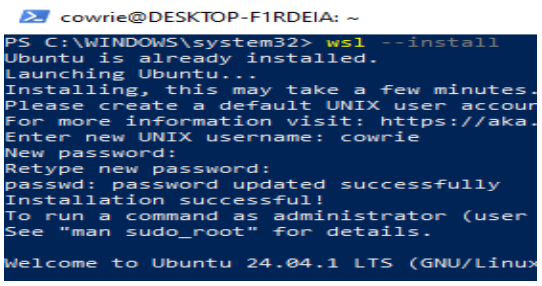
3.3 **3.3 Langkah Langkah Penelitian**

Untuk menjalankan Cowrie, beberapa perangkat lunak dan alat perlu dipasang pada sistem yang digunakan. WSL (*Windows Subsystem for Linux*), yaitu fitur bawaan Windows 10 yang memungkinkan peneliti untuk menjalankan Linux di dalam Windows diperlukan karena peneliti tidak menggunakan virtual machine seperti VMWare atau Virtual Box.



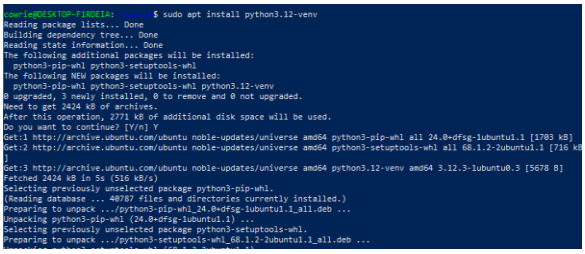
Gambar 3.1 Instalasi WSL dan Ubuntu

Kemudian user khusus digunakan untuk menjalankan honeypot Cowrie. User ini berfungsi untuk memisahkan honeypot dari bagian lain di sistem serta memastikan bahwa honeypot beroperasi dengan aman.



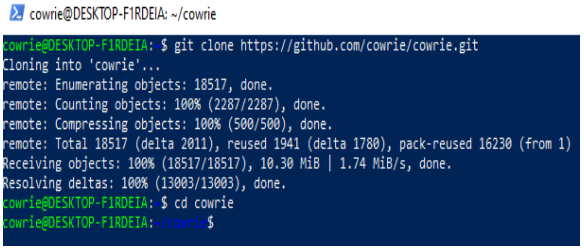
Gambar 3.2 Konfigurasi User

Python 3.9 keatas harus diinstal untuk menjalankan Cowrie, mengingat perangkat lunak ini ditulis dalam bahasa pemrograman Python. Selain itu, PIP (*Python Package manager*) dibutuhkan untuk mengelola dan menginstal *library* Python yang diperlukan oleh Cowrie.



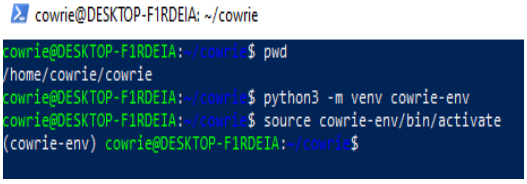
Gambar 3.3 Instalasi Python, PIP dan Virtual Environment

Setelah itu, Cowrie dapat diunduh dari repositori GitHub.



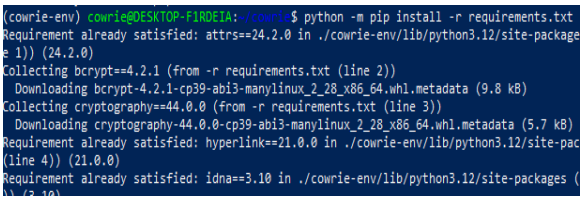
Gambar 3.4 Mengunduh Cowrie dari Github

Penggunaan virtual environment dalam menjalankan Cowrie merupakan praktik yang sangat dianjurkan. Dengan menggunakan virtual environment, lingkungan pengembangan Cowrie menjadi terisolasi, mudah dikelola, dan aman.



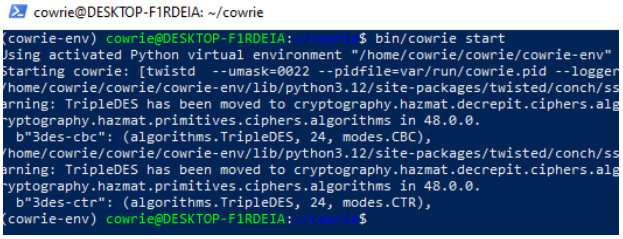
Gambar 3.5 Membuat dan Mengaktifkan Virtual Environment

Mengunduh dependensi yang tercantum dalam berkas requirements.txt menggunakan PIP.



Gambar 3.6 Mengunduh library dari requirements.txt

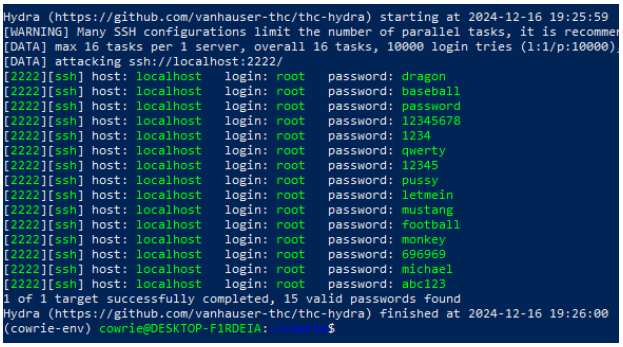
menjalankan cowrie dengan perintah bin/cowrie start.



Gambar 3.7 Menjalankan Cowrie

Peneliti melakukan simulasi serangan *brute force* pada honeypot yang telah dibuat. Dalam simulasi ini, peneliti menggunakan Hydra, sebuah tool yang populer untuk melakukan serangan brute force. Untuk daftar kombinasi username dan password yang digunakan dalam serangan, peneliti memanfaatkan wordlist dari SecLists. Wordlist ini dipilih karena berisi kombinasi username dan password yang paling umum digunakan, sehingga mewakili skenario serangan dunia nyata.

Gambar 3.8 Menjalankan hydra sebagai simulasi serangan brute force



IV. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini didapatkan bahwa hydra telah berhasil menemukan 15 kombinasi username dan password yang benar untuk mengakses sistem tersebut. Ini memberikan akses tidak sah ke sistem dan memungkinkan Anda melakukan berbagai tindakan, seperti mengambil alih kontrol penuh atas sistem, mencuri data sensitif, menggunakan sistem sebagai basis untuk serangan lain dan membuat perubahan pada konfigurasi sistem.

V. KESIMPULAN

Cowrie efektif digunakan untuk mendeteksi dan mencatat serangan brute force terhadap layanan SSH. Serangan Hydra cenderung memanfaatkan kombinasi username dan password yang umum, yang menunjukkan pentingnya menghindari kredensial default. Honeypot seperti Cowrie dapat menjadi alat penelitian yang bermanfaat untuk mengidentifikasi pola serangan dan meningkatkan langkah mitigasi.

REFERENSI

[1] Analisis Kinerja Honeypot Dionaea Dan Cowrie Dalam Mendeteksi Serangan. (2021). *Prosiding Seminar Nasional Teknoka*, *6*, 170-178. https://journal.uhamka.ac.id/index.php/teknoka/article/view/10276

[2] Asosiasi Penyelenggara Jasa Internet Indonesia. (2024, February 7). *Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. Asosiasi Penyelenggara Jasa Internet Indonesia. Retrieved December 16, 2024, from https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

[3] Ernawati, T., & Rachmat, F. F. F. (2021, February 28). Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(1), 180-186. https://doi.org/10.29207/resti.v5i1.2825

[4] Fikrie, M. (2024, August 28). *Serangan Siber ke RI Naik 6 Kali Lipat pada H1 2024, Mayoritas dari Dalam Negeri*. Kumparan. Retrieved December 16, 2024, from https://kumparan.com/kumparantech/serangan-siber-ke-ri-naik-6-kali-lipat-pada-h1-2024-mayoritas-dari-dalam-negeri-23PnYQpafrf

[5] Natanegara, T., Muhyidin, Y., & Singasatia, D. (2023, November 24). IMPLEMENTASI HONEYPOT COWRIE DAN SNORT SEBAGAI ALAT DETEKSI SERANGAN PADA SERVER. *Jurnal Mahasiswa Teknik Informatika (JATI))*, *7*(3), 1871-1877. https://doi.org/10.36040/jati.v7i3.6989