ELANG: Journal of Interdisciplinary Research
E-ISSN: 3025-2482

Implementasi Sistem Monitoring Cyber Attack Berbasis Honeypot Menggunakan Cowrie pada SMK Muhammadiyah 7 Gondanglegi

Daud Utomo[1], Daniel Rudiaman Sijabat[2]*
[1)]191116009@mhs.stiki.ac.id || [2)] daniel223@stiki.ac.id

[1,2]*Sekolah Tinggi Informatika & Komputer Indonesia, Informatika, Jl. Tidar 100 Malang, Indonesia*

Kata Kunci
Cowrie; Honeypot; Keamanan Cyber

****) Author Korespondensi***
daniel223@stiki.ac.id

Abstrak
Di era digital yang serba terkoneksi dengan internet, serangan siber menjadi ancaman yang semakin umum, termasuk di SMK Muhammadiyah 7 Gondanglegi. Penelitian ini bertujuan untuk mengimplementasikan sistem pemantauan serangan siber berbasis Honeypot menggunakan Cowrie di SMK Muhammadiyah 7 Gondanglegi. Honeypot adalah sistem yang dirancang untuk menarik perhatian dan mendeteksi serangan siber, dengan tujuan memahami pola dan teknik yang digunakan oleh penyerang. Cowrie, salah satu jenis Honeypot yang banyak digunakan, memiliki kemampuan untuk mensimulasikan lingkungan Secure Shell (SSH) dan serangan Brute Force, sehingga dapat mendeteksi berbagai jenis ancaman yang menargetkan protokol tersebut. Pada implementasi ini, Honeypot Cowrie akan merekam data serangan yang terjadi pada port SSH. Data yang terkumpul kemudian disimpan dalam database MySQL dan divisualisasikan menggunakan Kippo-Graph untuk mempermudah analisis lebih lanjut.

1. Pendahuluan

Di era digital yang semakin terkoneksi dengan internet, serangan siber telah menjadi ancaman yang signifikan bagi individu, organisasi, dan institusi pendidikan. Berbagai jenis serangan, seperti peretasan, malware, phishing, hingga *Distributed Denial of Service* (DDoS), terus meningkat dalam hal frekuensi dan kompleksitas (Sutarti & Khairunnisa, 2017). Salah satu bentuk serangan yang paling sering ditemukan adalah *brute force attack*, yaitu metode penyerangan yang mencoba menebak kredensial login dengan percobaan berulang-ulang hingga berhasil menembus sistem. Serangan ini sering kali menargetkan protokol-protokol penting, seperti *Secure Shell* (SSH) dan Telnet, yang digunakan untuk komunikasi dan manajemen jaringan.

SSH, meskipun memiliki mekanisme keamanan yang canggih, tetap rentan terhadap serangan *brute force*. Di sisi lain, Telnet, yang kurang umum digunakan dibandingkan SSH, menjadi target karena tidak memiliki enkripsi, sehingga informasi yang ditransmisikan lebih mudah disadap. Kerentanan ini menjadi perhatian serius, terutama bagi institusi pendidikan yang sangat bergantung pada jaringan internet untuk mendukung kegiatan belajar mengajar. SMK Muhammadiyah 7 Gondanglegi, sebagai salah satu institusi pendidikan dengan infrastruktur teknologi informasi yang berkembang, menghadapi tantangan serupa.

Penelitian tentang serangan siber telah banyak dilakukan, terutama terkait implementasi Honeypot sebagai alat pemantau dan analisis serangan. Honeypot adalah sistem yang dirancang untuk menarik perhatian penyerang dan mengumpulkan data tentang pola serta teknik serangan yang mereka gunakan (Dermawati & Siregar, 2020) (Sena, 2020). Salah satu Honeypot yang banyak digunakan adalah Cowrie, yang mampu mensimulasikan lingkungan SSH dan Telnet serta mencatat aktivitas serangan, termasuk *brute force attack* (Arkaan & Sakti, 2019). Penelitian sebelumnya telah menunjukkan efektivitas Cowrie dalam mendeteksi serangan pada protokol-protokol tersebut, namun studi tentang implementasi Cowrie yang terintegrasi dengan visualisasi data menggunakan Kippo-Graph di lingkungan pendidikan masih terbatas (Nurfadhilah, 2019) (Cowrie Project, n.d.).

Kebaruan dari penelitian ini terletak pada implementasi sistem monitoring berbasis Cowrie di SMK Muhammadiyah 7 Gondanglegi untuk mendeteksi serangan *brute force* dan protokol SSH maupun Telnet (NXNJZ, 2019). Selain itu, data yang diperoleh dari Honeypot akan divisualisasikan menggunakan Kippo-Graph, sebuah alat analisis yang memetakan data serangan dalam bentuk grafik sehingga mempermudah identifikasi pola serangan (Hassan, Ismail, & Periyadi, 2020) (Wastumirad & Darmawan, 2021). Pendekatan ini tidak hanya memungkinkan deteksi dini terhadap serangan, tetapi juga memberikan wawasan yang lebih mendalam mengenai ancaman siber yang dihadapi oleh institusi pendidikan.

Penelitian ini bertujuan untuk mengembangkan dan mengimplementasikan sistem monitoring serangan siber berbasis Honeypot menggunakan Cowrie yang terintegrasi dengan Kippo-Graph di SMK Muhammadiyah 7 Gondanglegi. Sistem ini diharapkan mampu meningkatkan keamanan jaringan sekolah dan memberikan kontribusi signifikan dalam mengatasi ancaman siber di sektor pendidikan. Temuan dari penelitian ini diharapkan dapat menjadi dasar bagi institusi lain dalam menerapkan sistem serupa untuk meningkatkan ketahanan jaringan mereka (Supriyadi & Gartina, 2007).

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif untuk merancang dan mengimplementasikan sistem monitoring serangan siber berbasis Honeypot menggunakan Cowrie. Metode kualitatif dipilih karena penelitian ini bertujuan untuk memahami pola serangan siber serta mengevaluasi efektivitas sistem yang diimplementasikan. Penelitian ini dilakukan melalui beberapa tahapan, yaitu:

1. **Pengumpulan Data**
   Data primer diperoleh melalui pengamatan langsung terhadap objek penelitian, yaitu jaringan komputer SMK Muhammadiyah 7 Gondanglegi. Selain itu, data sekunder dikumpulkan melalui studi literatur terkait Honeypot, keamanan protokol jaringan, dan serangan *brute force*.

2. **Pembuatan Model**
   Berdasarkan data yang diperoleh, dilakukan pemodelan sistem Honeypot Cowrie untuk memantau serangan yang menargetkan protokol SSH dan Telnet. Pemodelan ini mencakup skema interaksi antara sistem Honeypot, database MySQL, dan alat visualisasi Kippo-Graph.

3. **Analisis Kebutuhan**
   Tahap ini bertujuan untuk menentukan kebutuhan sistem, baik perangkat keras maupun perangkat lunak. Kebutuhan perangkat keras meliputi server dan perangkat jaringan, sedangkan kebutuhan perangkat lunak mencakup Honeypot Cowrie, MySQL, dan Kippo-Graph.

4. **Pembuatan Skema Penelitian**
   Skema penelitian dibuat untuk menggambarkan alur kerja sistem, mulai dari deteksi serangan oleh Honeypot Cowrie hingga visualisasi data serangan menggunakan Kippo-Graph.

5. **Desain Sistem**
   Tahap ini mencakup perancangan antarmuka sistem, struktur database, serta integrasi antara Honeypot Cowrie, database, dan Kippo-Graph.

6. **Implementasi dan Pengujian**
   Sistem yang telah dirancang diimplementasikan pada jaringan SMK Muhammadiyah 7 Gondanglegi. Pengujian dilakukan untuk mengevaluasi kinerja Honeypot dalam mendeteksi serangan, keakuratan data yang disimpan dalam database, dan kejelasan visualisasi yang dihasilkan oleh Kippo-Graph.

3. Hasil dan Pembahasan

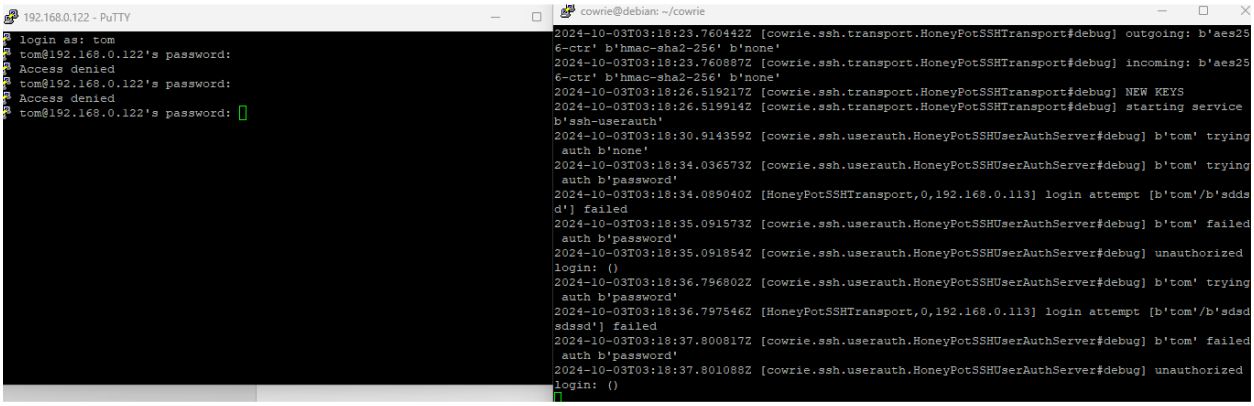
Pada tahap ini, dilakukan pengujian terhadap sistem keamanan jaringan komputer yang telah diimplementasikan pada server. Tujuan dari pengujian ini adalah untuk mengevaluasi efektivitas Honeypot Cowrie dalam mendeteksi serangan yang diarahkan ke server, khususnya serangan pada protokol SSH. Pengujian dilakukan dengan mensimulasikan serangan nyata menggunakan berbagai metode, salah satunya adalah melalui penggunaan SSH Putty.

3.1. Penyerangan pada Honeypot Cowrie

3.1.1 Penyerangan Menggunakan SSH Putty

Penyerangan ini dilakukan dengan memanfaatkan aplikasi SSH Putty untuk mencoba melakukan *brute force attack* pada server Honeypot. Tujuan dari pengujian ini adalah:

- Memastikan Honeypot Cowrie mampu mendeteksi dan mencatat setiap upaya masuk yang dilakukan melalui SSH.
- Mengamati bagaimana Cowrie mencatat detail serangan, seperti alamat IP penyerang, waktu serangan, nama pengguna, dan kata sandi yang digunakan dalam percobaan login.



Gambar 1. *Brute Force Attack pada Cowrie*

Honeypot Cowrie berhasil mencatat seluruh aktivitas penyerangan dengan detail, termasuk informasi berikut:

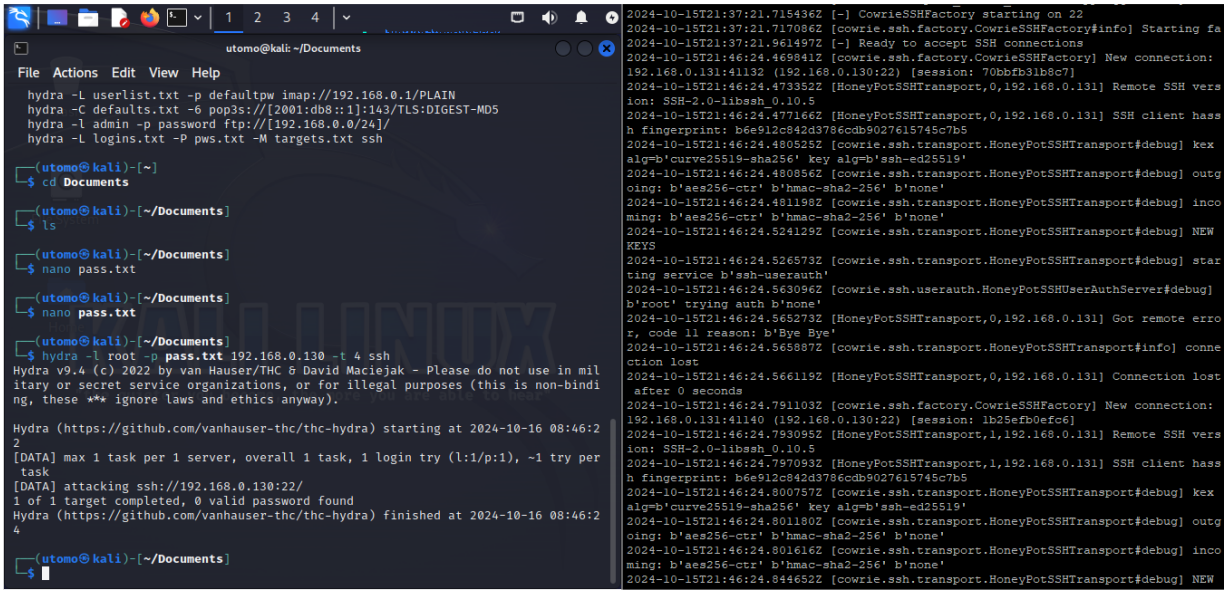
1. Alamat IP penyerang: 192.168.0.113.
2. Status percobaan login: Gagal. Semua *username* dan *password* yang diinputkan tidak berhasil membuka akses ke server.
3. Log Aktivitas: Tersimpan dalam database MySQL, termasuk detail percobaan login yang dilakukan.

Hasil pengujian menunjukkan bahwa sistem Honeypot Cowrie mampu:

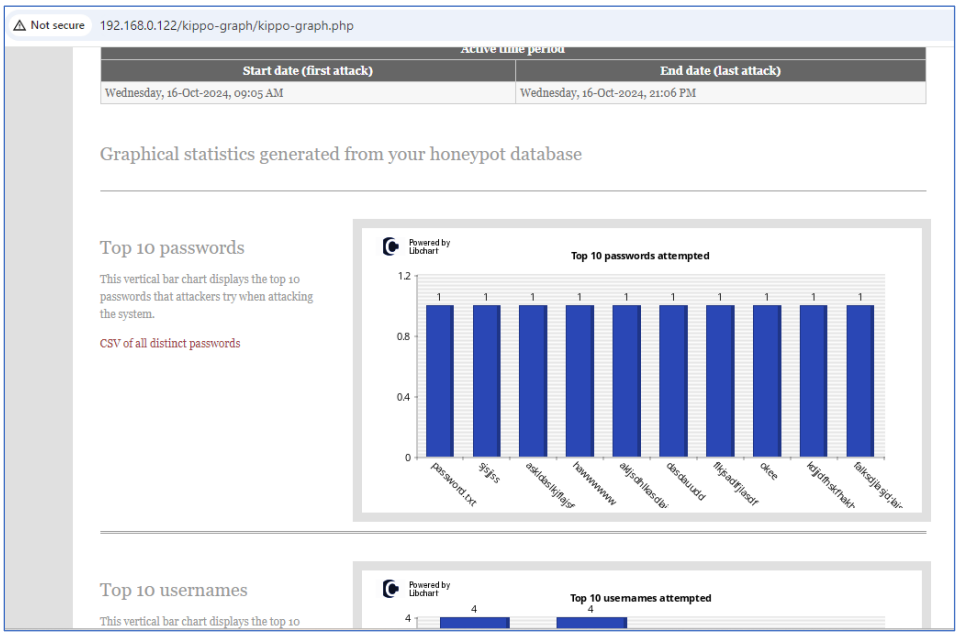
1. Mendeteksi dan mencatat setiap upaya penyerangan.
2. Memberikan informasi yang rinci dan akurat tentang serangan, sehingga mempermudah analisis pola serangan yang dilakukan.
3. Menjaga sistem server tetap aman tanpa terpengaruh oleh percobaan serangan.

3.1.2 Pengujian Penyerangan Menggunakan Hydra Kali Linux pada Honeypot Cowrie

Pengujian ini dilakukan dengan menggunakan *tool* Hydra pada sistem operasi Kali Linux untuk melakukan serangan *brute force* terhadap server Honeypot Cowrie. Hydra merupakan salah satu *tool* yang umum digunakan dalam simulasi serangan untuk mencoba kombinasi *username* dan *password* secara otomatis melalui file konfigurasi tertentu.



Gambar 2. *Brute Force Attack Menggunakan Hydra Kali Linux*



Gambar 3. *Tampilan Visualisasi Data Log Statistik*

Hasil simulasi serangan menggunakan Hydra menunjukkan:

- **Alamat IP penyerang**: 192.168.0.131 tercatat dalam log Cowrie.
- **Percobaan Login**: Semua percobaan menggunakan *username* dan *password* yang salah tidak berhasil membuka akses ke server.
- **Log Aktivitas Serangan**:
    - Cowrie mencatat detail setiap percobaan login, termasuk waktu, alamat IP, dan kredensial yang digunakan.
    - Data serangan berhasil divisualisasikan menggunakan Kippo-Graph untuk mempermudah analisis.

3.2 Pembahasan

Pengujian serangan brute force pada server Honeypot Cowrie menggunakan dua metode, yaitu melalui SSH Putty dan Hydra pada Kali Linux, memberikan hasil yang konsisten dalam menunjukkan efektivitas sistem Honeypot Cowrie.

1. Penyerangan Menggunakan SSH Putty

Pengujian dengan SSH Putty bertujuan untuk mengevaluasi kemampuan Honeypot Cowrie dalam mendeteksi dan mencatat aktivitas penyerangan. Berdasarkan hasil pengujian, Honeypot Cowrie berhasil mencatat seluruh aktivitas brute force yang dilakukan. Informasi yang direkam meliputi alamat IP penyerang (192.168.0.113), waktu serangan, dan kombinasi *username* serta *password* yang diinputkan.

Log aktivitas yang dihasilkan menunjukkan bahwa semua percobaan login gagal karena kredensial yang digunakan tidak valid. Honeypot Cowrie menyimpan semua data serangan ini dalam database MySQL untuk analisis lebih lanjut. Dengan demikian, pengujian ini membuktikan bahwa Honeypot Cowrie mampu mendeteksi setiap upaya serangan dengan akurat, menjaga keamanan sistem server, dan memberikan informasi rinci yang mempermudah analisis pola serangan.

2. Penyerangan Menggunakan Hydra Kali Linux

Pengujian kedua dilakukan dengan memanfaatkan tool Hydra pada sistem operasi Kali Linux untuk mensimulasikan serangan brute force secara otomatis. Hasil pengujian menunjukkan bahwa Honeypot Cowrie berhasil mencatat semua aktivitas penyerangan, termasuk alamat IP penyerang (192.168.0.131), waktu serangan, dan kredensial yang digunakan dalam setiap percobaan login.

Seperti pada pengujian sebelumnya, semua percobaan login gagal, sehingga sistem server tetap aman. Selain itu, data serangan berhasil divisualisasikan menggunakan Kippo-Graph, yang menyajikan log aktivitas dalam bentuk grafik dan statistik. Visualisasi ini memberikan kemudahan dalam memahami pola serangan dan menjadi dasar untuk pengembangan strategi mitigasi ancaman.

Hasil kedua pengujian menunjukkan bahwa Honeypot Cowrie mampu mendeteksi, mencatat, dan menjaga keamanan sistem server dari serangan brute force. Informasi yang direkam, baik dalam bentuk log aktivitas maupun visualisasi menggunakan Kippo-Graph, memberikan wawasan penting tentang metode dan pola serangan yang digunakan oleh penyerang. Hal ini membuktikan bahwa Honeypot Cowrie adalah alat yang efektif untuk memantau dan menganalisis ancaman siber, sekaligus meningkatkan kesadaran keamanan jaringan pada institusi pendidikan seperti SMK Muhammadiyah 7 Gondanglegi.

4. Kesimpulan

Hasil penelitian menunjukkan bahwa sistem monitoring serangan cyber berbasis Honeypot Cowrie yang diimplementasikan di SMK Muhammadiyah 7 Gondanglegi terbukti efektif mendeteksi dan mencatat aktivitas serangan, khususnya brute force pada protokol SSH dan Telnet. Informasi penting seperti alamat IP penyerang, waktu serangan, dan kredensial login yang digunakan berhasil direkam secara rinci. Data serangan yang dikumpulkan divisualisasikan dengan jelas melalui Kippo-Graph, memudahkan analisis pola serangan dan memberikan wawasan mendalam untuk langkah mitigasi. Pengujian menggunakan SSH Putty dan Hydra membuktikan bahwa Honeypot Cowrie mampu mencatat seluruh aktivitas penyerang, termasuk serangan otomatis. Implementasi sistem ini berhasil meningkatkan kesadaran keamanan jaringan di lingkungan sekolah dan menjadi solusi efektif untuk memantau serta menganalisis ancaman cyber. Penelitian ini memberikan dasar yang kuat bagi pengembangan kebijakan keamanan yang lebih baik di masa depan.

5. Referensi

Arkaan, N., & Sakti, D. V. S. Y. (2019). Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH. Jurnal Nasional Teknologi Dan Sistem Informasi, 5(2), 112-120.

Dermawati, R., & Siregar, M. H. (2020). Implementasi Honeypot Pada Jaringan Internet Labor Fakultas Teknik UNIKS Menggunakan Dionaea Sebagai Keamanan Jaringan. Jurnal Ilmiah Edutic: Pendidikan dan Informatika, 7(1), 20-30.

Nurfadhilah, A. (2019). Implementasi honeypot cowrie untuk mendeteksi serangan brute force pada Software Defined Network (SDN). Open Library Telkom University.

Hassan, R. H., Ismail, S. J. I., & Periyadi, P. (2020). Implementasi Honeypot Dengan Metode Honeytrap. eProceedings of Applied Science, 6(2).

Wastumirad, A. W., & Darmawan, M. I. (2021). Implementasi Honeypot Menggunakan Dionaea Dan Kippo Sebagai Penunjang Keamanan Jaringan Komunikasi Komputer. Jurnal Teknologi, 9(1), 80-91.

Supriyadi, A., & Gartina, D. (2007). Memilih Topologi Jaringan Dan Hardware Dalam Desain Sebuah Jaringan Komputer. Informatika Pertanian, 16(2), 1037-1053.

Sutarti, S., & Khairunnisa, K. (2017). Perancangan dan analisis keamanan jaringan nirkabel dari serangan DDOS (Distributed Denial Of Service) berbasis Honeypot. PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 4(2).

NXNJZ. (2019, January 12). Deploying an interactive SSH honeypot on Debian 9. NXNJZ.

Sena, B. (2020, March 16). Kamu tak semanis HoneyPot. Kresec STIKOM Bali.

Cowrie Project. (n.d.). Kippo-Graph: Visualizing Kippo Data. Cowrie Documentation.