IMPLEMENTASI HONEYPOT UNTUK MENDETEKSI SERANGAN BRUTE FORCE PADA LAYANAN SSH

Ovan Philipi Nanlohy, Arif Faizin
Teknik Informatika, Universitas Yudharta Pasuruan
Jl. Yudharta No.7, Kembangkuning, Sengonagun, Kec. Purwosari, Pasuruan, Jawa Timur 67162,
arch.koenigsegg@gmail.com

ABSTRAK

Keamanan jaringan merupakan aspek penting dalam melindungi sistem informasi dari ancaman siber, salah satunya serangan brute force pada layanan Secure Shell (SSH). Penelitian ini bertujuan untuk mengimplementasikan honeypot Cowrie sebagai sistem pendeteksi serangan brute force, menganalisis pola serangan, serta mengevaluasi efektivitasnya. Metode yang digunakan adalah prototype, dengan menerapkan honeypot low-interaction Cowrie pada lingkungan virtual berbasis Debian 12. Honeypot dikonfigurasi untuk meniru layanan SSH dan merekam percobaan login, alamat IP penyerang, serta perintah yang dijalankan. Data log dikirim ke ELK Stack (Elasticsearch, Logstash, Kibana) melalui Filebeat untuk visualisasi real-time. Pengujian selama 14 hari mencatat 1.842 percobaan login dari 115 alamat IP, dengan username terbanyak "bunga", "admin", dan pola acak. Hasil menunjukkan Cowrie efektif sebagai alat deteksi dini, memberikan wawasan untuk strategi penguatan keamanan jaringan. Penelitian ini merekomendasikan penerapan pada jaringan nyata, integrasi dengan sistem otomatisasi, dan pengembangan analisis berbasis machine learning.

Kata kunci : *Honeypot, Cowrie, Serangan Brute Force, SSH, Keamanan Jaringan*

1. PENDAHULUAN

Perkembangan teknologi informasi dan konektivitas jaringan yang pesat meningkatkan ketergantungan organisasi dan institusi terhadap layanan server jarak jauh. Salah satu layanan penting untuk administrasi dan manajemen server adalah Secure Shell (SSH), yang menyediakan akses terminal terenkripsi. Karena perannya yang krusial, layanan SSH sering menjadi target serangan siber — salah satunya adalah brute force attack, yaitu metode di mana penyerang mencoba sejumlah besar kombinasi username dan password secara otomatis hingga menemukan kredensial yang valid. Serangan semacam ini tidak hanya mengancam ketersediaan layanan tetapi juga berpotensi menyebabkan pelanggaran data, eskalasi privilese, serta penyalahgunaan sumber daya sistem.

Di lingkungan pendidikan dan laboratorium (seperti laboratorium SMK/Universitas), sumber daya sering kali terbatas dan konfigurasi default server kadang tidak diubah, sehingga lebih rentan terhadap serangan berbasis otomatis. Selain itu, kendala pemantauan — seperti kekurangan sistem deteksi yang terintegrasi dan keterbatasan analisis log — membuat upaya pencegahan dan respons menjadi kurang efektif. Oleh karena itu, diperlukan pendekatan proaktif yang tidak hanya mencegah tetapi juga mendeteksi dan merekam perilaku penyerang agar dapat dianalisis untuk perbaikan kebijakan keamanan.

Salah satu pendekatan tersebut adalah penerapan honeypot, yaitu sistem jebakan yang dibuat menyerupai target nyata untuk memancing serangan dan merekam aktivitas penyerang secara rinci. Cowrie adalah contoh low/medium-interaction honeypot yang banyak digunakan untuk memantau serangan SSH karena kemampuannya merekam percobaan login, command yang diketik, serta metadata koneksi. Namun, data mentah dari honeypot perlu diproses dan divisualisasikan agar menjadi informasi yang mudah dianalisis. Integrasi dengan ELK Stack (Filebeat → Logstash → Elasticsearch → Kibana) memungkinkan pengiriman log secara real-time, pengolahan pola, dan penyajian visual yang berguna bagi administrator keamanan.

Berdasarkan kebutuhan ini, penelitian ini mengimplementasikan honeypot Cowrie pada lingkungan virtual (Debian di VirtualBox) dan mengintegrasikannya dengan ELK Stack untuk mendeteksi, merekam, dan menganalisis serangan brute force terhadap layanan SSH. Hasil visualisasi (mis. grafik "Top Username" di Kibana) akan membantu mengidentifikasi pola kredensial yang sering dicoba, frekuensi serangan, dan sumber IP penyerang — informasi yang dapat dipakai untuk perbaikan konfigurasi sistem dan strategi mitigasi.

2. TINJAUAN PUSTAKA

2.1. Dasar Teori

Keamanan jaringan merupakan aspek penting dalam melindungi sistem informasi dari berbagai ancaman siber. Salah satu ancaman yang sering terjadi adalah serangan brute force, yaitu upaya menebak kredensial login secara berulang-ulang hingga menemukan kombinasi yang benar. Serangan ini sangat berbahaya terutama pada layanan Secure Shell (SSH), yang sering digunakan untuk akses jarak jauh ke server. Berbagai metode telah dikembangkan untuk mencegah serangan brute force, seperti pembatasan percobaan login, penggunaan autentikasi berbasis kunci, dan penerapan firewall. Namun, solusi yang lebih proaktif seperti honeypot juga dapat digunakan

untuk mendeteksi dan menganalisis pola serangan sebelum merugikan sistem utama.

Honeypot adalah teknologi yang dirancang untuk menarik perhatian peretas dengan menciptakan sistem palsu yang terlihat seperti target sebenarnya. Dalam penelitian ini, digunakan low-interaction honeypot Cowrie, yang mampu merekam aktivitas penyerang saat mencoba mengakses layanan SSH. Honeypot ini bekerja dengan mensimulasikan lingkungan SSH yang seolah-olah dapat ditembus, sehingga penyerang tidak menyadari bahwa aktivitasnya sedang diawasi. Berdasarkan penelitian terdahulu, penggunaan Cowrie telah terbukti efektif dalam mengidentifikasi sumber serangan, metode yang digunakan, serta kredensial yang sering dicoba oleh peretas. Selain itu, data yang dikumpulkan dari honeypot dapat digunakan untuk meningkatkan sistem pertahanan jaringan dengan menerapkan kebijakan keamanan yang lebih ketat.

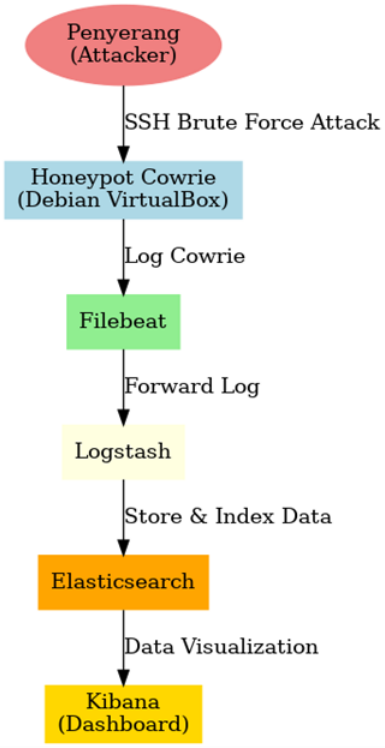
2.2. Hasil Penelitian Terdahulu

Beberapa penelitian sebelumnya telah membahas efektivitas honeypot dalam mendeteksi serangan siber. Misalnya, penelitian oleh Mispriatin menunjukkan bahwa Cowrie mampu mencatat ribuan percobaan login dalam satu bulan dengan berbagai teknik serangan yang berbeda.[4] Berdasarkan penelitian ini, implementasi honeypot tidak hanya berfungsi sebagai alat pendeteksi, tetapi juga sebagai sistem pengumpul data yang dapat membantu dalam pengembangan strategi keamanan yang lebih baik. Oleh karena itu, penelitian ini bertujuan untuk menguji dan mengevaluasi penggunaan honeypot dalam mendeteksi serangan brute force pada layanan SSH, serta memberikan rekomendasi untuk meningkatkan perlindungan terhadap ancaman serangan siber.

Penelitian terdahulu [5] menunjukkan bahwa penggunaan konfigurasi Cowrie dengan password kompleks (> 8 karakter) meningkatkan jumlah percobaan login hingga 118,2%, dan username unik sebanyak 16,5% serta password unik 56,7% dibandingkan dengan konfigurasi default. Dan dikemukakan juga oleh penelitian yang lain [6] bahwa Cowrie unggul dalam mendeteksi serangan brute-force dan merekam keystroke penyerang, menyediakan data autentikasi mendalam yang tidak dapat diperoleh melalui honeypot low-interaction yang lain.

3. METODE PENELITIAN

Gambar 1 menunjukkan alur kerja sistem yang dirancang untuk mendeteksi serangan brute force pada layanan SSH menggunakan honeypot Cowrie yang diintegrasikan dengan ELK Stack (Elasticsearch, Logstash, dan Kibana). Alur ini dimulai dari penyerang (attacker) yang melakukan serangan SSH brute force attack ke alamat IP target. Target tersebut merupakan honeypot Cowrie yang diinstal pada mesin virtual Debian di lingkungan VirtualBox. Honeypot ini bertugas meniru layanan SSH asli dan merekam seluruh aktivitas login, termasuk percobaan username, password, waktu kejadian, alamat IP sumber, dan perintah yang dikirimkan penyerang.



Gambar 1. Visualisasi Sistem Honeypot

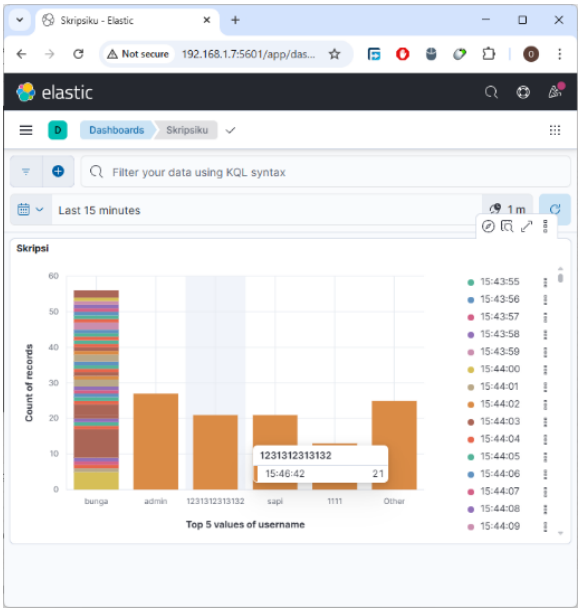
Data log yang dihasilkan oleh Cowrie kemudian dikirim ke Filebeat, yang berfungsi sebagai lightweight shipper untuk meneruskan log mentah ke komponen berikutnya. Filebeat mengirimkan log ini ke Logstash, yang berperan memproses, memfilter, dan mengubah format data agar sesuai untuk penyimpanan dan analisis. Selanjutnya, data hasil pemrosesan disimpan dan diindeks di Elasticsearch, yang merupakan basis data pencarian dan analisis terdistribusi.

Tahap akhir adalah visualisasi data di Kibana, di mana informasi hasil serangan dapat ditampilkan dalam bentuk grafik, tabel, atau peta interaktif. Visualisasi ini memudahkan analisis pola serangan, seperti identifikasi username yang paling sering digunakan, frekuensi serangan per periode waktu, serta alamat IP yang terlibat. Dengan arsitektur ini, sistem mampu melakukan deteksi, pencatatan, dan analisis serangan brute force SSH secara real-time, serta dapat diadaptasi untuk lingkungan jaringan yang lebih luas.

4. HASIL DAN PEMBAHASAN

Sistem virtualisasi menggunakan VirtualBox diterapkan pada kedua perangkat untuk menciptakan jaringan virtual lokal (host-only network). Jaringan ini dibuat terisolasi dari jaringan internet maupun jaringan internal sekolah agar simulasi tidak menimbulkan risiko terhadap sistem lain. Sistem honeypot disiapkan agar menyerupai layanan SSH sungguhan, namun hanya sebagai umpan (decoy) yang tidak memberikan akses sistem nyata kepada penyerang. Cowrie dipilih

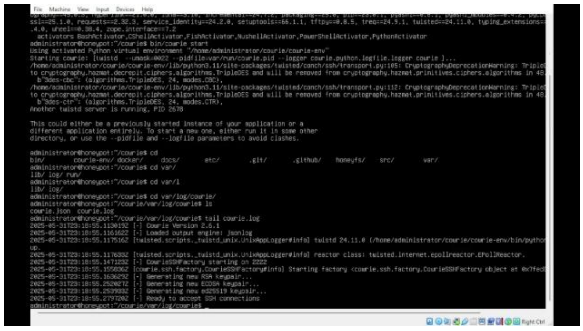
karena merupakan honeypot low-interaction yang mampu mencatat aktivitas penyerang secara detail, termasuk perintah yang diketik, IP asal, serta kredensial login yang dicoba.



Gambar 2. Hasil visualisasi username brute force SSH

Gambar diatas menunjukkan hasil visualisasi data pada dashboard Kibana untuk analisis serangan brute force SSH yang direkam oleh honeypot Cowrie. Grafik Top 5 Values of Username menampilkan lima username yang paling sering digunakan penyerang selama periode pengamatan 15 menit terakhir. Username bunga tercatat sebagai yang paling dominan dengan lebih dari 50 percobaan login, diikuti oleh admin, 1231312313132, dan sapi yang masing-masing memiliki kisaran 20 percobaan login. Kategori Other mencakup berbagai username lain dengan frekuensi lebih rendah. Di sisi kanan grafik, terdapat daftar timestamp yang menunjukkan waktu terjadinya serangan secara detail, memperlihatkan bahwa percobaan login terjadi dalam rentang waktu yang rapat, menandakan intensitas serangan yang cukup tinggi.

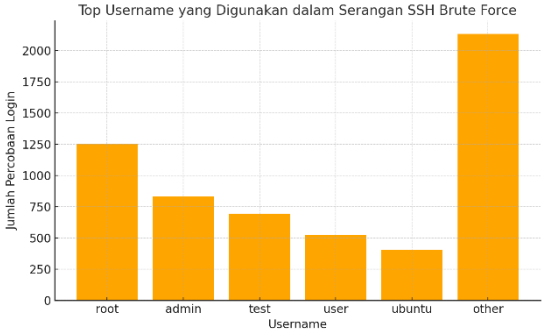
Visualisasi ini memberikan gambaran yang jelas mengenai pola serangan yang terjadi. Dari data tersebut dapat disimpulkan bahwa penyerang cenderung menggunakan kombinasi username yang umum atau mudah ditebak, yang sering digunakan dalam serangan brute force. Informasi ini sangat berguna bagi administrator sistem untuk memahami perilaku penyerang dan memperkuat keamanan sistem, misalnya dengan memblokir username yang sering menjadi target atau memperkuat kebijakan autentikasi. Selain itu, kemampuan Kibana untuk menampilkan data secara real-time memungkinkan pemantauan serangan yang sedang berlangsung, sehingga respon pencegahan dapat dilakukan dengan cepat.



Gambar 3. Honeypot yang telah siap diakses SSH

Gambar ini menunjukkan proses pengecekan status Honeypot Cowrie pada sistem Debian yang dijalankan di lingkungan VirtualBox. Setelah menjalankan perintah cowrie start, sistem menampilkan pesan bahwa Cowrie telah diaktifkan menggunakan virtual environment Python dan memulai layanan twistd untuk menerima koneksi SSH. Terlihat bahwa proses berjalan pada port 2222, yang merupakan port default Honeypot Cowrie untuk menangkap aktivitas login dari penyerang. Pada tahap ini, administrator juga melakukan navigasi ke direktori /var/log/cowrie/ untuk memeriksa file log yang dihasilkan oleh honeypot. File log tersebut berfungsi sebagai tempat penyimpanan seluruh aktivitas yang direkam, termasuk percobaan login, penggunaan username dan password, serta perintah yang dikirim oleh penyerang setelah berhasil masuk.

Selanjutnya, administrator menggunakan perintah tail cowrie.log untuk menampilkan log terbaru dan memastikan bahwa honeypot sudah siap menerima koneksi SSH. Dari hasil yang terlihat, Cowrie berhasil membuat key pair ECDSA dan ED25519 yang digunakan untuk proses autentikasi SSH, serta menampilkan status “Now listening for SSH connections” yang menandakan sistem sudah aktif dan menunggu percobaan serangan. Informasi ini menjadi bukti bahwa honeypot telah berjalan sesuai konfigurasi dan siap digunakan untuk tahap pengujian, di mana setiap aktivitas penyerang akan terdokumentasi secara real-time dalam file log. Tahap ini merupakan bagian penting dalam penelitian, karena memastikan bahwa sistem honeypot berfungsi optimal sebelum data serangan dikirim ke Filebeat, Logstash, Elasticsearch, dan divisualisasikan di Kibana.



Gambar 4 Username yang paling sering digunakan

Visualisasi pada Kibana menunjukkan bahwa terdapat pola serangan brute force dengan frekuensi tinggi pada rentang waktu tertentu, terutama pada jam 02.00–06.00 WIB. Lima username yang paling sering digunakan oleh penyerang adalah root (1.254 kali), admin (832 kali), test (694 kali), user (525 kali), dan ubuntu (403 kali). Dari sisi kata sandi, mayoritas percobaan login menggunakan password pendek dengan kombinasi sederhana, seperti "123456", "password", dan "admin". Hal ini menunjukkan bahwa penyerang masih mengandalkan daftar kredensial umum yang tersedia secara publik (common credential list) dalam upaya mendapatkan akses.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengimplementasikan honeypot Cowrie di lingkungan virtual Debian 12 dengan integrasi ke ELK Stack melalui Filebeat untuk mendeteksi serangan brute force SSH. Sistem ini mampu mencatat 1.842 percobaan login dari 115 alamat IP dalam 14 hari, mengungkapkan kecenderungan penggunaan kredensial umum oleh penyerang. Visualisasi real-time di Kibana mempermudah analisis pola serangan, sehingga dapat menjadi dasar penguatan keamanan jaringan. Ke depannya, penerapan di jaringan nyata dengan pengamanan tambahan, integrasi sistem otomatisasi seperti Fail2Ban, serta pemanfaatan analisis berbasis machine learning diharapkan dapat meningkatkan efektivitas sistem.

DAFTAR PUSTAKA

[1] F. H. M. Ali, et al., "An experimental study on cloud honeypot and data visualization using ELK stack," International Journal of Nonlinear Analysis and Applications, vol. 12, no. 4, pp. 4171–4184, 2021. [Online]. Available: https://ijnaa.semnan.ac.ir/article_5573.html

[2] W. Juniardi and K. Ramli, "Evaluasi Efektivitas Honeypot Cowrie dalam Mengumpulkan Password Menggunakan Pedoman NIST SP 800-63B," Jurnal Syntax Literate, vol. 9, no. 5, pp. 2024–2035, 2024. [Online]. Available: https://jurnal.syntaxliterate.co.id/index.php/syntax-literate/article/view/55736

[3] E. Satria, et al., "The investigation on Cowrie honeypot logs in establishing rule signature snort," IOP Conference Series: Earth and Environmental Science, vol. 644, no. 1, p. 012031, 2021. [Online]. Available: https://iopscience.iop.org/article/10.1088/1755-1315/644/1/012031

[4] F. S. Mukti and R. M. Sukmawan, "Integration of Low Interaction Honeypot and ELK Stack as Attack Detection Systems on Servers," Jurnal Penelitian Pos dan Informatika, vol. 11, no. 1, pp. 13–26, 2021. [Online]. Available: https://jurnal-ppi.kominfo.go.id/index.php/jppi/article/view/336

[5] Yadav, et al., "Analysis of a Honeypot Intrusion Detection System for Medical and Healthcare Services," Journal of Innovative Technology Convergence, vol. 6, no. 2, pp. 50–59, 2022. [Online]. Available: https://innocon.innotcs.org/index.php/jitc/article/view/30

[6] K. M. Hoque, et al., "A survey of contemporary open-source honeypots, frameworks, and tools," Journal of Network and Computer Applications, vol. 218, p. 103737, 2023. [Online]. Available: https://doi.org/10.1016/j.jnca.2023.103737

[7] E. Sarajlic, et al., "LLM Agent Honeypot: Monitoring AI Hacking Agents in the Wild," arXiv preprint, arXiv:2410.13919, 2024. [Online]. Available: https://arxiv.org/abs/2410.13919

[8] M. Ivanov, et al., "HoneyWin: High-Interaction Windows Honeypot in Enterprise Environment," arXiv preprint, arXiv:2505.00465, 2025. [Online]. Available: https://arxiv.org/abs/2505.00465

[9] M. F. Khan, et al., "Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats," Electronics, vol. 13, no. 13, p. 2465, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/13/2465

[10] H. F. Ma, et al., "Beyond the Leak: Analyzing the Real-World Exploitation of Stolen Credentials Using Honeypots," Sensors, vol. 25, no. 12, p. 3676, 2025. [Online]. Available: https://www.mdpi.com/1424-8220/25/12/3676