Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika
Volume 3, Nomor 4, Juli 2025
e-ISSN: 3031-8912; p-ISSN: 3031-8904; Hal. 240-246
DOI: https://doi.org/10.61132/merkurius.v3i4.949
Available online at: https://journal.arteii.or.id/index.php/Merkurius

Analisis Keamanan Layanan SSH terhadap Brute Force Attack

Putri Balqis[1] , Rakhmadi Rahman[2]
Sistem Informasi, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia
Email: puttbalqis23@gmail.com, rakhmadi.rahman@ith.ac.id

Abstract. *To securely access servers remotely, an important protocol in the modern era is Secure Shell (SSH). However, brute force attacks, which are automated attempts to guess repeated username and password combinations, are often the main target of this service. The purpose of this research is to evaluate the vulnerability of SSH services to brute force attacks and evaluate how effective Fail2Ban is as a mitigation tool. This method uses simulated experiments with two virtual machines; Kali Linux is used as the attacker with the Hydra tool and Ubuntu Server is used as the target. The results show that SSH is highly vulnerable to brute force attacks if not protected. Hundreds of login failures from the same IP without restrictions show this. After using Fail2Ban, the system can automatically find and block the attacker IP after three unsuccessful logins. With easy configuration and fast threat detection, Fail2Ban has been proven to improve the security of SSH services. This study suggests using Fail2Ban to improve the defense of SSH services against cyberattacks, especially brute force attacks.*

Keywords: *SSH, brute force, Fail2Ban, network security, cyberattack.*

Abstrak. Untuk mengakses server secara aman dari jarak jauh, protokol penting di era modern adalah Secure Shell (SSH). Namun, serangan brute force, yaitu upaya otomatis untuk menebak kombinasi username dan password yang berulang, seringkali menjadi sasaran utama layanan ini. Tujuan dari penelitian ini adalah untuk mengevaluasi kerentanan layanan SSH terhadap serangan brute force serta mengevaluasi seberapa efektif Fail2Ban sebagai alat mitigasi. Metode ini menggunakan simulasi eksperimen dengan dua mesin virtual; Kali Linux digunakan sebagai penyerang dengan alat Hydra dan Ubuntu Server digunakan sebagai target. Hasil penelitian menunjukkan bahwa SSH sangat rentan terhadap serangan brute force jika tidak dilindungi. Ratusan kegagalan login dari IP yang sama tanpa pembatasan menunjukkan ini. Setelah menggunakan Fail2Ban, sistem dapat secara otomatis menemukan dan memblokir IP penyerang setelah tiga kali login yang tidak berhasil. Dengan konfigurasi yang mudah dan deteksi ancaman yang cepat, Fail2Ban telah terbukti meningkatkan keamanan layanan SSH. Studi ini menyarankan untuk menggunakan Fail2Ban untuk meningkatkan pertahanan layanan SSH terhadap serangan siber, terutama serangan brute force.

Kata Kunci: SSH, brute force, Fail2Ban, Keamanan Jaringan, serangan siber.

1. PENDAHULUAN

Berbagai sektor, seperti pemerintah, bisnis, sekolah, dan layanan publik, telah menggunakan jaringan komputer lebih banyak karena kemajuan teknologi informasi. Keamanan jaringan menjadi komponen yang sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data dalam situasi ini. Secure Shell (SSH) adalah protokol yang paling umum digunakan untuk mengakses dan mengelola server secara jarak jauh. Karena komunikasinya terenkripsi, SSH lebih aman daripada protokol lama seperti Telnet. Namun, meskipun memiliki sistem keamanan yang kuat, layanan SSH masih menjadi sasaran utama serangan siber, terutama serangan brute force.

Brute force attack adalah jenis serangan yang dilakukan dengan otomatis mencoba berbagai kombinasi password dan username hingga menemukan yang benar. Serangan ini

Received: Juni 05, 2025; Revised: Juni 20, 2025; Accepted: Juli 06, 2025; Published: Juli 08, 2025

sangat efektif pada sistem yang tidak memiliki mekanisme perlindungan tambahan atau memiliki kredensial yang lemah. Seringkali, konfigurasi SSH standar tidak membatasi jumlah percobaan login, yang meningkatkan kemungkinan akses ilegal.

Dalam penelitian ini, alat Hydra digunakan untuk mengsimulasikan serangan brute force terhadap layanan SSH yang berjalan di Ubuntu Server. Selanjutnya, pengujian dilakukan untuk menggunakan Fail2Ban sebagai solusi untuk mengurangi serangan. Fail2Ban adalah alat yang berfungsi untuk memantau log dan dapat memblokir alamat IP penyerang setelah menemukan pola login yang tidak berhasil berulang. Tujuan dari penelitian ini adalah untuk mengevaluasi kemampuan Fail2Ban untuk menghentikan serangan brute force dan untuk memberikan pemahaman praktis tentang pentingnya proteksi tambahan pada layanan SSH untuk menjaga keamanan sistem jaringan.

2. TINJAUAN PUSTAKA

Keamanan jaringan komputer adalah bidang ilmu yang berkonsentrasi pada melindungi sistem, data, dan infrastruktur dari berbagai bahaya, baik internal maupun eksternal. Perlindungan layanan akses jarak jauh seperti Secure Shell (SSH) adalah komponen penting dalam keamanan jaringan karena merupakan protokol kriptografi yang umum digunakan untuk mengelola server secara aman dari berbagai lokasi. Dengan menyediakan enkripsi data dan autentikasi pengguna, protokol ini dapat menggantikan teknik lama seperti Telnet.

Meskipun SSH relatif aman, SSH masih rentan terhadap serangan brute force, yaitu upaya menebak kredensial secara berulang dengan alat bantu otomatis seperti Hydra. Serangan ini biasanya terjadi pada sistem yang menggunakan username dan password yang lemah dan tidak memiliki batasan login. Alat mitigasi seperti Fail2Ban diperlukan untuk mengatasi ancaman ini.

Proses Fail2Ban dimulai dengan memeriksa log sistem untuk menemukan pola upaya login gagal yang mencurigakan. Fail2Ban secara otomatis memblokir IP penyerang dengan aturan firewall jika jumlah percobaan melebihi ambang batas. Studi sebelumnya (Ridho et al., 2025; Utomo et al., 2024) menunjukkan bahwa Fail2Ban dapat secara signifikan mengurangi tingkat serangan brute force dan mudah digunakan pada server berbasis Linux. Oleh karena itu, metode ini menjadi solusi praktis untuk meningkatkan keamanan layanan SSH.

3. METODE PENELITIAN

Metode simulasi eksperimental digunakan dalam penelitian ini untuk menilai kerentanan layanan Secure Shell (SSH) terhadap serangan brute force dan kemanjuran Fail2Ban sebagai

mekanisme mitigasi. Sebagai platform virtualisasi, VMware Workstation digunakan untuk menjalankan seluruh operasi dalam lingkungan virtual.

Simulasi ini menggunakan dua komputer virtual. Mesin pertama menjalankan sistem operasi Kali Linux dan berfungsi sebagai peretas, sedangkan mesin kedua menggunakan server Ubuntu sebagai target yang menyediakan layanan SSH. Hydra adalah alat utama untuk melakukan serangan brute force, dan dikonfigurasi untuk mencoba berbagai kombinasi password dan username secara otomatis menggunakan file wordlist.

Eksperimen dilakukan dalam dua tahap utama. Tahap pertama bertujuan untuk melihat kemampuan layanan SSH untuk menerima percobaan login berulang dari IP yang sama dan merekam aktivitas yang terjadi pada log sistem /var/log/auth.log. Tahap kedua adalah simulasi serangan brute force terhadap layanan SSH tanpa sistem proteksi.

Pada tahap kedua, Fail2Ban harus diterapkan dan diuji pada server Ubuntu. Fail2Ban dikonfigurasi dengan parameter maxretry = 3, findtime = 180 (detik), dan bantime = 3600 (detik). Dengan demikian, jika tiga kali login gagal dalam waktu tiga menit, alamat IP akan diblokir selama satu jam. Serangan Hydra yang sama diulangi setelah konfigurasi selesai untuk melihat bagaimana sistem bertindak ketika Fail2Ban aktif.

Data dikumpulkan melalui beberapa metode, yaitu:

- Log sistem autentikasi SSH (/var/log/auth.log) untuk melacak percobaan login gagal dan reaksi sistem.
- Tangkapan terminal dari sisi attacker dan target untuk mendokumentasikan proses serangan dan pemblokiran.
- Screenshot sebagai dokumentasi visual dari setiap tahapan eksperimen, termasuk instalasi, konfigurasi, dan hasil simulasi.
- Log Fail2Ban dan status iptables untuk membuktikan pemblokiran IP penyerang.

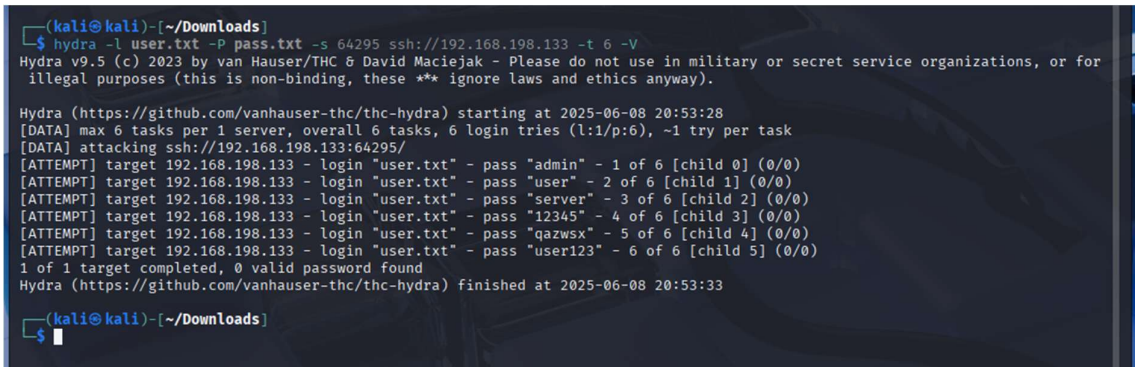
Analisis data dilakukan secara deskriptif dengan membandingkan kondisi sistem sebelum dan sesudah penerapan Fail2Ban. Fokus analisis adalah jumlah percobaan login, keberhasilan pemblokiran IP, dan kemampuan respon sistem untuk mendeteksi dan menghentikan serangan. Penelitian dengan metode ini diharapkan dapat menunjukkan efektivitas Fail2Ban sebagai solusi untuk mencegah serangan brute force pada layanan SSH.

4. HASIL DAN PEMBAHASAN

Tujuan dari penelitian ini adalah untuk menilai kerentanan layanan SSH terhadap serangan brute force dan mengevaluasi seberapa efektif Fail2Ban sebagai sistem mitigasi

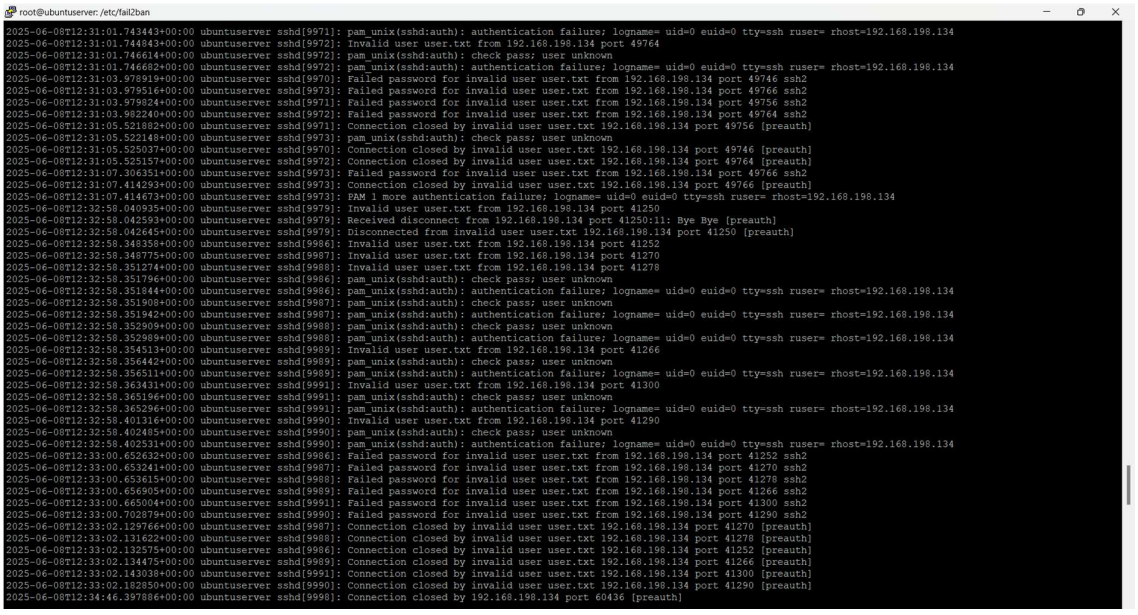
otomatis. Ini dimulai dengan dua skenario utama. Yang pertama adalah layanan SSH tanpa proteksi, dan yang kedua adalah layanan SSH dengan Fail2Ban yang aktif.

Pada skenario pertama, penyerang melakukan serangan brute force dengan menggunakan tool Hydra dari mesin Kali Linux terhadap server Ubuntu, yang secara otomatis menjalankan layanan SSH. Pengujian ini menghasilkan ribuan percobaan login otomatis dalam waktu singkat. Tanpa adanya reaksi atau perlindungan, sistem target mencatat semua aktivitas login gagal dalam berkas log /var/log/auth.log. Meskipun ratusan kali percobaan login gagal, tidak ada cara untuk memblokir IP penyerang. Hal ini menunjukkan bahwa sistem default tidak membatasi atau mendeteksi aktivitas mencurigakan, membuatnya sangat rentan terhadap serangan brute force. Gambar 4. 1 menunjukkan proses serangan ini.



Gambar 4. 1 Simulasi Serangan Brute Force SSH dengan Hydra

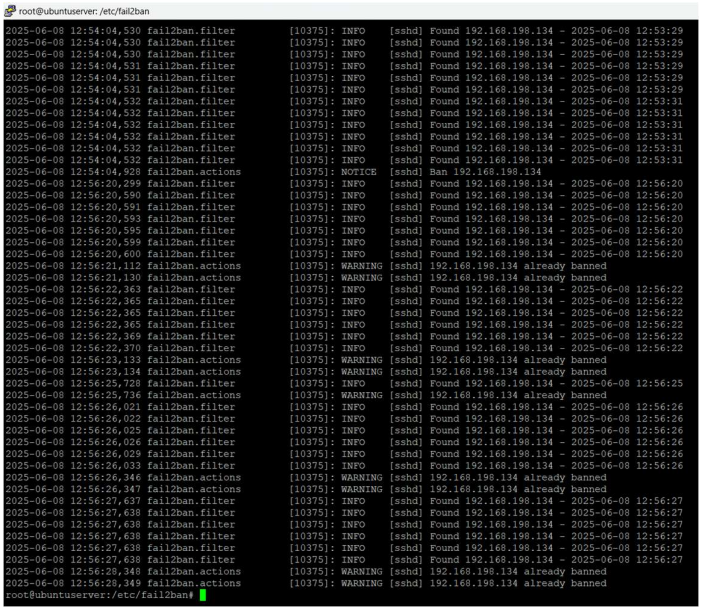
Selanjutnya, log sistem SSH yang menunjukkan percobaan login yang gagal secara terus-menerus ditampilkan pada Gambar 4. 2.



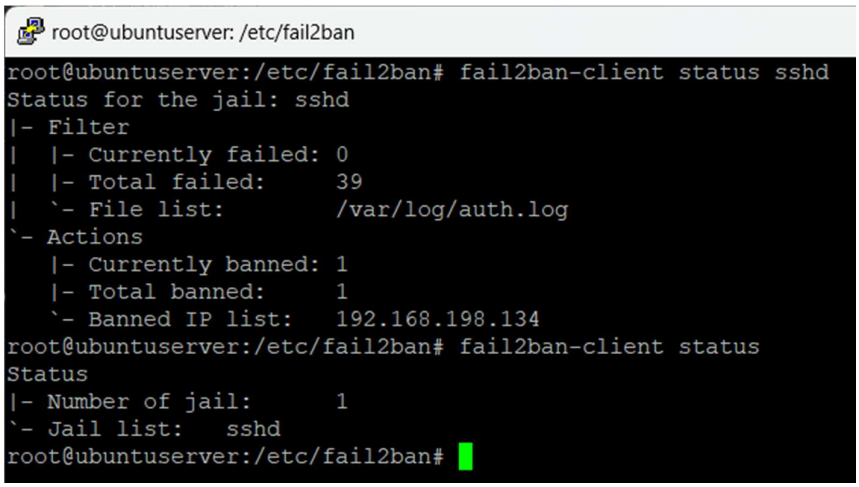
Gambar 4. 2 Log SSH Setelah Serangan Brute Force (Sebelum Fail2Ban)

Setelah langkah pertama selesai, Fail2Ban diinstal dan dikonfigurasi pada server Ubuntu. Fungsinya adalah untuk mengawasi log SSH dan memblokir IP address yang mencoba login tiga kali gagal dalam waktu tiga menit atau 180 detik. Dengan mengubah aturan iptables, pemblokiran dilakukan secara otomatis.

Serangan yang diulang dengan konfigurasi yang sama tidak menghasilkan hasil yang sama. Setelah tiga kali kegagalan login, Fail2Ban mendeteksi pola serangan dan memblokir alamat IP penyerang. Ini ditunjukkan pada log sistem (Gambar 4. 3) dan status Fail2Ban (Gambar 4. 4), yang menunjukkan bahwa satu IP aktif diblokir.



Gambar 4. 3 Log Sistem SSH Setelah Diblokir oleh Fail2Ban



Gambar 4. 4 Status Fail2Ban Menunjukkan IP Telah Diblokir

Hasilnya menunjukkan bahwa Fail2Ban dapat mendeteksi dan menanggapi serangan brute force secara real-time dengan baik. Alat ini tidak hanya menghentikan serangan, tetapi

juga mencegah tindakan lanjutan dari IP yang sama, yang membuat sistem lebih tahan terhadap serangan dari sumber yang sama.

Berikut ini adalah perbandingan kondisi sistem sebelum dan sesudah penerapan Fail2Ban untuk memperjelas hasil:

Tabel 4. 1 Perbandingan Kondisi Sebelum dan Sesudah Fail2Ban

Aspek	Sebelum Fail2Ban	Sesudah Fail2Ban
Proteksi Otomatis	Tidak tersedia	Tersedia (Fail2Ban aktif)
Respon terhadap serangan	Pasif (menerima semua percobaan)	Aktif (blokir IP otomatis)
Jumlah login gagal	Tidak terbatas	Maksimal 3 kali sebelum diblokir
Keamanan SSH	Rentan terhadap brute force	Lebih aman dan terkendali

Pembahasan ini menunjukkan bahwa menggunakan Fail2Ban menawarkan perlindungan yang signifikan secara mudah dan efektif. Untuk menggunakannya, hanya diperlukan konfigurasi sederhana yang dapat dilakukan oleh administrator sistem tingkat menengah, dan tidak membutuhkan perangkat keras atau software tambahan yang kompleks.

Namun, Fail2Ban memiliki beberapa keterbatasan meskipun berfungsi dengan baik. Alat ini tidak dapat menganalisis ancaman berbasis perilaku seperti sistem deteksi intrusi (IDS) atau sistem manajemen informasi keamanan dan peristiwa (SIEM). Pola login gagal dari log adalah satu-satunya respons yang dapat diterima oleh alat ini. Selain itu, Fail2Ban mungkin tidak dapat mengidentifikasi serangan yang tersebar dengan cepat jika peretas menggunakan teknik distribusi IP, seperti proxy atau botnet.

Oleh karena itu, Fail2Ban harus digunakan bersama dengan tindakan keamanan lainnya, seperti menggunakan kunci publik untuk SSH, mengatur firewall yang membatasi akses berdasarkan IP tertentu, dan melakukan monitoring sistem yang lebih menyeluruh. Namun, untuk server berskala kecil dan menengah yang belum memiliki sistem keamanan yang canggih, Fail2Ban tetap menjadi solusi mitigasi yang sangat bermanfaat dan mudah digunakan.

Akibatnya, penelitian ini menunjukkan bahwa penggunaan Fail2Ban secara signifikan melindungi layanan SSH dari serangan brute force, dan disarankan sebagai salah satu langkah penting dalam pengamanan server berbasis Linux.

5. KESIMPULAN

Hasil penelitian yang dilakukan melalui simulasi serangan brute force menggunakan Hydra terhadap layanan SSH menunjukkan bahwa sistem tanpa perlindungan tambahan sangat rentan terhadap percobaan akses ilegal. Karena layanan SSH secara default tidak membatasi jumlah percobaan login yang gagal, penyerang dapat menggunakan berbagai kombinasi username dan password secara teratur.

Sebagai alat mitigasi, Fail2Ban terbukti efektif dalam mencegah serangan kekerasan. Dengan konfigurasi yang tepat, Fail2Ban dapat melacak file log autentikasi SSH dan secara otomatis memblokir alamat IP yang melakukan percobaan login gagal jika melebihi batas. Dalam simulasi ini, IP penyerang diblokir dengan sukses setelah tiga kali percobaan login gagal. Pemblokiran ini meningkatkan keamanan layanan SSH dan menghentikan proses brute force secara langsung.

Fail2Ban sangat cocok digunakan sebagai alat tambahan untuk melindungi server skala kecil hingga menengah karena mudah digunakan dan tidak membutuhkan banyak sumber daya. Singkatnya, pengawasan log dan pemblokiran otomatis Fail2Ban adalah cara yang efektif untuk melindungi layanan SSH dari ancaman brute force attack.

6. DAFTAR PUSTAKA

[1]. Christopher, W., & Hermawan, R. Z. (2024). Pemantauan dan Pengawasan Serangan Siber SSH Brute Force di Indonesia dengan IBM QRadar Community Edition. Jurnal Ilmiah Teknik Informatika (TEKINFO), 25(2), 120-127.

[2]. Utomo, B. R., Jati, N. H., Jati, A. K., Saputro, I. A., & Purwidiantoro, M. H. (2024, December). Analisis Implementasi Keamanan Jaringan dengan Fail2ban Terhadap serangan Bruteforce. In Prosiding Seminar Nasional Amikom Surakarta (Vol. 2, pp. 1211-1223).

[3]. Ridho, M. R. M., Hafizh, A., Dani, I., & Ariyadi, T. (2025). Peningkatan Keamanan SSH Server Berbasis Linux melalui Implementasi Fail2Ban dan Uji Serangan Brute Force. *Jurnal Penelitian Multidisiplin Bangsa*, *1*(12), 2206-2214.

[4]. Mubarok, K., & Romli, M. A. (2025). Implementasi Metode Rule Based dalam Mendeteksi Serangan Brute Force pada Owncloud: Implementation of Rule Based Method in Detecting Brute Force Attacks on Owncloud. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *5*(1), 159-167.