JOURNAL OF COMPUTER SCIENCE AND INFORMATICS ENGINEERING
VOL. 05, NO. 3, JULY 2026: 325-337
Doi: https://doi.org/10.55537/cosie.v5i3.1767

e-ISSN 2827-8356
p-ISSN 2827-9999

Deteksi Serangan Brute Force SSH Berdasarkan Log Sistem pada Debian 12

Detection of SSH Brute Force Attacks Based on System Logs in Debian 12

Serliana Barutu*[1], Rasit Junaedi Silalahi[2], Lotar Mateus Sinaga[3]
Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas
[1]serlianabarutu@gmail.com, [2]junaedilu3344@gmail.com, [3] lotarmateus88@gmail.com

Received: June 23, 2026 | Revised: June 29, 2026 | Accepted: July 11, 2026

Abstrak

Layanan Secure Shell (SSH) di server Linux sering kali menjadi sasaran serangan brute force. Penelitian ini bertujuan untuk menguraikan ciri-ciri log autentikasi yang terjadi saat sistem operasi Debian 12 menghadapi serangan tersebut. Metode eksperimen diterapkan pada jaringan lokal dengan menggunakan server Debian 12 sebagai target dan Kali Linux sebagai sebagai penyerang, serta alat Hydra sebagai sarana untuk melakukan serangan. Uji coba dilakukan dengan tiga skenario berdasarkan jumlah volume serangan, yaitu 10, 100, 500 kali percobaan login, sementara layanan Fail2Ban dimatikan. Analisis data dilakukan dengan cara kuantitatif dan deskriptif, menggunkan metrik Success Rate dan Failed Login Rate yang didasarkan pada catatan dari journalctl serta auth.log. hasil uji coba menunjukkan bahwa semakin tinggi tingkat serangan, maka semakin besar juga jumlah log yang dihasilkan. Dalam skenario yang melibatkan tigkat keberhasilan sebesar 0,2% dengan menerima 1 password saja. Penelitian juga menemukan batasan pasa sesi OpenSSH (mencapai batasan maksimum upaya autentikasi), tetapi Hydra dapat memulai sesi baru secara otomatis. Jadi, versi mencatat detail ketidaknormalan tanpa kehilangan data, sehingga sangta cocok dijadikan dasar utama untuk audit keamanan server.
Kata kunci: Brute Force, Debian 12, Forensik Log, Journalctl, SSH

Abstract

The Secure Shell (SSH) service on Linux servers is frequently targeted by brute-force attacks. This study aims to outline the characteristics of authentication logs generated when the Debian 12 operating system faces such attacks. An experimental method was applied within a local network using a Debian 12 server as the target and Kali Linux as the attacker, with Hydra utilized as the tool to execute the attack. The experiments were conducted across three scenarios based on the volume of attack attempts: 10, 100, and 500 login attempts, while the Fail2Ban service was deactivated. Data analysis was performed quantitatively and descriptively, using Success Rate and Failed Login Rate metrics derived from records in journalctl and auth.log. The test results indicate that a higher attack volume corresponds to a larger amount of generated logs. In a scenario involving a success rate of 0.2%, only 1 password was accepted. The study also identified limitations in OpenSSH sessions (reaching the maximum authentication attempt limit), though Hydra was able to initiate new sessions automatically. Therefore, the system records detailed abnormalities without data loss, making it highly suitable as a primary foundation for server security audits.
Keywords: Brute Force, Debian 12, Forensik Log, Journalctl, SSH

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong meningkatnya kebutuhan akan sistem administrasi server yang dapat diakses dari jarak jauh, sambil tetap memastikan keamanan komunikasi. Salah satu protokol yang paling umum dipakai adalah Secure Shell (SSH) karena

e-ISSN 2827-8356
p-ISSN 2827-9999

menawarkan sistem autentikasi serta komunikasi yang terenkripsi, sehingga administrator dapat mengelola server dengan aman melalui jaringan publik. Penggunaan SSH kini menjadi norma pada berbagai sistem operasi yang berbasis Linux, termasuk Debian, karena mampu melindungi kerahasiaan, integritas, dan keaslian data selama proses komunikasi berlangsung. Namun, layanan SSH yang tidak dilindungi pada jaringan juga beresiko menjadi target serangan siber jika pengaturan keamanan dan metode autentikasi tidak diterapkan dengan baik [1]. Dengan bertambahnya penggunaan layanan akses jarak jauh dalam lingkungan komputasi modern, perlindungan terhadap layanan SSH menjadi hal yang sangat penting untuk menjaga keamanan infrastruktur jaringan [2].

Salah satu ancaman yang paling umum menyerang layanan SSH adalah serangan brute force, yaitu metode penyerangan yang mencoba berbagai kombinasi username dan password secara berulang hingga menemukan kredensial yang benar. Biasanya, serangan ini dilakukan dengan perangkat lunak otomatis yang dapat menghasilkan ribuan percobaan autentikasi dalam waktu singkat. Salah satu aplikasi yang banyak digunakan untuk uji penetrasi dan simulasi serangan adalah Hydra, karena mendukung berbagai protokol autentikasi, termasuk SSH, dan mampu menggunakan daftar kata sandi yang telah disiapkan [3]. Hal ini membuat server yang memiliki kata sandi yang lemah atau pengaturan autentikasi yang kurang baik beresiko lebih tinggi untuk mengalami akses yang tidak sah oleh pihak yang tidak berwenang [4].

Berbagai studi telah dilakukan untuk memperkuat keamanan layanan SSH dari serangan brute force. Beberapa penelitian menggunakan Fail2Ban sebagai metode pencegahan yang berfungsi dengan memantau log autentikasi dan memblokir alamat IP yang mencoba login berulang kali [6]. Penelitian lain menerapkan metode analisis log untuk menemukan pola serangan serta menilai seberapa efektif pengaturan keamanan di server Linux [8]. Selain itu, penerapan honeypot banyak dimanfaatkan untuk mengumpulkan data tentang perilaku penyerang sehingga pengelola dapat memahami ciri-ciri serangan yang terjadi sebelum diterapkan di lingkungan produksi [7]. Kemajuan terbaru dalam penelitian bahkan menggabungkan analisis log dengan pendekatan kecerdasan buatan untuk meningkatkan kemampuan dalam mendeteksi berbagai pola serangan siber[2].

Meskipun banyak penelitian menunjukkan hasil yang positif dalam mendeteksi dan mengurangi serangan brute force, sebagian besar fokus pada pengembangan metode pertahanan, penggunaan honeypot, atau model klasifikasi yang didasarkan pada kecerdasan buatan. Penelitian yang khususnya meneliti karakteristik serangan brute force dengan menggunakan log autentikasi dari sistem Debian 12 dan berbagai skenario jumlah percobaan login masih tergolong sedikit [13]. Namun, log autentikasi sangat penting sebagai sumber informasi dalam proses audit keamanan, analisis insiden, dan evaluasi konfigurasi layanan SSH karena mampu merekam setiap aktivitas autentikasi yang terjadi dalam sistem [14]. Oleh karena itu, analisis log autentikasi sangat diperlukan untuk memahami pola serangan serta karakteristik aktivitas penyerang yang tercatat selama serangan brute force.

Disisi lain, pengoptimalan pencatatan log sistem di infrastruktur jaringan server memerlukan pemetaan metrik kinerja deteksi yang tepat untuk menilai efektivitas sistem pertahanan dengan cara yang objektif [5]. Pengembangan model pengawasan keamanan berbasis analisis log pada penggunaan visualisasi data yang interaktif untuk membantu administrator dalam mendeteksi anomali jaringan [6]. Proses pemantauan yang teratur ini krusial karena identifikasi awal anomali dapat menghindar eksploitasi lebih lanjut sebelum hacker berhasil mendapatkan akses administrator server [7]. Selain aspek pengawasan, investigasi forensik digital mengenai aktivitas ilegal seperti brute force sangat bergantung pada validitas rekamanan log autentikasi yang tidak terpengaruh oleh pihak luar [11]. Karena itu, pengujian kinerja sistem operasi dalam mengelola lonjakan beban log autentikasi sangat penting untuk menjamin stabilitas kinerja server saat menghadapi serangan besar [12]. Penggabungan antara analisis metrik deteksi dan pencatatan log bawaan sistem pada akhirnya akan membangun dasar arsitektur keamanan

e-ISSN 2827-8356
p-ISSN 2827-9999

server yang responsif terhadap ancaman siber saat ini.

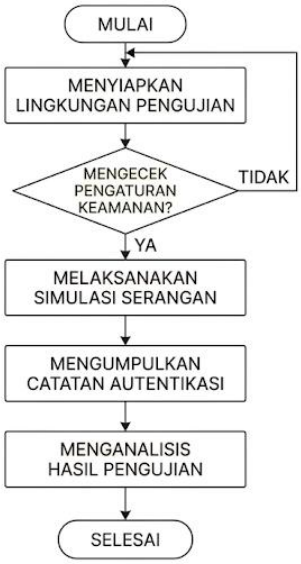
Berdasarkan isu yang ada, studi ini melakukan simulasi serangan brute force pada layanan SSH di sistem operasi Debian 12 dengan menggunakan aplikasi Hydra dalam tiga skenario pengujian, yakni 10 kali, 100 kali, dan 500 kali percobaan untuk masuk. Selama eksperimen berlangsung, layanan Fail2Ban dinonaktifkan sementara untuk memastikan bahwa mekanisme blokir otomatis tidak mengganggu proses brute force, sehingga seluruh kegiatan autentikasi dapat dicatat secara menyeluruh dalam log sistem. Log yang diperoleh kemudian dianalisis untuk menemukan pola serangan, jumlah upaya login yang gagal, alamat IP penyerang, serta ciri-ciri aktivitas autentikasi yang terjadi selama pengujian.

Hasil penelitian ini diharapkan bisa memberikan wawasan mengenai ciri-ciri serangan brute force terhadap layanan SSH berdasarkan analisis log autentikasi di Debian 12 dan menjadi acuan untuk administrator sistem dalam melakukan pemantauan, evaluasi, serta peningkatan keamanan layanan SSH. Selain itu, studi ini juga diharapkan dapat menjadi landasan bagi pengembangan penelitian selanjutnya yang berkaitan dengan analisis log serat penerapan mekanisme deteksi serangan pada sistem operasi yang berbasis Linux.

2. METODE PENELITIAN

Penelitian ini menerapkan metode eksperimen untuk menilai fitur-fitur serangan brute force terhadap layanan Secure Shell (SSH) di sistem operasi Debian 12. Pengujian dilaksanakan dalam jaringan lokal yang terdiri dari satu komputer sebagai server dan satu komputer sebagai penyerang. Server menggunakan layanan OpenSSH sebagai subjek pengujian, sedangkan komputer penyerang menjalankan sistem operasi Kali Linux dengan aplikasi Hydra untuk mensimulasikan serangan brute force. Metode eksperimen dipilih karena dapat menciptakan lingkungan pengujian yang terencana, di mana setiap proses autentikasi dapat diamati dan dianalisis dengan tepat.

Proses penelitian dimulai dengan menyiapkan lingkungan pengujian, mengecek pengaturan keamanan, melaksanakan simulasi serangan, mengumpulkan catatan autentikasi, hingga menganalisis hasil pengujian. Semua rangkaian penelitian ditampilkan pada Gambar 2.1, yang menggambarkan hubungan antara proses simulasi serangan menggunakan Hydra dan proses pencatatan log autentikasi di server Debian 12.

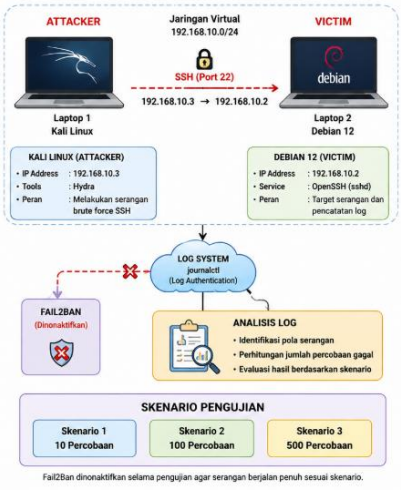


Gambar 1. Flowchart Penelitian

e-ISSN 2827-8356
p-ISSN 2827-9999

2.1 Lingkungan dan Skenario Pengujian

Lingkungan pengujian dibentuk dengan menggunakan dua perangkat yang terhubung dalam satu jaringan lokal. Server komputer memanfaatkan sistem operasi Debian 12 dan mengoperasikan layanan OpenSSH sebagai sasaran serangan, sementara komputer penyerang menggunakan Kali Linux untuk menjalankan Hydra. Topologi jaringan yang diterapkan dalam penelitian ini ditampilkan pada Gambar 2.2.



Gambar 2.Topologi Pengujian

Pengujian dilakukan dengan tiga skenario, yaitu 10 kali, 100 kali, dan 500 kali percobaan masuk. Ketiga skenario itu dimanfaatkan untuk mengidentifikasi perubahan pada karakteristik log autentikasi seiring dengan meningkatnya intensitas serangan. Selama eksperimen, layanan Fail2Ban dihentikan sesaat agar mekanisme pemblokiran IP tidak mengganggu proses brute force hingga jumlah percobaan login sesuai skenario tercapai. Setelah semua pengujian rampung, layanan Fail2Ban dihidupkan kembali untuk mengembalikan keadaan keamanan server.

Dalam setiap koneksi SSH menerapkan batasan jumlah autentikasi dalam satu sesi, sehingga setelah beberapa kali gagal login, akan muncul pesan ”maximum autentication attempts exceeded”. Keadaan itu tidak menghentikan keseluruhan proses brute force karena Hydra secara otomatis membuka sesi koneksi baru dan melanjutkan proses autentikasi hingga sekuruh jumlah percobaan yang ditentukan selesai. Oleh karena itu, baik skenario 100 maupun 500 percobaan masih bisa dilaksanakan meskipun setiap sesi SSH memiliki batas autentikasi.

2.2 Teknik Analisis Data

Data penelitian diambil dari log autentikasi yang dicatat oleh sistem operasi Debian 12 melalui journalctl da auth.log selama simulasi serangan brute force dilakukan. Data yang dianalisis mencakup alamat IP dari penyerang, nama pengguna, jumlah upaya login, jumlah autentikasi yang gagal, autentikasi yang berhasil, waktu kejadian, serta pesan sistem yang muncul selama proses pengujian. Data tersebut selanjutnya dianalisis dalam tiga skenario pengujian, yaitu 10, 100, dan 500 percobaan login untuk memahami karakteristik serangan berdasarkan peningkatan jumlah percobaan autentikasi.

Analisis dilaksanakan dengan pendekatan kuantitatif serta deskriptif. Analisis kuantitatif bertujuan untuk menilai hasil pengujian berdasarkan tingkat keberhasilan serangan (Success Rate), tingkat kegagalan autentikasi (Failed Login Rate), dan rata-rata durasi eksekusi setiap

e-ISSN 2827-8356
p-ISSN 2827-9999

skenario. Pada saat yang sama, analisis deskriptif diterapkan untuk menguraikan perubahan ciri-ciri log autentikasi yang dihasilkan selama simulasi brute force.

Tingkat keberhasilan serangan (Success Rate) dihitung menggunakan persamaan (1) dengan :

1. $N_{success}$ = jumlah autentikasi yang berhasil (accepted password).
2. $N_{attempt}$ = jumlah total percobaan login

Persamaan (1) diterapkan untuk menetukan persentase keberhasilan Hydra dalam mendapatkan kredensial yang tepat di setiap skenario pengujian.

Tingkat kegagalan autentikasi (Failed Login Rate) dihitung menggunakan persamaan (2) dengan :

1. N_{failed} = jumlah autentikasi gagal (failed password).
2. $N_{attempt}$ = jumlah total percobaan login

Persamaan (2) dipakai untuk menentukan persentase kegagalan autentikasi selama simulasi brute force.

Selain melakukan perhitungan kuantitatif, penelitian ini juga menganalisis konten log autentikasi yang dihasilkan oleh Debian 12. Analisis itu mencakup jumlah pesan kata sandi gagal, kata sandi diterima, alamat IP sumber serangan, nama pengguna yang digunakan, waktu kejadian, serta munculnya pesan maksimum upaya autentikasi terlampaui. Hasil analisis dari masing-masing skenario selanjutnya dibandingkan untuk memahami dampak peningkatan frekuensi percobaan login terhadap sifat log autentikasi pada layanan OpenSSH.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Lingkungan Pengujian

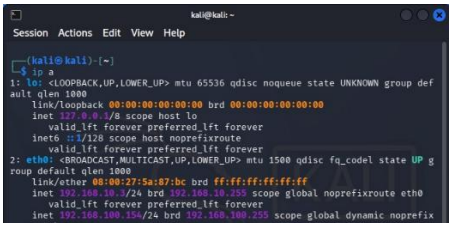
Penelitian ini dilakukan dengan memanfaatkan dua perangkat yang terhubung dalam jaringan lokal, yaitu satu komputer berperan sebagai server yang menjalankan sistem operasi Debian 12 satu komputer bertindak sebagai penyerang yang menggunakan Kali Linux. Interaksi antara kedua alat dilakukan melalui Secure Shell (SSH) sesuai dengan topologi jaringan yang telah dijelaskan pada metode penelitian.

Sebelum pengujian dilaksanakan, server disetting dengan alamat IP statis, layanan OpenSSH diaktifkan, dan pengguna mahasiswa dibuat sebagai sasaran autentikasi. Agar bisa mendapatkan semua aktivitas autentikasi selama simulasi brute force, layanan Fail2Ban dihentikan sementara dengan perintah systemctl stop fail2ban. Pemberhentian layanan ini bertujuan agar Fail2Ban tidak memblokir alamat Ip penyerang ketika jumlah upaya autentikasi yang gagal telah mencapai batas konfigurasi, sehingga proses penyerangan dapat berjalan hingga selesai dan seluruh log autentikasi dapat direkam oleh sistem. Setelah semua pengujian selesai, layanan Fail2Ban dihidupkan kembali agar sistem perlindungan server berjalan dengan baik.

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
ault qlen 1000
    link/ether 08:00:27:d8:49:8e brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.2/28 brd 192.168.10.15 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed8:498e/64 scope link
       valid_lft forever preferred_lft forever
```

Gambar 3. Konfigurasi Alamat IP server Pada Debian 12

e-ISSN 2827-8356
p-ISSN 2827-9999



Gambar 4. Konfigurasi Alamat IP Pada Kali Linux

Gambar 3.1 menunjukkan bahwa server Debian 12 menggunakan alamat IP 192.168.10.2, sedangkan Gambar 3.2 disisi penyerang menggunakan alamat IP 192.168.10.3. kedua perangkat berada pada subnet yang sama sehingga proses komunikasi SSH dapat berlangsung tanpa hambatan.

```
root@ser:~# id mahasiswa
uid=1004(mahasiswa) gid=1004(mahasiswa) groups=1004(mahasiswa),100(users)
root@ser:~#
```

Gambar 5. Verifikasi Akun Target

Akun mahasiswa digunakan untuk dijadikan sebagai target autentikasi selama proses simulasi serangan. Akun tersebut berhasil dibuat dan terdaftar pada sistem Debian 12 sehingga dapat dijadikan sebagai objek pengujian.

```
root@ser:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Thu 2026-07-02 16:10:50 WIB; 1h 4min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 803 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 811 (sshd)
      Tasks: 1 (limit: 5212)
     Memory: 2.8M
        CPU: 199ms
     CGroup: /system.slice/ssh.service
             └─811 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jul 02 16:10:49 ser systemd[1]: Starting ssh.service - OpenBSD Secure Shell ser>
Jul 02 16:10:50 ser systemd[1]: Started ssh.service - OpenBSD Secure Shell serv>
Jul 02 16:10:50 ser sshd[811]: Server listening on 0.0.0.0 port 22.
Jul 02 16:10:50 ser sshd[811]: Server listening on :: port 22.
lines 1-17/17 (END)
```

Gambar 6. Status Layanan SSH

Hasil verifikasi menunjukkan bahwa layanan OpenSSH sedang dalam kondisi active (running) sehingga siap menerima koneksi dari komputer penyerang.

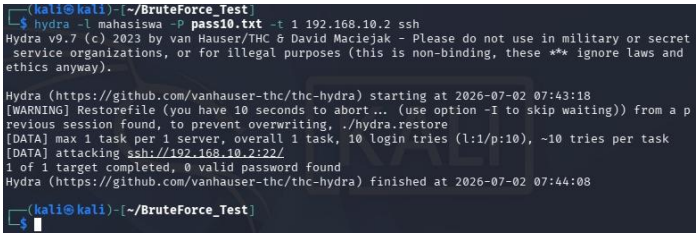
3.2 Hasil Pengujian

Pengujian dilaksanakan menggunakan Hydra dengan tiga skenario yang berbeda, yaitu 10, 100, dan 500 upaya login. Setiap skenario menggunakan akun sasaran mahasiswa dengan file rockyou.txt sebagai daftar kata. Semua kegiatan autentikasi dicatat menggunakan jounarctl dan auth.log.

3.2.1 Pengujian 10 Percobaan

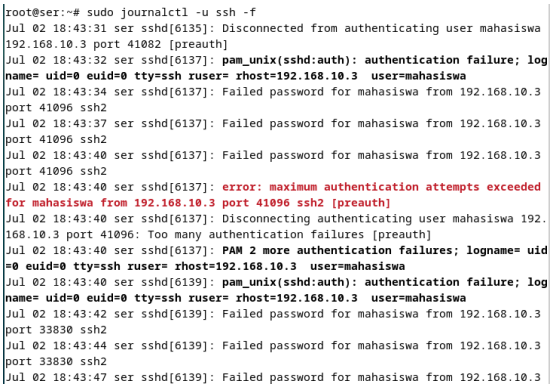
Dalam skenario pertama, Hydra dikonfigurasi untuk menjalankan sepuluh usaha login. Tujuan dari pengujian ini adalah untuk mengamati sifat awal log autentikasi saat jumlah percobaan masih sedikit.

e-ISSN 2827-8356
p-ISSN 2827-9999



Gambar 7. Hasil Hydra 10 Percobaan

Hydra berhasil melakukan sepuluh uji coba login ke layanan SSH. Setiap autentikasi berakhir dengan status gagal, sehingga kombinasi username dan password yang cocok masih belum ditemukan.



Gambar 8. Log journalctl 10 Percobaan

Log autentikasi menunjukkan setiap upaya login menghasilkan pesan password gagal. Data seperti alamat IP pelaku, nama pengguna, waktu autentikasi, dan status login berhasil dicatat secara menyeluruh.

Tabel 1. Hasil Pengujian 10 Percobaan

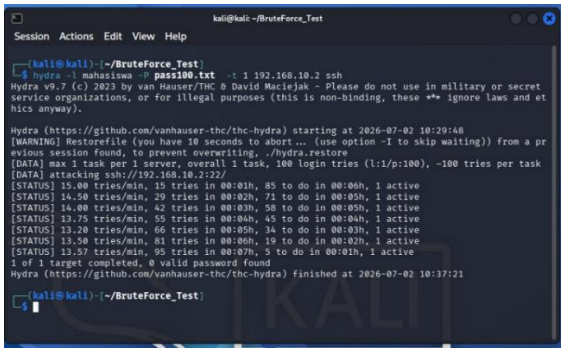
Parameter	Nilai
Jumlah Percobaan	10
Accepted Password	0
Failed Password	10
Succes Rate	0%
Failed Login Rate	100%

Berdasarkan hasil tersebut, dapat disimpulkan bahwa semua autentikasi gagal, sehingga Succes Rate menjadi 0%, sementara Failed Login Rate mencapai 100%. Walaupun kredensial yang tepat belum ditemukan, semua aktivitas login tercatat dengan baik sebagai data yang bisa dimanfaatkan untuk analisis keamanan

3.2.2 Pengujian 100 Percobaan

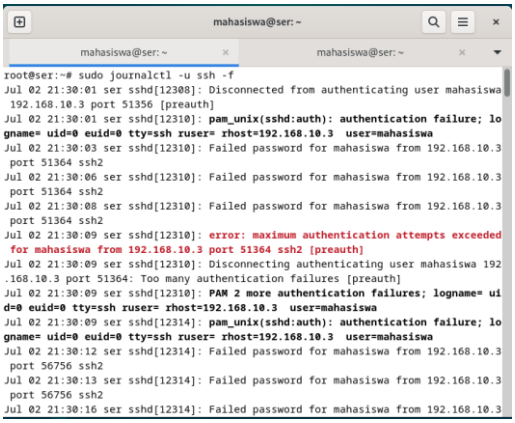
Dalam skenario kedua, frekuensi percobaan login ditingkatkan menjadi 100 kali untuk melihat perubahan karakteristik log autentikasi saat intensitas serangan meningkat.

e-ISSN 2827-8356
p-ISSN 2827-9999



Gambar 9. Hasil Pengujian Hydra 100 Percobaan

Hydra telah menyelesaikan semua tahap pengujian. Selama proses berlangsung, belum ada kombinasi kredensial yang tepat ditemukan, sehingga semua autentikasi tetap berstatus gagal.



Gambar 10. Log Autentikasi 100 Percobaan

Observasi menunjukkan kemunculan pesan maksimum percobaan autentikasi terlampaui pada beberapa sesi koneksi. Ini menunjukkan bahwa OpenSSH membatasi jumlah autentikasi dalam satu sesi, tetapi hydra secara otomatis membuka koneksi baru sehingga proses brute force dapat terus berlanjut hingga mencapai jumlah percobaan yang ditetapkan.

Tabel 2. Hasil Pengujian 100 Percobaan

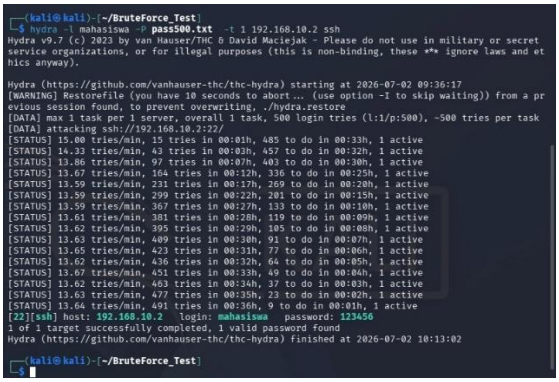
Parameter	Nilai
Jumlah Percobaan	100
Accepted Password	0
Failed Password	100
Succes Rate	0%
Failed Login Rate	100%

3.2.3 Pengujian 500 Percobaan

Skenario terakhir dilaksanakan dengan 500 upaya login guna menentukan apakah bertambahnya jumlah percobaan dapat meningkatkan kemungkinan keberhasilan serangan.

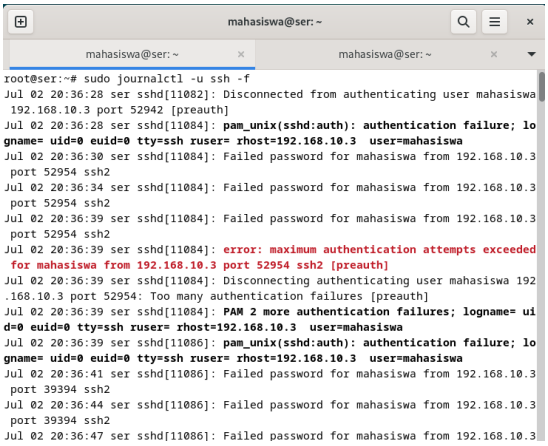
JOURNAL OF COMPUTER SCIENCE AND INFORMATICS ENGINEERING
VOL. 05, NO. 3, JULY 2026: 325-337
Doi: https://doi.org/10.55537/cosie.v5i3.1767

e-ISSN 2827-8356
p-ISSN 2827-9999

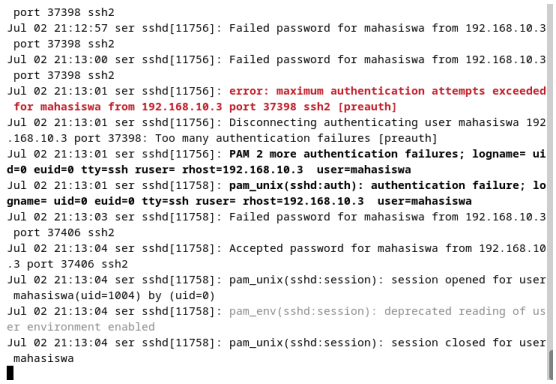


Gambar 11. Hasil Pengujian Hydra 500 Percobaan

Dalam situasi ini, Hydra berhasil mendapatkan kombinasi username dan password yang tepat sehingga proses brute force dihentikan secara otomatis.



Gambar 12. Log Autentikasi 500 Percobaan (Bagian 1)



Gambar 13. Log Autentikasi 500 Percobaan (Bagian 2)

Log autentikasi menunjukkan adanya dominasi pesan Gagal Kata Sandi yang kemudian diakhiri dengan munculnya pesan Kata Sandi Diterima. Hal ini menunjukkan bahwa kredensial berhasil diidentifikasi setelah banyak percobaan dilakukan.

e-ISSN 2827-8356
p-ISSN 2827-9999

Tabel 3. Hasil Pengujian 500 Percobaan

Parameter	Nilai
Jumlah Percobaan	500
Accepted Password	1
Failed Password	499
Succes Rate	0,2%
Failed Login Rate	99,8%

Hasil ini mengindikasikan bahwa kemungkinan sukses brute force bertambah seiring dengan meningkatnya jumlah upaya login, walaupun mayoritas autentikasi masih gagal.

3.3 Analisis Hasil Pengujian

Berdasarkan hasil pengujian yang telah dilakukan pada tiga skenario, yaitu 10, 100, dan 500 percobaan login, diperoleh rekapitulasi hasil sebagaimana ditunjukkan pada tabel 4.

Tabel 4. Rekapitulasi Hasil Pengujian

Parameter	10 Percobaan	100 Percobaan	500 Percobaan
Accepted Password	0	0	1
Failed Password	10	100	500
Total Percobaan	10	100	0,2%
Success Rate	0%	0%	99,8%
Failed Login Rate	100%	100%	100%

Berdasarkan Tabel 4 peningkatan jumlah upaya login berdampak pada kemungkinan keberhasilan serangan brute force. Dalam skenario 10 dan 100 percobaan, semua autentikasi dinyatakan gagal sehingga Rasio Success Rate sebesar 0% dan Rasio Failed Login Rate mencapai 100. Sementara itu, dalam skenario 500 percobaan, didapatkan 1 password Diterima dan 499 Password Gagal, sehingga Tingkat Success Rate naik menjadi 0,2% dan Failed Login Rate menjadi 99,8%.

Hasil tersebut mengindikasikan bahwa semakin banyak variasi kata sandi yang diuji, semakin tinggi kemungkinan Hydra mendapatkan kredensial yang salah. Semua aktivitas autentikasi juga berhasil dicatat oleh journalctl dan auth.log, sehingga log sistem dapat digunakan sebagai sumber informasi untuk audit keamanan maupun penyelidikan forensik digital.

3.4 Perbandingan dengan Penelitian Terdahulu

Tabel 5. Tabel Perbandingan Penelitian

Parameter	Penelitian Terdahulu 1	Penelitian Terdahulu 2	Penelitian Kami
Nama Author / Penulis	Fadilah Ramadhan, Sritrusta Sukaridhoto, dan R. Rizal Isnanto	Roni Sembiring, Janson Naiborhu, dan Dedi Budiarto	Serliana Barutu, Rasit Junaedi Silalahi

e-ISSN 2827-8356
p-ISSN 2827-9999

Judul Penelitian	Detection of SSH Brute Force Attacks Using Naïve Bayes Classification on Cowrie Honeypot Logs in a Virtualized Environment	Analisis Keamanan Layanan SSH terhadap Brute Force Attack	Deteksi Serangan Brute Force SSH Berdasarkan Log Sistem pada Debian 12
Tahun Terbit	2024 / 2025	2024	2026
Sistem Operasi & Lingkungan	Lingkungan Virtual (VM) menggunakan sistem Honeypot	Server Linux (Umum/Konfigurasi standar)	Debian 12 (Bookworm) & Kali Linux dalam Jaringan Lokal
Sumber Data / Sumber Log	Log dari data umpan Cowrie Honeypot	Log aktivitas network / service SSH umum	Log Sistem Resmi (auth.log dan journalctl) secara Native
Tools Penyerang / Simulasi	Brute Force Simulator umum	Penetration Testing Tools umum	Hydra dengan kamus kata (wordlist) rockyou.txt
Metode Skenario Pengujian	Klasifikasi Dataset menggunakan Algoritma Naïve BayesAnalisis Kelemahan	Analisis Kelemahan Port & Konfigurasi SSH	Pengujian Multiskala berbasis volume serangan (Skenario 10, 100, dan 500 Percobaan)
Hasil Temuan Utama / Parameter Sukses	Akurasi klasifikasi serangan berdasarkan deteksi pola log honeypot	Rekomendasi perkuatan enkripsi/keamanan port SSH	Karakteristik log mencatat lonjakan Failed Password hingga limit OpenSSH tercapai, serta mendeteksi Success Rate 0.2% pada 500 upaya.

Berdasarkan Tabel 5 inovasi penelitian ini dibandingkan dengan studi Ramadhan dkk. (berbasis honypot) dan sembiring dkk. (analisis umum) terletak pada (auth.log/journalctl) pada Debian 12 untuk memetakan serangan rill dari Hydra (rockyou.txt). Melalui pengujian multiskala (10, 100, 500 percobaan), terbukti bahwa penigkatan intensitas serangan meningkatkan Tingkat Keberhasilan dari 0% hingga 0,2% dan memicu batasan sesi (native behavioral limit) OpenSSH. Seluruh anomali ini mampu dicatat secara lengkap oleh log bawaan sistem tanpa memerlukan sumber daya eksternal, menjadikannya sangat efisien dan kuat sebagai dasar forensik digital server.

e-ISSN 2827-8356
p-ISSN 2827-9999

3. KESIMPULAN

Berdasarkan analisis dan pengujian yang telah dilaksanakan dapat disimpulkan bahwa log native Debian 12 (auth.log dan journalctl) dapat merekam seluruh aktivitas serangan brute force SSH dengan konsisten tanpa kehilangan informasi. Pengujian multiskla dengan Hydra (10, 100, 500 percobaan) menunjukkan bahwa peningkatan volume serangan sebanding dengan jumlah log yang dihasilkan, di mana skenario 500 percobaan berhasil meningkatkan Succes Rate menjadi 0,2% (1 Password yang Diterima). Walaupun OpenSSH di Debian 12 memiliki aturan batasan sesi (maximum authentication attempts exceeded), fitur ini belum sepenuhnya mengehntikan serangan karena Hydra dapat membuat sesi baru secara otomatis hingga pengujian selesai.

Berbeda dengan studi sebelumnya, sumbangan utama dari penelitian ini adalah pemetaan sifat log berdasarkan tingkat intensitas serangan serta evaluasi menyeluruh dengan menggunakan metrik kinerja deteksi. Optimalisasi analisis log bawaan Debian 12 terbukti sangat handal dan efisien sebagai dasar utama dalam proses audit keamanan, penyelidikan insiden, dan kenutuhan forensik digital pada server Linux.

DAFTAR PUSTAKA

[1] A. A. Hamza and J. s urayh Al-Janabi, “Detecting Brute Force Attacks on SSH and FTP Protocol Using Machine Learning: A Survey,” *J. Al-Qadisiyah Comput. Sci. Math.*, vol. 16, no. 1, pp. 21–31, Mar. 2024, doi: 10.29304/jqcsm.2024.16.11432.

[2] R. Mukherjee, “irpSSHa: Identifying and Reporting SSH Brute Force Attackers,” Nov. 29, 2024, *Social Science Research Network, Rochester, NY*: 5038715. doi: 10.2139/ssrn.5038715.

[3] “Brute-force attack mitigation on remote access services via software-defined perimeter | Scientific Reports.” Accessed: Jun. 21, 2026. [Online]. Available: https://www.nature.com/articles/s41598-025-01080-5

[4] F. Bäumer, M. Brinkmann, and J. Schwenk, “Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation,” May 07, 2024, *arXiv*: arXiv:2312.12422. doi: 10.48550/arXiv.2312.12422.

[5] F. Bäumer, M. Maehren, M. Brinkmann, and J. Schwenk, “Finding SSH Strict Key Exchange Violations by State Learning,” in *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2025, pp. 246–260. doi: 10.1145/3719027.3765208.

[6] A. A. Prasetyo, Herianto, Yahya, and N. Syamsiyah, “Detection of SSH Brute Force Attacks Using Naïve Bayes Classification on Cowrie Honeypot Logs in a Virtualized Environment,” *J. Technol. Inf. Data Anal.*, vol. 2, no. 1, pp. 62–65, Jun. 2025, doi: 10.70491/tifda.v2i1.88.

[7] P. Balqis and R. Rahman, “Analisis Keamanan Layanan SSH terhadap Brute Force Attack,” *Merkurius J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 3, no. 4, pp. 240–246, Jul. 2025, doi: 10.61132/merkurius.v3i4.949.

[8] O. P. Nanlohy and A. Faizin, “Implementasi Honeypot Untuk Mendeteksi Serangan Brute Force Pada Layanan SSH,” *JATI J. Mhs. Tek. Inform.*, vol. 9, no. 6, pp. 9454–9457, Nov. 2025, doi: 10.36040/jati.v9i6.15590.

[9] A. Nursetyo, B. Sugiarto, K. Kusnadi, S. M. Saleh, and B. A. Umam, “Pengujian Fail2Ban sebagai Mekanisme Pertahanan terhadap Serangan Brute Force,” *J. Media Inform.*, vol. 7, no. 1, pp. 335–343, Feb. 2026, doi: 10.55338/jumin.v7i1.7891.

[10] A. Ardiansyah, A. A. M. Suradi, and W. Saputra, “Strategi Keamanan Router MikroTik: Deteksi dan Mitigasi Serangan Brute Force Berbasis Scripting,” *JUKI J. Komput. Dan Inform.*, vol. 7, no. 1, pp. 12–19, May 2025, doi: 10.53842/juki.v7i1.970.

[11] M. R. M. Ridho, A. Hafizh, I. Dani, and T. Ariyadi, “Peningkatan Keamanan SSH Server Berbasis Linux melalui Implementasi Fail2Ban dan Uji Serangan Brute Force,” *J. Penelit. Multidisiplin Bangsa*, vol. 1, no. 12, pp. 2206–2214, May 2025, doi: 10.59837/jpnmb.v1i12.431.

e-ISSN 2827-8356
p-ISSN 2827-9999

[12] L. M. Sinaga and P. B. N. Simangunsong, "Analisis Keamanan SSH dengan Menggunakan Algoritma ECDSA pada Server Debian," *J. Multimed. Dan Teknol. Inf. Jatilima*, vol. 7, no. 5, pp. 1039–1049, Feb. 2026, doi: 10.54209/jatilima.v7i5.2146.
[13] T. Jeremya, A. Lombu, L. Daeli, and S. Bulolo, "Implementasi dan Analisis Keamanan Layanan SSH Server Menggunakan Autentikasi RSA dalam Lingkungan Virtualisasi dan Putty," *JITKO J. Inov. Teknol. Dan Komput.*, vol. 3, no. 1, pp. 33–45, Sep. 2025, doi: 10.54209/jitko.v3i1.143.
[14] A. B. Simbolon, D. Kiswanto, D. Siregar, and A. S. L. Gaol, "Rancang Bangun Sistem Analisis Log Jaringan Berbasis Web Untuk Deteksi Real-Time Ancaman Canggih Dan Gerakan Lateral," *J. Inform. Dan Tek. Elektro Terap.*, vol. 14, no. 1, Jan. 2026, doi: 10.23960/jitet.v14i1.8219.
[15] "Pattern-and Similarity-Based Realtime Risk Monitoring of SSH Brute Force Attacks with Bloom Filters," ResearchGate. Accessed: Jun. 21, 2026. [Online]. Available: https://www.researchgate.net/publication/385807996_Pattern-and_Similarity-Based_Realtime_Risk_Monitoring_of_SSH_Brute_Force_Attacks_with_Bloom_Filters
[16] A. Satpute, S. Nikam, V. Gaikwad, Y. Kakade, and C. Mhaske, "AI-Driven Intrusion Detection System Using SSH Honeypots," *ICCK Trans. Cybersecurity*, vol. 1, no. 1, pp. 3–12, Aug. 2025, doi: 10.62762/TC.2025.521799.
[17] J. Zhou, J. Yao, X. Chen, S. Yu, Q. Xuan, and X. Yang, "Lateral Movement Detection via Time-aware Subgraph Classification on Authentication Logs," Nov. 15, 2024, *arXiv*: arXiv:2411.10279. doi: 10.48550/arXiv.2411.10279.
[18] "Implementasi port knocking dinamis berbasis waktu pada router untuk pengamanan akses SSH | IT-Explore: Jurnal Penerapan Teknologi Informasi dan Komunikasi." Accessed: Jun. 21, 2026. [Online]. Available: https://ejournal.uksw.edu/itexplore/article/view/14448
[19] "Brute Force Attack | OWASP Foundation." Accessed: Jun. 21, 2026. [Online]. Available: https://owasp.org/www-community/attacks/Brute_force_attack