JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 2 April 2026, Page 194-202
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Pengujian Fail2Ban sebagai Mekanisme Pertahanan terhadap Serangan Brute Force

Arif Nursetyo[1*], Bambang Sugiarto[2], Kusnadi[3], Sahlan M. Saleh[4], Busro Akramul Umam[5]

[1,2,3]Teknik Informatika, Unversitas Catur Insan Cendekia, Kota Cirebon, Indonesia
[4]Informatika, Unversitas Yapis Papua, Papua, Indonesia
[5]Teknik Informatika, Universitas Islam Madura, Madura, Indonesia
Email: [1]arif.nursetyo@cic.ac.id, [2]bambang.sugiarto@cic.ac.id, [3]kusnadi@cic.ac.id, [4]sahlanmsaleh@gmail.com, [5]busro.umam@gmail.com
Email Penulis Korespondensi: [1]arif.nursetyo@cic.ac.id

Abstrak− Penelitian ini bertujuan mengevaluasi efektivitas Fail2Ban sebagai mekanisme pertahanan terhadap serangan brute force pada layanan SSH. Lingkungan eksperimen dibangun menggunakan dua mesin virtual: Ubuntu Server sebagai target dan Kali Linux sebagai penyerang. Fail2Ban dikonfigurasi melalui file jail.local dengan parameter maxretry=5, findtime=3m, dan bantime=1h. Serangan brute force dilakukan menggunakan Hydra dengan wordlist rockyou.txt terhadap akun root. Hasil simulasi menunjukkan bahwa Fail2Ban mendeteksi 28 percobaan login gagal dan secara otomatis memblokir IP penyerang (192.168.0.107). Temuan ini membuktikan bahwa Fail2Ban mampu memberikan perlindungan efektif terhadap serangan brute force berbasis SSH dengan konfigurasi yang tepat. Penelitian ini relevan untuk penguatan keamanan server Linux dan dapat dijadikan referensi praktis dalam pengembangan sistem pertahanan berbasis log monitoring.

Kata Kunci: Fail2Ban, Brute Force Attack, SSH Security, Hydra, Intrusion Prevention System

Abstract− This study evaluates the effectiveness of Fail2Ban as a defense mechanism against brute-force attacks on SSH services. The experimental setup involved two virtual machines: Ubuntu Server as the target and Kali Linux as the attacker. Fail2Ban was configured via the jail.local file with parameters maxretry=5, findtime=3m, and bantime=1h. A brute-force attack was launched using Hydra with the rockyou.txt wordlist against the root account. The results showed that Fail2Ban detected 28 failed login attempts and automatically blocked the attacker's IP address (192.168.0.107). These findings demonstrate that Fail2Ban provides effective protection against SSH brute-force attacks when properly configured. The study highlights its relevance for strengthening Linux server security and offers practical insights for implementing log-based intrusion prevention systems.

Keywords: Fail2Ban, Brute Force Attack, SSH Security, Hydra, Intrusion Prevention System

1. PENDAHULUAN

Keamanan sistem informasi merupakan aspek fundamental dalam pengelolaan infrastruktur teknologi di era digital. Pertumbuhan layanan berbasis jaringan, khususnya server yang menyediakan akses jarak jauh melalui protokol Secure Shell (SSH), telah meningkatkan risiko serangan siber [1]. Salah satu bentuk serangan yang paling umum adalah brute force attack, yaitu upaya sistematis untuk menebak kredensial login dengan mencoba kombinasi username dan password secara berulang. Serangan ini, meskipun sederhana, tetap menjadi ancaman serius karena dapat mengakibatkan pencurian data, pengambilalihan kontrol server, dan penyalahgunaan sumber daya jaringan [2], [3]. Dalam konteks ini, Fail2Ban hadir sebagai solusi berbasis intrusion prevention system (IPS) yang bekerja dengan memantau log autentikasi dan secara otomatis memblokir alamat IP yang menunjukkan pola serangan. Fail2Ban banyak digunakan pada server berbasis Linux karena sifatnya yang ringan, fleksibel, dan mudah dikonfigurasi [4]. Prinsip kerja Fail2Ban adalah membaca file log, mendeteksi percobaan login gagal yang melebihi ambang batas tertentu, kemudian menambahkan aturan pada firewall (misalnya iptables) untuk memblokir IP penyerang dalam jangka waktu tertentu [5], [6]. Dengan mekanisme ini, Fail2Ban mampu mengurangi risiko keberhasilan brute force sekaligus menekan beban sistem akibat serangan berulang [7].

Sejumlah penelitian sebelumnya telah membahas mekanisme pertahanan terhadap brute force. Misalnya, beberapa studi menekankan penggunaan IDS/IPS tradisional seperti Snort atau Suricata untuk mendeteksi pola serangan berbasis paket jaringan [8], [9]. Penelitian lain mengusulkan honeypot sebagai sarana mendeteksi aktivitas brute force dengan cara menjebak penyerang [10], [11]. Ada pula studi yang membandingkan efektivitas rate limiting pada layanan SSH [12]. Namun, sebagian besar penelitian tersebut memiliki keterbatasan, antara lain fokus pada deteksi tanpa pencegahan langsung, kompleksitas implementasi yang tinggi, minim simulasi praktis dengan tool serangan nyata, serta kurangnya dokumentasi sistematis berbasis workflow yang dapat direproduksi. Penelitian ini hadir untuk mengisi kesenjangan tersebut dengan kontribusi baru berupa pengujian praktis Fail2Ban

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 2 April 2026, Page 194-202
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

dalam skenario realistis menggunakan dua mesin virtual, yaitu Ubuntu Server sebagai target dan Kali Linux sebagai attacker [13], [14]. Simulasi brute force nyata dilakukan menggunakan Hydra dengan wordlist rockyou.txt, sehingga hasil lebih representatif terhadap serangan di lapangan [15]. Dokumentasi sistematis berupa konfigurasi, perintah, output log, dan status pemblokiran disajikan agar penelitian dapat direproduksi dan dijadikan referensi pembelajaran. Analisis efektivitas Fail2Ban juga dilakukan untuk menunjukkan keunggulannya sebagai solusi ringan dan praktis dibandingkan mekanisme pertahanan lain yang lebih kompleks.

Tujuan utama penelitian ini adalah untuk mengevaluasi efektivitas Fail2Ban sebagai mekanisme pertahanan terhadap serangan brute force pada layanan SSH. Penelitian dilakukan dengan cara mengkonfigurasi Fail2Ban pada Ubuntu Server agar mampu mendeteksi dan memblokir percobaan login yang mencurigakan. Selanjutnya, simulasi serangan brute force dilakukan menggunakan Hydra dari Kali Linux terhadap akun root pada server target. Melalui konfigurasi parameter maxretry, findtime, dan bantime, penelitian ini menganalisis sejauh mana Fail2Ban dapat memberikan perlindungan otomatis terhadap serangan berulang. Selain itu, penelitian ini juga menyajikan dokumentasi sistematis berupa konfigurasi, hasil serangan, dan status pemblokiran, sehingga dapat dijadikan referensi akademik maupun praktis. Dengan demikian, penelitian ini berkontribusi pada penguatan keamanan server berbasis Linux serta memperkaya literatur mengenai mekanisme pertahanan berbasis log monitoring yang ringan, reproducible, dan relevan untuk kebutuhan administrator, peneliti, maupun mahasiswa. Lingkungan simulasi terdiri dari dua mesin virtual dalam subnet yang sama (192.168.0.0/24), dengan Ubuntu Server beralamat IP 192.168.0.103 dan Kali Linux sebagai attacker beralamat IP 192.168.0.107. Fail2Ban dikonfigurasi dengan parameter maxretry=5, findtime=3m, dan bantime=1h. Serangan brute force dilakukan dengan Hydra terhadap akun root menggunakan wordlist rockyou.txt. Hasil simulasi menunjukkan bahwa Fail2Ban berhasil mendeteksi 28 percobaan login gagal dan memblokir IP attacker (192.168.0.107) secara otomatis, membuktikan efektivitas Fail2Ban dalam skenario nyata. Penelitian ini memberikan kontribusi pada penguatan keamanan server berbasis Linux dengan pendekatan praktis dan terukur. Dokumentasi hasil simulasi dapat digunakan sebagai bahan ajar dalam mata kuliah keamanan jaringan, sistem operasi, maupun laboratorium penetrasi. Dengan adanya analisis kesenjangan, penelitian ini menegaskan posisi Fail2Ban sebagai solusi yang relevan, ringan, dan efektif dibandingkan mekanisme lain yang lebih kompleks. Hasil penelitian diharapkan dapat menjadi referensi bagi administrator, peneliti, maupun mahasiswa dalam memahami dan mengimplementasikan mekanisme pertahanan terhadap brute force, sekaligus memperkuat literatur akademik mengenai sistem pertahanan berbasis log monitoring.

2. METODOLOGI PENELITIAN

2.1 Desain Penelitian

Penelitian ini menggunakan desain eksperimen simulasi dengan pendekatan kuasi-eksperimental. Lingkungan penelitian dibangun dalam bentuk virtual lab untuk memastikan kontrol penuh terhadap variabel dan kondisi jaringan. Desain penelitian melibatkan dua peran utama: server target yang dilengkapi Fail2Ban dan attacker yang menggunakan Hydra untuk melakukan brute force. Variabel independen dalam penelitian ini adalah konfigurasi Fail2Ban (parameter maxretry, findtime, dan bantime), sedangkan variabel dependen adalah efektivitas sistem dalam mendeteksi dan memblokir IP penyerang. Desain ini dipilih karena memungkinkan pengamatan langsung terhadap interaksi antara serangan brute force dan mekanisme pertahanan Fail2Ban dalam kondisi terkontrol.

2.2 Perangkat dan Perangkat Lunak

Perangkat keras yang digunakan adalah:

1. Komputer dengan spesifikasi prosesor AMD Ryzen 5 6000H, RAM 16 GB, dan penyimpanan 512 GB, yang menjalankan dua mesin virtual melalui VMware.
2. Mesin pertama adalah Ubuntu Server dengan alamat IP 192.168.0.103, berfungsi sebagai target serangan.
3. Mesin kedua adalah Kali Linux dengan alamat IP 192.168.0.107, berfungsi sebagai attacker.

Perangkat lunak utama yang digunakan meliputi:

1. Fail2Ban pada Ubuntu Server, sebagai mekanisme pertahanan berbasis log monitoring.
2. Hydra pada Kali Linux, sebagai tool brute force untuk melakukan simulasi serangan SSH.
3. VMware Workstation sebagai platform virtualisasi untuk menjalankan kedua sistem operasi.
4. Linux utilities seperti ifconfig, systemctl, dan fail2ban-client untuk konfigurasi jaringan, manajemen layanan, dan verifikasi status.

Kombinasi perangkat keras dan perangkat lunak ini dipilih karena mendukung simulasi realistis, fleksibel, dan dapat direproduksi.

2.3 Prosedur Penelitian

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024 Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 2 April 2026, Page 194-202
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Prosedur penelitian dilakukan dalam beberapa tahap sistematis meliputi:

1. Konfigurasi Jaringan: Menentukan alamat IP masing-masing mesin virtual agar berada dalam subnet yang sama (192.168.0.0/24).
2. Instalasi Fail2Ban: Menggunakan perintah sudo apt install fail2ban -y untuk memastikan Fail2Ban terpasang pada Ubuntu Server.
3. Konfigurasi Fail2Ban: Membuat file jail.local dari jail.conf dan mengatur parameter pada bagian [sshd] dengan nilai maxretry=5, findtime=3m, dan bantime=1h.
4. Aktivasi Layanan: Menjalankan Fail2Ban dengan systemctl restart fail2ban dan memastikan status aktif melalui systemctl status fail2ban.
5. Verifikasi Awal: Mengecek status jail SSH dengan fail2ban-client status sshd untuk memastikan sistem siap memantau log autentikasi.
6. Simulasi Serangan: Menjalankan Hydra dari Kali Linux dengan perintah hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.103. Hydra mencoba login ke akun root menggunakan wordlist populer.
7. Monitoring Log: Mengamati file /var/log/auth.log pada Ubuntu Server untuk mendeteksi percobaan login gagal.
8. Verifikasi Pemblokiran: Mengecek kembali status jail SSH dengan fail2ban-client status sshd untuk memastikan IP attacker diblokir.

2.4 Pengujian dan Validasi

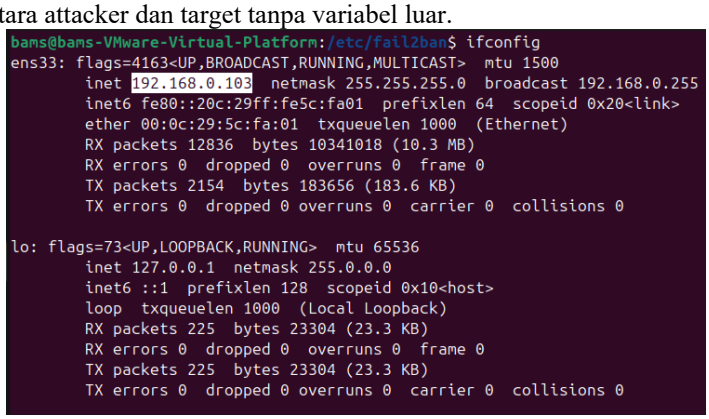
Pengujian dilakukan dengan cara mengukur respons Fail2Ban terhadap serangan brute force yang dilancarkan oleh Hydra. Validasi efektivitas dilakukan melalui beberapa indikator:

1. Jumlah percobaan login gagal: Fail2Ban harus mendeteksi percobaan gagal sesuai parameter maxretry.
2. Pemblokiran IP attacker: Fail2Ban harus menambahkan IP attacker ke daftar banned setelah ambang batas tercapai.
3. Durasi pemblokiran: IP attacker harus tetap diblokir selama periode bantime yang ditentukan.
4. Reproduksibilitas hasil: Proses harus dapat diulang dengan hasil konsisten, yaitu pemblokiran otomatis terhadap IP attacker.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Konfigurasi Jaringan

Tahap awal penelitian dilakukan dengan memastikan bahwa kedua mesin virtual, yaitu Ubuntu Server sebagai target dan Kali Linux sebagai attacker, berada dalam satu subnet. Hasil eksekusi perintah ifconfig pada Ubuntu menunjukkan bahwa interface ens33 memiliki alamat IP 192.168.0.103, sedangkan pada Kali Linux interface eth0 memiliki alamat IP 192.168.0.107. Kedua alamat IP berada dalam jaringan 192.168.0.0/24 dengan netmask 255.255.255.0. Kondisi ini memastikan bahwa komunikasi antar mesin dapat berlangsung tanpa hambatan, sehingga serangan brute force dapat disimulasikan secara langsung. Analisis dari hasil ini menunjukkan bahwa pemilihan jaringan lokal memberikan keuntungan berupa kontrol penuh terhadap lalu lintas data. Dengan demikian, setiap percobaan login gagal yang dilakukan oleh attacker dapat tercatat dalam log server tanpa adanya gangguan eksternal. Hal ini juga memudahkan proses monitoring dan validasi hasil, karena administrator dapat fokus pada interaksi antara attacker dan target tanpa variabel luar.

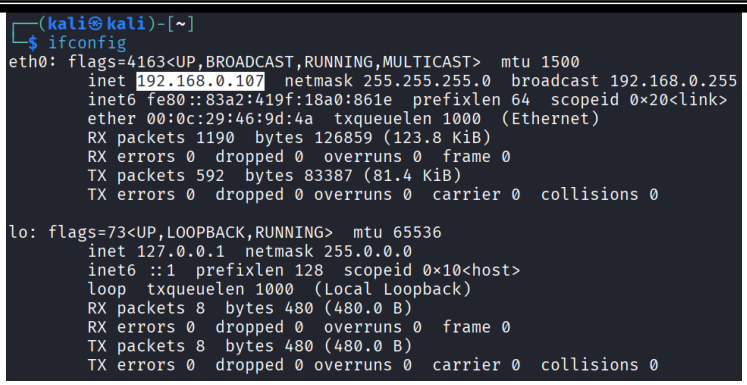


Gambar 1. Alamat IP Ubuntu Server

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 2 April 2026, Page 194-202
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



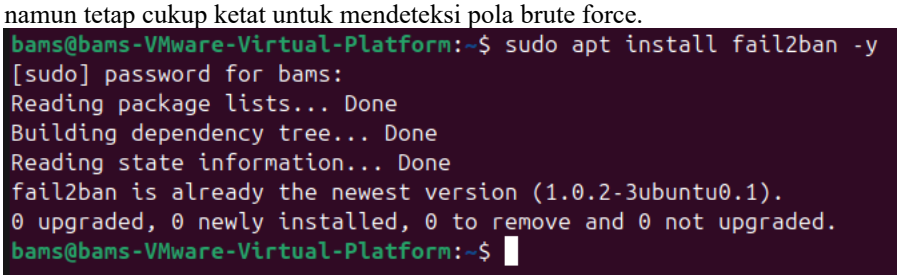
Gambar 2. Alamat IP Kali Linux

3.2 Hasil Instalasi dan Konfigurasi Fail2Ban

Langkah berikutnya adalah instalasi Fail2Ban pada Ubuntu Server. Perintah sudo apt install fail2ban -y menunjukkan bahwa Fail2Ban versi terbaru telah terpasang. Direktori konfigurasi /etc/fail2ban menjadi pusat pengaturan, di mana file jail.conf disalin menjadi jail.local untuk keperluan modifikasi. Hal ini sesuai dengan praktik standar agar konfigurasi asli tetap terjaga. Pada file jail.local, bagian [sshd] diaktifkan dengan parameter sebagai berikut:

a. enabled = true
b. port = ssh
c. logpath = /var/log/auth.log
d. maxretry = 5
e. findtime = 3m
f. bantime = 1h

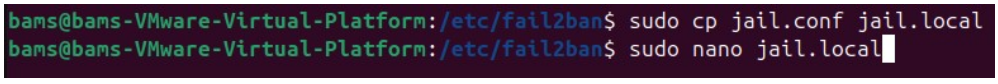
Hasil konfigurasi ini menunjukkan bahwa Fail2Ban akan memblokir IP penyerang apabila terdapat lebih dari lima percobaan login gagal dalam waktu tiga menit. IP yang diblokir tidak akan dapat mengakses server selama satu jam. Analisis terhadap parameter ini menunjukkan keseimbangan antara keamanan dan fleksibilitas. Dengan maxretry = 5, sistem masih memberikan toleransi terhadap kesalahan login yang mungkin dilakukan pengguna sah, namun tetap cukup ketat untuk mendeteksi pola brute force.



Gambar 3. Proses Install Fail2ban



Gambar 4. Pindah Direktori Ke Fail2ban



Gambar 5. Proses Penyalinan jail.conf menjadi jail.local

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 2 April 2026, Page 194-202
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
enabled = true
port    = ssh
logpath = /var/log/auth.log
maxretry = 5
findtime = 3m
bantime = 1h
backend = %(sshd_backend)s
```

Gambar 6. Konfigurasi File jail.local

3.3 Aktivasi Layanan Fail2Ban

Setelah konfigurasi selesai, layanan Fail2Ban dijalankan kembali dengan perintah sudo systemctl restart fail2ban untuk memuat ulang hasil konfigurasi dan sudo systemctl enable fail2ban digunakan untuk mengaktifkan layanan fail2ban. Hasil status menunjukkan bahwa fail2ban aktif dengan PID 5972, menggunakan memori sekitar 19 MB, dan siap memproses log autentikasi. Verifikasi awal melalui fail2ban-client status sshd menunjukkan bahwa belum ada percobaan login gagal maupun IP yang diblokir. Hal ini menandakan sistem dalam kondisi normal sebelum serangan dilakukan. Analisis dari hasil ini menegaskan bahwa Fail2Ban bekerja sebagai daemon yang terus-menerus memantau log. Aktivasi layanan merupakan tahap krusial, karena tanpa status aktif, konfigurasi tidak akan berfungsi. Dengan status "active (running)", sistem siap menghadapi serangan brute force yang akan disimulasikan.

```
bams@bams-VMware-Virtual-Platform:/etc/fail2ban$ sudo systemctl restart fail2ban
bams@bams-VMware-Virtual-Platform:/etc/fail2ban$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
bams@bams-VMware-Virtual-Platform:/etc/fail2ban$ sudo systemctl enable fail2ban && sudo systemctl status fail2ban

Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-12-03 14:41:57 WIB; 45s ago
       Docs: man:fail2ban(1)
   Main PID: 5972 (fail2ban-server)
      Tasks: 5 (limit: 4545)
     Memory: 19.2M (peak: 20.2M)
        CPU: 365ms
     CGroup: /system.slice/fail2ban.service
             └─5972 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Dec 03 14:41:57 bams-VMware-Virtual-Platform systemd[1]: Started fail2ban.service - Fail2Ban >
Dec 03 14:41:57 bams-VMware-Virtual-Platform fail2ban-server[5972]: 2025-12-03 14:41:57,905 f>
Dec 03 14:41:58 bams-VMware-Virtual-Platform fail2ban-server[5972]: Server ready
```

Gambar 7. Cek Status Layanan Fail2Ban

```
bams@bams-VMware-Virtual-Platform:/etc/fail2ban$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
bams@bams-VMware-Virtual-Platform:/etc/fail2ban$
```

Gambar 8. Kondisi Awal Status Client Sebelum Proses Eksploitasi

3.4 Hasil Simulasi Serangan Brute Force

Sebelum dilakukan serangan, Langkah awal yang harus dilakukan adalah dengan install Hydra dengan perintah sudo apt install hydra -y, hal ini dilakukan agar Hydra terpasang pada mesin penyerang yaitu Kali Linux. Simulasi serangan dilakukan dari Kali Linux menggunakan Hydra. Perintah yang digunakan adalah hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.103. Hydra mencoba login ke akun root pada server target

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 2 April 2026, Page 194-202
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

menggunakan wordlist rockyou.txt. Output menunjukkan bahwa Hydra melakukan percobaan login dengan kecepatan sekitar 30–58 percobaan per menit. Meskipun jumlah percobaan relatif kecil dibandingkan kapasitas wordlist yang besar, hal ini cukup untuk memicu deteksi Fail2Ban. Analisis dari hasil ini menunjukkan bahwa Hydra bekerja sesuai fungsinya sebagai tool brute force. Kecepatan serangan yang relatif rendah disebabkan oleh pembatasan protokol SSH, yang secara default membatasi jumlah koneksi paralel. Namun, meskipun kecepatan terbatas, pola serangan tetap jelas yaitu percobaan login berulang dengan kombinasi password yang berbeda. Pola ini menjadi indikator utama bagi Fail2Ban untuk melakukan deteksi.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install hydra -y
[sudo] password for kali:
hydra is already the newest version (9.6-3).
hydra set to manually installed.
The following packages were automatically installed and are no longer req
uired:
  amass-common               libsoup2.4-common
  firmware-ti-connectivity   libsqlcipher1
  gir1.2-girepository-2.0    libtheora0
  libarmadillo14             libtheoradec1
  libbluray2                 libtheoraenc1
  libbson-1.0-0t64           libudfread0
  libdisplay-info2           libvpx9
  libgdal36                  libwireshark18
  libgdata-common            libwiretap15
  libgdata22                 libwsutil16
  libgeos3.13.1              libx264-164
  libgirepository-1.0-1      linux-image-6.12.25-amd64
  libgpgmepp6t64             python3-bluepy
  libhdf4-0-alt              python3-click-plugins
  libinstpatch-1.0-2         python3-gpg
  libjs-jquery-ui            python3-kismetcapturebtgeiger
  libjs-underscore           python3-kismetcapturefreaklabszigbee
  libmongoc-1.0-0t64         python3-kismetcapturertl433
  libnet1                    python3-kismetcapturertladsb
  libobjc-14-dev             python3-kismetcapturertlamr
```

Gambar 9. Pemasangan Hydra Pada Kali Linux

```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-03 14:51:02
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
revious session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking ssh://192.168.0.103:22/
[STATUS] 58.00 tries/min, 58 tries in 00:01h, 14344343 to do in 4121:57h, 14 active
[STATUS] 38.00 tries/min, 114 tries in 00:03h, 14344287 to do in 6291:22h, 14 active
[STATUS] 30.29 tries/min, 212 tries in 00:07h, 14344189 to do in 7893:49h, 14 active
```

Gambar 10. Proses Eksploitasi Hydra dengan Kali Linux

3.5 Hasil Deteksi dan Pemblokiran oleh Fail2Ban

Setelah beberapa menit serangan berlangsung, Fail2Ban mendeteksi adanya 28 percobaan login gagal. Sesuai konfigurasi, Fail2Ban kemudian secara otomatis memblokir alamat IP attacker, yaitu 192.168.0.107. Verifikasi melalui perintah fail2ban-client status sshd menunjukkan status sebagai berikut:

a. Total gagal login: 28
b. Currently banned: 1
c. Banned IP list: 192.168.0.107

Hasil ini membuktikan bahwa Fail2Ban bekerja sesuai dengan parameter yang ditentukan. IP attacker diblokir setelah ambang batas tercapai, dan status pemblokiran dapat diverifikasi secara langsung. Analisis dari hasil ini menunjukkan efektivitas Fail2Ban dalam mencegah brute force. Dengan pemblokiran otomatis, attacker tidak dapat melanjutkan serangan, sehingga risiko keberhasilan brute force dapat ditekan. Fail2Ban efektif dalam mendeteksi dan memblokir serangan brute force SSH. Dengan konfigurasi yang tepat, Fail2Ban mampu memberikan perlindungan signifikan tanpa membebani sistem. Penelitian ini memberikan kontribusi akademis dan praktis, serta mengisi kesenjangan penelitian sebelumnya dengan pengujian praktis, simulasi nyata, dan

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 2 April 2026, Page 194-202
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

dokumentasi sistematis. Fail2Ban terbukti sebagai solusi ringan, efisien, dan efektif untuk melindungi server berbasis Linux dari ancaman brute force.

```
bams@bams-VMware-Virtual-Platform:/etc/fail2ban$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     28
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.0.107
bams@bams-VMware-Virtual-Platform:/etc/fail2ban$
```

Gambar 11. Hasil Eksploitasi Pada Ubuntu Server

Tabel 1 menunjukkan bahwa perbandingan sebelum dan sesudah serangan menunjukkan transformasi kondisi sistem dari keadaan normal menjadi terproteksi setelah simulasi brute force dilakukan. Sebelum serangan, jaringan antara Ubuntu Server dan Kali Linux berjalan normal tanpa gangguan, log autentikasi tidak mencatat percobaan login gagal, status Fail2Ban menunjukkan nol pada indikator gagal maupun IP terblokir, daftar IP banned kosong, dan server menerima koneksi SSH secara normal. Namun setelah Hydra dijalankan dari Kali Linux dengan wordlist rockyou.txt, tercatat 28 percobaan login gagal di log, Fail2Ban mendeteksi pola serangan sesuai konfigurasi maxretry=5 dan findtime=3m, lalu secara otomatis memblokir IP attacker (192.168.0.107) selama satu jam. Kondisi ini mengubah status server: koneksi dari attacker ditolak, daftar IP banned terisi, dan proteksi Fail2Ban terbukti efektif. Dengan demikian, tabel tersebut menegaskan bahwa Fail2Ban mampu mendeteksi serangan brute force SSH secara cepat, memberikan respon otomatis berupa pemblokiran IP, serta menjaga server tetap aman tanpa mengganggu koneksi sah, sehingga menjawab permasalahan penelitian mengenai efektivitas mekanisme pertahanan berbasis log monitoring.

Tabel 1. Kondisi Server Sebelum dan Sesudah Serangan

Aspek yang Diamati	Sebelum Serangan	Sesudah Serangan
Status Jaringan	Ubuntu Server (192.168.0.103) dan Kali Linux (192.168.0.107) aktif, komunikasi normal.	Jaringan tetap aktif, namun IP attacker (192.168.0.107) diblokir oleh Fail2Ban.
Log Autentikasi	Tidak ada percobaan login gagal yang tercatat di /var/log/auth.log.	Tercatat 28 percobaan login gagal dari IP attacker.
Status Fail2Ban (sshd)	Currently failed: 0, Total failed:0, Currently banned:0	Currently failed: 0, Total failed:28, Currently banned:1
Daftar IP Terblokir	Kosong	IP penyerang masuk daftar banned
Aktivitas Hydra	Belum dijalankan	Hydra melakukan serangan brute force
Respon Server	Server menerima koneksi normal	Server menolak koneksi dari IP attacker
Efektifitas Proteksi	Belum teruji	Terbukti efektif memblokir serangan

3.6 Pembahasan Efektivitas Fail2Ban

Hasil penelitian menunjukkan bahwa Fail2Ban efektif dalam mendeteksi dan memblokir serangan brute force SSH. Efektivitas ini dapat dianalisis dari beberapa aspek:

a. Fail2Ban mampu mendeteksi pola serangan dalam waktu singkat, yaitu setelah 28 percobaan login gagal. Hal ini sesuai dengan parameter maxretry=5 dan findtime=3m.
b. Fail2Ban secara otomatis menambahkan aturan pada firewall untuk memblokir IP attacker. Pemblokiran berlangsung selama satu jam, sesuai dengan parameter bantime=1h.
c. Fail2Ban hanya menggunakan sekitar 19 MB memori, menunjukkan bahwa mekanisme ini ringan dan tidak membebani sistem.
d. Proses dapat diulang dengan hasil konsisten, yaitu pemblokiran otomatis terhadap IP attacker.

Dibandingkan dengan mekanisme lain seperti IDS atau honeypot, Fail2Ban menawarkan keunggulan berupa kemudahan implementasi dan efisiensi. IDS tradisional hanya memberikan peringatan tanpa otomatis memblokir IP, sementara honeypot memerlukan konfigurasi yang lebih kompleks. Fail2Ban, dengan konfigurasi sederhana, mampu memberikan perlindungan langsung.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 2 April 2026, Page 194-202
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

3.7 Kontribusi Akademis dan Praktis

Penelitian ini memberikan kontribusi akademis berupa dokumentasi sistematis mengenai konfigurasi Fail2Ban, simulasi serangan brute force, dan hasil pemblokiran. Dokumentasi ini dapat dijadikan bahan ajar dalam mata kuliah keamanan jaringan dan sistem operasi. Selain itu, penelitian ini memberikan kontribusi praktis bagi administrator server, yaitu menunjukkan bahwa Fail2Ban dapat diimplementasikan dengan mudah untuk melindungi layanan SSH. Analisis kesenjangan menunjukkan bahwa penelitian sebelumnya cenderung fokus pada deteksi tanpa pencegahan langsung, kompleksitas implementasi, minim simulasi praktis, dan kurangnya dokumentasi sistematis. Penelitian ini mengisi kesenjangan tersebut dengan pengujian praktis, simulasi nyata menggunakan Hydra, dokumentasi sistematis, dan analisis efektivitas Fail2Ban.

3.8 Implikasi dan Rekomendasi

Implikasi dari penelitian ini adalah bahwa Fail2Ban dapat dijadikan solusi utama untuk melindungi server berbasis Linux dari serangan brute force SSH. Rekomendasi yang dapat diberikan adalah:

a. Penggunaan Fail2Ban secara luas pada server produksi untuk melindungi layanan SSH.
b. Penyesuaian parameter sesuai kebutuhan, misalnya memperpanjang bantime atau memperketat maxretry.
c. Integrasi dengan mekanisme lain seperti IDS atau honeypot untuk meningkatkan lapisan pertahanan.
d. Pengembangan penelitian lanjutan untuk membandingkan Fail2Ban dengan mekanisme lain, seperti rate limiting atau firewall berbasis AI.

4. KESIMPULAN

Penelitian ini membuktikan bahwa Fail2Ban merupakan mekanisme pertahanan yang efektif terhadap serangan brute force pada layanan SSH. Melalui konfigurasi parameter maxretry=5, findtime=3m, dan bantime=1h, sistem berhasil mendeteksi 28 percobaan login gagal dan secara otomatis memblokir IP penyerang (192.168.0.107). Hasil ini menunjukkan bahwa Fail2Ban tidak hanya mampu mendeteksi pola serangan, tetapi juga memberikan pencegahan langsung dengan respon cepat dan ringan tanpa membebani sistem. Dibandingkan dengan mekanisme lain seperti IDS/IPS tradisional, honeypot, atau rate limiting, Fail2Ban menawarkan solusi yang lebih sederhana, praktis, dan mudah diimplementasikan pada server berbasis Linux. Selain efektivitas teknis, penelitian ini juga memberikan kontribusi akademik berupa dokumentasi sistematis yang dapat direproduksi, sehingga relevan untuk pembelajaran di bidang keamanan jaringan maupun sistem operasi. Dengan demikian, Fail2Ban dapat dijadikan referensi penting bagi administrator, peneliti, dan mahasiswa dalam memahami serta mengimplementasikan mekanisme pertahanan berbasis log monitoring. Penelitian ini menegaskan posisi Fail2Ban sebagai solusi yang ringan, efisien, dan efektif dalam memperkuat keamanan server Linux dari ancaman brute force.

UCAPAN TERIMAKASIH

Rasa syukur dan terima kasih yang sebesar-besarnya kepada Allah SWT atas rahmat dan karunia-Nya sehingga penelitian ini dapat diselesaikan dengan baik. Ucapan terima kasih juga disampaikan kepada Universitas Catur Insan Cendekia yang telah memberikan dukungan akademik dan fasilitas penelitian, sehingga proses simulasi dan pengujian dapat berjalan sesuai rencana. Tidak lupa juga kepada rekan-rekan dosen dan tim yang telah memberikan masukan, bantuan teknis, serta motivasi selama pelaksanaan penelitian. Oleh karena itu, segala bentuk bantuan, baik langsung maupun tidak langsung, menjadi bagian penting dalam keberhasilan penelitian ini. Semoga hasil penelitian ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan jaringan, serta menjadi kontribusi nyata bagi dunia akademik dan praktisi teknologi informasi.

REFERENCES

[1] M. Ridho, A. Hafizh, I. Dani, and T. Ariyadi, “Peningkatan Keamanan SSH Server Berbasis Linux melalui Implementasi Fail2Ban dan Uji Serangan Brute Force,” vol. 1, no. 12, 2025, [Online]. Available: https://ejournal.amirulbangunbangsapublishing.com/index.php/jpnmb/index

[2] R. K. Abdullah, M. T. Fudhail, and S. Mujahidin, “Penggunaan Snort dan Fail2ban sebagai IDS untuk Mengatasi Brute Force Attack dengan Notifikasi Telegram: Studi Kasus pada Institusi XYZ,” *Jurnal Sistem dan Teknologi Informasi (JustIN)*, vol. 12, no. 3, p. 530, Jul. 2024, doi: 10.26418/justin.v12i3.79617.

[3] B. Rizky Utomo, N. A. Hanan Jati, A. Kusuma Jati, I. Ady Saputro, and M. Hari Purwidiantoro, “SEMINAR NASIONAL AMIKOM SURAKARTA (SEMNASA) 2024,” 2024.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024 Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**

[4] M. Hardjianto, "Sistem Monitoring Serangan Ssh Dengan Metode Intrusion Prevention System (IPS) Fail2ban Menggunakan Python Pada Sistem Operasi Linux," *Jurnal TICOM: Technology of Information and Communication*, vol. 11, no. 1, 2022.

[5] R. Ramadhan, J. Latuny, and S. J. Litiloly, "PERANCANGAN PENGAMANAN SERVER APACHE MENGGUNAKAN FIREWALL IPTABLES DAN FAIL2BAN," 2022.

[6] B. G. Akwaronwu, I. U. Akwaronwu, and O. J. Adeniyi, "Brute Force Attack Detection in Network Traffic Using Convolutional Neural Networks," *Original Research Article Akwaronwu et al.; Asian J. Res. Com. Sci*, vol. 2025, no. 5, pp. 387–402, 2025, doi: 10.9734/ajrcos/2025/v18i5662ï.

[7] Z. H. Abdelwahab, A. G. Abdellatif, I. M. Ibrahim, M. I. Ahmed, and A. A. Elmahallawy, "Robustness of Cloud Security against Brute-force Attack," *Advanced Sciences and Technology Journal*, vol. 0, no. 0, pp. 0–0, Dec. 2024, doi: 10.21608/astj.2024.341331.1015.

[8] B. Wibowo and L. Hafiz, "Risk Analysis of Bruteforce Attacks on Webserver with Telegram Notifications," *Jurnal Komputer dan Elektro Sains*, vol. 3, no. 1, pp. 28–32, Jan. 2025, doi: 10.58291/komets.v3i1.305.

[9] A. Noor, A. S. Aldafian, M. Tahir, M. Ersa, N. Firmansyah, and S. N. Khofifah, "Jurnal Restikom : Riset Teknik Informatika dan Komputer Implementasi IDS Wireshark untuk Deteksi Serangan DDoS SLOW HTTPS di Kali Linux," vol. 7, no. 2, pp. 148–161, 2025, [Online]. Available: https://restikom.nusaputra.ac.id

[10] O. P. Nanlohy and A. Faizin, "IMPLEMENTASI HONEYPOT UNTUK MENDETEKSI SERANGAN BRUTE FORCE PADA LAYANAN SSH," 2025.

[11] 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," *Journal TIFDA (Technology Information and Data Analytic)*, vol. 2, no. 1, pp. 62–65, Jun. 2025, doi: 10.70491/tifda.v2i1.88.

[12] A. Ali Hamza and J. s Urayh Al-Janabi, "Detecting Brute Force Attacks on SSH and FTP Protocol Using Machine Learning: A Survey," *Journal of Al-Qadisiyah for Computer Science and Mathematics*, vol. 16, no. 1, Mar. 2024, doi: 10.29304/jqcsm.2024.16.11432.

[13] M. Maisa, A. Dzarin, H. Mulyo, and A. Sucipto, "Kombinasi Algoritma Brute Force Dan Haversine Pada Sistem Informasi Geografis Fasilitas Kesehatan BPJS," *Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, 2024.

[14] N. T. Fadilla Inggriani, J. M. Parenreng, and M. Syahid Nur Wahid, "Implementasi Log Mikrotik Berbasis Database PostgreSQL dengan Teknologi Logging Syslog terhadap Serangan Brute Force," JIMU, 2025.

[15] T. A. Nuriansyah, M. A. Rahmadan, and E. Saputra, "Keamanan FTP Server Berbasiskan IPS Menggunakan Sistem Operasi Linux Ubuntu Versi 24.04. Jurnal Penelitian Multidisiplin Bangsa," vol. 2, no. 1, pp. 49–55, 2025, doi: 10.59837/jpnmb.v2i1.428.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **04/12/2025**; Accepted: **05/01/2026**; Published: **02/04/2026**