Implementasi Fail2Ban dan ELK Stack untuk Mitigasi Serangan Brute Force pada REST API Login E-Learning Berbasis Docker

Anggi Widi Laksono[1] Achmad Noercholis[2], Fransiska Sisilia Mukti[3]
[1,2,3]Fakultas Teknologi dan Desain, Institut Teknologi dan Bisnis Asia Malang
[1]anggiwidik@gmail.com, [2]anoercholis@asia.ac.id, [3]ms.frans@asia.ac.id

ABSTRACT

The increasing adoption of digital learning systems (E-Learning) has raised the need for security mechanisms capable of protecting authentication services from cyber threats. One of the most common threats is a brute force attack, which exploits repeated login attempts using automated username and password combinations. This study aims to implement Fail2Ban and the ELK Stack to mitigate brute force attacks on a Docker-based E-Learning Login REST API. The research employed an experimental method by developing a containerized environment consisting of an E-Learning Login REST API, Fail2Ban, Filebeat, Logstash, Elasticsearch, Kibana, and attacker containers. Brute force attack simulations were conducted using Hydra against the authentication service. Data were collected from authentication logs, Fail2Ban logs, and security monitoring results visualized through Kibana dashboards. The results show that Fail2Ban successfully detected 180 failed login attempts originating from six attacker IP addresses and automatically blocked all attacker IPs, achieving a mitigation success rate of 100%. The average mitigation response time ranged from 0.314 to 0.443 seconds with a bantime of 500 seconds. Furthermore, the ELK Stack successfully provided real-time visualization of failed login activities, attacker IP addresses, and blocking actions. The findings indicate that the integration of Fail2Ban and the ELK Stack in a Docker environment is effective in improving the security of the E-Learning Login REST API against brute force attacks through centralized detection, mitigation, and security monitoring mechanisms.

Keywords: brute force attack, Login REST API, E-Learning, Fail2Ban, ELK Stack, Docker.

ABSTRAK

Perkembangan sistem pembelajaran digital (E-Learning) meningkatkan kebutuhan akan mekanisme keamanan yang mampu melindungi layanan autentikasi dari berbagai ancaman siber. Salah satu ancaman yang sering terjadi adalah serangan brute force yang dilakukan melalui percobaan login berulang menggunakan kombinasi username dan password secara otomatis. Penelitian ini bertujuan mengimplementasikan Fail2Ban dan ELK Stack untuk mitigasi serangan brute force pada REST API Login E-Learning berbasis Docker. Metode penelitian yang digunakan adalah eksperimen dengan membangun lingkungan container yang

terdiri atas REST API Login E-Learning, Fail2Ban, Filebeat, Logstash, Elasticsearch, Kibana, dan attacker. Pengujian dilakukan melalui simulasi serangan brute force menggunakan Hydra terhadap layanan autentikasi. Data penelitian diperoleh dari log autentikasi, log Fail2Ban, serta hasil monitoring keamanan yang divisualisasikan melalui dashboard Kibana. Hasil penelitian menunjukkan bahwa Fail2Ban berhasil mendeteksi 180 percobaan login gagal yang berasal dari 6 alamat IP attacker dan melakukan pemblokiran otomatis terhadap seluruh IP penyerang dengan tingkat keberhasilan mitigasi sebesar 100%. Rata-rata waktu respons mitigasi berada pada rentang 0,314–0,443 detik dengan bantime selama 500 detik. ELK Stack juga berhasil menampilkan aktivitas login gagal, alamat IP penyerang, dan proses pemblokiran secara real-time. Hasil penelitian menunjukkan bahwa integrasi Fail2Ban dan ELK Stack berbasis Docker efektif dalam meningkatkan keamanan REST API Login E-Learning terhadap serangan brute force melalui mekanisme deteksi, mitigasi, dan monitoring keamanan secara terpusat.

Kata Kunci: brute force attack, REST API Login, E-Learning, Fail2Ban, ELK Stack, Docker.

A. Pendahuluan

Transformasi digital telah mendorong institusi pendidikan untuk memanfaatkan berbagai layanan berbasis teknologi informasi dalam mendukung aktivitas akademik dan administrasi. Pemanfaatan sistem pembelajaran digital (E-Learning) memungkinkan proses belajar mengajar dilakukan secara fleksibel dan efisien melalui platform berbasis web maupun aplikasi daring. Perkembangan teknologi informasi tersebut juga didukung oleh pemanfaatan jaringan komputer dan layanan berbasis internet yang semakin luas dalam lingkungan pendidikan (Pratama & Wijaya, 2023). Selain memberikan kemudahan akses terhadap materi pembelajaran, sistem E-Learning juga menyimpan berbagai informasi penting seperti data pengguna, data akademik, nilai, serta aktivitas pembelajaran yang perlu dilindungi dari ancaman keamanan siber (Arieska & Mukti, 2023). Keamanan jaringan menjadi salah satu aspek penting dalam menjaga keberlangsungan layanan teknologi informasi karena ancaman siber yang terus berkembang dapat menargetkan berbagai komponen sistem, mulai dari infrastruktur jaringan hingga layanan autentikasi pengguna (Pratikno et al., 2025).

Seiring meningkatnya penggunaan layanan digital pendidikan, ancaman keamanan terhadap sistem autentikasi juga semakin berkembang. Salah satu ancaman yang sering terjadi adalah brute force attack, yaitu teknik serangan yang dilakukan dengan mencoba berbagai kombinasi username dan password secara berulang hingga memperoleh akses ke dalam sistem (Mulyanto et al., 2022). Selain brute force attack, berbagai ancaman lain seperti penyusupan jaringan, eksploitasi layanan, dan akses tidak sah juga berpotensi mengganggu ketersediaan layanan pendidikan berbasis digital (Saputra & Hidayat, 2022; Mukti, 2022). Keamanan layanan autentikasi menjadi aspek penting karena kegagalan dalam melindungi akun pengguna dapat menyebabkan kebocoran data serta penyalahgunaan akses terhadap sistem pembelajaran (Nugroho & Setiawan, 2023; Arifin & Saputro, 2023).

Berbagai penelitian telah dilakukan untuk meningkatkan keamanan layanan berbasis jaringan. Ridho dkk. (2025) menunjukkan bahwa implementasi Fail2Ban mampu meningkatkan keamanan server Linux dengan melakukan pemblokiran otomatis terhadap alamat IP yang terindikasi melakukan serangan brute force. Penelitian lain yang dilakukan oleh Rustianto dkk. (2025) membuktikan bahwa integrasi mekanisme pemblokiran otomatis dengan sistem monitoring mampu meningkatkan kemampuan deteksi dan visualisasi aktivitas serangan secara real-time. Selain itu, penggunaan pendekatan Intrusion Prevention System (IPS) juga telah banyak diterapkan sebagai solusi mitigasi ancaman keamanan jaringan melalui mekanisme pencegahan otomatis terhadap aktivitas mencurigakan (Setiawan & Prakoso, 2023).

Selain kemampuan mitigasi, monitoring keamanan secara real-time menjadi kebutuhan penting dalam pengelolaan sistem informasi modern. ELK Stack yang terdiri atas Elasticsearch, Logstash, dan Kibana merupakan platform yang banyak digunakan untuk mengumpulkan, memproses, menyimpan, dan memvisualisasikan log keamanan secara terpusat (Ramadhan &

Kurniawan, 2024; Firmansyah & Hidayat, 2024). Integrasi ELK Stack dengan sistem keamanan telah terbukti mampu meningkatkan kemampuan analisis aktivitas serangan dan membantu administrator dalam melakukan investigasi insiden keamanan (Mukti & Sukmawan, 2021). Pemanfaatan log monitoring juga dapat digunakan sebagai dasar dalam proses mitigasi serangan serta evaluasi efektivitas sistem keamanan yang diterapkan (Mulyanto et al., 2022).

Dalam beberapa tahun terakhir, penelitian keamanan jaringan juga berkembang ke arah penerapan kecerdasan buatan dan machine learning untuk meningkatkan akurasi deteksi ancaman. Penelitian Pratama dkk. (2025) menunjukkan bahwa kombinasi Convolutional Neural Network (CNN) dan Long Short-Term Memory (LSTM) mampu meningkatkan kemampuan deteksi intrusi jaringan. Selain itu, analisis lalu lintas jaringan menggunakan pendekatan machine learning juga menunjukkan potensi yang tinggi dalam proses klasifikasi aktivitas jaringan dan identifikasi ancaman siber (Mukti, 2023). Meskipun demikian, pendekatan tersebut umumnya memerlukan sumber daya komputasi yang lebih besar dibandingkan mekanisme mitigasi berbasis aturan seperti Fail2Ban.

Penelitian sebelumnya telah membahas implementasi Fail2Ban sebagai mekanisme mitigasi brute force (Ridho et al., 2025; Rustianto et al., 2025), penggunaan ELK Stack sebagai platform monitoring keamanan (Ramadhan & Kurniawan, 2024; Firmansyah & Hidayat, 2024; Mukti & Sukmawan, 2021), serta berbagai pendekatan keamanan jaringan berbasis deteksi intrusi (Saputra & Hidayat, 2022; Setiawan & Prakoso, 2023; Mukti, 2022). Selain itu, penelitian mengenai keamanan akses jaringan menunjukkan bahwa mekanisme autentikasi, otorisasi, dan monitoring akses secara terpusat mampu meningkatkan keamanan infrastruktur jaringan serta mengurangi risiko akses tidak sah (Ramadhan & Kusmawan, 2026). Namun, penelitian yang mengintegrasikan Fail2Ban dan ELK Stack untuk mendeteksi, memitigasi, dan memvisualisasikan aktivitas brute force pada REST

API Login E-Learning berbasis Docker masih relatif terbatas. Padahal, REST API banyak digunakan sebagai mekanisme autentikasi pada aplikasi dan platform pembelajaran digital modern. Selain itu, teknologi container seperti Docker telah banyak digunakan untuk meningkatkan fleksibilitas, portabilitas, dan kemudahan pengelolaan layanan aplikasi modern (Pratama & Wijaya, 2023).

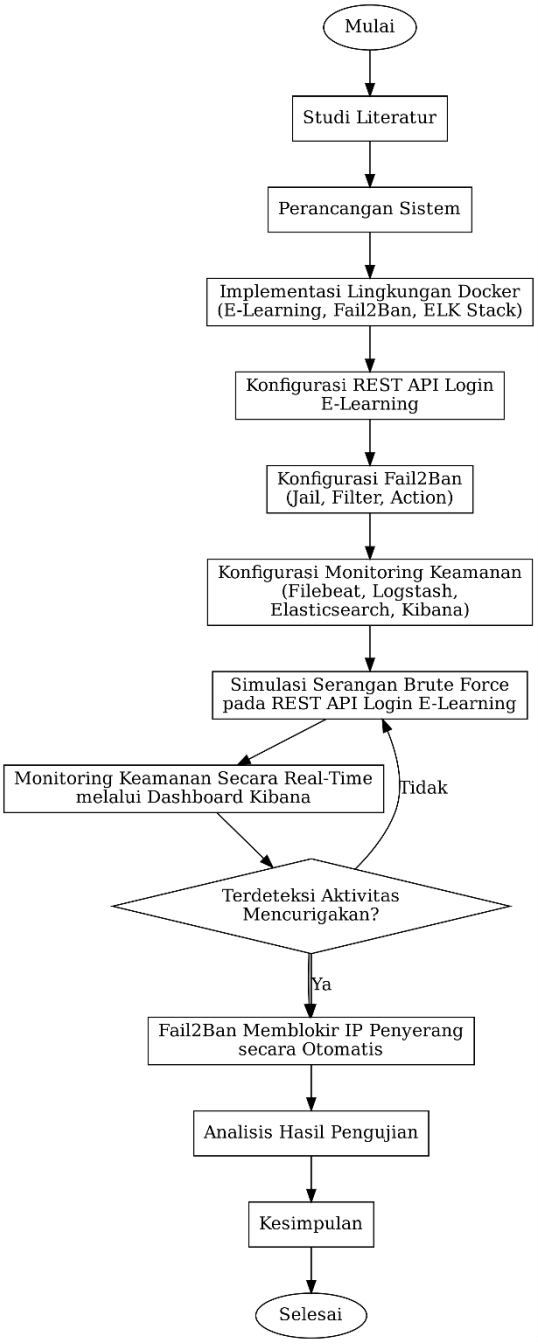
Berdasarkan permasalahan tersebut, penelitian ini bertujuan mengimplementasikan Fail2Ban dan ELK Stack untuk mitigasi serangan brute force pada REST API Login E-Learning berbasis Docker. Sistem yang dibangun diharapkan mampu mendeteksi percobaan login yang mencurigakan, melakukan pemblokiran otomatis terhadap alamat IP penyerang, serta menyediakan monitoring keamanan secara real-time melalui dashboard Kibana untuk mendukung keamanan layanan autentikasi pada platform pembelajaran digital.

B. Metode Penelitian

Penelitian ini menggunakan metode eksperimen (experimental research) untuk mengimplementasikan dan mengevaluasi efektivitas Fail2Ban dan ELK Stack dalam mitigasi serangan brute force pada REST API Login E-Learning berbasis Docker. Metode eksperimen dipilih karena penelitian berfokus pada pengujian langsung terhadap kemampuan sistem dalam mendeteksi, memitigasi, dan memantau aktivitas serangan yang dilakukan pada layanan autentikasi pengguna.

1. Desain Penelitian

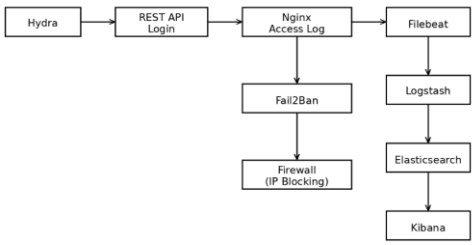
Tahapan penelitian dimulai dari studi literatur, perancangan sistem, implementasi lingkungan Docker, konfigurasi Fail2Ban dan ELK Stack, simulasi serangan brute force, pengumpulan data, analisis hasil pengujian, hingga penarikan kesimpulan. Studi literatur dilakukan untuk memperoleh landasan teori mengenai keamanan jaringan, brute force attack, Fail2Ban, Docker, ELK Stack, serta keamanan layanan autentikasi berbasis REST API



Gambar 1. Alur Penelitian

2. Arsitektur Sistem

Sistem dibangun menggunakan lingkungan Docker yang terdiri atas beberapa container yang saling terhubung melalui Docker Network. Arsitektur sistem terdiri atas container attacker, REST API Login E-Learning, Fail2Ban, Filebeat, Logstash, Elasticsearch, dan Kibana. Container attacker digunakan untuk mensimulasikan serangan brute force menggunakan Hydra. REST API Login E-Learning berfungsi sebagai target serangan sekaligus penyedia layanan autentikasi pengguna. Fail2Ban bertugas mendeteksi aktivitas login gagal dan melakukan pemblokiran otomatis terhadap alamat IP yang terindikasi melakukan serangan. Filebeat digunakan untuk mengirimkan log keamanan ke Logstash yang selanjutnya diproses dan disimpan pada Elasticsearch. Data log kemudian divisualisasikan secara real-time menggunakan Kibana.



Gambar 2. Arsitektur Sistem

Gambar 2 menunjukkan arsitektur sistem yang digunakan dalam penelitian. Proses pengujian dimulai dari container attacker yang menjalankan Hydra untuk

melakukan simulasi serangan brute force terhadap endpoint REST API Login E-Learning. Setiap aktivitas autentikasi dicatat pada Nginx Access Log yang berfungsi sebagai sumber log utama sistem.

Log autentikasi kemudian diproses oleh dua komponen berbeda. Fail2Ban memantau Nginx Access Log untuk mendeteksi percobaan login gagal yang melebihi batas yang telah ditentukan. Apabila terdeteksi aktivitas brute force, Fail2Ban akan menjalankan mekanisme firewall untuk melakukan pemblokiran otomatis terhadap alamat IP penyerang. Di sisi lain, Filebeat mengirimkan log ke Logstash untuk diproses sebelum disimpan pada Elasticsearch. Data log yang tersimpan selanjutnya divisualisasikan melalui Kibana sehingga administrator dapat melakukan monitoring keamanan secara real-time.

3. Implementasi Sistem

Implementasi sistem dilakukan menggunakan Docker Compose untuk mengelola seluruh layanan yang digunakan dalam penelitian. REST API Login E-Learning dibangun sebagai layanan autentikasi yang menyediakan endpoint login untuk proses verifikasi pengguna. Fail2Ban dikonfigurasi untuk memantau log autentikasi dan melakukan pemblokiran otomatis apabila jumlah percobaan login gagal melebihi batas yang telah ditentukan. ELK Stack dikonfigurasi untuk mengumpulkan, memproses, menyimpan, dan menampilkan data log keamanan secara terpusat melalui dashboard Kibana.

4. Skenario Pengujian

Pengujian dilakukan dengan mensimulasikan serangan brute force menggunakan Hydra terhadap REST API Login E-Learning. Pengujian melibatkan enam alamat IP attacker yang melakukan percobaan login menggunakan kombinasi username dan password yang tidak valid.

Parameter pengujian meliputi:

a. Jumlah percobaan login gagal.
b. Jumlah alamat IP yang terdeteksi.
c. Jumlah alamat IP yang berhasil diblokir.
d. Waktu respons mitigasi Fail2Ban.
e. Aktivitas monitoring yang ditampilkan pada dashboard Kibana.

5. Teknik Pengumpulan Data

Data penelitian diperoleh melalui observasi langsung terhadap log autentikasi, log Fail2Ban, serta dashboard monitoring Kibana. Data yang dikumpulkan meliputi jumlah login gagal, alamat IP penyerang, aktivitas pemblokiran, dan waktu respons mitigasi sistem.

6. Teknik Analisis Data

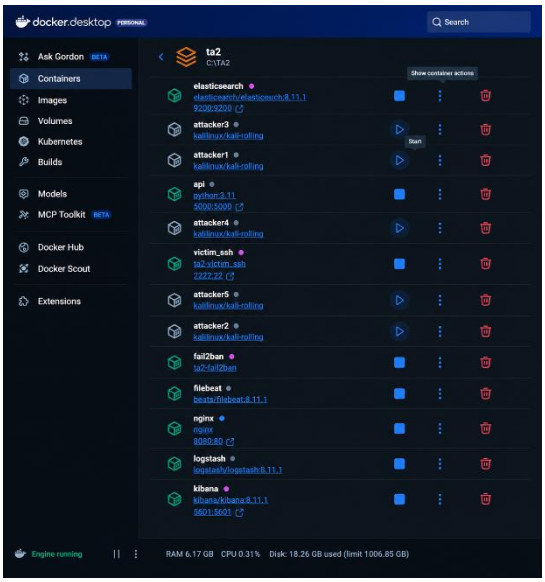
Data yang diperoleh dianalisis menggunakan metode statistik deskriptif. Analisis dilakukan dengan membandingkan jumlah percobaan login gagal, jumlah alamat IP yang berhasil diblokir, tingkat keberhasilan mitigasi, dan waktu respons sistem selama proses pengujian berlangsung. Hasil analisis digunakan untuk mengevaluasi efektivitas Fail2Ban dan ELK Stack dalam meningkatkan keamanan REST API Login E-Learning terhadap serangan brute force.

C.Hasil Penelitian dan Pembahasan

1. Implementasi Sistem

Implementasi sistem dilakukan menggunakan lingkungan Docker yang terdiri atas beberapa container, yaitu container attacker, REST API Login E-Learning, Fail2Ban, Filebeat, Logstash, Elasticsearch, dan Kibana. Seluruh container dihubungkan melalui Docker Network sehingga memungkinkan komunikasi antar layanan berlangsung secara terintegrasi.

Arsitektur sistem dirancang untuk mendukung proses deteksi, mitigasi, dan monitoring keamanan terhadap serangan brute force pada layanan autentikasi. Container attacker digunakan untuk mensimulasikan aktivitas serangan, sedangkan REST API Login E-Learning berfungsi sebagai target pengujian. Fail2Ban berperan sebagai mekanisme mitigasi otomatis dan ELK Stack digunakan sebagai sistem monitoring keamanan secara real-time.

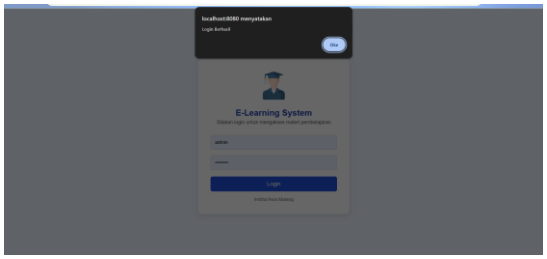


Gambar 3. Implementasi Lingkungan Docker

Berdasarkan hasil implementasi, seluruh container berhasil dijalankan dan dapat berkomunikasi dengan baik sehingga sistem mitigasi dan monitoring keamanan dapat beroperasi secara optimal.

2. Implementasi REST API Login E-Learning

REST API Login E-Learning dibangun sebagai layanan autentikasi yang menyediakan endpoint login untuk proses verifikasi pengguna. Endpoint ini menerima data username dan password dari pengguna, kemudian melakukan proses validasi sebelum memberikan respons autentikasi.



Gambar 4. Implementasi REST API Login E-Learning

Pada kondisi normal, pengguna yang memasukkan autentikasi yang valid akan memperoleh respons login berhasil dan dapat mengakses layanan yang tersedia. Seluruh aktivitas autentikasi dicatat pada log sistem untuk keperluan monitoring dan analisis keamanan.

3. Implementasi Fail2Ban

Fail2Ban diimplementasikan sebagai mekanisme mitigasi otomatis terhadap serangan brute force. Konfigurasi dilakukan dengan menentukan parameter maxretry, findtime, dan bantime untuk mendeteksi aktivitas login yang mencurigakan pada REST API Login E-Learning.

```
[nginx-api-login]
enabled=true
port=http,https
filter=nginx-api-login
logpath=/var/log/nginx/access.log

maxretry=5
findtime=60
bantime=500

action=iptables[name=API,port=http,protocol=tcp]
```

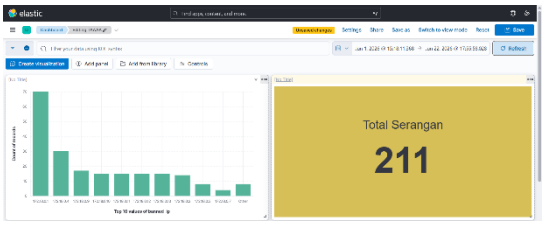
Gambar 5. Konfigurasi Fail2Ban

Ketika jumlah percobaan login gagal melebihi batas yang telah ditentukan, Fail2Ban secara otomatis melakukan pemblokiran terhadap alamat IP penyerang. Informasi pemblokiran dicatat pada log sistem dan dikirimkan ke ELK Stack untuk keperluan monitoring.

4. Implementasi ELK Stack

ELK Stack terdiri atas Elasticsearch, Logstash, dan Kibana yang berfungsi sebagai sistem monitoring keamanan. Filebeat digunakan untuk mengirimkan log autentikasi dan log Fail2Ban ke

Logstash sebelum disimpan ke Elasticsearch.



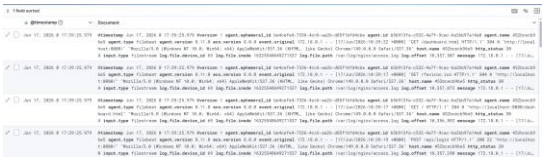
Gambar 6. Implementasi ELK Stack

Gambar 6 menunjukkan dashboard monitoring yang dibangun menggunakan Kibana. Dashboard menampilkan visualisasi jumlah alamat IP yang diblokir oleh Fail2Ban serta distribusi aktivitas serangan berdasarkan alamat IP penyerang. Data yang ditampilkan berasal dari log keamanan yang telah dikumpulkan oleh Filebeat, diproses oleh Logstash, dan disimpan pada Elasticsearch.

Berdasarkan hasil implementasi, ELK Stack berhasil mengintegrasikan proses pengumpulan, penyimpanan, dan visualisasi log keamanan secara terpusat. Dashboard Kibana memungkinkan administrator memantau aktivitas serangan dan status pemblokiran alamat IP secara real-time sehingga memudahkan proses analisis keamanan sistem.

5. Pengujian Login Normal

Pengujian login normal dilakukan untuk memastikan bahwa REST API Login E-Learning dapat melayani proses autentikasi pengguna yang sah. Pengujian dilakukan menggunakan username dan password yang valid melalui endpoint login yang telah disediakan.



Gambar 7. Log Aktivitas Login Berhasil pada Dashboard Kibana

Gambar 7 menunjukkan aktivitas login berhasil yang tercatat pada sistem. Ketika pengguna memasukkan autentikasi yang valid, server memberikan respons HTTP 200 (OK) sebagai tanda bahwa proses autentikasi berhasil dilakukan. Aktivitas login tersebut dicatat pada log sistem dan ditampilkan pada dashboard Kibana untuk keperluan monitoring.

Hasil pengujian menunjukkan bahwa pengguna berhasil memperoleh akses ke sistem E-Learning tanpa memicu mekanisme pemblokiran Fail2Ban. Hal ini menunjukkan bahwa konfigurasi Fail2Ban mampu membedakan aktivitas login yang sah dengan aktivitas serangan brute force.

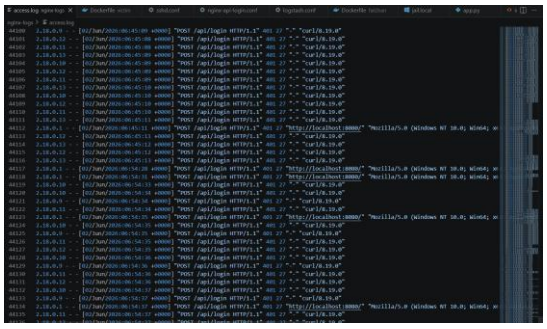
6. Hasil Pengujian Serangan Brute Force

Pengujian dilakukan menggunakan tools Hydra dari container attacker menuju endpoint login pada REST API Login E-Learning. Simulasi dilakukan menggunakan enam alamat IP attacker yang melakukan percobaan login berulang menggunakan

kombinasi username dan password yang tidak valid untuk memperoleh akses secara tidak sah ke dalam sistem.

Gambar 8. Simulasi Serangan Brute Force

Gambar 8 menunjukkan proses simulasi serangan brute force yang dilakukan dari container attacker menuju endpoint login pada REST API Login E-Learning. Serangan dilakukan melalui percobaan autentikasi berulang menggunakan autentikasi yang tidak valid sehingga menghasilkan respons *unauthorized* dari server.



Gambar 9. Monitoring Log Serangan pada REST API Login E-Learning

Gambar 9 menunjukkan log autentikasi yang berhasil dicatat pada server selama simulasi serangan brute force terhadap endpoint REST API Login E-Learning. Setiap percobaan login menggunakan autentikasi yang tidak valid menghasilkan respons HTTP 401 (Unauthorized) dan direkam ke dalam file access.log. Log tersebut memuat informasi alamat IP sumber, waktu kejadian, metode HTTP, endpoint yang diakses, serta status respons yang diberikan oleh server. Selanjutnya, log autentikasi dikirimkan ke ELK Stack untuk proses monitoring dan dianalisis oleh Fail2Ban sebagai dasar dalam mendeteksi aktivitas brute force.

Hasil pengujian menunjukkan bahwa seluruh aktivitas serangan berhasil tercatat pada log sistem dan terdeteksi oleh Fail2Ban. Total percobaan login gagal yang teridentifikasi selama pengujian mencapai 180 percobaan yang berasal dari enam 6 IP attacker. Setelah jumlah percobaan login gagal melebihi batas yang telah ditentukan, Fail2Ban secara otomatis melakukan pemblokiran terhadap alamat IP penyerang sehingga serangan tidak dapat dilanjutkan.

Tabel 1. Hasil Deteksi dan Mitigasi Serangan Brute Force

Parameter	Hasil
Jumlah Simulasi Serangan	6 kali
Jumlah IP Attacker	6
Total Login Gagal	180
Total IP Diblokir	6
Tingkat Keberhasilan Deteksi	100%
Bantime	500 detik
File Monitoring	/var/log/nginx/access.log
Mitigasi Otomatis	Berhasil
Monitoring log Real-Time	Berhasil

Berdasarkan hasil pengujian, seluruh alamat IP attacker berhasil diblokir secara otomatis oleh Fail2Ban setelah memenuhi batas percobaan login gagal yang telah ditentukan.

Selain tingkat keberhasilan mitigasi, penelitian ini juga mengukur selisih waktu antara terdeteksinya aktivitas serangan hingga proses pemblokiran dilakukan oleh Fail2Ban. Parameter tersebut digunakan untuk mengetahui kecepatan respons sistem dalam melakukan mitigasi terhadap serangan brute force.

Tabel 2. Rekapitulasi Selisih Waktu Respon Mitigasi Otomatis (Mitigation Latency)

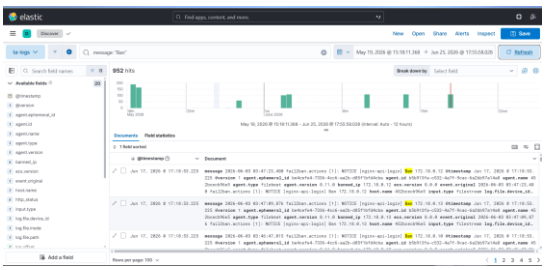
NO	IP Attacker	Waktu Serangan	Waktu Pemblokiran	Selisih Waktu (Detik)	Keterangan
1	172.18.0.10	2026-06-02 06:22:10,210	2026-06-02 06:22:10,577	0,367 Detik	Sukses Diblokir
2	172.18.0.9	2026-06-02 06:21:09,920	2026-06-02 06:21:10,250	0,330 Detik	Sukses Diblokir
3	172.18.0.13	2026-06-02 06:21:01,410	2026-06-02 06:21:01,853	0,443 Detik	Sukses Diblokir
4	172.18.0.12	2026-06-02 06:35:01,210	2026-06-02 06:35:01,630	0,420 Detik	Sukses Diblokir
5	172.18.0.11	2026-06-02 06:21:05,900	2026-06-02 06:21:06,214	0,314 Detik	Sukses Diblokir
6	172.18.0.7	2026-06-02 06:34:57,430	2026-06-02 06:34:57,786	0,356 Detik	Sukses Diblokir

Berdasarkan data pada Tabel 2, seluruh alamat IP attacker berhasil

diblokir dalam waktu kurang dari satu detik setelah ambang batas percobaan login gagal terpenuhi. Nilai mitigation latency yang diperoleh berada pada rentang 0,314–0,443 detik dengan rata-rata waktu respons sebesar 0,372 detik.Hasil tersebut menunjukkan bahwa Fail2Ban mampu memberikan respons mitigasi yang cepat dalam mendeteksi dan memblokir aktivitas brute force pada REST API Login E-Learning.

7. Monitoring Keamanan Menggunakan Kibana

Aktivitas login normal, login gagal, dan proses pemblokiran berhasil divisualisasikan melalui dashboard Kibana secara real-time. Informasi yang ditampilkan meliputi alamat IP pengguna, alamat IP penyerang, waktu kejadian, jumlah percobaan login gagal, serta status pemblokiran yang dilakukan oleh Fail2Ban.



Gambar 10. Dashboard Monitoring Keamanan

Visualisasi log pada Kibana mempermudah administrator dalam melakukan pemantauan keamanan dan analisis aktivitas autentikasi yang terjadi pada REST API Login E-Learning. Selain itu, dashboard Kibana juga membantu administrator dalam mengidentifikasi pola serangan brute force dan mengevaluasi efektivitas mekanisme mitigasi yang diterapkan.

8. Pembahasan

Hasil penelitian menunjukkan bahwa integrasi Fail2Ban dan ELK Stack mampu memberikan mekanisme mitigasi dan monitoring keamanan yang saling melengkapi pada REST API Login E-Learning. Pada kondisi normal, pengguna yang menggunakan kredensial valid dapat melakukan login tanpa terdeteksi sebagai aktivitas mencurigakan dan tanpa mengalami pemblokiran oleh Fail2Ban. Sebaliknya, ketika terjadi percobaan login berulang menggunakan kredensial yang tidak valid, sistem mampu mengidentifikasi aktivitas tersebut sebagai serangan brute force dan melakukan pemblokiran otomatis terhadap alamat IP penyerang.

Berdasarkan hasil pengujian, Fail2Ban berhasil mendeteksi 180 percobaan login gagal yang berasal dari 6 alamat IP attacker dan melakukan pemblokiran terhadap seluruh alamat IP tersebut dengan tingkat keberhasilan mitigasi mencapai 100%. Selain itu, hasil pengukuran menunjukkan bahwa waktu respons mitigasi (mitigation latency) berada pada rentang 0,314

hingga 0,443 detik. Hasil tersebut menunjukkan bahwa mekanisme pemblokiran dapat dilakukan dengan cepat setelah ambang batas percobaan login gagal terpenuhi.

Temuan penelitian ini sejalan dengan penelitian Ridho dkk. (2025) yang menunjukkan bahwa Fail2Ban efektif dalam mengurangi risiko serangan brute force melalui mekanisme pemblokiran otomatis. Hasil penelitian ini juga mendukung penelitian Rustianto dkk. (2025) yang menyatakan bahwa integrasi mekanisme mitigasi dengan sistem monitoring mampu meningkatkan kemampuan deteksi dan respons terhadap ancaman keamanan.

Selain berfungsi sebagai mekanisme mitigasi, ELK Stack juga mampu menyediakan monitoring keamanan secara real-time melalui dashboard Kibana. Aktivitas login berhasil, login gagal, percobaan brute force, dan pemblokiran IP oleh Fail2Ban dapat divisualisasikan secara terpusat sehingga memudahkan administrator dalam melakukan pemantauan dan analisis keamanan sistem. Hasil ini mendukung penelitian Ramadhan dan Kurniawan (2024) serta Firmansyah dan Hidayat (2024) yang menunjukkan bahwa monitoring log terpusat dapat meningkatkan efektivitas analisis keamanan.

Berdasarkan keseluruhan hasil pengujian, integrasi Fail2Ban dan ELK Stack berbasis Docker terbukti mampu meningkatkan keamanan REST API Login E-Learning melalui mekanisme deteksi, mitigasi, dan monitoring keamanan yang terintegrasi. Sistem yang dibangun mampu membedakan aktivitas login pengguna yang sah dengan aktivitas serangan brute force sehingga keamanan layanan autentikasi dapat ditingkatkan tanpa mengganggu proses login pengguna yang valid.

D. Kesimpulan

Penelitian ini berhasil mengimplementasikan Fail2Ban dan ELK Stack untuk mitigasi serangan brute force pada REST API Login E-Learning berbasis Docker. Sistem yang dibangun terdiri atas layanan REST API Login E-Learning, Fail2Ban sebagai mekanisme mitigasi otomatis, serta ELK Stack yang digunakan untuk monitoring dan visualisasi log keamanan secara real-time.

Hasil pengujian menunjukkan bahwa Fail2Ban mampu mendeteksi aktivitas brute force yang dilakukan melalui percobaan login berulang menggunakan autentikasi yang tidak valid. Dari enam alamat IP attacker yang digunakan dalam pengujian, seluruh IP berhasil dideteksi dan diblokir secara otomatis setelah memenuhi batas percobaan login gagal yang telah ditentukan. Total percobaan login gagal yang terdeteksi mencapai 180 percobaan dengan tingkat keberhasilan mitigasi sebesar 100%. Selain itu, waktu respons

mitigasi yang diperoleh berada pada rentang 0,314–0,443 detik, menunjukkan bahwa Fail2Ban mampu memberikan respons pemblokiran secara cepat terhadap aktivitas serangan.

Implementasi ELK Stack juga berhasil mendukung proses monitoring keamanan dengan menampilkan aktivitas login gagal, alamat IP penyerang, dan status pemblokiran secara real-time melalui dashboard Kibana. Hasil penelitian menunjukkan bahwa integrasi Fail2Ban dan ELK Stack berbasis Docker mampu meningkatkan keamanan REST API Login E-Learning melalui mekanisme deteksi, mitigasi, dan monitoring keamanan yang terintegrasi tanpa mengganggu aktivitas login pengguna yang sah.

Sebagai pengembangan di masa mendatang, penelitian dapat dilakukan dengan menambahkan mekanisme deteksi berbasis machine learning, penerapan Multi-Factor Authentication (MFA), serta pengujian pada lingkungan produksi dengan jumlah pengguna dan skenario serangan yang lebih kompleks.

DAFTAR PUSTAKA

Arieska, A. E. B., & Mukti, F. S. (2023). Pemanfaatan one-time password dan algoritma advanced encryption standard dalam sistem login internet kampus. G-Tech: Jurnal Teknologi Terapan, 7(3).

Arifin, M., & Saputro, D. (2023). Analisis keamanan autentikasi API berbasis token pada aplikasi web modern. Jurnal Sistem Informasi, 19(2), 112–120.

Firmansyah, R., & Hidayat, T. (2024). Implementasi monitoring keamanan server menggunakan Elasticsearch dan Kibana. Jurnal Informatika dan Sistem Informasi, 10(2), 130–139.

Mukti, F. S. (2022). Analisis dan implementasi sistem keamanan jaringan menggunakan pendekatan intrusion detection system. Techno.Com, 21(3), 511–522.

Mukti, F. S. (2023). In-depth network traffic analysis using machine learning perspective: Characterization and classification. Journal of Network and Computer Applications, 212, 103565. https://doi.org/10.1016/j.jnca.2023.103565

Mukti, F. S., & Sukmawan, R. M. (2021). Integration of low interaction honeypot and ELK

Stack as attack detection systems on servers. Jurnal Penelitian Pos dan Informatika, 11(2), 113–126.

Mulyanto, A., Pratama, R., & Likmi, F. (2022). Analisis mitigasi brute force attack menggunakan log monitoring pada server SSH. Jurnal Sistem Informasi dan Teknologi, 5(3), 77–85.

Nugroho, A., & Setiawan, M. (2023).

Analisis keamanan REST API menggunakan pendekatan autentikasi dan monitoring sistem. Jurnal RESTI, 7(1), 88–96.

Pratama, F. P. A., Sulistyo, D. A., & Mukti, F. S. (2025). Peningkatan akurasi deteksi intrusi jaringan dengan model hybrid convolutional neural network dan long short-term memory. JURASIK (Jurnal Riset Sistem Informasi dan Teknik Informatika), 10(2), 528–539.

Pratama, Y., & Wijaya, E. (2023). Penerapan Docker container untuk optimasi layanan aplikasi berbasis cloud. Jurnal Informatika, 11(3), 177–186.

Ramadhan, A., & Kusmawan, M. R. H. (2026). Implementasi Cisco ISE (Identity Service Engine) sebagai Network Access Control (NAC) untuk meningkatkan keamanan akses jaringan pada simulasi infrastruktur TI modern. Pendas: Jurnal Ilmiah Pendidikan Dasar, 11(2).

Ramadhan, F., & Kurniawan, B. (2024). Implementasi ELK Stack untuk monitoring keamanan server berbasis log. Jurnal Teknologi Informasi dan Komputer, 8(1), 44–53.

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.

Rustianto, A., Fadillah, A., & Kasih, J. (2025). Pencegahan dan visualisasi serangan brute force menggunakan Fail2Ban, Prometheus, dan Grafana. Jurnal Publikasi Teknik Informatika, 4(2), 195–209.

Saputra, D., & Hidayat, R. (2022). Implementasi intrusion detection system pada keamanan jaringan komputer berbasis Linux. Jurnal Teknologi Informasi dan Ilmu Komputer, 9(2), 233–242.

Setiawan, H., & Prakoso, A. (2023). Analisis mitigasi ancaman keamanan jaringan menggunakan pendekatan intrusion prevention system. Jurnal Nasional Teknologi Informasi, 12(1), 21–30.