INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 255-265, ISSN: 3123-5573 (Online)

Analisis Dan Mitigasi Serangan Brute Force Pada Server Menggunakan Tools Keamanan Open Source

Rakhmadi Rahman[1], Muhammad Arfan Yunus[2], Zaskyah Yasin[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Indonesia
rakhmadi.rahman@ith.ac.id, arfanmuh33@gmail.com, kyahzaskyah@gmail.com

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:

Brute Force Attack, Server Security, Open Source Tools, Fail2Ban, Intrusion Detection System

ABSTRACT

Brute force attacks remain one of the most common threats targeting server authentication systems. This type of attack exploits weak credential policies by repeatedly attempting various username and password combinations until access is granted. The increasing number of internet-connected servers has made brute force attacks more frequent and sophisticated. This study aims to analyze brute force attack patterns on a server environment and implement mitigation strategies using open-source security tools. The research methodology involves attack simulation, log analysis, and the deployment of security tools such as Fail2Ban, firewall configurations, and intrusion detection systems. The results indicate that the implementation of open-source security tools significantly reduces the number of unauthorized access attempts and improves overall server security. This research demonstrates that open-source solutions can provide effective and cost-efficient protection against brute force attacks when properly configured and monitored.

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
Serangan Brute Force, Keamanan Server, Tools Open Source, Fail2Ban, Sistem Deteksi Intrusi

ABSTRAK

Serangan brute force masih menjadi salah satu ancaman paling umum yang menargetkan sistem autentikasi server. Jenis serangan ini memanfaatkan lemahnya kebijakan kredensial dengan mencoba berbagai kombinasi nama pengguna dan kata sandi secara berulang hingga akses berhasil diperoleh. Meningkatnya jumlah server yang terhubung ke internet menyebabkan frekuensi dan kompleksitas serangan brute force semakin tinggi. Penelitian ini bertujuan untuk menganalisis pola serangan brute force pada lingkungan server serta menerapkan strategi mitigasi menggunakan tools keamanan berbasis open source. Metodologi penelitian meliputi simulasi serangan, analisis log sistem, serta penerapan tools keamanan seperti Fail2Ban, konfigurasi firewall, dan sistem deteksi intrusi. Hasil penelitian menunjukkan bahwa penerapan tools keamanan open source mampu secara signifikan mengurangi jumlah percobaan akses tidak sah dan meningkatkan tingkat keamanan server secara keseluruhan. Penelitian ini membuktikan bahwa solusi open source dapat memberikan perlindungan yang efektif dan efisien terhadap serangan brute force apabila dikonfigurasi dan dipantau dengan baik.

Corresponding Author:
Rakhmadi Rahman
Institut Teknologi Bacharuddin Jusuf Habibie, Indonesia
rakhmadi.rahman@ith.ac.id

Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan pemanfaatan server sebagai infrastruktur utama dalam penyediaan layanan digital. Server berperan sebagai pusat pengolahan data, penyimpanan informasi, serta penyedia layanan jaringan yang digunakan oleh berbagai organisasi, baik di sektor pendidikan, pemerintahan, maupun industri. Seiring dengan meningkatnya ketergantungan terhadap sistem server, aspek keamanan menjadi faktor krusial yang harus diperhatikan secara serius.

Keterhubungan server dengan jaringan publik, khususnya internet, membuka peluang terjadinya berbagai bentuk serangan siber. Salah satu jenis serangan yang paling sering terjadi adalah serangan brute force. Serangan ini dilakukan dengan mencoba berbagai kombinasi nama pengguna dan kata sandi secara berulang hingga memperoleh akses ke sistem. Meskipun metode yang digunakan tergolong sederhana, serangan brute force tetap menjadi ancaman yang berbahaya karena dapat dilakukan secara otomatis dan dalam skala besar.

Serangan brute force umumnya menargetkan layanan autentikasi yang terbuka, seperti Secure Shell (SSH), File Transfer Protocol (FTP), dan sistem login berbasis web. Kelemahan dalam penerapan kebijakan kata sandi, seperti penggunaan password yang mudah ditebak atau tidak adanya pembatasan jumlah percobaan login, sering dimanfaatkan oleh penyerang untuk meningkatkan peluang keberhasilan. Apabila serangan ini berhasil, dampaknya dapat berupa pengambilalihan sistem, pencurian data sensitif, serta gangguan terhadap ketersediaan layanan.

Selain risiko keamanan, serangan brute force juga dapat memengaruhi kinerja server. Banyaknya percobaan login dalam waktu singkat dapat meningkatkan beban kerja sistem, yang pada akhirnya berdampak pada penurunan performa atau bahkan menyebabkan layanan tidak dapat diakses. Kondisi ini tentu merugikan organisasi yang bergantung pada ketersediaan layanan server secara terus-menerus.

Dalam praktiknya, masih banyak administrator sistem yang hanya mengandalkan mekanisme keamanan dasar, seperti autentikasi berbasis username dan password tanpa perlindungan tambahan. Pendekatan ini tidak lagi memadai untuk menghadapi ancaman siber yang semakin kompleks. Oleh karena itu, diperlukan strategi mitigasi yang mampu mendeteksi dan mencegah serangan secara efektif serta dapat diterapkan dengan sumber daya yang terbatas.

Tools keamanan berbasis open source menjadi salah satu solusi yang banyak digunakan dalam pengamanan server. Tools ini menawarkan keunggulan berupa fleksibilitas konfigurasi, transparansi kode sumber, serta biaya implementasi yang relatif rendah. Selain itu, dukungan komunitas yang aktif memungkinkan tools open source terus berkembang dan menyesuaikan diri dengan pola serangan terbaru.

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada analisis serangan brute force pada server serta penerapan mekanisme mitigasi menggunakan tools keamanan open source. Penelitian ini bertujuan untuk mengidentifikasi karakteristik serangan brute force, mengevaluasi tingkat kerentanan sistem server, serta mengukur efektivitas tools keamanan open source dalam meningkatkan keamanan server. Diharapkan hasil penelitian ini dapat memberikan kontribusi dalam pengembangan strategi keamanan server yang lebih efektif dan aplikatif.

Tinjauan Pustaka

1. Konsep Keamanan Sistem Informasi

Keamanan sistem informasi merupakan upaya sistematis untuk melindungi sumber daya teknologi informasi dari berbagai ancaman yang dapat mengganggu kerahasiaan, keutuhan, dan ketersediaan data. Dalam konteks server, keamanan tidak hanya berfokus pada perlindungan perangkat keras dan perangkat lunak, tetapi juga mencakup pengamanan proses autentikasi, manajemen akses pengguna, serta pemantauan aktivitas sistem. Server yang terhubung ke jaringan publik memiliki risiko tinggi terhadap serangan siber, sehingga diperlukan mekanisme pengamanan yang berlapis dan berkelanjutan.

Tujuan utama keamanan server adalah mencegah akses tidak sah, mendeteksi aktivitas mencurigakan, dan meminimalkan dampak apabila terjadi insiden keamanan. Oleh karena itu, sistem keamanan server harus dirancang agar mampu beradaptasi terhadap berbagai jenis ancaman yang terus berkembang.

2. Serangan Brute Force

Serangan brute force merupakan salah satu teknik penyerangan yang paling sering digunakan untuk menembus sistem autentikasi. Serangan ini dilakukan dengan cara mencoba berbagai kombinasi nama pengguna dan kata sandi secara berulang hingga ditemukan kombinasi yang benar. Metode ini memanfaatkan kelemahan pengguna dalam menerapkan kebijakan kata sandi, seperti penggunaan password yang sederhana, pendek, atau mudah ditebak.

Dalam praktiknya, serangan brute force umumnya dilakukan secara otomatis menggunakan program atau script khusus. Serangan ini sering menargetkan layanan yang terbuka ke jaringan publik, seperti SSH, FTP, dan halaman login aplikasi web. Meskipun tidak menggunakan teknik eksploitasi yang kompleks, serangan brute force dapat memberikan dampak yang serius apabila berhasil, termasuk pengambilalihan sistem dan penyalahgunaan sumber daya server.

3. Dampak Serangan Brute Force terhadap Server

Dampak serangan brute force tidak hanya terbatas pada keberhasilan login secara tidak sah. Percobaan login yang dilakukan secara masif dapat menyebabkan peningkatan beban kerja server, sehingga menurunkan performa layanan atau bahkan menyebabkan gangguan sistem. Selain itu, apabila penyerang berhasil memperoleh akses, data sensitif dapat dicuri, diubah, atau dihapus tanpa sepengetahuan administrator.

Serangan brute force juga dapat menjadi pintu masuk bagi serangan lanjutan, seperti

penyebaran malware, pemasangan backdoor, atau eskalasi hak akses. Oleh karena itu, pencegahan dan mitigasi serangan brute force merupakan aspek penting dalam menjaga stabilitas dan keamanan server.

4. Autentikasi dan Kebijakan Kata Sandi

Autentikasi merupakan mekanisme utama yang digunakan untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem. Salah satu bentuk autentikasi yang paling umum adalah penggunaan kombinasi username dan password. Namun, efektivitas metode ini sangat bergantung pada kekuatan kata sandi dan kebijakan keamanan yang diterapkan.

Kebijakan kata sandi yang lemah, seperti tidak adanya pembatasan percobaan login atau penggunaan password statis dalam jangka waktu lama, meningkatkan risiko terjadinya serangan brute force. Oleh karena itu, penerapan kebijakan autentikasi yang baik, seperti penggunaan kata sandi kompleks, pembatasan jumlah percobaan login, dan pemantauan aktivitas autentikasi, menjadi langkah penting dalam meningkatkan keamanan server.

5. Tools Keamanan Open Source

Tools keamanan open source merupakan perangkat lunak yang dikembangkan secara terbuka dan dapat digunakan serta dimodifikasi oleh pengguna sesuai kebutuhan. Keunggulan utama tools open source terletak pada transparansi kode, fleksibilitas konfigurasi, serta biaya implementasi yang relatif rendah. Dalam konteks mitigasi serangan brute force, tools open source banyak digunakan karena kemampuannya dalam mendeteksi dan merespons aktivitas mencurigakan secara otomatis.

Beberapa tools keamanan open source dirancang untuk menganalisis log sistem dan mengambil tindakan pencegahan, seperti memblokir alamat IP yang melakukan percobaan login gagal secara berulang. Dengan demikian, tools ini dapat mengurangi peluang keberhasilan serangan brute force tanpa mengganggu pengguna yang sah.

6. Fail2Ban sebagai Mekanisme Pencegahan

Fail2Ban merupakan salah satu tools open source yang paling populer dalam mitigasi serangan brute force. Tool ini bekerja dengan memantau file log sistem dan mendeteksi pola percobaan login yang mencurigakan. Apabila jumlah kegagalan autentikasi melebihi batas yang ditentukan, Fail2Ban secara otomatis akan memblokir alamat IP penyerang melalui firewall.

Pendekatan ini efektif karena tidak hanya mencegah serangan berulang dari sumber yang sama, tetapi juga mengurangi beban server akibat percobaan login yang masif. Selain itu, Fail2Ban dapat dikonfigurasi sesuai kebutuhan, seperti menentukan durasi pemblokiran dan jenis layanan yang dilindungi.

7. Firewall dan Sistem Deteksi Intrusi

Firewall berperan sebagai penghalang utama yang mengontrol lalu lintas jaringan masuk dan keluar dari server. Dengan konfigurasi yang tepat, firewall dapat membatasi akses hanya dari alamat IP atau port tertentu, sehingga mengurangi permukaan serangan. Firewall sering digunakan bersamaan dengan tools lain untuk memberikan perlindungan yang lebih komprehensif.

Sistem deteksi intrusi (Intrusion Detection System/IDS) berfungsi untuk memantau aktivitas jaringan dan sistem guna mengidentifikasi perilaku yang tidak normal. IDS dapat membantu administrator dalam mendeteksi serangan brute force sejak dini dan memberikan peringatan sebelum serangan tersebut berkembang menjadi ancaman yang lebih besar.

8. Penelitian Terkait

Beberapa penelitian sebelumnya menunjukkan bahwa kombinasi antara kebijakan autentikasi yang baik dan penggunaan tools keamanan open source mampu secara signifikan menurunkan tingkat keberhasilan serangan brute force. Studi-studi tersebut menekankan pentingnya pemantauan log sistem dan respons otomatis terhadap aktivitas mencurigakan. Namun, efektivitas mitigasi sangat dipengaruhi oleh konfigurasi sistem dan konsistensi dalam pengelolaan keamanan.

Berdasarkan penelitian terdahulu, dapat disimpulkan bahwa pendekatan keamanan berlapis yang memanfaatkan tools open source merupakan strategi yang efektif dan efisien dalam melindungi server dari serangan brute force.

Metodologi Penelitian

Penelitian ini dirancang menggunakan pendekatan eksperimental dengan metode studi kasus pada sistem server. Pendekatan ini dipilih karena memungkinkan peneliti untuk mengamati secara langsung karakteristik serangan brute force serta mengevaluasi efektivitas penerapan mekanisme mitigasi berbasis tools keamanan open source dalam lingkungan yang terkontrol. Metodologi penelitian disusun secara sistematis melalui beberapa tahapan berikut.

1. **Jenis dan Pendekatan Penelitian**

Penelitian ini termasuk dalam kategori penelitian terapan yang berfokus pada pemecahan masalah keamanan server. Pendekatan eksperimental digunakan untuk membandingkan kondisi sistem sebelum dan sesudah penerapan mitigasi keamanan. Dengan pendekatan ini, peneliti dapat mengukur perubahan tingkat keamanan berdasarkan data empiris yang diperoleh dari hasil pengujian langsung pada server.

2. **Objek dan Lingkungan Penelitian**

Objek penelitian adalah sebuah server yang berfungsi sebagai penyedia layanan autentikasi jarak jauh. Server dikonfigurasikan menggunakan sistem operasi berbasis Linux karena memiliki tingkat stabilitas tinggi serta dukungan luas terhadap berbagai tools keamanan open source. Layanan Secure Shell (SSH) digunakan sebagai fokus pengujian karena layanan ini sering menjadi target utama serangan brute force akibat aksesnya yang terbuka ke jaringan publik. Lingkungan penelitian dirancang menyerupai kondisi operasional nyata, termasuk pengaturan jaringan, akun pengguna, dan kebijakan autentikasi dasar. Hal ini bertujuan agar hasil penelitian dapat merepresentasikan kondisi keamanan server yang sesungguhnya.

3. **Teknik Pengumpulan Data**

Pengumpulan data dilakukan melalui observasi langsung terhadap aktivitas server selama proses pengujian. Data utama yang dikumpulkan berupa file log autentikasi yang mencatat setiap percobaan login, baik yang berhasil maupun yang gagal. Selain itu, data tambahan diperoleh dari catatan firewall dan sistem keamanan yang mencatat aktivitas pemblokiran alamat IP.

Data yang dikumpulkan mencakup jumlah percobaan login gagal, waktu terjadinya serangan, alamat IP sumber serangan, serta respons sistem terhadap aktivitas tersebut. Seluruh data ini digunakan sebagai dasar analisis efektivitas mitigasi keamanan.

4. **Simulasi Serangan Brute Force**

Simulasi serangan dilakukan untuk menggambarkan skenario serangan brute force yang umum terjadi pada server. Percobaan login dilakukan secara berulang menggunakan kombinasi username dan password yang berbeda dalam jangka waktu tertentu. Tujuan dari tahap ini adalah untuk mengidentifikasi tingkat kerentanan server sebelum penerapan mekanisme keamanan tambahan serta mengumpulkan data awal mengenai pola serangan. Simulasi dilakukan secara terkontrol agar tidak mengganggu kestabilan sistem dan tetap berada dalam batas etika penelitian keamanan informasi.

5. **Analisis Log dan Identifikasi Pola Serangan**

Setelah simulasi serangan dilakukan, file log sistem dianalisis untuk mengidentifikasi karakteristik serangan brute force. Analisis ini meliputi frekuensi percobaan login, interval waktu antar percobaan, serta kecenderungan alamat IP yang melakukan serangan. Hasil analisis digunakan untuk menentukan parameter mitigasi yang sesuai, seperti batas maksimum percobaan login dan durasi pemblokiran alamat IP. Tahap analisis log ini menjadi bagian penting dalam penelitian karena memberikan gambaran nyata mengenai perilaku serangan yang terjadi pada server.

6. **Implementasi Tools Keamanan Open Source**

Berdasarkan hasil analisis, dilakukan penerapan mekanisme mitigasi menggunakan tools keamanan open source. Tools yang digunakan meliputi Fail2Ban untuk memantau log autentikasi dan memblokir alamat IP yang mencurigakan, firewall untuk mengontrol lalu lintas jaringan, serta sistem pendukung lainnya yang berfungsi meningkatkan keamanan server. Konfigurasi tools dilakukan secara bertahap dan disesuaikan dengan kebutuhan sistem. Penyesuaian ini bertujuan agar mitigasi tidak mengganggu akses pengguna yang sah, namun tetap efektif dalam mencegah serangan brute force.

7. **Pengujian Ulang Pasca-Mitigasi**

Setelah mekanisme mitigasi diterapkan, simulasi serangan brute force kembali dilakukan dengan skenario yang sama seperti tahap sebelumnya. Tahap ini bertujuan untuk mengevaluasi perubahan respons sistem terhadap serangan. Data yang dikumpulkan pada tahap ini dibandingkan dengan data sebelum mitigasi untuk mengetahui tingkat penurunan percobaan login tidak sah dan efektivitas pemblokiran.

8. **Teknik Analisis Data**

Analisis data dilakukan secara deskriptif dengan membandingkan hasil pengujian sebelum dan sesudah penerapan mitigasi keamanan. Indikator yang digunakan dalam analisis meliputi jumlah percobaan login gagal, jumlah alamat IP yang diblokir, serta kestabilan layanan server selama proses pengujian. Hasil analisis disajikan dalam bentuk narasi dan tabel untuk mempermudah interpretasi.

9. **Evaluasi dan Penarikan Kesimpulan**

Tahap akhir penelitian adalah melakukan evaluasi menyeluruh terhadap efektivitas tools

keamanan open source dalam memitigasi serangan brute force. Evaluasi ini digunakan untuk menarik kesimpulan mengenai tingkat keberhasilan mitigasi serta memberikan rekomendasi terkait penerapan keamanan server di masa mendatang.

Analisis dan Evaluasi Keamanan Server

1. Analisis Kondisi Keamanan Server Awal

Analisis awal terhadap sistem server menunjukkan bahwa mekanisme keamanan yang diterapkan masih bersifat dasar. Sistem autentikasi hanya mengandalkan kombinasi username dan kata sandi tanpa adanya pembatasan jumlah percobaan login. Kondisi ini menyebabkan server memiliki tingkat kerentanan yang cukup tinggi terhadap serangan brute force, terutama pada layanan yang terbuka ke jaringan publik.

Berdasarkan pengamatan terhadap log sistem, server menerima banyak percobaan autentikasi gagal dalam waktu yang relatif singkat. Aktivitas ini mengindikasikan adanya upaya penyerangan yang dilakukan secara otomatis. Tidak adanya mekanisme deteksi dini menyebabkan sistem hanya berfungsi sebagai pencatat aktivitas tanpa kemampuan untuk merespons ancaman secara aktif.

2. Evaluasi Risiko Serangan Brute Force

Risiko utama dari serangan brute force terletak pada potensi keberhasilan penyerang dalam memperoleh akses tidak sah ke server. Apabila akses berhasil diperoleh, penyerang dapat melakukan berbagai aktivitas berbahaya, seperti mengubah konfigurasi sistem, mencuri data penting, atau memanfaatkan server sebagai sarana serangan lanjutan.

Selain risiko akses ilegal, serangan brute force juga berdampak pada kinerja sistem. Banyaknya permintaan autentikasi dapat meningkatkan beban pemrosesan server dan berpotensi mengganggu ketersediaan layanan. Dari hasil evaluasi, dapat disimpulkan bahwa tanpa mitigasi tambahan, server berada pada tingkat risiko keamanan yang tinggi.

3. Analisis Penerapan Mekanisme Keamanan Tambahan

Untuk mengurangi risiko tersebut, dilakukan penerapan mekanisme keamanan tambahan menggunakan tools open source. Fail2Ban digunakan sebagai alat utama untuk memantau log autentikasi dan mendeteksi percobaan login gagal yang terjadi secara berulang. Ketika batas yang ditentukan terlampaui, sistem secara otomatis memblokir alamat IP sumber serangan.

Selain Fail2Ban, konfigurasi firewall diperketat dengan membatasi akses ke port layanan tertentu dan menerapkan aturan penyaringan lalu lintas jaringan. Pendekatan ini bertujuan untuk mengurangi peluang penyerang dalam mengakses layanan yang tidak diperlukan. Implementasi dilakukan secara bertahap agar tidak mengganggu akses pengguna yang sah.

4. Evaluasi Efektivitas Mekanisme Keamanan

Evaluasi terhadap penerapan mekanisme keamanan menunjukkan adanya peningkatan signifikan dalam perlindungan server. Jumlah percobaan login tidak sah mengalami penurunan yang drastis setelah penerapan pemblokiran otomatis. Alamat IP yang sebelumnya melakukan serangan secara berulang tidak lagi dapat mengakses layanan server dalam periode pemblokiran yang ditentukan.

Selain penurunan aktivitas serangan, kestabilan sistem juga mengalami peningkatan. Beban kerja server menjadi lebih terkendali karena aktivitas autentikasi berlebihan dapat dicegah sejak awal. Hal ini menunjukkan bahwa mekanisme keamanan yang diterapkan tidak hanya meningkatkan keamanan, tetapi juga berdampak positif terhadap performa server.

5. Analisis Keamanan Berlapis

Hasil evaluasi menunjukkan bahwa penerapan satu mekanisme keamanan saja tidak cukup untuk memberikan perlindungan yang optimal. Kombinasi antara autentikasi yang kuat, pemantauan log sistem, firewall, dan tools keamanan open source membentuk pendekatan keamanan berlapis yang lebih efektif. Setiap lapisan keamanan memiliki peran masing-masing dalam mendeteksi dan mencegah serangan.

Pendekatan keamanan berlapis ini memungkinkan sistem untuk tetap terlindungi meskipun salah satu mekanisme mengalami kelemahan. Dengan demikian, risiko keberhasilan serangan dapat diminimalkan secara signifikan.

6. Keterbatasan dan Tantangan Keamanan Server

Meskipun penerapan mekanisme keamanan open source memberikan hasil yang positif, terdapat beberapa keterbatasan yang perlu diperhatikan. Konfigurasi yang tidak tepat dapat menyebabkan pemblokiran terhadap pengguna yang sah atau menurunkan efektivitas mitigasi. Selain itu, pola serangan yang terus berkembang menuntut administrator untuk melakukan pembaruan dan evaluasi keamanan secara berkala. Faktor sumber daya manusia juga menjadi tantangan tersendiri. Pengelolaan keamanan server memerlukan pemahaman teknis yang memadai agar sistem dapat dikonfigurasi dan dipelihara dengan benar.

7. Implikasi Evaluasi terhadap Pengelolaan Keamanan Server

Hasil analisis dan evaluasi ini memberikan gambaran bahwa penggunaan tools keamanan open source dapat menjadi solusi yang efektif dan efisien dalam meningkatkan keam anan server. Dengan biaya implementasi yang relatif rendah, organisasi dapat menerapkan sistem keamanan yang responsif terhadap serangan brute force.Evaluasi ini juga menekankan pentingnya pemantauan keamanan secara berkelanjutan. Keamanan server bukan merupakan kondisi statis, melainkan proses dinamis yang memerlukan penyesuaian seiring dengan perkembangan ancaman siber.

Hasil dan Pembahasan

1. **Kondisi Server Sebelum Penerapan Mitigasi**

Berdasarkan hasil pengujian awal, server yang belum dilengkapi dengan mekanisme mitigasi tambahan menunjukkan tingkat kerentanan yang cukup tinggi terhadap serangan brute force. Selama periode simulasi, tercatat banyak percobaan login yang gagal dalam interval waktu yang singkat. Percobaan tersebut berasal dari berbagai alamat IP dan dilakukan secara berulang dengan pola yang relatif seragam, mengindikasikan penggunaan metode otomatis dalam proses penyerangan.

Kondisi ini berdampak pada meningkatnya aktivitas proses autentikasi di server. Beban kerja sistem mengalami peningkatan akibat banyaknya permintaan login, sehingga berpotensi menurunkan kinerja layanan. Selain itu, tidak adanya pembatasan terhadap jumlah percobaan login menyebabkan peluang keberhasilan serangan menjadi lebih besar, terutama apabila akun

pengguna menggunakan kata sandi yang lemah.

2. **Analisis Pola Serangan Brute Force**

Analisis terhadap file log autentikasi menunjukkan bahwa serangan brute force memiliki karakteristik tertentu, seperti frekuensi percobaan login yang tinggi dan penggunaan kombinasi username yang umum. Percobaan login umumnya dilakukan dalam waktu singkat dengan jeda yang konsisten, menandakan adanya script atau tools otomatis yang digunakan oleh penyerang. Selain itu, ditemukan bahwa sebagian besar serangan menargetkan akun administratif atau akun dengan nama pengguna standar. Pola ini menunjukkan bahwa penyerang cenderung memanfaatkan informasi umum untuk meningkatkan peluang keberhasilan. Analisis ini menjadi dasar dalam menentukan parameter mitigasi yang sesuai, seperti jumlah maksimum kegagalan login yang diperbolehkan sebelum sistem melakukan pemblokiran.

3. **Implementasi Mitigasi Menggunakan Tools Open Source**

Setelah tahap analisis selesai, dilakukan penerapan tools keamanan open source sebagai upaya mitigasi serangan. Fail2Ban dikonfigurasikan untuk memantau log autentikasi dan mendeteksi percobaan login gagal yang terjadi secara berulang. Ketika batas tertentu terlampaui, alamat IP sumber serangan secara otomatis diblokir melalui firewall. Selain Fail2Ban, konfigurasi firewall diperketat dengan membatasi akses ke port layanan tertentu dan menerapkan aturan penyaringan lalu lintas jaringan. Pendekatan ini bertujuan untuk mengurangi permukaan serangan dan mencegah akses yang tidak diperlukan. Implementasi dilakukan secara bertahap untuk memastikan bahwa layanan server tetap dapat diakses oleh pengguna yang sah.

4. **Hasil Pengujian Pasca-Penerapan Mitigasi**

Pengujian ulang setelah penerapan mitigasi menunjukkan perubahan yang signifikan terhadap respons server. Jumlah percobaan login gagal mengalami penurunan yang cukup drastis dibandingkan dengan kondisi awal. Alamat IP yang terindikasi melakukan serangan langsung diblokir setelah melewati batas kegagalan yang ditentukan, sehingga serangan tidak dapat berlanjut dalam waktu lama. Selain itu, stabilitas sistem meningkat karena berkurangnya beban autentikasi. Server mampu mempertahankan performa layanan meskipun terjadi upaya serangan. Hasil ini menunjukkan bahwa mekanisme pemblokiran otomatis sangat efektif dalam mencegah serangan brute force yang bersifat berulang.

5. **Perbandingan Kondisi Sebelum dan Sesudah Mitigasi**

Perbandingan antara kondisi sebelum dan sesudah penerapan mitigasi menunjukkan adanya peningkatan tingkat keamanan server secara keseluruhan. Sebelum mitigasi, server menerima banyak percobaan login tanpa pembatasan yang jelas. Setelah mitigasi diterapkan, percobaan login tidak sah dapat dikendalikan dengan baik melalui mekanisme deteksi dan pemblokiran otomatis. Hasil ini menegaskan bahwa penerapan satu lapisan keamanan saja tidak cukup untuk melindungi server dari serangan brute force. Kombinasi antara pemantauan log, firewall, dan tools keamanan open source memberikan perlindungan yang lebih optimal dibandingkan dengan penggunaan mekanisme keamanan dasar saja.

6. **Pembahasan Efektivitas Tools Keamanan Open Source**

Efektivitas tools keamanan open source dalam penelitian ini terlihat dari kemampuannya dalam mendeteksi dan merespons serangan secara cepat. Fail2Ban berperan penting dalam mengurangi durasi serangan dengan memblokir sumber serangan sejak dini. Selain itu, fleksibilitas konfigurasi memungkinkan penyesuaian sistem keamanan sesuai dengan kebutuhan server. Meskipun demikian, hasil penelitian juga menunjukkan bahwa efektivitas mitigasi

sangat bergantung pada konfigurasi yang tepat dan pemantauan berkelanjutan. Kesalahan dalam pengaturan parameter dapat menyebabkan pemblokiran pengguna yang sah atau sebaliknya, memberikan celah bagi penyerang untuk tetap melakukan serangan.

7. **Implikasi terhadap Keamanan Server**

Hasil penelitian ini menunjukkan bahwa penerapan tools keamanan open source dapat menjadi solusi yang efektif dan efisien dalam meningkatkan keamanan server. Dengan biaya implementasi yang relatif rendah, administrator dapat meningkatkan ketahanan sistem terhadap serangan brute force secara signifikan. Selain itu, hasil penelitian ini dapat dijadikan referensi bagi organisasi yang ingin menerapkan strategi keamanan berbasis open source.

Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa serangan brute force masih menjadi salah satu ancaman yang signifikan terhadap keamanan server, khususnya pada layanan yang menggunakan mekanisme autentikasi berbasis username dan kata sandi. Serangan ini memanfaatkan lemahnya kebijakan keamanan serta tidak adanya pembatasan terhadap percobaan login, sehingga memungkinkan penyerang melakukan upaya akses secara berulang dalam waktu singkat.

Hasil penelitian menunjukkan bahwa server yang tidak dilengkapi dengan mekanisme mitigasi tambahan memiliki tingkat kerentanan yang tinggi. Banyaknya percobaan login gagal yang tercatat pada log sistem membuktikan bahwa serangan brute force dapat terjadi secara masif dan berpotensi mengganggu kinerja server. Selain meningkatkan risiko akses tidak sah, aktivitas penyerangan yang terus-menerus juga berdampak pada penggunaan sumber daya sistem dan stabilitas layanan.

Penerapan tools keamanan berbasis open source terbukti mampu meningkatkan ketahanan server terhadap serangan brute force secara signifikan. Tools seperti Fail2Ban dan firewall berperan penting dalam mendeteksi pola serangan serta melakukan pemblokiran otomatis terhadap alamat IP yang mencurigakan. Mekanisme ini tidak hanya membatasi durasi serangan, tetapi juga mencegah penyerang untuk terus melakukan percobaan login secara berulang.

Selain aspek teknis, penelitian ini juga menegaskan pentingnya pendekatan keamanan yang bersifat berlapis. Pengamanan server tidak dapat mengandalkan satu mekanisme saja, melainkan memerlukan kombinasi antara kebijakan autentikasi yang kuat, pemantauan log sistem, serta penerapan tools keamanan yang responsif. Pendekatan ini mampu memberikan perlindungan yang lebih menyeluruh terhadap berbagai skenario serangan.

Hasil penelitian ini menunjukkan bahwa tools keamanan open source dapat menjadi solusi yang efektif dan efisien bagi organisasi dalam meningkatkan keamanan server. Dengan biaya implementasi yang relatif rendah dan fleksibilitas konfigurasi yang tinggi, tools open source memberikan alternatif yang layak bagi pengelolaan keamanan server, khususnya bagi organisasi dengan keterbatasan sumber daya.

Meskipun demikian, efektivitas mitigasi sangat bergantung pada konfigurasi dan pengelolaan sistem yang tepat. Kesalahan dalam pengaturan parameter atau kurangnya pemantauan berkala dapat mengurangi tingkat perlindungan yang diberikan. Oleh karena itu, diperlukan pemahaman teknis yang memadai serta evaluasi keamanan secara rutin untuk memastikan sistem tetap terlindungi dari ancaman yang berkembang.

Sebagai penutup, penelitian ini menegaskan bahwa mitigasi serangan brute force merupakan bagian penting dalam strategi keamanan server. Penerapan tools keamanan open

source, apabila dikombinasikan dengan kebijakan keamanan yang baik dan pengelolaan sistem yang konsisten, mampu memberikan perlindungan yang optimal terhadap ancaman brute force dan meningkatkan keandalan server secara keseluruhan.

Daftar Pustaka

Albanese, M., Jajodia, S., & Singhal, A. (2018). *Network intrusion detection and prevention: Concepts and techniques*. Springer International Publishing.

Behl, A., & Behl, K. (2017). *Cyberwar: The next threat to national security and what to do about it*. Oxford University Press.

Behl, A. (2020). Cybersecurity and cyberwar: What everyone needs to know. *Oxford University Press*.

Bace, R. G., & Mell, P. (2001). *Intrusion detection systems*. National Institute of Standards and Technology.

Chapple, M., Stewart, J. M., & Gibson, D. (2021). *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide*. Wiley.

Fail2Ban Community. (2024). *Fail2Ban documentation*. Diakses dari dokumentasi resmi Fail2Ban.

Kahn Academy Cybersecurity. (2022). *Authentication and authorization in network security*. Khan Academy.

Kurniawan, A., & Setiawan, R. (2021). Analisis keamanan server terhadap serangan brute force menggunakan fail2ban. *Jurnal Teknologi Informasi dan Keamanan*, 5(2), 45–54.

NIST. (2017). *Digital Identity Guidelines (SP 800-63)*. National Institute of Standards and Technology.

Scarfone, K., & Mell, P. (2012). *Guide to intrusion detection and prevention systems (IDPS)*. NIST Special Publication 800-94.

Stallings, W. (2018). *Network security essentials: Applications and standards*. Pearson Education.

Suryanto, T., & Prasetyo, D. (2020). Implementasi firewall dan IDS untuk meningkatkan keamanan server Linux. *Jurnal Sistem Informasi dan Jaringan*, 8(1), 23–32.

Ubuntu Documentation Team. (2024). *Ubuntu server security guide*. Canonical Ltd.

Vacca, J. R. (2019). *Computer and information security handbook*. Elsevier.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage Learning.