Penerapan Fail2Ban Untuk Keamanan Dalam Integrasi Asterisk IP PBX Dengan Microsoft Teams

1st Faiz Rifqi Ramadhan
Fakultas Teknik Elektro
Telkom University
Kota Bandung, Indonesia
faizrifqi@student.telkomuniversity.ac.id

2nd Bagus Aditya
Fakultas Teknik Elektro
Telkom University
Kota Bandung, Indonesia
goesaditya@telkomuniversity.ac.id

3rd Akhmad Hambali
Fakultas Teknik Elektro
Telkom University
Kota Bandung, Indonesia
ahambali@telkomuniversity.ac.id

***Abstrak* — Dengan didasari adanya perubahan teknologi yang terus meningkat, penggunaan dalam server virtual (cloud) menjadikan tantangan tersendiri dalam penggunaanya. Dengan adanya ancaman yang sangat kompleks seperti brute-force, Fail2Ban adalah software yang dapat digunakan untuk mencegah upaya login oleh akses yang tidak sah. Penelitian ini bertujuan untuk mengetahui efektifitas Fail2Ban dalam menangani serangan dari akses yang tidak sah maupun serangan brute-force. Penelitian ini menggunakan metode studi eksperimental dengan menerapkan konfigurasi Fail2Ban pada layanan SSH dan Asterisk serta melakukan pengujian penggunaan tools hydra untuk mensimulasikan serangan brute-force. Sistem kerja Fail2Ban didasari dengan melakukan pemantauan log dan mengamati pola akses login yang tidak sah. Hasil dari pengujian dapat menunjukan bahwa Fail2Ban dapat secara efektif dalam pemblokiran IP.**

Kata kunci : Fail2Ban, hydra, brute-force, Asterisk, SSH

I. PENDAHULUAN

Dengan adanya perubahan teknologi yang terus meningkat, banyak individu atau perusahaan beralih menggunakan cloud atau server virtual untuk infrastruktur sistem yang dibuat. Serangan siber menjadi meningkat ketika menggunakan server virtual (cloud). Salah satu dari serangan siber yang sangat umum terjadi adalah brute-force attack, yang dimana brute-force memanfaatkan metode serangan yang mencoba kombinasi username dan password untuk login guna mendapatkan akses yang sah atau akses yang diizinkan login oleh server.

Dalam menangani permasalahan tersebut, diperlukan adanya keamanan tambahan yang secara fungsi dapat memantau dan dapat secara otomatis melakukan tindakan dalam menangani serangan brute-force. Solusi yang dapat digunakan yaitu dengan memanfaatkan Fail2Ban untuk meningkatkan keamanan sistem. Pada dasarnya, sistem kerja Fail2Ban adalah dengan melakukan pemantauan log yang ada pada sistem. Dalam hal ini, jika adanya pola serangan berulang dari akses login yang tidak sah akan secara otomatis Fail2Ban akan membolkir alamat IP penyerang.

Keunggulan yang dimiliki Fail2Ban adalah dapat secara otomatis mengedintifikasi dan melakukan tindakan tanpa adanya konfirmasi pengguna. Fail2Ban juga merupakan perangkat lunak yang fleksibel, serta dapat dikonfigurasi untuk berbagai layanan. Dalam penelitian ini, Fail2Ban diimplementasi untuk menjaga keamanan server dari akses login yang tidak sah atau individu yang tidak memiliki izin untuk memasuki server. Layanan SSH dan Asterisk merupakan fokus utama untuk pengimplementasian sistem keamanan Fail2Ban. Kedua layanan ini merupakan target umum yang dijadikan titik untuk serangan brute-force ketika menggunakan server virtual (cloud). Penelitian ini difokuskan untuk mengetahui mekanisme kerja serta efektifitas Fail2Ban dalam menangani serangan dengan sistem yang menggunakan server vritual (cloud) sebagai komponen utama.

II. KAJIAN TEORI

A. Fail2Ban

Fail2Ban adalah aplikasi yang dimana berfungsi sebagai pelindung sistem yang dimana Fail2Ban bekerja dengan memantau log aktivitas dan secara otomatis dapat memblokir alamat IP yang terindikasi melakukan login yang tidak sah secara berulang dan terus-menerus. Fail2Ban bekerja dengan dasar pemantauan frekuensi kegagalan login[1].

B. Brute-force

Brute-force merupakan suatu metode yang dimana berfungsi untuk menjebol kemungkinan kode rahasia yang ada. Untuk memecahkan permasalahan autentikasi, brute-force mencari kemungkinan password tertentu dengan memasukan kombinasi password yang banyak[2].

C. Hydra

Hydra merupakan salah satu tool atau aplikasi untuk mendeteksi kerentanan yang mungkin dieksploitasi oleh penyerang. Penggunaan tools Hydra adalah untuk meretas password yang akan disimulasikan berdasarkan kombinasi username dan password yang telah dibuat[3].

III. METODE

Dalam pengimplementasian Fail2Ban untuk keamanan dalam integrasi Asterisk IP PBX dengan Microsoft Teams, studi eksperimental merupakan pendekatan yang digunakan, dengan cara menerapkan secara langsung konfigurasi Fail2Ban pada sistem. Dalam bagian ini merupakan, konfigurasi, mekanisme cara kerja, dan pengujian Fail2Ban.

A. Konfigurasi

Table 1 Konfigurasi Fail2Ban untuk layanan Asterisk

```
[asterisk]
enabled = true
port = 5060,5061
filter = asterisk
logpath =/var/log/asterisk/messages.log
maxretry = 3
bantime = -1
findtime = 600
backend = auto
action = %(action_)s
ignoreip =
```

Konfigurasi Fail2Ban untuk layanan Asterisk yang ada pada table adalah konfigurasi sederhana yang dimana Fail2Ban membaca log yang ada pada asterisk yaitu /var/log/asterisk/messages.log, serta melakukan penyesuaian beberapa parameter seperti maxretry, bantime, findtime, backend, dan action.

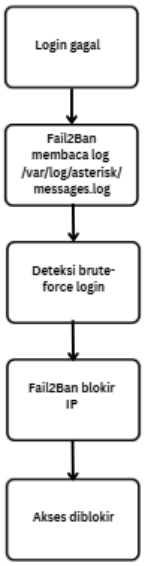
Table 2 Konfigurasi Fail2Ban untuk layanan SSH

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = -1
findtime = 600
backend = auto
action = %(action_)s
ignoreip =
```

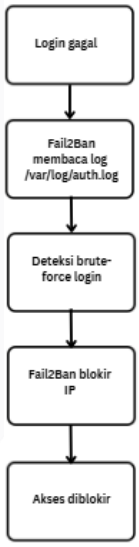
Konfigurasi Fail2Ban dalam layanan SSH yang ditunjukan pada table 2 adalah konfigurasi sederhana yang dalam hal ini Fail2Ban membaca log autentikasi yang ada pada sistem, yaitu /var/log/auth.log, serta melakukan penyesuaian beberapa parameter seperti maxretry, bantime, findtime, backend, dan action.

B. Mekanisme Cara Kerja Fail2Ban

Fail2Ban merupakan aplikasi atau software yang pada dasarnya melakukan pemantauan dan melakukan penganalisisan file log yang ada pada sistem. Pada dasarnya, Fail2Ban bekerja dengan mengamati pola login dari akses yang tidak sah. Jika terdapat pola akses terjadi berulang dan secara terus menerus melebihi angka dari parameter yang telah dikonfigurasi untuk Fail2Ban seperti maxretry dan findtime, maka secara otomatis Fail2Ban akan memblokir alamat IP penyerang karena terindikasi sebagai serangan brute-force. Berikut merupakan gambaran cara kerja pada Fail2Ban.



Gambar 1 Mekanisme cara kerja Fail2Ban (Asterisk)



Gambar 2 Mekanisme cara kerja Fail2Ban (SSH)

C. Pengujian Fail2Ban

Pengujian Fail2Ban ini dilakukan dengan tujuan untuk memastikan bahwa Fail2Ban dapat bekerja dengan baik dalam mengatasi upaya akses login yang tidak sah. Pengujian ini bertujuan untuk memastikan apakah Fail2Ban secara otomatis dapat memblokir alamat IP (akses login yang tidak sah) yang melakukan percobaan berulang.

Hydra merupakan tools yang digunakan untuk melakukan pengujian Fail2Ban untuk layanan SSH. Dalam hal ini menggunakan hydra bertujuan untuk melihat respon Fail2Ban dalam menangani brute-force. Dengan adanya

pengujian ini, diharapkan Fail2Ban secara otomatis mengambil tindakan pemblokiran IP penyerang.

Gambar 3 Pengujian serangan Fail2Ban SSH menggunakan hydra

Dalam pengujian serangan menggunakan hydra, terdapat 20 serangan login dari akses yang tidak sah secara terus menerus. Sserangan yang terjadi sebanyak 20 kali didasari oleh kombinasi username dan password yang telah diterapkan. Pengujian penyerangan dengan menggunakan hydra telah berhasil dengan ditunjukan oleh gambar 2.

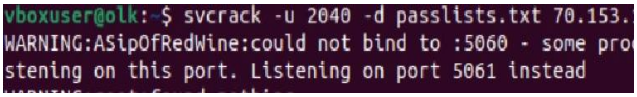
Gambar 4 Verifikasi IP terblokir (SSH)

IP yang digunakan untuk penyerangan masuk dalam IP list yang terblokir dan hal ini membuktikan bahwa Hydra berhasil melakukan serangan brute-force.

Gambar 5 Percobaan login setelah dilakukan pengujian serangan brute-force (SSH)

Pada gambar 5 ditunjukan upaya login manual dengan menggunakan password yang telah diberi izin oleh sistem. Dalam hal ini Fail2Ban bekerja dengan melakukan pemblokiran IP yang menyebabkan IP yang digunakan untuk penyerangan tidak bisa dipakai untuk melakukan percobaan login kembali.

Selain dengan adanya pengujian Fail2Ban untuk layanan SSH, dalam hal ini juga dilakukan pengujian Fail2Ban untuk layanan Asterisk. Pengujian Fail2Ban untuk layanan asterisk diuji dengan memanfaatkan tools SIPVicious untuk melakukan simulasi serangan brute-force.



Gambar 6 Pengujian serangan Fail2Ban Asterisk menggunakan SIPVicious

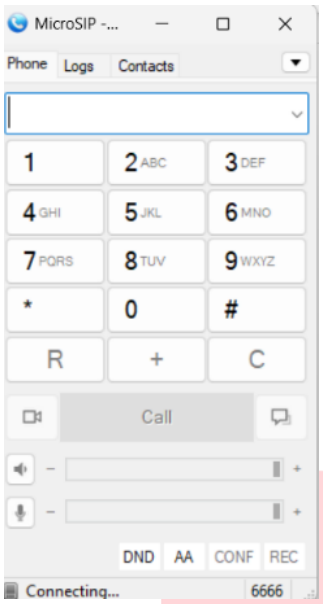
Gambar 6 menunjukan SIPVicious telah berhasil melakukan serangan brute-force dengan mencoba login pada nomor SIP 2040.

Gambar 7 Log fail2Ban Asterisk

Dengan adanya gambar yang ditunjukan oleh gambar 7, simulasi pengujian dengan menggunakan SIPVicious dapat terlihat pada log asterisk. Dalam gambar 7 ditunjukan bahwa nomor ekstensi 2040 yang digunakan untuk simulasi serangan brute-force dengan menggunakan SIPVicious gagal autentikasi sebanyak 5 kali.

Gambar 8 Verifikasi IP terblokir (Asterisk)

IP yang digunakan untuk simulasi penyerangan masuk ke dalam IP list yang terblokir dan dapat dibuktikan bahwa SIPVicious berhasil melakukan serangan brute-force.



Gambar 9 Percobaan login setelah dilakukan pengujian serangan brute-force (Asterisk)

Dalam gambar 9, dapat ditunjukan bahwa autentikasi SIP tidak dapat dilakukan dengan nomor ekstensi yang berbeda tetapi masih dalam 1 jaringan yang sama dalam pengujian serangan brute-force. Hal ini disebabkan oleh Fail2Ban yang memblokir IP yang digunakan untuk pengujian serangan brute-force.

IV. HASIL DAN PEMBAHASAN

Dengan didasarkan hasil penelitian yang telah diperoleh, dapat disimpukan bahwa Fail2Ban merupakan software yang dapat memblokir IP secara otomatis setelah mengamati serta mendeteksi jumlah gagal login dari akses yang tidak sah. Dalam hal ini, Fail2Ban mampu menangani serangan dari login akses yang tidak sah berdasarkan konfigurasi yang telah dibuat, seperti maxretrty=3, findtime=300. Telah terbukti konfigurasi yang ada dalam Fail2Ban dapat berjalan dengan baik dengan dasar IP yang digunakan oleh penyerang dapat terblokir jika melewati batas maxretry dan dalam waktu kurang dari findtime.

Hal lain yang menunjukan bahwa sistem kerja Fail2Ban berhasil adalah ketika alamat IP yang digunakan untuk pengujian sebagai akses login yang tidak sah tidak dapat melakukan koneksi kembali. Hal ini mengindikasikan bahwa Fail2Ban tidak hanya mendeteksi serangan, tetapi juga dapat melakukan tindakan pemblokiran IP.

V. KESIMPULAN

Fail2Ban merupakan software yang efektif dalam pemantauan, pendeteksian, dan pengeksekusian terhadap akses login yang tidak sah. IP yang digunakan untuk login dari akses yang tidak sah tidak dapat terhubung atau terkoneksi kembali ke dalam sistem. Dalam hal ini menunjukan bahwa Fail2Ban merupakan aplikasi atau software yang mendukung pemanfaatan server virtual (cloud) yang difungsikan sebagai keamanan tambahan sistem terhadapat autentikasi dari pihak yang tidak memiliki izin untuk masuk ke dalam sistem.

Dari hasil pengujian, Fail2Ban mampu secara efetktif menangani serangan brute-force. Tindakan Fail2Ban secara otomatis dilakukan tanpa interverensi dari administrator yang hal ini menjadikannya solusi yang efisien dalam menangani proses autentikasi oleh pihak yang tidak memiliki izin.

REFERENSI

[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] U. Kristen Satya Wacana Salatiga, “Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack Artikel Ilmiah Program Studi Teknik Informatika Fakultas Teknologi Informasi,” 2016.

[3] D. R. Az Zahra, F. P. Ilham, H. N. Ramdhani, and A. Setiawan, “Penerapan dan Pengujian Keamanan SSH Pada Server Linux menggunakan Hydra,” *Journal of Internet and Software Engineering*, vol. 1, no. 3, p. 10, Jun. 2024, doi: 10.47134/pjise.v1i3.2627.