ANALISIS IMPLEMENTASI KEAMANAN JARINGAN DENGAN FAIL2BAN TERHADAP SERANGAN BRUTEFORCE

Bayu Rizky Utomo*[1], Naufal Hanan Jati A*[2], Arig Kusuma Jati [3], Indrawan Ady Saputro[4], Moch. Hari Purwidiantoro[5]
[12345]Prodi Informatika, STMIK Amikom Surakarta
[12345]Sukoharjo Indonesia
Email: [1]bayu.10423@mhs.amikomsolo.ac.id,
[2]naufal.10413@mhs.amikomsolo.ac.id , [3]arig.10425@mhs.amikomsolo.ac.id,
[4]indrawanadysaputro@dosen.amikomsolo.ac.id , [5]hari@gmail.com

Abstract

Malicious attacks on network security continue to increase over time. Even though in this globalization era, everyone uses the internet. Servers that are open to public networks are often the target of brute force attacks, especially on ports that allow Secure Shell (SSH) access. This research explores the process of securing the Ubuntu server system from brute force attacks on SSH ports through the implementation of Fail2ban. Open port analysis using Nmap to find out ports that are vulnerable to attacks. Next, a brute force attack using Hydra on the SSH port was carried out to test the system's vulnerability. After the initial attack attempt is successful, Fail2ban is implemented to reduce the risk of brute force by initiating login attempts. Vulnerabilities in network security systems currently mean that server users or administrators need a system to help identify future attacks from irresponsible parties to prevent undesirable things from happening.

Keywords: *Attack, brute force, fail2ban*

Abstraksi

Serangan berbahaya pada keamanan jaringan terus meningkat dari waktu ke waktu. Padahal zaman globalisani ini semua sudah menggunakan internet. Server yang terbuka terhadap jaringan publik sering kali menjadi sasaran serangan brute force, terutama pada port yang mengizinkan akses Secure Shell (SSH). Penelitian ini mengeksplorasi proses pengamanan sistem server Ubuntu dari serangan brute force pada port SSH melalui implementasi Fail2ban. Analisis port terbuka menggunakan Nmap untuk mengetahui port yang rentan terhadap serangan. Selanjutnya, serangan brute force menggunakan Hydra pada port SSH dilakukan untuk menguji kerentanan sistem. Setelah percobaan serangan awal berhasil, Fail2ban diimplementasikan untuk mengurangi risiko brute force dengan melakukan pembatasan percobaan login. Kerentanan dalam sistem keamanan jaringan pada saat ini membuat pengguna sebuah server atau administrator memerlukan sebuah sistem untuk membantu dalam mengidentifikasi serangan-serangan di masa yang akan datang dari pihak yang tidak bertanggung jawab untuk mencegah terjadinya hal-hal yang tidak di inginkan.
Kata Kunci: *serangan, brute force, fail2ban*

1. PENDAHULUAN

Serangan berbahaya pada keamanan jaringan terus meningkat dari waktu ke waktu, karena banyaknya serangan pada jaringan tidak bisa diprediksi sehingga ancaman yang terjadi juga sangat berbahaya [1]. Miliaran hal saat ini sudah terhubung satu sama lain melalu jaringan internet. Keamanan jaringan sangat dibutuhkan untuk mengantisipasi hal ini, mempedulikan keamanan pada saat ini menjadi sangat krusial dan sangat dibutuhkan pada zaman dimana internet dapat diakses oleh siapapun tanpa mengenal kalangan usia [2].

Sebuah sistem pastinya memiliki server yang digunakan untuk saling berinteraksi antara pengguna jaringan. Namun server juga memiliki kerentanan yang harus di waspadai. Saat kita bekerja pada bagian server kita harus selalu waspada pada serangan yang mengancam seperti meretas kata sandi dan username, mencoba mendapatkan hak akses server tanpa ijin sangat berbahaya bagi sistem [3]. Permasalahan ini menjadi latar belakang untuk mengangkat topik mengenai eksploitasi jaringan menggunakan metode brute force. Brute force adalah sebuah teknik yang bergantung pada kecepatan dan ketelitian komputer untuk membuat sebuah kombinasi sampai menemukan kombinasi yang benar [4].

Serangan ini menggunakan kali linux yang akan menyerang port ssh pada linux Ubuntu versi 21.04 Lts yang sudah di install pada virtual box. Vitual box adalah perangkat lunak yang digunakan untuk memvisualisakan sistem operasi open source seperti linux agar dapat digunakan sebagai sebuah media belajar untuk melakukan sebuah uji coba agar lebih efektif [5]. Penyerangan dilakukan pada port ssh linux ubuntu yang terbuka. Port yang biasanya terbuka untuk serangan adalah port 22 tcp. Port ini sangat rentan terhadap serangan apabila user tidak dapat mengatur port dengan baik sehingga sering disalah gunakan oleh orang tidak bertanggung jawab untuk mendapatkan hak akses ke server [6].

Tools yang digunakan dalam penyerangan brute force adalah hydra yang dijalankan pada kali linux. Hydra dapat menganalisis hak akses yang digunakan oleh server melalui port yang terbuka. Selain hydra tools yang dapat digunakan dalam melakukan serangan brute force adalah medusa dan crack penyerangan yang dilakukan adalah mencoba membuka kunci atau kata sandi yang digunakan oleh admin melalui wordlist yang sudah dibuat untuk melakukan percobaan hingga ditemukan id dan password yang tepat [7].

Tools-tools yang mudah diakses ini menyebabkan kerentanan dalam jaringan komputer sangat berbahaya. Pemilik server melakukan antisipasi dengan cara menggunaan seorang administrator untuk mengelola server yang dimilikinya. Namun, bahkan setelah menggunakan administrator masih bisa terjadi kejebolan server atau adanya penyusup tidak bertanggung jawab masuk ke dalam server dan melakukan perubahan tanpa diketahui administrator. Tentunya seorang administrator tidak dapat memantau selama dua puluh empat jam terhadap server yang di kelolanya.

Masalah tersebut dapat diatasi dengan menggunakan autoblock terhadap penyusup atau penyerang sehingga dapat melakukan pencegahan selama 7x24 jam terhadap server yang selalu aktif. Tools Fail2ban dapat menjadi salah satu solusi untuk melakukan pencegahan terhadap serangan yang menuju pada server. Tools ini dapat melakukan block terhadap ip yang tidak dikenal oleh server dan dapat melakukan block secara otomatis pada percobaan memasukkan username dan password secara berulang. Tools ini sangat mudah untuk di install karena free dan open source sehingga sangat cocok untuk administrator baik yang pemula maupun sudah expert dalam bidang ini. Melalui fail2ban dapat dilakukan ban ip selama beberapa waktu sesuai dengan konfigurasi yang sudah dilakukan oleh administrator.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu yang Relevan

2.1.1. Penelitian Tentang Serangan Brute Force

Meningkatnya serangan siber dan pencurian data yang sensitif sering menjadi topik utama untuk dibahas pada perkembangan teknologi saat ini. Semakin banyak aplikasi yang mengarahkan penggunanya atau berorientasi menggunakan server. Untuk mengantisipasi serangan yang harus dilakukan adalah melakukan ujicoba penetrasi terhadap server termasuk serangan brute force yang menyerang pada port terbuka. Ujicoba simulasi penyerangan dilakukan dengan mendapatkan username dan password [8]. Peneliti selanjutnya juga menjelaskan bahwa pencegahan serangan brute force pada VPS (Virtual Private Server) menggunakan metode IPS (Intrusion Prevention System) dari metode tersebut didapatkan sebuah hasil apabila sebuah sistem jika ada serangan percobaan 5 kali login pada sessio SSH akan dilakukan blokir IP. Lalu dilakukan pengujian terhadapa fail2ban sesuai dengan metode IPS didapatkan hasil bahwa fail2ban memberikan performa yang memuaskan dalam melakukan tugasnya untuk memblokir ip dan memvisualisasikan IP yang diblokir [9].

2.2. Konsep atau Teori yang Relevan

2.2.1. Serangan Brute Force dengan Hydra pada Linux Ubuntu

Negara indonesia menduduki peringkat dua teratas di dalam negara yang sering mengalami serangan brute force. Pada bulan januari sampai desember 2023 di deteksi terjadi kurang lebih 61 juta lebih serangan bruteforce.Generic.RDP yang menyerang server. Ubuntu adalah sistem operasi linux open source yang berbasis debian dan pertama kali diterbitkan pada tahun 2004. Ubuntu saat perilisan memiliki 3 edisi yaitu dekstop,server,dan core yang dapat berjalan baik di komputer main pada virtual server. Maka dari itu diperlukan sebuah sistem untuk mengantisipasi serangan Brute Force Hydra pada kerentanan rendah [11].

2.2.2. Penggunaan Fail2ban sebagai Tools pencegahan

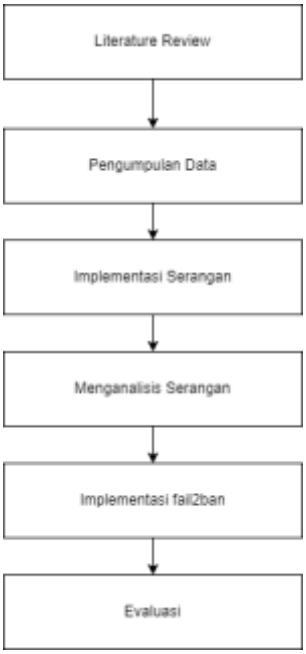
Pada penelitian sebelumnya yang menggunakan metode studi kasus dan eksperimen terhadap server linux ubuntu fail2ban digunakan untuk melakukan block serangan terhadap percobaan login yang dilakukan oleh penyerang sebanyak 6 kali , lalu fail2ban akan langsung memutus serangan terhadap penyerang. Pemutusan koneksi dilakukan oleh fail2ban yang sudah terinstall pada target. Pembatasan beberapa kali percobaan yang dapat dilakukan di konfigurasi pada jail.conf serta menyimpan history penyerangan lalu dikirimkan melalui blocklist.de [10].

2.3. Kerangka Konseptual

Berdasarkan penelitian sebelumnya fail2ban secara teknis digunakan untuk melakukan pemblokiran terhadap ip yang tidak dikenal melakukan beberapa kali percobaan login sebagai administrator pada server dengan melakukan ban pada ip secara otomatis serta dapat menyimpan log serangan pada directory yang sudah di atur oleh administrator. Tools ini juga dapat melakukan pengiriman peringatan melalui email dengan menggunakan tools lain yaitu blocklist.de , sehingga admin akan lebih cepat dalam melakukan antisipasi serangan. Alat ini dipilih karena memiliki fitur yang lengkap dan cocok dalam melakukan antisipasi serangan brute force serta mudahnya dalam melakukan pemasangan fail2ban pada linux ubuntu versi 24.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi kasus dan eksperimen yang dilakukan secara mandiri pada menggunakan server linux ubuntu sebagai target dan kali linux sebagai penyerang. Studi kasus dilakukan untuk dijadikan referensi dari penelitian sebelumnya sebagai panduan untuk melakukan eksperimen. Eksperimen ini dilakukan pada virtual server yang terdapat pada virtual machine. Eksperimen dilakukan dari penyerangan lalu melakukan pencegahan menggunakaan tools fail2ban. Alur penelitian dapat dilihat pada gambar 1.



Gambar 1. Metode Penyerangan

3.1. Literature Review

Sebelum melakukan percobaan dilakukan berbagai macam literature review. Proses ini berfungsi untuk mencari referensi-referensi pada jurnal penelitain yang sudah dibuat sebelumnya yang sesuai dengan penelitian ini. Penelitian sebelumnya digunakan untuk mendukung argumen yang diberikan pada penelitian ini

3.2. Pengumpulan Data

Penyerang mengumpulkan data-data terlebih dahulu mengenai server yang akan diserang . Misalnya, mencari ip address korban , membuat list username dan password yang mungkin digunakan pada server yang akan diserang,mencari port ssh yang terbuka. Biasanya port yang terbuka adalah tcp 22 atau umtp 25 sebagai default apabila belum diubah. Melakukan pengumpulan data menggunakan tools nmap untuk mendapatkan ip jaringan yang dipakai dan melihat port yang terbuka. Setelah selesai mengumpulkan data-data korban, pelaku akan mulai penyerangan menggunakan celah dari port ssh dengan memanfaatkan karakteristik flow dan upaya login yang gagal pada ssh[12].

3.3. Implementasi Serangan

Selanjutnya adalah melakukan pen testing. Pen testing adalah sebuah percobaan yang dilakukan secara offensive untuk mengidentifikasi, mengukur , dan mengecek kerentanan terhadap sebuah keamanan sistem yang bertujuan untuk memperkuat sistem yang akan dibuat[13]. Hydra dapat memproses dengan cepat saat melakukan serangan brute force dengan melakukan berkali-kali percobaan untuk mendapatkan sebuah data username dan password yang cocok pada server dengan menyerang port

ssh yang terbuka. Apabila korban serangan tidak menggunakan firewall atau perlindungan yang lain hydra akan sangat mudah untuk mendapatkan akses pada server yang dituju.

3.4. Menganalisis Serangan

Setelah melakukan serangan yang harus dilakukan adalah menganalisis serangan tentang apa yang diserang dan tentang bagaimana penyerang bisa masuk. Dalam kasus serangan brute force penyerang mendapatkan akses login dengan cara melakukan berulang-kali percobaan login sesuai dengan username list dan password list yang sudah dibuat oleh penyerang[14]. Dari berulang kali percobaan ini akan di dapatkan password yang cocok yang dapat digunakan untuk login ke dalam server.

3.5. Konfigurasi dan Implementasi Fail2ban Secara optimal

Fail2ban memiliki konfigurasi yang dapat diatur oleh admin sesuai dengan keinginan bagaimana tools ini akan bekerja. Konfigurasi fail2ban dapat dilakukan pada file yang bernama jail.conf disini admin akan mengatur berapa percobaan yang dapat dilakukan sebelum fail2ban memblokir sebuah IP. Di dalam jail.conf ini admin juga dapat mengatur kapan waktu ban pada IP lalu port mana yang akan dilakukan proteksi serta dimana directory untuk menyimpan log ip yang sudah diblokir.

Konfigurasi yang optimal dalam menggunakan fail2ban adalah jumlah percobaan memasukkan password salah dapat dibatasi maksimal 2 atau 3 kali lalu untuk waktu ban dapat di atur ban 3 hari apabila salah memasukkan password sesuai percobaan yang sudah dilakukan. Port yang sering terbuka dan di serang adalah port SSH dan directory untuk menyimpan log sering dipilih pada /var/log/auth.log

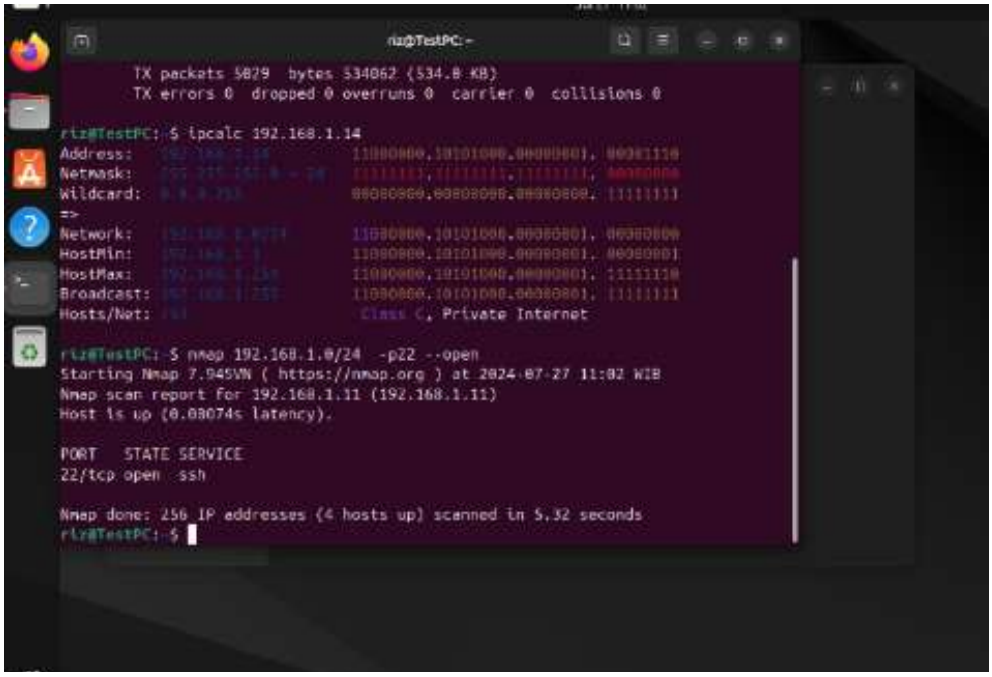
3.6. Evaluasi

Setelah melakukan implementasi fail2ban lalu dilakukan evaluasi apakah tools fail2ban masih memiliki celah untuk dapat diserang atau tidak. Dengan cara melakukan beberapa kali percobaan lagi dalam memasukkan password yang salah maksimal 5 kali untuk memastikan bahwa tools fail2ban bekerja dengan baik dan tidak memiliki celah lagi untuk diserang pada percobaan-percobaan yang sudah dilakukan.

4. HASIL DAN PEMBAHASAN

4.1. Menganalisis Port Terbuka pada IP yang Dituju

Seperti pada gambar 2 berikut ini apabila kita berada pada jaringan yang sama kita dapat mengakses ip dari jaringan wifi atau router yang kita gunakan. Setelah mendapatkan ip lalu lakukan proses scan port yang terbuka menggunakan nmap berikan ip yang dituju dan lihat port 22 yang biasanya digunakan untuk ssh.



Gambar 2. Analisis Ip jaringan menggunakan ip calc.

4.2. Implementasi Serangan Hydra

Pada gambar 3 dibawah ini percobaan melakukakan serangan brute force berhasil dilakukan serangan hydra pada port ssh untuk IP 192.168.1.14. Percobaan penyerangan menggunakan hydra dibutuhkan waktu sekitar 5 menit untuk menganalisis username dan password dari wordlist yang sudah dibuat sebelumnya. Di dapatkan username dan password yang digunakan oleh server ubuntu yang diserang. Ini menandakan bahwa apabila kita tidak menggunakan tools.

Gambar 3. Implementasi serangan menggunakan hydra.

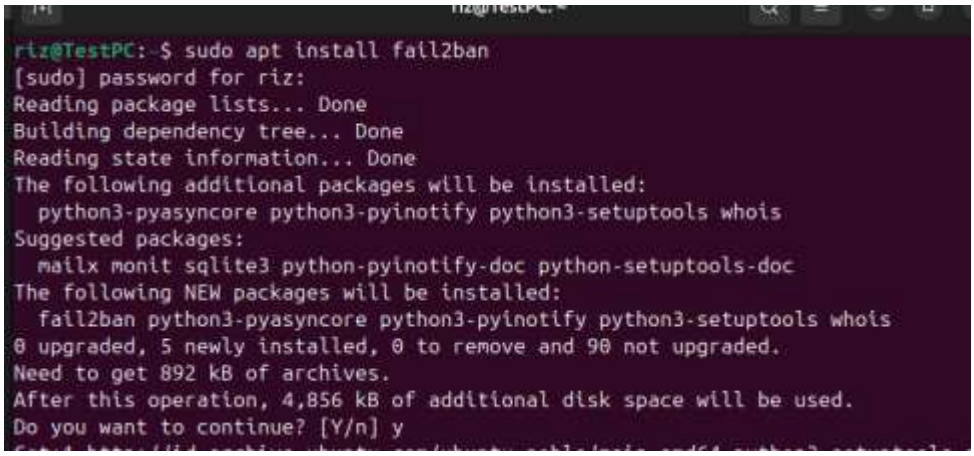
4.3. Melakukan percobaan password salah

Dapat dilihat pada gambar 4 dilakukan beberapa kali percobaan password salah tetapi masih dapat terus mencoba sampai berulang-kali. Ini termasuk dalam celah keamanan yang memerlukan tools untuk mencegah percobaan memasukkan password yang salah berulang kali sehingga dapat mengantisipiasi serangan brute force dan mencegah penyerang mendapatkan hak akses tanpa seijin pengguna.

Gambar 4. Percobaan memasukkan password salah berulang kali sebelum menggunakan tools.

4.4. Implementasi Fail2ban

4.4.1. Instalasi Fail2ban



Gambar 5. Instalasi fail2ban.

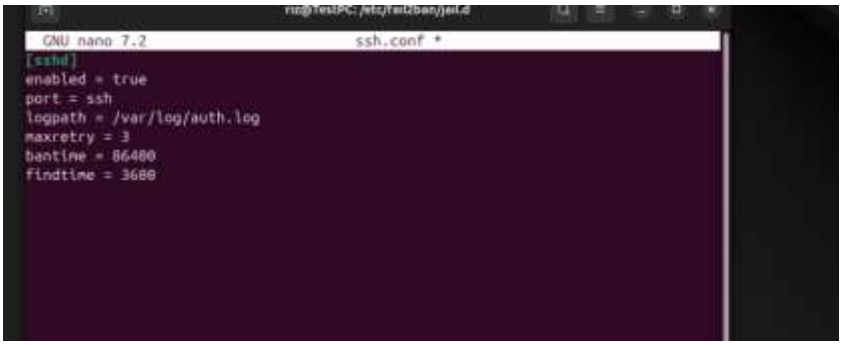
Sebelum menjalankan tools fail2ban alangkah baiknya mengecek dulu apakah fail2ban sudah di install dengan command sudo apt install fail2ban apabila belum di install akan muncul prompt seperti pada gambar 5 pada linux ubuntu. User cukup menginput Y untuk menjalankan instalasi fail2ban pada linux ubuntu 24.04.

4.4.2. Konfigurasi fail2ban

Gambar 6. Change directory jail.d.

Sebelum melakukan konfigurasi pada fail2ban di linux ubuntu user harus pindah directory dulu ke *directory* fail2ban jail.d. *Directory* ini yang nantinya akan dilakukan konfigurasi fail2bannya pada nano conf. proses ini dilakukan sebelum admin memasuki file jail.conf untuk melakukan konfigurasi pengaturan yang di inginkan oleh admin bagaimana fail2ban akan bekerja sesuai yang di harapkan oleh pengguna. Sehingga fail2ban dapat dijalankan secara optimal.

4.4.3. Konfigurasi SSHD dalam Fail2ban



Gambar 7. Configurasi sshd pada fail2ban.

Setelah memasuki sshd konfigurasi bisa dapat memasukkan prompt untuk mengatur konfigurasi fail2ban. Seperti pada gambar 7 enabled berarti bahwa fail2ban nya diaktifkan atau tidak. True untuk mengaktifkan dan False untuk menonaktifkan. Selanjutnya adalah port ini menandakan port mana yang akan kita lindungi dengan fail2ban pada perobaan ini menggunakan port ssh. Logpath berfungsi sebagai path untuk memunculkan log fail2ban ini bebas dimana saja. Selanjutnya adalah maxretry ini berfungsi untuk memberikan batasan dalam memasukkan password atau username yang salah pada percobaan kali ini maksimal 3 kali. Bantime adalah waktu ban yang akan diberikan pada ip yang memasukkan password salah berulang kali. Percobaan ini menggunakan waktu ban satu hari.

4.5. Melakukan Percobaan implementasi Serangan Setelah Fail2ban

Apabila fail2ban sudah di install, percobaan serangan brute force dengan hydra sudah tidak dapat dilakukan lagi. Akan muncul prompt yang mengatakan bahwa percobaan yang dilakukan hydra sudah di disable ini menandakan bahwa fail2ban sudah

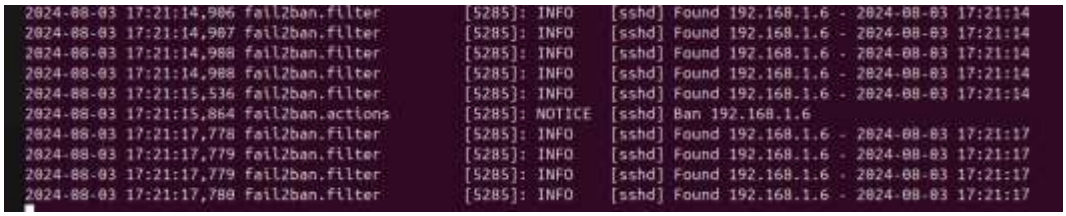
bekerja dalam memblokir serangan bruteforce pada linux ubuntu. Prompt yang muncul bisa dilihat pada gambar 8.

Gambar 8. Percobaan serangan hydra setelah implementasi fail2ban.

Begitupula percobaan memasukkan password yang salah berkali-kali juga akan di ban secara otomatis oleh fail2ban sesuai dengan maxretry yang sudah di atur oleh user. Perlakuan percobaan password ini hanya untuk memastikan apakah fail2ban bekerja dengan baik atau tidak. Percobaan bisa dilihat pada gambar 9 yang memunculkan prompt connection closed pada ip yang dituju.

Gambar 9. Percobaan memasukkan password salah berulang kali.

4.6. Evaluasi Perfoma Fail2ban Terhadap Serangan



Gambar 10. Log pada fail2ban.

Performa fail2ban sesuai dengan yang diharapkan , tools ini memblokir setiap 3 kali percobaan memasukkan password salah yang dilakukan oleh hydra di dalam kali linux untuk menyerang linux ubuntu. Fail2ban juga memberikan log serangan sesuai yang diharapkan untuk mengidentifikasi siapa yang melakukan percobaan penyerangan server linux ubuntu versi 24.04 ini. Hasil ini sesuai dengan penelitian-penelitian sebelumnya yang melakukan percobaan penyerangan penetrasi testing pada dua server yang berbeda. Fail2ban memblokir IP yang melakukan serangan serta memberikan log IP penyerang yang melakukan percobaan pada server. Tools ini dapat memblokir serangan

dari hydra dengan sangat baik sebelum hydra dapat menemukan username dan password target.

5. KESIMPULAN

Kesimpulan yang didapatkan dari penelitian ini adalah bagaimana cara mengantisipasi serangan brute force dengan tools fail2ban.

1. Penelitian ini menunjukkan bahwa pengamanan server Ubuntu dengan Fail2ban efektif dalam mencegah serangan brute force pada port SSH. Nmap dapat mendeteksi port terbuka yang rentan, seperti port 22, dan tanpa perlindungan tambahan, serangan brute force dengan Hydra dapat berhasil. Namun, setelah Fail2ban diaktifkan, sistem otomatis memblokir IP yang berulang kali salah memasukkan kata sandi, sehingga mengurangi risiko keamanan.
2. Fail2ban terbukti sebagai langkah sederhana namun kuat untuk mencegah akses yang tidak sah dan menutup celah keamanan akibat upaya brute force. Fail2ban merupakan tools yang cukup mudah untuk melakukan konfigurasi pada linux ubuntu karena termasuk tools yang bersifat open source.
3. Penelitian ini dapat dikembangkan lebih lanjut dari berbagai aspek, dikarenakan fail2ban sendiri memiliki fleksibilitas yang luar biasa bisa di terapkan dalam sistem operasi,server, maupun web server. Diharapkan penelitian ini dapat memberikan dampak untuk kemajuan keamanan jaringan yang lebih baik karena berevolusinya tipe-tipe serangan di masa yang akan datang , maka Fail2ban juga harus dikembangkan lebih jauh tidak hanya dalam aspek serangan brute force saja.

DAFTAR PUSTAKA

[1] S. K. Wanjau, G. M. Wambugu, and G. N. Kamau, “SSH-Brute Force Attack Detection Model based on Deep Learning,” *Int. J. Comput. Appl. Technol. Res.*, vol. 10, no. 01, pp. 42–50, 2021, doi: 10.7753/ijcatr1001.1008.

[2] M. M. Raikar and S. M. Meena, “SSH brute force attack mitigation in Internet of Things (IoT) network : An edge device security measure,” *ICSCCC 2021 - Int. Conf. Secur. Cyber Comput. Commun.*, no. July, pp. 72–77, 2021, doi: 10.1109/ICSCCC51823.2021.9478131.

[3] V. Grover, “An Efficient Brute Force Attack Handling Techniques for Server Virtualization,” *SSRN Electron. J.*, pp. 1–4, 2020, doi: 10.2139/ssrn.3564447.

[4] S. A. Rahmah, "Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web," *J. Comput. Digit. Bus.* , vol. 2, no. 3, pp. 112–119, 2023.

[5] R. Umbarwati, B. Basori, and T. L. A. Sucipto, "Penerapan Model Pembelajaran Group Investigation Dan Media Pembelajaran Virtual Box Untuk Meningkatkan Keaktifan Dan Hasil Belajar Siswa Pada Mata Pelajaran Sistem Operasi Kelas X Multimedia Smk N 6 Surakarta," *J. Ilm. Pendidik. Tek. dan Kejuru.*, vol. 13, no. 1, p. 61, 2020, doi: 10.20961/jiptek.v13i1.24268.

[6] I. Marzuki, "Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux," *J. Teknol. Inf. Indones.*, vol. 2, no. 2, pp. 18–24, 2019, doi: 10.30869/jtii.v2i2.312.

[7] Dewa Made Julijati Putra, I Nyoman Namo Yoga Anantra, Putu Adhitya kusuma, Putu Damar Jagat Pratama, Gede Arna Jude Saskara, and I Made Edy Listartha, "Analisis Perbandingan Serangan Hydra, Medusa Dan Ncrack Pada Password Attack," *J. Inform. Teknol. dan Sains*, vol. 4, no. 4, pp. 461–466, 2022, doi: 10.51401/jinteks.v4i4.2192.

[8] F. Fachri, "Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 1, pp. 51–58, 2023, doi: 10.25126/jtiik.20231015872.

[9] Farhannullah and M. Hardjianto, "Sistem Monitoring Serangan SSH dengan Metode Intrusion Prevention System (IPS) Fail2ban Menggunakan Python Pada Sistem Operasi Linux," *J. Ticom Technol. Inf. Commun.*, vol. 11, no. 1, pp. 33–38, 2022, doi: 10.70309/ticom.v11i1.68.

[10] I. Kurniawan, "Sistem Pencegahan Serangan Bruteforce Pada Ubuntu Server Dengan Menggunakan Fail2Ban," *Infomatek*, vol. 18, no. 2, p. 89, 2017, doi: 10.23969/infomatek.v18i2.496.

[11] G. Patoni, Y. Muhyidin, D. Singasatia, and K. Penulis, "Implementasi Wazuh Pada Ubuntu Server Untuk Mendeteksi Serangan Brute Force Hydra," *J. Ris. Sist. Inf. dan Tek. Inform.*, vol. 2, no. 5, pp. 145–156, 2024.

[12] N. Hubballi, N. Tiwari, and P. Khandait, "POSTER: Distributed SSH Bruteforce Attack Detection with Flow Content Similarity and Login Failure Reputation," *Proc. 15th ACM Asia Conf. Comput. Commun. Secur. ASIA CCS 2020*, pp. 916–918, 2020, doi: 10.1145/3320269.3405443.

[13] G. Deng *et al.*, "PentestGPT: An LLM-empowered Automatic Penetration Testing Tool," 2023, [Online]. Available: http://arxiv.org/abs/2308.06782

[14] S. Bahri, "Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 136–147, 2023, doi: 10.60076/indotech.v1i3.239.