Jurnal Publikasi Teknik Informatika
Volume. 4 Nomor. 2 Mei 2025
e-ISSN: 2808-8972; p-ISSN: 2808-9367, Hal. 195-209
DOI: https://doi.org/10.55606/jupti.v4i2.5144
Available online at: https://journalcenter.org/index.php/jupti

Pencegahan dan Visualisasi Serangan *Brute Force* Menggunakan Fail2Ban, *Prometheus*, dan Grafana Studi Kasus di Sekolah Tinggi Teknologi Terpadu Nurul Fikri

April Rustianto[1*] , Arif Fadillah[2] , Jemiro Kasih[3]
[1-3]Sekolah Tinggi Teknologi Terpadu Nurul Fikri, Indonesia
Email : april.rustianto@dosen.nurulfikri.ac.id [1], afadillah713@gmail.com [2], jemiro.kasih@nurulfikri.ac.id [3]

*Korespondensi penulis: april.rustianto@dosen.nurulfikri.ac.id**

Abstract. *Brute force attacks are a common method used by attackers to breach authentication systems, both on Secure Shell (SSH) services and website login pages such as WordPress. In educational institutions, particularly at the Nurul Fikri Integrated Technology College, authentication system security is crucial for maintaining data confidentiality and integrity. Prior to this research, the system in use was not equipped with an automated defense mechanism capable of responding to brute force attacks quickly and effectively. This research aims to implement Fail2Ban, an open-source application designed to automatically block IP addresses that make failed login attempts exceeding a certain threshold. The research method involved testing two scenarios: an attack on the SSH service using Nmap, and an attack on the WordPress login page using a Python script. The Fail2Ban configuration set the maxretry parameters to five failed attempts, a findtime of 10 minutes, and a bantime of 3 minutes. The test results showed that Fail2Ban successfully blocked the attacker's IP address according to the specified parameters, thus preventing further login attempts. To enhance monitoring capabilities, Fail2Ban is integrated with Prometheus and Grafana using a combination of the Fail2Ban Exporter, Python scripts, and Push Gateway. This integration produces an interactive dashboard that displays metrics such as the number of blocked IP addresses, total failed login attempts, and the status of active blocks. This data visualization allows system administrators to monitor attack activity in real-time and take additional precautions if necessary. Thus, Fail2Ban implementation is not only effective in preventing brute-force attacks but also improves situational awareness and rapid response to security incidents in educational institutions.*

Keywords: *Brute Force Attack, Fail2Ban, Prometheus, SSH Security, WordPress Login.*

Abstrak. Serangan *brute force* merupakan salah satu metode umum yang digunakan penyerang untuk membobol sistem autentikasi, baik pada layanan Secure Shell (SSH) maupun halaman login situs web seperti WordPress. Di lingkungan institusi pendidikan, khususnya di Sekolah Tinggi Teknologi Terpadu Nurul Fikri, keamanan sistem autentikasi menjadi aspek krusial untuk menjaga kerahasiaan dan integritas data. Sebelum penelitian ini dilakukan, sistem yang digunakan belum dilengkapi mekanisme pertahanan otomatis yang mampu merespons serangan *brute force* secara cepat dan efektif. Penelitian ini bertujuan untuk mengimplementasikan Fail2Ban, sebuah aplikasi *open-source* yang dirancang untuk secara otomatis memblokir alamat IP yang melakukan percobaan login gagal melebihi ambang batas tertentu. Metode penelitian melibatkan pengujian pada dua skenario, yaitu serangan terhadap layanan SSH menggunakan *Nmap*, serta serangan terhadap halaman login WordPress menggunakan skrip Python. Konfigurasi Fail2Ban menetapkan parameter *maxretry* sebanyak lima kali percobaan gagal, *findtime* selama 10 menit, dan *bantime* selama 3 menit. Hasil pengujian menunjukkan bahwa Fail2Ban berhasil memblokir alamat IP penyerang sesuai dengan parameter yang ditetapkan, sehingga mencegah upaya login selanjutnya. Untuk meningkatkan kemampuan pemantauan, Fail2Ban diintegrasikan dengan Prometheus dan Grafana menggunakan kombinasi Fail2Ban Exporter, skrip Python, dan Push Gateway. Integrasi ini menghasilkan *dashboard* interaktif yang menampilkan metrik seperti jumlah IP yang diblokir, total percobaan login gagal, serta status pemblokiran yang sedang aktif. Visualisasi data ini memungkinkan administrator sistem untuk memantau aktivitas serangan secara *real-time* dan mengambil tindakan pencegahan tambahan jika diperlukan. Dengan demikian, implementasi Fail2Ban tidak hanya efektif dalam mencegah serangan *brute force*, tetapi juga meningkatkan kesadaran situasional dan respons cepat terhadap insiden keamanan di lingkungan institusi pendidikan.

Kata kunci: *Brute Force*, Fail2Ban, *Prometheus*, SSH, *Login WordPress*.

Received: April 12, 2025; Revised: April 29, 2025; Accepted: Mei 15, 2025; Published: Mei 31, 2025

1. PENDAHULUAN

Sekolah Tinggi Teknologi Terpadu Nurul Fikri adalah sebuah perguruan tinggi yang memadukan keilmuan praktis di bidang teknologi informasi dengan pengembangan kepribadian islami, kompeten dan berkarakter. Karena Sekolah Tinggi Teknologi Terpadu Nurul Fikri merupakan perguruan tinggi yang berorientasi pada teknologi, tentunya *server* dan *website* menjadi suatu komponen yang sangat penting untuk menunjang kebutuhan terkait proses bisnis yang berlangsung. Namun, seiring dengan teknologi yang semakin maju, timbul juga ancaman yang semakin canggih dan beragam. Hal ini terbukti dengan adanya beberapa kejadian peretasan situs *web* yang dimiliki Sekolah Tinggi Teknologi Terpadu Nurul Fikri. Terhitung dari Januari 2024 hingga September 2024 sudah 4 *website* berbasis Wordpress yang terkena serangan.

Banyak kemungkinan celah yang memungkinakan penyerang dapat meretas situs *website* Sekolah Tinggi Teknologi Terpadu Nurul Fikri. Pada penelitian ini penulis akan melakukan pencegahan terhadap salah satu jenis serangan yaitu serangan *brute force*. Alasan mengapa penulis memilih untuk mencegah serangan *brute force* adalah karena pada beberapa kasus yang terjadi, setelah dilakukan pemeriksaan terhadap *file log*, ditemukan indikasi serangan *brute force* dengan melakukan percobaan *login* berulang terhadap halaman *administrator Wordpress*.

Salah satu alat untuk mencegah serangan *brute force* adalah menggunakan aplikasi Fail2ban, Fail2ban melindungi sistem dari serangan *brute force* dengan memantau *log file* dan mendeteksi pola kegagalan autentikasi berulang, seperti upaya *login* yang gagal. Ketika Fail2ban mendeteksi sejumlah percobaan *login* yang gagal dari alamat *IP* yang sama dalam jangka waktu tertentu, Fail2ban secara otomatis memblokir *IP* tersebut untuk sementara dengan menambahkan aturan pada *firewall*.

Berdasarkan penjelasan diatas maka diperlukan sistem *monitoring* berbasis grafis yang dapat menampilkan dan mencatat serangan sehingga dapat memudahkan seorang *administrator* dalam memantau dan melakukan tindakan ketika terjadi serangan. Disinilah Prometheus dan Grafana hadir untuk melakukan hal tersebut, Prometheus akan mencatat serangan yang terjadi dengan retensi waktu yang dapat diatur sesuai kebutuhan, kemudian Grafana yang akan menampilkan serangan tersebut dalam tampilan *dashboard monitoring*.

2. TINJAUAN LITERATUR

Keamanan Informasi

Keamanan informasi merupakan upaya untuk menjaga aset informasi dari berbagai ancaman yang berpotensi terjadi. Oleh karena itu, keamanan informasi berkontribusi dalam menjaga keberlangsungan bisnis, meminimalkan risiko yang ada, serta memaksimalkan keuntungan dari investasi. Semakin besar volume informasi perusahaan yang diolah, disimpan, dan dibagikan, semakin tinggi pula potensi terjadinya kerusakan, kehilangan, atau kebocoran data ke pihak eksternal yang tidak diinginkan.

Cyber Security

Keamanan siber atau *cyber security* mencakup serangkaian kebijakan, konsep keamanan, langkah perlindungan, aturan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, serta teknologi yang dirancang untuk melindungi pengguna dunia maya dari berbagai ancaman dan risiko yang mungkin terjadi.

Cyber attack

Cyber attack atau serangan siber adalah aksi yang dilakukan secara daring dengan tujuan untuk merusak sistem komputer, mencuri informasi, atau mengganggu operasional layanan digital. Semua aksi atau tindakan kejahatan yang dilakukan pada ruang digital atau *cyber space* disebut dengan *cyber crime*. Berikut beberapa jenis serangan siber yang sering dilakukan:

Malware

Malware atau *Malicious Software*, adalah program berbahaya yang dibuat untuk melakukan tindakan merugikan pada sistem komputer. *Malware* sering digunakan oleh pihak-pihak dengan niat buruk untuk memanipulasi data dan informasi, seperti mencuri data pribadi, membajak akun, atau melakukan kejahatan serupa lainnya.

Ransomware

Ransomware merupakan jenis *malware* yang berfungsi untuk mengenkripsi data pada perangkat komputer atau sistem lainnya. Setelah data terkunci, pelaku kejahatan meminta korban membayar sejumlah uang sebagai tebusan agar data tersebut dapat dipulihkan atau didekripsi kembali. *Ransomware* biasanya menyusup ke dalam sistem melalui lampiran mencurigakan dalam email, situs web yang telah terinfeksi, atau dengan memanfaatkan celah keamanan pada perangkat lunak atau sistem operasi.

Brute Force

Serangan *brute force* adalah metode yang sangat sederhana dan langsung untuk menyelesaikan masalah. Dalam konteks pembobolan kata sandi, *algoritma brute force* akan mencoba semua kemungkinan kata sandi berdasarkan karakter dan panjang yang ditentukan, yang tentu saja menghasilkan sejumlah besar kombinasi.

Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) merupakan jenis serangan siber yang berbahaya dan sulit diatasi. Tujuan utama serangan ini adalah membuat kinerja *server* menurun secara drastis dengan membanjirinya menggunakan banyak permintaan palsu, hingga server menjadi *overload* dan tidak dapat merespons permintaan yang sah. Serangan *DDoS* dapat mengakibatkan gangguan parah pada lapisan aplikasi dan jaringan komputer, sehingga membahayakan keberlangsungan *web server*

Phishing

Phishing adalah tindakan yang dilakukan untuk memperoleh informasi pribadi pengguna secara tidak sah dengan memanfaatkan *email* dan situs *web* palsu yang dirancang seperti tampilan situs resmi. Informasi yang biasanya dicari oleh pelaku *phising*, atau *phisher*, meliputi kata sandi akun hingga data penting lain. *Phisher* sering menggunakan *email*, *banner*, atau jendela *pop-up* untuk mengarahkan pengguna ke situs *web* palsu, di mana mereka diminta memberikan data pribadi. Dalam situasi ini, *phisher* memanfaatkan kelalaian atau kurangnya kehati-hatian pengguna untuk mencuri informasi berharga tersebut.

SQL Injection

SQL Injection merupakan jenis serangan siber dimana penyerang menyisipkan kode berbahaya ke dalam perintah *SQL* dengan tujuan mengakses data yang seharusnya tidak dapat diakses oleh pengguna biasa. Serangan ini berpotensi menyebabkan kebocoran data dalam jumlah besar dan sering kali digunakan untuk menyerang aplikasi berbasis *web*.

Fail2ban

Merupakan sistem keamanan yang bertugas melindungi berbagai jenis *server* dan mencatat hasilnya dalam bentuk *log*. Penerapan sistem ini pada *server* bertujuan untuk memperkuat keamanan lalu lintas jaringan dari potensi serangan yang dapat merusak atau mengganggu layanan *server*. Fail2ban beroperasi dengan cara memblokir *IP address* yang diduga berupaya menyerang atau melanggar keamanan sistem dalam periode waktu tertentu, sehingga koneksi dari *IP* yang mencurigakan tersebut dihentikan sementara.

Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah sebuah aplikasi perangkat lunak yang dirancang untuk mengidentifikasi aktivitas mencurigakan atau pola lalu lintas tidak normal dalam sistem atau jaringan komputer[11]. Dengan memantau dan menganalisis data yang masuk maupun keluar, IDS berfungsi sebagai alat keamanan yang membantu mendeteksi potensi ancaman, seperti upaya akses tidak sah, serangan siber, atau aktivitas berbahaya lainnya. Sistem ini memainkan peran penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data, sehingga menjadi komponen krusial dalam strategi keamanan jaringan *modern.*

Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) merupakan sebuah perangkat lunak atau perangkat keras yang bekerja untuk mengawasi lalu lintas jaringan, mendeteksi aktivitas mencurigakan, dan mencegah penyusupan atau peristiwa yang menyebabkan kerusakan jaringan secara dini [12]. *Intrusion Prevention System* (IPS) biasanya diposisikan secara inline di jalur utama lalu lintas jaringan, sehingga mampu menganalisis dan memfilter data sebelum mencapai sistem tujuan.

Secure Shell (SSH)

Secure Shell (SSH) adalah sebuah cara untuk melakukan login jarak jauh yang aman dari satu komputer ke komputer lain, baik di jaringan lokal (LAN) maupun melalui internet[13]. Protokol SSH memanfaatkan enkripsi untuk menjaga kerahasiaan data yang ditransmisikan antara klien dan server, sehingga informasi penting seperti nama pengguna, kata sandi, maupun instruksi tidak mudah diakses oleh pihak yang tidak berwenang. SSH biasanya digunakan untuk mengelola sistem operasi berbasis Unix atau Linux dari jarak jauh.

Prometheus

Prometheus adalah *database time-series open source* yang umumnya digunakan untuk memantau sistem serta berfungsi sebagai alat peringatan. Sejak pertama dirilis pada 2012, banyak organisasi atau perusahaan yang mengadopsi Prometheus untuk sistem mereka. Saat ini, Prometheus telah menjadi proyek *open source* yang berdiri sendiri. Prometheus menggunakan sistem berbasis *Pull*, dimana *server* Prometheus secara berkala "meminta" data dari aplikasi yang sedang berjalan

Fail2ban *Exporter*

Fail2ban *exporter* adalah Sebuah perangkat lunak yang mengumpulkan metrik, kemudian mengekspornya ke Prometheus. Fail2ban *Exporter* adalah alat pengumpul metrik yang digunakan dalam ekosistem Prometheus untuk memantau aktivitas dan status Fail2ban

pada sistem. Alat ini berfungsi untuk mengumpulkan data seperti jumlah IP yang diblokir, status jail, serta statistik serangan yang terdeteksi oleh Fail2ban.

Dashboard

Dashboard adalah representasi visual dari data yang digunakan untuk memantau keadaan atau mendukung pemahaman yang lebih baik. *Dashboard* juga merupakan representasi visual yang menampilkan informasi penting, yang dirancang untuk memudahkan pengguna dalam memantau data.

Grafana

Grafana adalah perangkat lunak *open source* untuk visualisasi dan analitik. Alat ini memungkinkan pengguna untuk memvisualisasikan, mengatur peringatan, dan menjelajahi metrik yang disimpan. Grafana berfungsi untuk mengubah data dari *database time-series* (TSDB) menjadi tampilan visual yang menarik.

Python

Python adalah bahasa pemrograman tingkat tinggi yang terkompilasi, sering digunakan untuk menangani basis data, big data, analisis data, dan kecerdasan buatan. Selain berfokus pada data dan perhitungan, Python juga dapat digunakan untuk pengembangan web server, Internet of Things (IoT), dan berbagai aplikasi lainnya.

Push Gateway

Push Gateway merupakan salah satu komponen dalam ekosistem Prometheus yang dirancang untuk mengatasi keterbatasan metode pengumpulan data berbasis pull. Secara *default*, Prometheus mengakses endpoint secara berkala untuk menarik data metrik. Namun, pendekatan ini kurang efektif untuk aplikasi yang bersifat sementara, seperti batch job atau skrip otomatis yang berjalan dalam waktu singkat. Pada situasi tersebut, aplikasi tidak memiliki cukup waktu untuk diekspos dan diakses oleh Prometheus. Untuk mengatasi kendala ini, Push Gateway memungkinkan aplikasi untuk mengirimkan (push) metrik mereka langsung ke gateway, yang kemudian akan menyimpannya agar bisa diambil oleh Prometheus pada waktu pengumpulan berikutnya.

3. METODE

Pada bagian ini berisi penjelasan tentang jenis penelitian/desain penelitian.

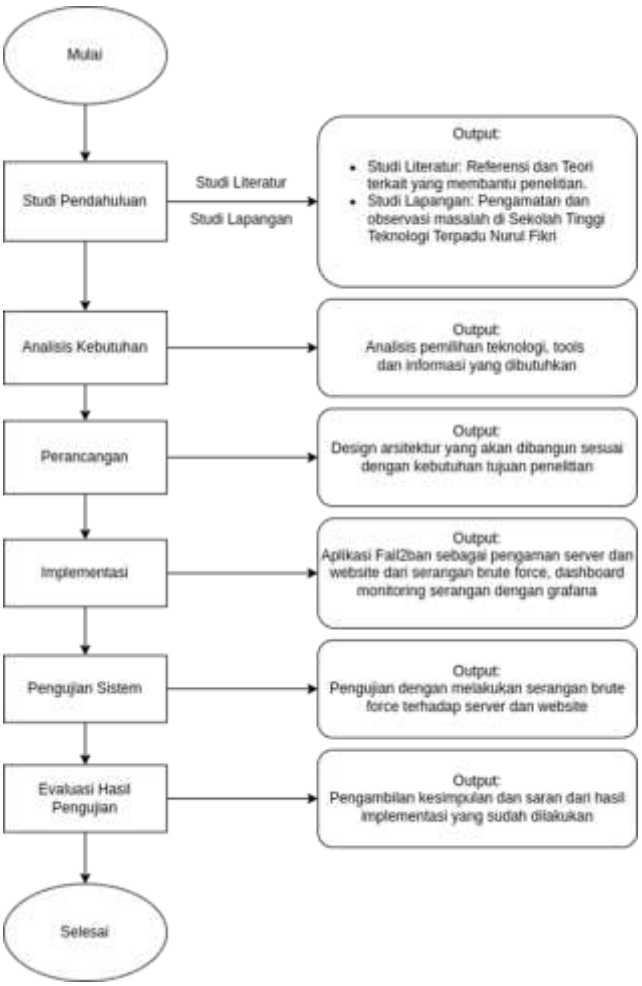
Metode pengumpulan data dan metode pengujian

Pada penelitian ini metode pengumpulan data yang digunakan adalah eksperimental. Peneliti melakukan simulasi serangan terhadap server untuk kemudian dilakukan pengamatan secara sistematis terhadap aktivitas server yang diserang, melalui log yang dihasilkan oleh

Fail2ban dan data metrik yang dikumpulkan oleh Prometheus. Eksperimen dilakukan terhadap interaksi antara komponen-komponen sistem keamanan untuk mendapatkan data kuantitatif tentang serangan yang berhasil diblokir dan keandalan sistem monitoring dalam menampilkan status serangan.

Pengujian adalah salah satu tahapan penting pada setiap penelitian. Dalam penelitian ini dilakukan dengan metode *Black Box Testing* dengan tujuan untuk memastikan implementasi sistem yang dilakukan dapat berjalan dengan baik. Pengujian dilakukan dengan mensimulasikan serangan brute force dan memantau reaksi Fail2ban. Pengujian dilakukan menggunakan software Nmap dan script Python untuk melakukan serangan brute force yang memungkinkan kita mengamati apakah Fail2ban dapat memblokir Alamat IP yang teridentifikasi melakukan serangan.

Metode penelitian



Gambar 1. Tahapan Penelitian

Gambar 1 memaparkan tahapan penelitian beserta hasil yang didapatkan pada setiap tahapan.

Studi Pendahuluan

Pada tahap ini, dilakukan pengumpulan informasi awal tentang topik penelitian, studi mendalam terhadap literatur terkait, serta pengamatan langsung di lapangan untuk memahami objek penelitian secara lebih mendalam.

Analisis Kebutuhan

Pada tahap ini, dilakukan analisis kebutuhan dengan diskusi bersama tim IT Sekolah Tinggi Teknologi Terpadu Nurul Fikri terkait kebutuhan, serta pengamatan langsung di lapangan untuk memahami objek proyek tugas akhir secara lebih mendalam. Setelah dilakukan analisis kebutuhan, maka didapati kebutuhan berupa Sistem pengamanan server terhadap serangan brute force yang dapat melakukan deteksi dan melakukan tindakan pencegahan secara otomatis. Dashboard monitoring yang dapat menampilkan status serangan yang terjadi agar kemudian administrator dapat mengetahui serangan secara dini.

Perancangan

Pada tahapan ini, penulis akan merancang Solusi pengamanan server dan website dari serangan brute force dan merancang dashboard monitoring untuk menampilkan serangan yang terjadi.

Implementasi

Tahapan implementasi melibatkan penerapan Solusi keamanan server dan website dari serangan brute force. Proses ini mencakup instalasi software, konfigurasi sistem, pengaturan aturan keamanan, dan integrasi dengan sistem monitoring.

Pengujian Sistem

Setelah dilakukan tahapan implementasi, selanjutnya dilakukan pengujian sistem untuk memastikan konfigurasi Fail2ban berfungsi dengan baik dalam melindungi *server* dan *website* dari serangan *brute force*. Pengujian ini mencakup pengecekan fungsionalitas, di mana Fail2ban harus dapat mendeteksi dan memblokir percobaan *login* yang gagal secara berulang. Pengujian dilakukan dengan simulasi serangan untuk memverifikasi bahwa kebijakan keamanan berjalan sesuai dengan yang diharapkan dan berhasil melindungi infrastruktur dari ancaman *brute force*. Pengujian terhadap fungsionalitas *dashboard* monitoring juga dilakukan guna memastikan data serangan ditampilkan dengan akurat.

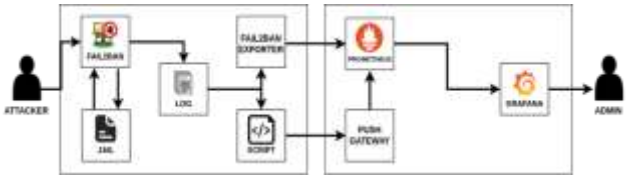
Evaluasi Hasil

Pada tahap ini, akan dilakukan penilaian terhadap keberhasilan penerapan Fail2ban dalam meningkatkan keamanan *server* dan *website*. Evaluasi ini mencakup analisis terhadap sejauh mana tujuan keamanan tercapai, identifikasi masalah yang muncul, dan perumusan rekomendasi untuk perbaikan di masa mendatang.

4. HASIL DAN PEMBAHASAN

Bagian ini hasil penelitian dan pembahasan penelitian menjelaskan tentang hasil implementasi sistem yang dirancang berdasarkan masalah dan tujuan penelitian yang telah dirumuskan.

Arsitektur Sistem



Gambar 2. Arsitektur Sistem

Tabel 1. Perangkat lunak yang digunakan

Perangkat Lunak	Versi	Fungsi
Fail2ban	v1.0.2	Bertindak sebagai *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS)
Prometheus	3.1.0	Mengumpulkan data metrik dari log Fail2ban.
Grafana	11.4.0	Menampilkan data metrik dengan visualisasi yang mudah dibaca.
Nmap	7.94SVN	Melakukan serangan brute force terhadap layanan SSH
Python	3.12.3	Melakukan serangan brute force terhadap halaman login Wordpress.

Gambar 2 menggambarkan rancangan arsitektur yang akan dilaksanakan pada penelitian ini, Fail2ban akan bertindak sebagai sistem pendeteksi serangan (*Intrusion Detection System*) dan sistem pencegahan terhadap serangan (*Intrusion Prevention System*). Kemudian Prometheus dan Grafana yang akan memvisualisasikan log serangan yang tejadi dalam bentuk *dashboard monitoring*. Tabel 1 Menunjukan perangkat lunak yang digunakan selama penelitian berlangsung.

Pengujian dan Hasil

Pengujian dilakukan dengan metode *blackbox testing* dengan tujuan untuk mengidentifikasi kelemahan sistem, memastikan bahwa hasil keluaran sesuai dengan data yang dimasukkan setelah dieksekusi, serta mencegah adanya kekurangan dan kesalahan dalam aplikasi sebelum digunakan oleh pengguna [20].

Pengujian brute force SSH dengan menggunakan Nmap dilakukan dengan melakukan sepuluh kali percobaan serangan dengan user list dan password list masing-masing sebanyak 10.000.

Tabel 2. Hasil Pengujian *Brute Force* Terhadap *Service* SSH

No	Total Percobaan Login	Jumlah Login Gagal Sebelum Pemblokiran
1	10.000	5
2	10.000	5
3	10.000	5
4	10.000	5
5	10.000	5
6	10.000	5
7	10.000	5
8	10.000	5
9	10.000	5
10	10.000	5

Gambar 3. Status *jail* ssh

Tabel 2 menunjukkan bahwa dari sepuluh kali pengujian yang dilakukan terhadap service SSH, Fail2Ban secara konsisten berhasil memblokir IP penyerang tepat setelah 5 kali percobaan login gagal, meskipun serangan mencoba hingga 10.000 kali. Gambar 3 menampilkan status serangan terhadap *service* SSH yang meliputi informasi *Currently failed, Total failed, Currently banned, Total banned, dan Banned IP list*.

Gambar 4. Dashboard monitoring status jail ssh

Tabel 3. Hasil pengujian tampilan *dashboard monitoring jaih* ssh

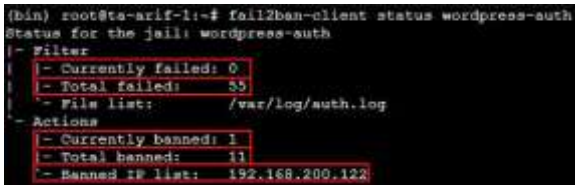
No	*Nama*	*Value Pada* **Fail2ban**	*Value Pada Grafana*
1	Current Failed	0	0
2	Total Failed	26	26
3	Current Banned	1	1
4	Total Banned	4	4
5	IP Banned	192.168.99.208	192.168.99.208
6	Max Retry	5	5
7	Find Time	10 Menit	10 Menit
8	Band Time	3 Menit	3 Menit

Gambar 4 menampilkan halaman *dashboard monitoring* status serangan terhadap *service* SSH yang meliputi informasi *Max retries*, *Find time*, *Band time*, *Currently failed*, *Total failed*, *Currently banned*, Total *banned*, dan *Banned IP list*. Tabel 3 Menunjukan bahwa nilai yang ada pada status Fail2ban untuk *service* sshd sama dengan nilai yang ditampilkan pada *dashboard* Grafana. Tabel 3 menunjukan bahwa nilai yang ada pada status Fail2ban untuk *service* sshd sama dengan nilai yang ditampilkan pada *dashboard* Grafana.

Pengujian *brute force* halaman *login* admin Wordpress dengan menggunakan *skrip* Python dilakukan dengan melakukan sepuluh kali percobaan serangan dengan *user list* dan *password list* masing-masing sebanyak 10.000.

Tabel 4. Hasil Pengujian *Brute Force* Terhadap Halaman *Admin* Wordpress

No	Total Percobaan Login	Jumlah Login Gagal Sebelum Pemblokiran
1	10.000	5
2	10.000	5
3	10.000	5
4	10.000	5
5	10.000	5
6	10.000	5
7	10.000	5
8	10.000	5
9	10.000	5
10	10.000	5



Gambar 5. Status *jail* Wordpress.

Tabel 4 menunjukkan bahwa dari sepuluh kali pengujian yang dilakukan terhadap halaman *admin* Wordpress, Fail2Ban secara konsisten berhasil memblokir *IP* penyerang tepat setelah 5 kali percobaan *login* gagal, meskipun serangan mencoba hingga 10.000 kali. Gambar 5 menampilkan status serangan terhadap halaman *login admin* Wordpress yang meliputi informasi *currently failed*, *total failed*, *currently banned*, total *banned*, *banned IP list*.

Gambar 6. *Dashboard monitoring* status *jail* Wordpress.

Gambar 6 menampilkan halaman *dashboard monitoring* status serangan terhadap halaman *login admin* Wordpress yang meliputi informasi *max retries*, *find time, band time, currently failed, total failed, currently banned, total banned,* dan *banned IP list*.

Tabel 5. Hasil pengujian tampilan *dashboard monitoring jail* Wordpress.

No	***Nama***	***Value Pada* Fail2ban**	***Value Pada Grafana***
1	Current Failed	0	0
2	Total Failed	55	55
3	Current Banned	1	1
4	Total Banned	11	11
5	IP Banned	192.168.200.122	192.168.200.122
6	Max Retry	5	5
7	Find Time	10 Menit	10 Menit
8	Band Time	3 Menit	3 Menit

Tabel 5. Menunjukan bahwa nilai yang ada pada status Fail2ban untuk layanan *Wordpress-auth* sama dengan nilai yang ditampilkan pada *dashboard* Grafana.

Evaluasi Hasil

Hasil efektivitas pengujian dari kedua skenario pengujian terhadap SSH dan halaman *login* WordPress dihitung dengan menggunakan rumus sebagai berikut

Pengukuran efektivitas = ((Total serangan – *login* gagal sebelum blokir) / Total percobaan) x 100%

= ((100.000 – 50) / 100.000) * 100%

= 99,95%

Seluruh data hasil aktivitas serangan berhasil ditampilkan di *dashboard* Grafana tanpa perbedaan nilai dengan sistem Fail2Ban. Informasi seperti *Total Failed, Current Banned, IP Banned,* dan parameter lainnya tersaji dengan konsisten.

Perbandingan

Penelitian sebelumnya dari Kris Andre Prasetyo, Mohammad Idhom, Henni Endah Wahanani, 2020, hanya melakukan implementasi pencegahan serangan *Brute Force* Pada *multiple server* dengan menggunakan Fail2ban. Sementara penelitian lain dari Farhannullah, Mardi Hardjianto, 2022, hanya melakukan implementasi pencegahan akses tidak sah melalui SSH.

Penelitian ini menambahkan aspek pemantauan melalui *dashboard* Grafana untuk memberikan visibilitas dan analisis yang lebih mendalam mengenai serangan yang terjadi. Selain itu, penelitian ini menambahkan implementasi pengamanan serangan *bruteforce* terhadap *website* berbasis Wordpress.

5. KESIMPULAN

Berdasarkan hasil pengujian terhadap dua skenario serangan *brute force*, yaitu melalui layanan SSH menggunakan Nmap dan halaman *login admin* WordPress menggunakan skrip Python, Fail2Ban terbukti efektif dalam mencegah serangan. Dalam setiap pengujian, dilakukan 10.000 percobaan *login*. Fail2Ban secara konsisten memblokir *IP* penyerang setelah mendeteksi 5 kali *login* gagal, sesuai dengan konfigurasi *maxretry*. Dari 10 kali pengujian pada ssh dan 10 kali pengujian pada *login admin* WordPress, hasilnya menunjukkan bahwa tidak ada upaya *brute force* yang berhasil melanjutkan serangan setelah melewati ambang batas kegagalan *login*. Hal ini menunjukkan bahwa Fail2Ban efektif dalam mencegah serangan *brute force* dengan tingkat keberhasilan pencegahan sebesar 99,95% baik terhadap serangan ke level sistem (SSH) maupun ke aplikasi *web* (WordPress).

Integrasi dilakukan dengan memanfaatkan Fail2ban *Exporter*, skrip Python, dan *Push Gateway* untuk mengekspos metrik sehingga dapat dibaca oleh Prometheus. Setelah data berhasil diambil oleh Prometheus kemudian data tersebut ditampilkan pada *dashboard* Grafana. Dengan integrasi tersebut seluruh data yang tercatat oleh Fail2Ban, seperti jumlah *login* gagal, IP yang diblokir, serta durasi pemblokiran, berhasil ditampilkan pada *dashboard* Grafana. Nilai-nilai tersebut tampil identik antara Fail2Ban dan Grafana, menandakan bahwa integrasi berjalan dengan baik. Hal ini memberikan kemudahan bagi administrator dalam melakukan pemantauan terhadap ancaman keamanan, serta mendukung proses analisis insiden dengan tampilan yang informatif dan terpusat.

REFERENSI

Azzahrah, B. T., Naufal, M., Hamdi, R., Raynee, R., & Layla, Z. (2024). Tantangan pertahanan dan keamanan data cyber dalam era digital: Studi kasus dan implementasi. *Jurnal Pendidikan Tambusai, 8*(2), 23934–23943.

Dawamsyach, F., Ruslianto, I., & Ristian, U. (2023). Implementation of IPS (Intrusion Prevention System) Fail2ban on server for DDoS and brute force attacks. *CESS (Journal of Computer Engineering and System Sciences), 8*(1), 149. https://doi.org/10.24114/cess.v8i1.40259

Dm, M. Y., & Lim, J. (2022). *Jurnal Pendidikan dan Konseling*, 4, 8018–8023.

Dwiyatno, S., Rachmat, E., Sari, A. P., & Gustiawan, O. (2020). Implementasi virtualisasi server berbasis Docker container. *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 7*(2), 165–175. https://doi.org/10.30656/prosisko.v7i2.2520

Febriyanti, N. M. D., Sudana, A., & ... (2021). Implementasi black box testing pada sistem informasi manajemen dosen. *Jurnal Teknologi Rekayasa Teknik Informatika*, *2*(3). https://doi.org/10.24843/JTRTI.2021.v02.i03.p12

Hartono, B. (2023). Ransomware: Memahami ancaman keamanan digital. *Bincang Sains dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Helmiawan, M. A., Akbar, Y. H., & Mahardika, F. (2024). *Keamanan teknologi informasi: Teori, risiko, dan strategi pertahanan di era digital*. https://ebook.lppmunsap.org/index.php/books/article/view/6/8

Holopainen, M. (2021). *Monitoring container environment with Prometheus and Grafana* (p. 50). https://www.theseus.fi/bitstream/handle/10024/497467/Holopainen_Matti.pdf

Horeb, A. (2023). Perancangan dashboard untuk memantau kinerja dosen Fakultas Teknologi Informasi di Universitas Tarumanagara. *Jurnal Ilmu Komputer dan Sistem Informasi*, *11*(1). https://doi.org/10.24912/jiksi.v11i1.24084

Kustyandi, A., & Noor, S. (2021). Sistem informasi monitoring serangan keamanan mail. *Jurnal Ilmiah*, 8(2), 42–54.

Prometheus. (n.d.). *Push gateway*. https://prometheus.io/docs/practices/pushing

Puriwigati, A. N., & Buana, U. M. (2020). Sistem informasi manajemen-keamanan informasi.

Rahman, D., Amnur, H., & Rahmayuni, I. (2020). Monitoring server dengan Prometheus dan Grafana serta notifikasi Telegram. *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, *1*(4), 133–138. https://doi.org/10.30630/jitsi.1.4.19

Rifandi, R. (2021). Raspberry dengan aplikasi Telegram berbasis Internet of Things. *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, *8*(1). https://doi.org/10.30656/prosisko.v8i1.3101

Siddiq, A., Yudiastuti, H., & Panjaitan, F. (2020). Analisis perilaku malware dengan metode surface analysis dan runtime analysis. *Jurnal Software Engineering Ampera*, *1*(3), 160–174. https://doi.org/10.51519/journalsea.v1i3.53

Sumayyah, Z. I., Permana, S. D. S., Tsabit, M., & Setiawan, A. (2024). Penerapan dan mitigasi teknik Slowloris dalam serangan distributed denial-of-service (DDoS) terhadap website ilegal dengan Kali Linux. *Jurnal Internet Software Engineering*, *1*(2), 14. https://doi.org/10.47134/pjise.v1i2.2694

Syaputera, A., Riska, R., & Mardiana, Y. (2023). Hotspot network security system from brute force attack using Pfsense external firewall (Case study of Wifi-Ku.Net Hotspot). *Jurnal Komputer, Informasi dan Teknologi*, *3*(1), 205–218. https://doi.org/10.53697/jkomitek.v3i1.1286

Taufan, P. (2022). Pengamanan jaringan komputer dengan intrusion prevention system (IPS) berbasis SMS Gateway. *Teknologipintar.org*, *2*(6), 1–13.