202010370311139
Irfan Rosyadi
Prodi Informatika

BAB II

TINJAUAN PUSTAKA

2.1 Studi Literatur

Studi literatur ini menganalisis sejumlah penelitian sebelumnya yang terdiri dari judul, latar belakang penelitian, metode yang digunakan, hasil penelitian dan saran pengembangan. Hasil dari studi literatur dapat dilihat dalam Tabel 2.1.

Tabel 2.1 Penelitian Terdahulu

No	Judul	Latar Belakang	Metode	Hasil	Saran Pengembangan
1	Sharing SSH Threat Intelligence across Multiple Servers using WebSocket and Fail2Ban	Fail2Ban umumnya per-server; attacker bisa pindah server jadi perlu berbagi IP terblokir antar node.	Integrasi Fail2Ban + WebSocket untuk broadcast IP terban real-time; uji multi-VPS & cek sinkronisasi via log.	IP yang diblokir tersebar ke semua node dalam hitungan detik sehingga pertahanan kolaboratif terhadap brute force SSH lebih cepat.	Perluas untuk endpoint login web dan skala lebih besar; tambah benchmark kuantitatif (latensi, risiko false sharing).
2	Penerapan Tools Fail2Ban Untuk Mencegah Serangan Brute	Login web e-learning rentan brute force dan berisiko ambil alih akun.	Implementasi Fail2Ban dan set batas gagal login + ban IP + bandingkan sebelum–sesudah.	Fail2ban mendeteksi percobaan brute force dan membloki	Tambahkan metrik kuantitatif (time-to-ban, jumlah percobaan diblok, false

	Force Pada Web Server Online Learning Uhamka			r IP penyerang; perbandingan sebelum–sesudah menunjukkan perlindungan meningkat terhadap percobaan login berulang.	positive) dan pengukuran performa; uji pada endpoint login berbeda.
3	Pencegahan dan Visualisasi Serangan Brute Force Menggunakan Fail2Ban, Prometheus, dan Grafana (Studi Kasus di STT Terpadu Nurul Fikri)	Brute force menyerang SSH & login web, perlu pertahanan otomatis + monitoring real-time.	Konfigurasi Fail2Ban (maxretry/findtime/bantime) + simulasi serangan + ekspor metrik ke Prometheus & visualisasi Grafana.	Fail2ban berhasil memblokir IP penyerang sesuai parameter; dashboard Grafana menampilkan jumlah IP diblokir, total login gagal, dan status ban aktif.	Fokus evaluasi pada endpoint login web; lakukan uji sensitivitas parameter; tambahkan pengukuran performa dan analisis false positive.
4	Implementation of IPS (Intrusion	Server menghadapi ancaman, butuh	Deploy Fail2ban sebagai IPS, konfigurasi rules/jail untuk	Fail2ban dapat memitigasi	Persempit evaluasi ke brute force web login;

	Prevention System) Fail2ban on Server for DDoS and Brute Force Attacks	mitigasi otomatis model IPS..	mendeteksi pola serangan dari log lalu menerapkan tindakan pemblokiran otomatis.	serangan yang terdeteksi dengan ban otomatis, menunjukkan perilaku IPS untuk perlindungan server.	laporkan metrik jelas (latensi ban, percobaan diblok) serta analisis false positive dan overhead server.
5	Analisis Keamanan Jaringan Server terhadap Serangan Dictionary Menggunakan Fail2Ban dengan Notifikasi Telegram	Banyak autentikasi gagal akibat serangan dictionary/brute force, admin butuh blocking + alert cepat.	Fail2Ban memantau log & ban IP + integrasi notifikasi Telegram ke admin.	Sistem memblokir IP penyerang dan mengirim notifikasi Telegram untuk meningkatkan kesiapsiagaan respons insiden.	Adaptasi filter untuk log login web, tambah dashboard/metrics dan evaluasi false positive serta overhead performa.
6	Analysis of Brute Force Attack Logs Toward NGINX Web Server on Dashboar	Web server sering jadi target brute force, butuh visibilitas serangan dari log.	Forensik log kuantitatif + centralized logging (Wazuh + ELK), parsing log jadi metadata & dashboard.	Dashboard menampilkan aktivitas brute force dan menyediakan ringkasan	Mengintegrasikan automated response dan mengevaluasi pencegahan end-to-end serta

	d (Improved Log Logging System Using Forensic Investigation Method) et and Fail2Ban			/kuantifikasi serangan sehingga memudahkan investigasi lanjutan berbasis metadata log.	overhead operasional
7	Comprehensive Analysis and Evaluation of Anomalous User Activity in Web Server Logs	Log web besar/ kompleks, anomali kecil bisa lolos kalau hanya rule-based.	Deteksi anomali dengan Isolation Forest, clustering dengan DBSCAN, validasi hasil melalui evaluasi pakar.	Framework mampu menemukan aktivitas outlier dari log Nginx dan mendukung keputusan keamanan yang lebih tepat berdasarkan pola anomali.	Gunakan output ML untuk memicu respons otomatis (mis. aturan Fail2ban/IPS) dan uji pada dataset brute force.
8	Implementation of Intrusion Prevention System (IPS) as a Website-Based Server	Perlu sistem keamanan server yang mudah dipantau/dikelola via web &	Pengembangan sistem monitoring/manajemen IPS berbasis web & mobile.	Menyediakan mekanisme pemantauan dan pengelolaan aktivitas	Integrasikan dengan mekanisme pencegahan spesifik (Fail2ban) dan evaluasi pada skenario

	Security System and Mobile Application	aplikasi mobile.		terkait IPS melalui web/mobile.	brute force login web dengan metrik terukur.
9	Pengujian dan Mitigasi Kerentanan Website Sistem Informasi Akademik Universitas Ma'arif Nahdlatul Ulama Kebumen dengan OWASP ZAP	Sistem Website perlu diuji celahnya dan diberi rekomendasi mitigasi.	Vulnerability assessment menggunakan OWASP ZAP untuk mengidentifikasi isu keamanan dan memberikan rekomendasi hardening.	Menghasilkan temuan kerentanan dan rekomendasi mitigasi berdasarkan hasil pemindaian.	Kombinasikan dengan kontrol brute force (Fail2ban/rate limiting /MFA) dan lakukan uji ulang untuk verifikasi perbaikan.
10	Analisis dan Implementasi Algoritma Bcrypt dengan Affine Cipher untuk Pengamanan Password pada Aplikasi Web	Password perlu diproteksi (hash/enkripsi) untuk mengurangi risiko penyalahgunaan saat data bocor.	Implementasi pengamanan password menggunakan Bcrypt (dan Affine Cipher sebagai mekanisme tambahan) pada konteks aplikasi web.	Meningkatkan keamanan penyimpanan password menggunakan pendekatan kriptografi sehingga menyulitkan pemulihan	Kombinasikan dengan kontrol serangan online (Fail2ban, rate limiting, MFA) dan evaluasi keamanan autentikasi end-to-end.

				password dari data tersimpan .	

2.2 Web Server

Web server merupakan komponen penting dalam layanan internet yang berfungsi menjalankan World Wide Web (WWW) melalui layanan HTTP/HTTPS [1]. Dalam prosesnya, web server menerima request dari pengguna lalu memprosesnya menjadi response berupa tampilan halaman web [1]. Perkembangan website saat ini membuat web server bukan lagi sekadar menampilkan teks, tetapi juga mendukung konten multimedia dan fitur interaktif [1]. Implementasi web server juga beragam, misalnya Apache dan Nginx yang banyak digunakan untuk kebutuhan layanan web modern [1]. Karena web server menangani lalu lintas akses pengguna dan menyimpan aktivitas pada log, aspek keamanan dan monitoring menjadi sangat relevan untuk memastikan ketersediaan layanan dan mengurangi risiko penyalahgunaan akses.

2.3 Keamanan Web Server

Seiring meningkatnya penggunaan website, potensi tindakan negatif seperti pembobolan sistem juga meningkat, sehingga upaya preventif perlu dilakukan oleh administrator untuk menjaga sistem tetap aman [1]. Salah satu pendekatan yang ditekankan dalam penelitian terkait adalah monitoring log sebagai metode administrator memantau kondisi sistem melalui catatan aktivitas yang tersimpan pada log server [1]. Namun, monitoring manual sering memakan waktu karena admin harus masuk ke server dan memeriksa log satu per satu [1]. Oleh karena itu, kebutuhan akan Centralized Log Management (CLM) muncul agar pemantauan dapat dilakukan terpusat dan lebih efektif untuk menunjang strategi pengamanan yang kuat [1]. Untuk membangun CLM, beberapa tool populer digunakan seperti ELK/EFK stack, walaupun dalam praktik tertentu pembuatan

visualisasi dan pemrosesan log masih dapat menuntut konfigurasi manual jika log masih mentah [1].

2.4 Brute Force Attack

Brute force merupakan teknik serangan yang dilakukan penyerang untuk memperoleh akses dengan mencoba berbagai kombinasi sampai ditemukan kombinasi yang benar. Dalam web server, brute force sering diarahkan ke halaman login dengan mencoba kombinasi username dan password secara berulang [1]. Paper analisis brute force pada Nginx menegaskan bahwa celah yang dimanfaatkan untuk memaksa masuk ke dalam sistem melalui percobaan kombinasi kredensial administrator [1]. Definisi brute force juga dijelaskan sebagai upaya menebak atau menelusuri semua kemungkinan password dengan karakter dan panjang tertentu sehingga kombinasi yang dicoba sangat banyak [2]. Variasi umum lainnya adalah dictionary attack, yaitu penyerang menggunakan daftar kata sandi (wordlist) untuk meningkatkan peluang keberhasilan, dan penelitian terkait menunjukkan bahwa program seperti Hydra dapat digunakan untuk melakukan serangan jenis ini [8]. Karena karakteristik brute force bersifat repetitif dan meninggalkan jejak pada log, pendekatan berbasis log monitoring dan IPS berbasis log menjadi opsi yang relevan untuk pencegahan[9].

2.5 Analisis Log

Penelitian analisis log brute force pada Nginx menunjukkan pendekatan deteksi berbasis pengumpulan log dari SSH dan Nginx, kemudian dilakukan pengolahan log oleh Wazuh untuk memproses log mentah menjadi informasi log yang lebih mudah dipahami sehingga ancaman brute force lebih mudah diidentifikasi [1]. Dalam arsitektur tersebut, Wazuh agent mengirim log ke Wazuh master, kemudian log diproses menggunakan rule bawaan sehingga menghasilkan metadata log yang dapat ditampilkan dalam dashboard [1]. Penelitian yang sama juga menjelaskan pemanfaatan komponen ELK, khususnya Elasticsearch dan Kibana, untuk membangun dashboard monitoring log pada server[1]. Selain untuk monitoring, analisis metadata log dalam paper

tersebut dapat digunakan untuk meninjau karakteristik serangan brute force yang terjadi dan memberi informasi mengenai kondisi keamanan server [1]. Sebagai perluasan perspektif, penelitian lain membahas pendekatan analitik pada log web server menggunakan teknik anomaly detection seperti Isolation Forest yang dikombinasikan dengan analisis statistik dan clustering untuk mengidentifikasi pola aktivitas pengguna yang menyimpang di data web server dengan skala besar [10]. Walaupun fokusnya bukan Fail2ban, studi ini menguatkan bahwa log web server sangat kaya informasi dan dapat dianalisis dengan berbagai pendekatan, dari rule-based sampai machine learning, tergantung tujuan keamanan yang ingin dicapai.

2.6 Fail2ban

Fail2ban merupakan aplikasi open-source yang dirancang untuk memantau log autentikasi dan melakukan pemblokiran IP ketika jumlah percobaan login gagal melewati batas jumlah tertentu [3]. Pada konfigurasi Fail2ban, terdapat parameter penting yaitu maxretry, findtime, dan bantime: maxretry menyatakan batas maksimal percobaan sampai IP diblokir; findtime adalah jangka waktu untuk mencapai maxretry; bantime adalah lama pemblokiran IP [2]. Contoh implementasi menunjukkan penggunaan maxretry=3, findtime=120 detik, bantime=600 detik pada skenario penelitian IPS fail2ban untuk serangan DDoS dan brute force [2]. Dalam praktik implementasi di server Linux, Fail2ban bekerja melalui konfigurasi serta menentukan logpath yang dimonitor [6]. Penelitian implementasi Fail2ban pada web server online learning juga menunjukkan pengaturan bantime, findtime, maxretry, dan banaction sebagai bagian penting dari pencegahan serangan [6]. Selain pemblokiran, Fail2ban dapat dikombinasikan dengan mekanisme pemberitahuan agar admin segera mengetahui adanya serangan, misalnya melalui Telegram yang digunakan untuk mengirim notifikasi hasil deteksi dan pemblokiran [8].

2.7 Evaluasi Fail2ban

Efektivitas Fail2ban dapat dinilai dari keberhasilannya memblokir upaya serangan sebelum terjadi login yang berhasil. Dalam penelitian yang menguji serangan pada SSH dan halaman login website, Fail2ban dikonfigurasi dengan maxretry 5, findtime 10 menit, dan bantime 3 menit, dan hasilnya menunjukkan IP penyerang berhasil diblokir sesuai parameter sehingga mencegah percobaan serangan lanjutan [3]. Penelitian yang sama juga menunjukkan integrasi Fail2ban dengan Prometheus dan Grafana untuk menampilkan metrik dalam dashboard secara realtime [3]. Pada bagian evaluasi, penelitian tersebut menghitung efektivitas pencegahan dan melaporkan tingkat keberhasilan pencegahan sebesar 99,95% pada skenario pengujian [3]. Di sisi lain, implementasi IPS Fail2ban untuk DDoS dan brute force menunjukkan bahwa perubahan parameter jail seperti maxretry dapat memengaruhi pola serangan yang tercatat, bila serangan tidak mencapai maxretry, maka sistem tidak melakukan ban dan tidak mencatat serangan [2]. Paper tersebut juga menyinggung dampak serangan dan penerapan sistem terhadap performa server, misalnya perbedaan dampak DDoS dan brute force pada sumber serta perbedaan kecepatan aksi ban/unban [2].