202010370311139
Irfan Rosyadi
Prodi Informatika

BAB I

PENDAHULUAN

1.1 Latar Belakang

Web server merupakan komponen penting dalam layanan internet karena melayani permintaan pengguna melalui HTTP/HTTPS dan menjadi fondasi bagi berbagai aplikasi digital, termasuk layanan akademik, e-learning, dan website institusi. Namun, keterhubungan server ke internet juga meningkatkan risiko keamanan. Penelitian pada Online Learning UHAMKA menunjukkan bahwa layanan akademik daring tidak terlepas dari ancaman brute force sehingga diperlukan mekanisme proteksi yang dapat diterapkan langsung pada server [1]. Penelitian lain yang mengimplementasikan IPS berbasis Fail2Ban juga menegaskan bahwa serangan dapat mengganggu kinerja server dan keamanan data di dalamnya [2], sedangkan penelitian analisis log brute force pada Nginx menunjukkan bahwa web server dan halaman administrator website merupakan target penting dalam serangan siber [6].

Salah satu ancaman yang sering muncul pada layanan autentikasi server adalah brute force attack, yaitu percobaan masuk dengan menebak banyak kombinasi username dan password sampai ditemukan pasangan yang benar. Serangan ini dapat diarahkan ke layanan SSH maupun ke halaman login website seperti WordPress [3], [6]. Selain itu, variasi seperti dictionary attack juga menjadi perhatian karena memanfaatkan wordlist dan alat otomatis untuk mencoba kombinasi kata sandi secara sistematis [8]. Penelitian pengamanan password berbasis bcrypt dan affine cipher juga menunjukkan bahwa brute force dan sniffing tetap menjadi ancaman nyata pada aplikasi web, sehingga proteksi login memerlukan lapisan keamanan tambahan [4].

Urgensi pengamanan server dan aplikasi web juga diperkuat oleh data serangan siber di Indonesia. Penelitian IPS berbasis website dan aplikasi mobile mencatat bahwa menurut laporan Honeynet Project BSSN, Indonesia memiliki

riwayat serangan siber sebesar 316,1 juta kali pada tahun 2020, meningkat dibandingkan 98,2 juta pada tahun 2019, dan port 80 termasuk salah satu port yang paling sering menjadi target serangan [9]. Penelitian implementasi IPS Fail2Ban pada server terhadap DDoS dan brute force juga menyebut bahwa port 22 dan port 80 termasuk port dengan jumlah serangan tinggi [2]. Sementara itu, penelitian pengujian keamanan website dengan OWASP ZAP menunjukkan bahwa aplikasi web di lingkungan pendidikan tinggi tetap rentan terhadap ancaman siber dan dapat mengalami insiden nyata seperti peretasan, sehingga pengujian dan mitigasi keamanan tetap diperlukan [7].

Berbagai penelitian telah menawarkan pendekatan untuk mengurangi risiko tersebut. Penelitian UHAMKA menunjukkan bahwa Fail2Ban dapat mendeteksi login attempts dan melakukan ban pada IP address penyerang melalui perbandingan sebelum dan sesudah penerapan [1]. Penelitian Nurul Fikri mengembangkan implementasi ini dengan menambahkan Prometheus dan Grafana sehingga administrator dapat memantau jumlah IP yang diblokir, total percobaan login gagal, dan status ban aktif secara real-time [3]. Penelitian lain memperluas kolaborasi keamanan dengan membagikan banned IP secara real-time antar server SSH menggunakan WebSocket dan Fail2Ban [5], sedangkan penelitian Wazuh berkontribusi pada sisi monitoring dan investigasi forensik melalui metadata log brute force [6]. Di luar pendekatan berbasis log seperti Fail2Ban, pengamanan login web juga dapat diperkuat dengan metode lain seperti CAPTCHA dan multi-factor authentication (MFA). CAPTCHA bekerja dengan menambahkan tantangan verifikasi untuk membatasi percobaan otomatis oleh bot, sedangkan MFA menambahkan lapisan autentikasi tambahan setelah username dan password sehingga akses tidak hanya bergantung pada satu faktor kredensial. Berbeda dengan kedua metode tersebut, Fail2Ban bekerja pada sisi server dengan memantau log autentikasi dan memblokir IP yang menunjukkan pola percobaan login berulang. Dengan demikian, CAPTCHA lebih berfokus pada pembatasan interaksi otomatis, MFA berfokus pada penguatan autentikasi, sedangkan Fail2Ban berfokus pada deteksi pola serangan dan respon otomatis berbasis log. Meskipun demikian, masih terdapat

ruang pengembangan untuk penelitian yang secara khusus memfokuskan implementasi dan evaluasi Fail2Ban pada form login WordPress di lingkungan server Linux virtual, dengan pengujian sebelum–sesudah, variasi parameter, evaluasi false positive, dan pengamatan dampaknya terhadap kualitas layanan login.

1.2 Rumusan Masalah

1. Seberapa efektif Fail2ban mencegah brute force pada form login web?
2. Bagaimana dampak penerapan fail2ban terhadap kinerja server?

1.3 Tujuan Penelitian

1. Mengukur efektivitas deteksi dan pemblokiran Fail2ban pada skenario brute force web login.
2. Melakukan evaluasi dampak penerapan Fail2ban terhadap performa server dan kualitas layanan.

1.4 Batasan Masalah

1. Serangan yang diuji terbatas pada brute force web login aplikasi WordPress.
2. Implementasi Fail2ban dilakukan pada server linux.
3. Tidak membahas malware, privilege escalation, maupun DDoS skala besar.
4. Pengujian dilakukan di lingkungan server virtual.