ABSTRAK

ADAPTIVE SECURE SHELL DEFENSE AGENTS (ASDA) UNTUK MITIGASI SERANGAN *BRUTE FORCE*

(2025:xv + 60 halaman + 10 gambar + 6 tabel + 12 lampiran)

ARISTO TELY

062140352351

JURUSAN TEKNIK ELEKTRO

PROGRAM STUDI SARJANA TERAPAN TEKNIK TELEKOMUNIKASI

POLITEKNIK NEGERI SRIWIJAYA

Serangan *brute force* terhadap layanan *Secure Shell* (SSH) merupakan salah satu bentuk ancaman siber yang paling umum menyerang *server cloud*. Fail2Ban telah banyak digunakan untuk mendeteksi dan memblokir alamat IP yang mencoba *login* secara berulang, namun mekanismenya bersifat lokal dan tidak mampu menyebarkan informasi pemblokiran ke *server* lain. Penelitian ini mengembangkan *Adaptive Secure Shell Defense Agents* (ASDA), yaitu sistem pertahanan adaptif yang terdistribusi dan mampu membagikan informasi IP berbahaya secara *real-time* ke seluruh *node* melalui protokol WebSocket. Sistem terdiri dari tiga agen *client* yang berjalan di *server cloud* berbeda dan satu *server* pusat sebagai perantara komunikasi. Setiap *client* melakukan deteksi *brute force* menggunakan Fail2Ban, lalu mengirimkan data IP dalam format JSON ke *server* WebSocket untuk didistribusikan ke seluruh *client* lain. Pengujian dilakukan selama sembilan hari dengan memanfaatkan lalu lintas serangan asli dari internet tanpa simulasi internal. Hasilnya menunjukkan sebanyak 5.260 IP berhasil terdeteksi dan 5.247 di antaranya (99,75%) dipropagasikan secara sukses antar *node*, dengan waktu rata-rata propagasi hanya 126 milidetik. ASDA terbukti mampu meningkatkan skala dan efisiensi mitigasi serangan *brute force* SSH dalam lingkungan *cloud* terdistribusi secara nyata, ringan, dan tanpa ketergantungan *orchestrator*.

Kata kunci: SSH, *brute force*, Fail2Ban, WebSocket, pertahanan adaptif, sistem terdistribusi.

ABSTRACT

ADAPTIVE SECURE SHELL DEFENSE AGENTS (ASDA) *FOR BRUTE FORCE ATTACK MITIGATION*

(2025:xv + 60 *pages* + 10 *pictures* + 6 *tables* + 12 *attachments*)

ARISTO TELY

062140352351

ELECTRICAL ENGINEERING DEPARTMENT

STUDY PROGRAM BACHELOR OF APPLIED TELECOMMUNICATION ENGINEERING

STATE POLYTECHNIC OF SRIWIJAYA

One of the most common security risks aimed at cloud-based infrastructure is brute force attacks on Secure Shell (SSH) services. Although Fail2Ban is frequently used to identify and block IP addresses that make repeated login attempts, it is intrinsically limited to local mitigation. It cannot spread blocking actions across dispersed servers. This study presents the Adaptive Secure Shell Defense Agents (ASDA), a compact and practical defense framework that leverages distributed cooperation to enhance SSH brute force protection. ASDA uses WebSocket as a real-time, bidirectional communication channel between nodes and incorporates Fail2Ban as a local detection engine. The system comprises three client agents and one central WebSocket server acting as a policy broker. When a brute force attempt is detected, the client sends structured JSON data containing the offending IP to the server, which rebroadcasts it to all other clients for immediate blocking. The system was deployed on real cloud infrastructure and tested over nine days under authentic internet-based attack conditions. Results show that out of 5,260 detected IP addresses, 5,247 (99.75%) were successfully propagated and blocked within an average delay of 126 milliseconds. These findings demonstrate that ASDA effectively enhances SSH defense across cloud nodes without relying on orchestration tools.

Keywords: SSH, *brute force*, Fail2Ban, WebSocket, *adaptive defense*, *distributed system.*