RANCANG BANGUN SISTEM KEAMANAN LAPIS GANDA UNTUK OTOMATISASI PEMBLOKIRAN IP PENYERANG BERBASIS
FAIL2BAN DAN API MIKROTIK PADA REVERSE PROXY NGINX DI LINGKUNGAN VIRTUALISASI PROXMOX PT GLOBAL
INTERMEDIA NUSANTARA
Munif Adam Ashidiqi, Ir. Muhammad Arrofiq, S.T., M.T., Ph.D., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

RANCANG BANGUN SISTEM KEAMANAN LAPIS GANDA UNTUK OTOMATISASI PEMBLOKIRAN IP PENYERANG BERBASIS FAIL2BAN DAN API MIKROTIK PADA REVERSE PROXY NGINX DI LINGKUNGAN VIRTUALISASI PROXMOX PT GLOBAL INTERMEDIA NUSANTARA

Munif Adam Ashidiqi

22/494463/SV/20833

Penelitian ini bertujuan merancang dan mengimplementasikan sistem keamanan berlapis pada lingkungan virtual Proxmox dengan mengintegrasikan Nginx sebagai titik observasi *log*, Fail2ban sebagai mekanisme deteksi serangan berbasis *log*, dan Mikrotik API sebagai eksekutor pemblokiran IP pada tingkat jaringan. Pengujian sistem dilakukan melalui simulasi empat skenario serangan, yaitu *scanning*, *brute force*, *Denial of Service (DoS)*, dan *SQL Injection*, yang masing-masing diuji sebanyak 10 kali sehingga total pengujian berjumlah 40 percobaan. Evaluasi kinerja sistem dilakukan berdasarkan waktu respon pemblokiran, rata-rata waktu respon, persentase keberhasilan deteksi serangan, serta persentase pemblokiran IP secara *real-time* dengan ambang batas waktu respon ≤ 2 detik. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi seluruh skenario serangan dengan tingkat keberhasilan deteksi sebesar 100% serta melakukan pemblokiran IP secara *real-time* pada tingkat jaringan dengan persentase pemblokiran *real-time* sebesar 95%. Dengan demikian, sistem keamanan berlapis yang dirancang terbukti mampu bekerja secara efektif dan responsif dalam mendeteksi serta merespons aktivitas mencurigakan secara otomatis.

Kata kunci: keamanan jaringan, Fail2ban, Mikrotik API, Nginx, Proxmox, pemblokiran IP otomatis.

RANCANG BANGUN SISTEM KEAMANAN LAPIS GANDA UNTUK OTOMATISASI PEMBLOKIRAN IP PENYERANG BERBASIS
FAIL2BAN DAN API MIKROTIK PADA REVERSE PROXY NGINX DI LINGKUNGAN VIRTUALISASI PROXMOX PT GLOBAL
INTERMEDIA NUSANTARA
Munif Adam Ashidiqi, Ir. Muhammad Arrofiq, S.T., M.T., Ph.D., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

DESIGN AND IMPLEMENTATION OF A MULTI-LAYER SECURITY SYSTEM FOR AUTOMATED BLOCKING OF ATTACKER IP BASED ON FAIL2BAN AND MIKROTIK API ON AN NGINX REVERSE PROXY IN A PROXMOX VIRTUALIZATION ENVIRONMENT AT PT GLOBAL INTERMEDIA NUSANTARA

Munif Adam Ashidiqi

22/494463/SV/20833

This research aims to design and implement a multi-layer security system in a Proxmox virtual environment by integrating Nginx as a log observation point, Fail2ban as a log-based attack detection mechanism, and the Mikrotik API as an executor for IP blocking at the network level. System testing was conducted through simulations of four attack scenarios, namely scanning, brute force, Denial of Service (DoS), and SQL Injection, each tested 10 times, resulting in a total of 40 experimental trials. The system performance was evaluated based on blocking response time, average response time, attack detection success rate, and the percentage of real-time IP blocking with a response time threshold of ≤ 2 seconds. The test results indicate that the system successfully detected all attack scenarios with a detection success rate of 100% and performed real-time IP blocking at the network level with a real-time blocking rate of 95%. Therefore, the proposed multi-layer security system has proven to be effective and responsive in automatically detecting and responding to suspicious activities.

Keyword: *network security, Fail2ban, Mikrotik API, Nginx, Proxmox, automated IP blocking.*