ABSTRAK

DAVE TRAVIS. Analisis Keamanan Jaringan Berbasis MikroTik Dengan Metode *Port Knocking* dan *Auto-Blocking*. Dibimbing oleh FERDI CHAHYADI dan RIFALDI HERIKSON.

Keamanan layanan manajemen router MikroTik kategori *low-cost* menjadi perhatian serius mengingat lebih dari empat juta perangkat terpapar di internet dengan mayoritas masih menggunakan konfigurasi *default* yang rentan. Penelitian ini merancang, mengimplementasikan, dan mengevaluasi arsitektur pertahanan berlapis berbasis port knocking pada router MikroTik hAP lite (RB941-2nD-TC) yang menangani empat vektor ancaman secara simultan: serangan *brute force*, *reconnaissance* dan *sniffing*, penyalahgunaan *knock sequence*, serta pemalsuan identitas jaringan (IP *spoofing*). Arsitektur mencakup MAC *whitelist* pada RAW *table*, *static* ARP *reply-only*, *bogon address-list*, *cross-subnet ingress filter*, mekanisme port knocking dua tahap (7000→8000), deteksi penyalahgunaan berbasis *cascade* tiga tahap, *brute-force-detector* berbasis *scripting* RouterOS, dan notifikasi *real-time* via Bot Telegram. Pengujian menggunakan metode *penetration testing* berbasis NIST SP 800-115 dalam kerangka *Design Science Research* (DSR) dengan matriks dua belas kondisi yang mengombinasikan dua sistem operasi, tiga sumber jaringan, dan dua fase implementasi, dilakukan pada auto-blocking saja, port knocking saja, dan metode gabungan keduanya secara terpisah. Hasil menunjukkan arsitektur secara konsisten mengubah status port dari *open* menjadi *filtered*, memblokir *brute force* dalam rata-rata kurang dari 10 detik, mendeteksi penyalahgunaan *knock sequence* secara efektif, serta mencegah akses melalui *spoofing* pada seluruh sumber yang dapat diuji, dengan keandalan notifikasi Telegram mencapai R = 1,0. Perbandingan ketiga metode mengonfirmasi bahwa auto-blocking dan port knocking saling melengkapi pada lapisan pertahanan yang berbeda, dan metode gabungan terbukti paling unggul dengan menutup seluruh celah struktural yang teridentifikasi pada kedua metode tunggal tanpa peningkatan beban komputasi pada perangkat.

Kata kunci: port knocking, MikroTik, keamanan jaringan, *brute force*, *sniffing*, *IP spoofing*, RouterOS, NIST SP 800-115, *Design Science Research*, VPS *transparent relay*

ABSTRACT

DAVE TRAVIS. MikroTik-Based Network Security Analysis Using Port Knocking and Auto-Blocking Methods. Supervised by FERDI CHAHYADI dan RIFALDI HERIKSON.

The security of management services on low-cost MikroTik routers has become a critical concern, as more than four million devices are exposed to the internet while still operating under vulnerable default configurations. This study designs, implements, and evaluates a layered defense architecture based on port knocking on a MikroTik hAP lite router (RB941-2nD-TC), addressing four simultaneous attack vectors: brute force attacks, reconnaissance and sniffing, knock sequence abuse, and network identity spoofing (IP spoofing). The architecture encompasses MAC whitelisting in the RAW table, static ARP reply-only, bogon address-list, cross-subnet ingress filtering, a two-stage port knocking mechanism (7000→8000), three-stage cascade-based knock sequence abuse detection, a RouterOS scripting-based brute-force-detector, and real-time Telegram Bot notifications. Testing was conducted using a NIST SP 800-115 penetration testing methodology within a Design Science Research (DSR) framework, employing a twelve-condition matrix combining two attacker operating systems, three network sources, and two implementation phases, applied separately to auto-blocking alone, port knocking alone, and the combined method. Results demonstrate that the architecture consistently changed management port status from open to filtered, blocked brute force attempts within an average of under 10 seconds, effectively detected knock sequence abuse, and prevented re-entry via spoofing across all end-to-end testable sources, with Telegram notification reliability achieving R = 1.0. Comparison across the three methods confirms that auto-blocking and port knocking complement each other by addressing distinct layers of defense, with the combined method proving superior by closing all structural gaps identified in each standalone approach without increasing the router's computational load.

Keywords: port knocking, MikroTik, network security, brute force, sniffing, IP spoofing, RouterOS, NIST SP 800-115, Design Science Research, VPS transparent relay