OTOMATISASI KONFIGURASI PORT BLOCKING DAN PORT KNOCKING PADA PERANGKAT ROUTER MIKROTIK MENGGUNAKAN ANSIBLE

Oleh

Andika Kurniawan Sianipar, NIM 2215101011

Program Studi Ilmu Komputer

Jurusan Teknik Informatika

ABSTRAK

Router MikroTik rentan terhadap serangan brute force pada layanan FTP dan SSH, terutama ketika konfigurasi keamanan masih dilakukan secara manual serta menggunakan pola Port Knocking statis. Penelitian ini bertujuan mengembangkan sistem otomatisasi Port Blocking dan Port Knocking dinamis menggunakan Ansible berbasis event-driven untuk meningkatkan keamanan akses perangkat router MikroTik. Penelitian menggunakan metode eksperimen dengan tahapan NDLC yang meliputi analysis, design, dan simulation prototyping. Pengujian dilakukan pada lingkungan simulasi GNS3 dengan menggunakan MikroTik CHR, Ansible Rulebook, Ansible Playbook, webhook, dan script MikroTik. Hasil pengujian menunjukkan bahwa sistem berhasil mendeteksi aktivitas brute force, mengirim event ke Ansible Controller, memasukkan IP penyerang ke blacklist, serta merotasi urutan Port Knocking secara otomatis. Interval scheduler 10 detik menjadi konfigurasi paling seimbang pada pengujian ketahanan. Selain itu, konfigurasi otomatis membutuhkan rata-rata 5,12 detik dibandingkan konfigurasi manual 154,79 detik, sehingga pada skenario pengujian efisiensi penelitian ini diperoleh efisiensi waktu sebesar 96,69%. Berdasarkan hasil pengujian, sistem yang dikembangkan mampu meningkatkan keamanan serta mempercepat proses konfigurasi pada router MikroTik.

Kata-kata kunci: MikroTik, Ansible, Port Blocking, Port Knocking Dinamis, Event-Driven Automation.

AUTOMATION OF PORT BLOCKING AND PORT KNOCKING CONFIGURATION ON MIKROTIK ROUTER DEVICES USING ANSIBLE

By

Andika Kurniawan Sianipar, NIM 2215101011

Computer Science Study Program

Department of Informatics Engineering

ABSTRACT

MikroTik routers are vulnerable to brute force attacks on FTP and SSH services, particularly when security configurations are still performed manually and static Port Knocking patterns are employed. This research aims to develop an automated system for Port Blocking and dynamic Port Knocking using event-driven Ansible to enhance the security of MikroTik router access. The research employs an experimental method with stages of the Network Development Life Cycle (NDLC), comprising analysis, design, and simulation prototyping. Testing was conducted in a GNS3 simulation environment utilizing MikroTik CHR, Ansible Rulebook, Ansible Playbook, webhooks, and MikroTik scripts. The test results indicate that the system successfully detects brute force activity, sends events to the Ansible Controller, adds the attacker's IP address to the blacklist, and automatically rotates the Port Knocking sequence. A 10-second scheduler interval was found to be the most balanced configuration in the resilience testing. Furthermore, automated configuration required an average of 5.12 seconds compared to 154.79 seconds for manual configuration, resulting in a time efficiency of 96.69% in the efficiency testing scenario. Based on the test results, the developed system is able to enhance security and accelerate the configuration process on MikroTik routers.

Keyword: MikroTik, Ansible, Port Blocking, Dynamic Port Knocking, Event-Driven Automation.