Abstrak

Keamanan sistem jaringan menjadi aspek kritis dalam menghadapi ancaman siber yang semakin kompleks. Salah satu layanan yang rentan terhadap serangan adalah Secure Shell (SSH), yang sering menjadi target serangan brute force untuk mendapatkan akses yang tidak sah. Dalam skripsi ini, kami memfokuskan pada penggunaan Intrusion Prevention System (IPS) untuk meningkatkan keamanan SSH pada perangkat MikroTik. Metode penelitian ini melibatkan uji coba langsung terhadap sistem dengan mengimplementasikan IPS pada perangkat MikroTik dan melakukan serangkaian serangan brute force terhadap layanan SSH. Kami memantau dan menganalisis kemampuan IPS dalam mendeteksi dan merespons serangan dengan cepat serta efektif. Pengujian dilakukan dengan variasi konfigurasi IPS untuk menentukan setup yang paling optimal dalam melindungi layanan SSH.Hasil penelitian menunjukkan bahwa penggunaan IPS pada MikroTik dapat secara signifikan mengurangi risiko serangan brute force terhadap layanan SSH. IPS berhasil mendeteksi pola serangan dengan akurasi yang tinggi dan merespons dengan cepat dengan mengambil tindakan pencegahan yang sesuai, seperti pemblokiran alamat IP yang mencurigakan. Dengan optimalisasi konfigurasi IPS, kami mencapai tingkat keamanan yang lebih tinggi tanpa mengorbankan ketersediaan layanan.Temuan ini menunjukkan bahwa penggunaan IPS pada perangkat MikroTik adalah langkah yang efektif dalam meningkatkan keamanan sistem jaringan, khususnya dalam melindungi layanan SSH dari serangan brute force. Skripsi ini memberikan kontribusi penting dalam pemahaman dan penerapan solusi keamanan yang dapat diimplementasikan oleh organisasi untuk melindungi infrastruktur jaringan mereka dari ancaman siber yang semakin berkembang.

Kata kunci: Sistem Keamanan, SSH, *Brute Force*, *Intrusion Prevention System*.

Abstract

Network system security is a critical aspect in facing increasingly complex cyber threats. One service that is vulnerable to attack is Secure Shell (SSH), which is often the target of brute force attacks to gain unauthorized access. In this thesis, we focus on the use of the Intrusion Prevention System (IPS) to improve SSH security on MikroTik devices. This research method involves directly testing the system by implementing IPS on a MikroTik device and carrying out a series of brute force attacks against the SSH service. We monitor and analyze IPS's ability to detect and respond to attacks quickly and effectively. Testing was carried out with various IPS configurations to determine the most optimal setup for protecting SSH services. The research results show that the use of IPS on MikroTik can significantly reduce the risk of brute force attacks against SSH services. IPS successfully detects attack patterns with high accuracy and responds quickly by taking appropriate countermeasures, such as blocking suspicious IP addresses. By optimizing the IPS configuration, we achieve a higher level of security without sacrificing service availability. These findings show that the use of IPS on MikroTik devices is an effective step in increasing network system security, especially in protecting SSH services from brute force attacks. This thesis makes an important contribution to the understanding and application of security solutions that can be implemented by organizations to protect their network infrastructure from growing cyber threats.

***Keywords**: Security System, SSH, Brute Force, Intrusion Prevention System*