ABSTRAK

Serangan brute-force adalah serangan siber yang sering menargetkan protokol SSH dan RDP. Serangan ini dapat menyebabkan kerugian yang signifikan bagi organisasi. Salah satu solusi untuk mendeteksi serangan brute-force adalah dengan menggunakan Security Information and Event Management (SIEM). SIEM dapat memantau aktivitas login dan mengidentifikasi pola yang mencurigakan. Penelitian ini menggunakan Wazuh, salah satu platform SIEM open-source yang populer, untuk mendeteksi serangan brute-force yang menargetkan protokol SSH dan RDP. Hasil penelitian menunjukkan bahwa Wazuh dapat mendeteksi serangan brute-force dengan baik. Wazuh dapat memblokir alamat IP yang mencoba login dengan kata sandi yang salah berulang kali. Penelitian ini memberikan informasi yang bermanfaat bagi organisasi dalam upaya meningkatkan keamanannya dari serangan brute-force. Organisasi dapat menggunakan SIEM, seperti Wazuh, untuk mendeteksi serangan brute-force dan memberikan respons yang cepat dan tepat.

Kata Kunci: Serangan brute-force, SIEM, Wazuh, SSH, RDP

ABSTRACT

Brute-force attacks are a common type of cyber attack that target SSH and RDP protocols. These attacks can cause significant damage to organizations. One solution for detecting brute-force attacks is to use Security Information and Event Management (SIEM). SIEM can monitor login activity and identify suspicious patterns. This study uses Wazuh, a popular open-source SIEM platform, to detect brute-force attacks targeting SSH and RDP protocols. The results of the study show that Wazuh can detect brute-force attacks effectively. Wazuh can block IP addresses that attempt to log in with the wrong password repeatedly. This study provides valuable information for organizations in their efforts to improve their security against brute-force attacks. Organizations can use SIEM, such as Wazuh, to detect brute-force attacks and provide a timely response.

Keyword: Brute-force attack, SIEM, Wazuh, SSH, RDP