ABSTRAK

Badan Siber dan Sandi Negara Republik Indonesia (BSSN RI) melakukan publikasi terkait Lanskap Keamanan Siber Indonesia 2022 pada awal tahun 2023. Laporan tersebut melaporkan hasil monitoring, anomali trafik, dugaan insiden siber, dan ancaman siber kedepannya. Terdapat ancaman siber yang diprediksi oleh BSSN RI akan muncul di tahun 2023 salah satunya brute-force terhadap Remote Desktop Protocol (RDP). Indonesia termasuk dalam negara dengan kasus tertinggi terhadap brute-force.

Untuk itu, sistem deteksi dibangun dengan Intrusion Detection System (IDS) yang terimplementasi pada virtual Machine menggunakan Wazuh. Simulasi dan implementasi dilakukan mulai dari tahap installation, implementation, sampai dengan melakukan analisis terhadap hasil deteksi IDS. Kemudian, penetration testing dilakukan untuk melakukan simulasi SSH brute-force terhadap virtual Machine yang terpasang Wazuh menggunakan hydra tool tool. Wazuh tersebut dipasang untuk mendeteksi penetration testing yang dijalankan tersebut. Setelah itu, hasil penetration testing yang dilakukan dideteksi oleh Wazuh dalam bentuk log. Log tersebut dianalisis dengan melakukan perbandingan antara log yang dideteksi Wazuh secara default dengan log yang dideteksi Wazuh setelah implementasi rule.

Hasil deteksi menghasilkan perbandingan. Simulasi hydra tool yang pertama kali dijalankan, dideteksi oleh Wazuh dengan jumlah 4000 hits. Setelah implementasi rule dengan active response, hasil deteksi Wazuh terhadap penetration testing kedua kali dideteksi oleh Wazuh dengan 1777 hits. Dengan demikian, terdapat penurunan jumlah hits sekitar 58% yang menunjukkan bahwa rule active response dapat meningkatkan kapabilitas Wazuh dalam mendeteksi hydra tool dalam simulasi SSH brute-force.

Kata Kunci: *active response, brute-force, hydra tool tools, Intusion Detection System, Wazuh.*