ABSTRACT

Badan Siber dan Sandi Negara Republik Indonesia (BSSN RI) publicated Lanskap Keamanan Siber Indonesia 2022 on 2023. The report showed monitoring results, anomaly traffic, alleged cyber incident, and cyber threat prediction in the future. Remote Desktop Protocol (RDP) brute-force was one of cyber threat will occur on 2023 predicted by BSSN RI. Indonesia was included one of countries with the highest brute-force case.

To deal with the cases, detection system is implemented with Wazuh on virtual Machine. Simulation and implementation is carried out and started from installation, implementation, until IDS detection results analyzing. Then, penetration testing is carried out to run SSH brute-force simulation to Wazuh implemented virtual Machine with hydra tool tool. Wazuh is installed to detect the penetration testing. Then, penetration testing result is detected by Wazuh in log format. The log is analyzed with determining the detected log by Wazuh with default rule to the log is detected by Wazuh implemented rule.

Detection results has the comparison. The first simulated hydra tool tools, detected by Wazuh with 4000 hits. After rule implementation with active response, detection result from penetration testing simulation is detected by Wazuh with 1777 hits. Thus, reduction of hits total achieved 58% that showed the active response rule can increase Wazuh detection capabilities of hydra tool with SSH brute-force simulation.

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