ABSTRACT

The development of increasingly advanced technology can lead to crimes such as data theft, data destruction, and system and network damage. These issues require in-depth defense systems to maintain data integrity and systems to keep data in perfect condition. From the results of system analysis using the Quality of Service (QOS) method, SNORT IDPS which is integrated with honeypot cowrie can increase throughput quality in scenario 1 for ICMP flooding attack 42834 bit/s after scenario 2 produces 63741 bit/s, for UDP flooding attack scenario 1 produces 26567 bit/s after scenario 2 produces 29060 bit/s and for MITM attack in scenario 1 produces 428 34 bit/s after scenario 2 results in 63741 bit/s . Delay, in scenario 1 for ICMP flooding attack 24.07ms after scenario 2 produced 22.88 ms, for UDP flooding attack scenario 1 produced 24.47 ms after scenario 2 generated 15.49 and for MITM attack in scenario 1 produced 22.23 ms after scenario 2 generated 21.09 ms. jitter in scenario 1 for ICMP flooding attack 12.59 ms after scenario 2 generated 11.55 ms, for UDP flooding attack scenario 1 produces 5.8 ms after scenario 2 generates 3.7 and for MITM attack in scenario 1 produces 12.5 ms after scenario 2 generates 11.5 ms. and packet loss in scenario 1 for ICMP flooding attack is 0.29% after scenario 2 is generated 0.19% ms, for UDP flooding attack scenario 1 is generated 0.65% after scenario 2 is generated 0.34% and for MITM attack in scenario 1 is generated 0.42 % after scenario 2 is generated 0.35%.

Keywords: *SNORT, Cowrie Honeypot, Distributed Denial Of Service (DDoS) dan Man in the Middle (MITM) throghput,delay,jitter and packet loss*