# ABSTRAK

Perkembangan teknologi yang semakin maju dapat menimbulkan kejahatan misalnya pencurian data, perusakan data, dan kerusakan sistem dan jaringan.Masalah-masalah ini memerlukan sistem pertahanan yang mendalam untuk menjaga integritas data dan sistem untuk menjaga data dalam kondisi sempurna. Dari hasil analisis sistem menggunakan metode*Qualyty of Service* (QOS) ini SNORT IDPS yang diintergrasikan dengan *honeypotcowrie* dapat meningkatkan kulitas nilai *throghput* pada skenario 1 untuk serangan ICMP *flooding* 42834 bit/s setelah dilakukan skenario 2 dihasilkan 63741 bit/s, untuk serangan UDP *flooding* skenario 1 menghasilkan 26567 bit/s setelah dilakukan skenario ke 2 dihasilkan 29060 bit/s dan untuk serangan MITM pada skenario 1 menghasilkan 42834 bit/s setelah skenario 2 dihasilkan 63741 bit/s . D*elay*, pada skenario 1 untuk serangan ICMP *flooding* 24,07ms setelah dilakukan skenario 2 dihasilkan 22,88 ms, untuk serangan UDP *flooding* skenario 1 menghasilkan 24,47 ms setelah dilakukan skenario ke 2 dihasilkan 15,49 dan untuk serangan MITM pada skenario 1 menghasilkan 22,23 ms setelah skenario 2 dihasilkan 21,09 ms.*jitter* pada skenario 1 untuk serangan ICMP *flooding* 12.59 ms setelah dilakukan skenario 2 dihasilkan 11.55 ms, untuk serangan UDP *flooding* skenario 1 menghasilkan 5.8 ms setelah dilakukan skenario ke 2 dihasilkan 3.7 dan untuk serangan MITM pada skenario 1 menghasilkan 12,5 ms setelah skenario 2 dihasilkan 11,5 ms. dan *packet loss* pada skenario 1 untuk serangan ICMP *flooding* 0.29% setelah dilakukan skenario 2 dihasilkan 0.19% ms, untuk serangan UDP *flooding* skenario 1 menghasilkan 0.65% setelah dilakukan skenario ke 2 dihasilkan 0.34% dan untuk serangan MITM pada skenario 1 menghasilkan 0.42 % setelah skenario 2 dihasilkan 0.35%.

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