BAB V
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dijelaskan pada BAB sebelumnya, maka dapat disimpulkan bahwa:

1. Snort dapat dijadikan IDPS dikarenakan dapat mendeteksi dan pemblokiran serangan ICMP *flooding,* UDP *flooding* dan MiTM.
2. Pengujian yang dilakukan 2 skenario untuk mengukur kinerja snort IDPS yaitu ketika adanya serangan tetapi snort IDPS belum aktif dan ketika snort IDPS diaktifkan.
3. 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%.ICMP *Flooding, packet delivery ratio* yang dihasilakan di skenario 1 adalah 70,73% dan diskenario 2 adalah 80,50% .selanjutnya pengujian UDP *flooding, packet loss* yang dihasilkan oleh skenario 1 adalah 34,84% dan skenario 2 adalah 65,57%. Terakhir percobaan serangan MiTM yang dihasilkan pada skenario 1 adalah 57,70% dan Skenario 2 adalah 61,52%.

5.2 SARAN

1. Untuk penelitian selanjutnya dapat menggunakan tools selain DMZ, Honeypot dan Snort untuk menguji serangan dengan metode IDPS.
2. Pada penelitian berikutnya melakukan percobaan dengan serangan SSH Brute Force atau yang lebih bervariasi.