BAB V
KESIMPULAN

5.1 Kesimpulan

Dari penelitian ini dapat disimpulkan, sebagai berikut :

1. Untuk melakukan pendeteksian serangan DDOS serta melakukan pemantauan lalu lintas paket data jaringan pada router Mikrotik dapat menggunakan aplikasi *Instrussion Detection System* atau *Network Security Monitoring*. Security Onion dapat bertindak sebagai IDS atau NSM, pada penelitian ini Security Onion bertindak sebagai NSM
2. Analisis serangan DDOS dapat menggunakan metode Live Forensic yang memadu padankan sistem Operasi Security Onion dengan fitur Sguil Tool. Sguil Tool dapat melakukan pemantuan lalu lintas jaringan secara real-time, ini dapat membantu metode live forensic yang melakukan analisis secara langsung. Variabel data yang ditarik dari monitoring jaringan dengan Sguil Tool yaitu *Status, CNT, Alert ID, Date/Time, Source IP, Source Port, Destination IP, Destination Port, Message.*
3. Metode analisis yang digunakan pada penlitian ini adalah Live Forensic, metode ini dilakukan disaat sistem jaringan berjalan.
4. Pada hasil pengujian percobaan serangan pertama, kedua, ketiga, serangan dilakukan dengan masing – masing 30 kali percobaan, ini dimaksudkan untuk mendapatkan hasil yang sesuai dengan analisis, dengan begitu dapat ditarik kesimpulan bahwa serangan DDOS tidak dapat terdeteksi oleh log activity router Mikrotik, namun adanya peningkatan CPU Load dan penurunan pada Free Memory dari router Mikrotik. Dengan tambahan aplikasi pihak ketiga yaitu Sguil Tool, lalu lintas jaringan dan DDOS dapat terdeteksi dengan baik.

5.2 Saran

Saran pada penelitian selanjutnya, berdasarkan penelitian ini, yaitu :

1. Hal ini dimaksudkan pada penelitian selanjutnya, untuk melakukan monitoring jaringan, dapat menggunakan Security Onion versi terbaru, yang lebih baik
2. Pada penelitian selanjutnya diahrapkan lebih banyak parameter yang digunakan, seperti stempel waktu, jenis serangan, grafik serangan, dan grafik lalu lintas paket data, dapat digunakan untuk menghasilkan lebih banyak data untuk hasil penelitian yang lebih akurat.
3. Penelitian ini menggunakan perangkat jaringan router Mikrotik, diharapkan pada penelitian dimasa mendatang dapat menggunakan perangkat jaringan berbeda.