BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan simulasi serangan *DDoS TCP SYN Flood* pada *resource server*, lalu menganalisis serangan *TCP SYN Flood* terhadap *resource server* menggunakan *Wireshark*, dan menarik data forensik sebagai bukti digital sebagai hasil penelitian, maka dapat ditarik beberapa temuan penelitian sebagai kesimpulan. Berikut temuan penelitian ini:

1. Mendapatkan hasil analisis serangan pada *server* dengan menggunakan aplikasi *Wireshark* 3.4, dari proses penyerangan yang dilakukan dapat ditarik informasi bahwa serangan *DDoS* menggunakan aplikasi *Tcp SYN Flooding*. Hasil penelitian ini membuktikan bahwa peneliti berhasil menggunakan aplikasi *Wireshark* 3.4 untuk melakukan analisis serangan *DDoS TCP SYN Flood* pada *resource server*.
2. Informasi dari hasil *capture* pada aplikasi *Wireshark 3.4* setelah melakukan analisa bahwa tenyata ditemukan aktivitas yang tidak wajar melakukan komunikasi data pada *Protocol TCP* dengan IP 10.1.1.4, 10.1.1.5, dan 10.1.1.6 terhadap *server* dengan IP 192.168.100.6. Berikut hasil analisis dari serangan *DDoS TCP SYN Flood* yaitu IP 10.1.1.4, 10.1.1.5, dan 10.1.1.6 dengan rentang waktu antara detik 87.692618 sampai dengan detik 103.191153. IP 10.1.1.4 mengirimkan 89063 paket, IP 10.1.1.5 mengirimkan 115501 paket, dan IP 10.1.1.6 mengirimkan 241159 paket, setalah di *filtering logical* hasilnya

menjadi. IP 10.1.1.4 mengirimkan 401 paket, IP 10.1.1.5 mengirimkan 15801 paket, dan IP 10.1.1.6 mengirimkan 138236 paket, *DDoS TCP SYN Flood* memiliki karakteristik yaitu dapat melakukan *Ping* atau mengirim pesan secara bertubi-tubi dengan rentan waktu yang sangat singkat, diakibatkan setiap paket yang dikirim oleh penyerang akan di terima oleh *server* lalu *server* mengirim respon dari paket si penyerang, namun paket tersebut diabaikan sehingga *server* tetap menunggu respon si pengirim paket, jadinya proses menunggu *server* tersebut mampu membuat jaringan *server* menjadi *down* akibat beban yang masuk berlebihan.

3. Proses pembuktian data pada *server* menggunakan pendekatan metode *Live Forensics* dan melakukan simulasi serangan menggunakan aplikasi *Hping3* dari sistem operasi *Kali Linux*, lalu menggunakan metode *filtering logical* pada aplikasi *Wireshark* untuk pencarian informasi data dari *Log Activity, IP Address List, IO Graph* dan *Flow Graph*.

5.2 Saran

Pada penelitian ini, terdapat beberapa keterbatasan dan kekurangan. Keterbatasan dan kekurangan ini bisa dijadikan acuan dan pertimbangan untuk penelitian selanjutnya. Adapun saran yang dihasilkan dalam penelitian ini adalah sebagai berikut:

1. Analisis serangan *DDoS* pada *server* yang dilakukan masih cukup sederhana, sehingga masih dapat dilakukan pengembangan untuk

memperoleh hasil yang lebih akurat untuk keperluan bukti digital atas serangan *DDoS TCP SYN Flood* pada *server*.

2. Menggunakan seleksi fitur atau algoritma lain pada penelitian selanjutnya untuk melihat kemungkinan meningkatkan akurasi hasil.
3. Penelitian ini hanya menggunakan jaringan *local host* sebagai eksperimen dari serangan *DDoS TCP SYN Flood,* dikarenakan perhitungan resiko yang akan ditanggung oleh peneliti.