BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian analisis malware Trojan danaBot, maka dapat disimpulkan bahwa:

1) Mendeteksi *sample* malware danabot dapat menggunakan tools *virus total* malware yang ditemukan pada saat analisis 58/69. Tidak hanya malware yang terdeteksi tetapi juga banyak informasi detail dalam virus total seperti md5, SHA 256, tipe file hingga size malware.
2) Mengecek keaslian md5 dan SHA 256 pada malware, guna meyakinkan bahwa malware yang dianalisis dalam bentuk apk tidak dalam keadaan rusak atau *corrupt*.
3) Melakukan *decompiler* aplikasi danabot menggunakan ida pro. Didapatkan hasil *hex code, ascii code* pada malware.
4) Peneliti menggunakan metode statis analisis dengan tools ida pro

5.2 Saran

Sebagai penutup penelitian ini, peneliti berharap apa yang peneliti sajikan dalam laporan ini memberikan manfaat dan ilmu bagi pembaca. Peneliti menyadari bahwa penelitian ini masih memiliki kekurangan, untuk itu peneliti memberikan saran sebagai berikut:

1) Untuk melindungi pengguna dari *Trojan.DanaBot* dapat menggunakan Malwarebytes perlindungan real-time.
2) Untuk metode penelitian selanjutnya, dapat dilakukan menggunakan metode dinamis malware analisis dengan menganalisis jejak instruksi, perubahan register, panggilan jaringan dan sistem, penulisan memori menggunakan emulator.
3) Malware adalah topik penelitian yang sangat luas. Ada banyak macam dan jenis nya begitu pula perkembangan nya yang cepat. Karena itu selain menggunakan reverse

engineering, mendeteksi malware dapat juga menggunakan *deep learning* dan *signature base detection.*

4) Peneliti berharap adanya penyempurnaan dalam penelitian yang akan dating agar mendapatkan hasil yang lebih baik.

5) Peneliti menyarankan untuk lebih hati-hati dan bijak dalam mendownload aplikasi dan menggunakan internet.