BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pembahasan pada bab sebelumnya, maka dapat di tarik beberapa kesimpulan yaitu :

1. Proses analisis *malware* menggunakan 3 metode yaitu analisa statis, analisa dinamis, dan network analisis. Proses analisis statis dan dinamis secara otomatis dilakukan oleh *tools* cuckoo sehingga *malware* dapat dianalisis lebih lanjut melalui *report* yang di hasilkan dan *tools* cuckoo. Dan untuk network analisis peneliti melakukan percobaan menggunakan wireshark secara *real time* untuk menganalisis jaringan dari malware njRAT.
2. Berdasarkan hasil analisis pada bab pembahasan, hasil scanning yang dilakukan oleh tools virus total terdeteksi 59/70 anti-malware yang menyatakan bahwa aplikasi *Server.exe* mengandung malware didalanya dan untuk hasil analisis dari *tools* cuckco memiliki skor 4.8 /10 yang menandakan bahwa adanya tanda tanda yang mencurigakan dari malware njRAT ini.
3. Hasil dari analisis statis menggunakan *tools* cuckcoo ditemukan beberapa *string* dan *library* windows yang di duga digunakan oleh malware njRAT saat proses injeksi, dan hasil dari analisis perilaku pada malware njRAT ditemukan beberapa aktivitas yang mencurigakan seperti pengaksesan dan perubahan pada *registry* yang diduga digunakan oleh malware njRAT untuk masuk ke akses yang lebih dalam. Sedangkan untuk *network analysis* ditemukan beberapa temuan seperti *ip* dan *port* yang di gunakan oleh *controller* selain itu di temukan juga jenis paket yang digunakan oleh *controller*.

5.2 Saran

Dalam menutup penelitian skripsi ini, penulis mengharap semoga apa yang penulis sajikan dapat memberikan manfaat bagi para pembaca, penulis dan pengguna Windows. Pada penelitian ini masih terdapat banyak kekurangan

sehingga penulis memberikan saran yang membangun dalam melakukan penelitian selanjutnya

1. Diharapkan dapat melakukan analisis statis dan dinamis secara manual.
2. Menggunakan *tools* yang sesuai dengan *trend malware* yang akan datang.
3. Membahas dan mengeksplor *tools* Cuckoo Sandbox lebih jauh dan lebih mendalam, khusunya pada bagian analisis statis.