Bab 5
Kesimpulan Dan Saran

5.1 Kesimpulan

Setelah melakukan simulasi serangan, deteksi serangan RAT pada laptop korban, dan analisis terhadap hasil penelitian, maka dapat ditarik beberapa temuan penelitian sebagai kesimpulan berikut ini :

1. Cara kerja serangan *Remote Access Trojan (RAT)* jenis *malware* njRAT, dari proses penyerangan yang dilakukan dapat diperoleh informasi bahwa serangan RAT memiliki karakteristik yang dapat mengendalikan atau meremote laptop korban yang bisa menghapus data, disconnect laptop, pengambilan log data, mengganti nama file/folder, dapat merubah data-data korban, mengetahui password, mengetahui aktivitas yang dilakukan pada laptop korban. Hasil penelitian ini membuktikan bahwa aplikasi *Wireshark* mampu mendeteksi serangan pada laptop korban.
2. Proses melakukan serangan *Remote Access Trojan (RAT)* menggunakan MikroTik Router membantu memberikan akses jaringan secara lokal tanpa menggunakan akses internet dengan penentuan IP Address baik pada laptop korban dan laptop attacker. Bukti digital pada laptop korban bisa didapatkan dengan melakukan simulasi penyebaran program *malware* jenis njRAT diantaranya File Manager, Run File, Remote Desktop, Remote Cam, Microphone, Remote Shell, Process Manager, Registry, Keylogger, Open Chat, Get Password, Server (Update, Uninstall, Restart, Close, Disconnect, Rename), dan Open Folder.
3. Meningkatkan keamanan data dari serangan *Remote Access Trojan (RAT)* melalui simulasi ini melalui pemblokiran paket data dengan menentukan *firewall traffic* dalam jaringan IP Address di laptop korban dan manfaat yang didapatkan dari MikroTik yang bisa menyerang laptop korban tanpa jaringan internet dengan menghubungkan 2 (dua) buah Router dengan menggunakan aplikasi Winbox.
4. Analisis dan pengujian yang dilakukan dengan Metode *Dynamic Static*

5.2 Saran

1. Melakukan perbandingan terhadap beberapa penelitian sebelumnya tentang bagaimana peningkatan keamanan data dari serangan program *malware* jenis RAT lainnya untuk bisa membangun keamanan data pada jaringan yang lebih baik kedepannya.
2. Penelitian selanjutnya agar mengembangkan proses investigasi adanya penyerangan program *malware* jenis RAT dengan beberapa client.