BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil pembahasan skripsi ini dapat memberikan kesimpulan sebagai berikut :

1. Terdapat kelemahan bila jaringan wireless Mikrotik ini belum diatur sistem keamanannya, seperti bisa merubah konfigurasi yang ada di Mikrotik tersebut.
2. Dari hasil pengujian bahwa sistem keamanan Hide SSID mampu terlihat bila menggunakan Kali Linux.
3. Access List pun bisa diatasi dengan mudah, dengan menggunakan mac changer yang ada di Kali Linux.
4. Security Profile yang menggunakan enkripsi WPA/WPA2 apabila menggunakan passphrase yang lemah masih memungkinkan untuk dilakukan proses cracking password.
5. Block winbox dan block service SSH juga masih lemah dalam mengamankan jaringan wireless Mikrotik ini.
6. Sistem keamanan port knocking ini menawarkan keamanan dengan cara memproteksi Mikrotik dengan melakukan blocking telnet, SSH, ataupun winbox. Dari hasil pengujian jika membobol sistem keamanan ini harus mengirikan paket ICMP terlebih dahulu, tetapi waktu yang diberikan hanya terbatas.

5.2 Saran

Berdasarkan kesimpulan dan analisa yang dilakukan, berikut ini adalah saran-saran yang dapat diberikan :

1. Ketika menggunakan sistem keamanan security profile berenkripsi WPA/WPA2, gunakan passphrase yang menggabungkan antara huruf, tanda baca, angka, dan huruf besar ataupun kecil sehingga tidak bisa ditebak oleh hacker.
2. Butuh seorang maintenance yang khusus menangani jaringan wireless
3. Waktu yang diberikan saat pengiriman paket ICMP/Ping pada port knocking diubah menjadi 30 detik saja.