BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil penelitian yang dilakukan pada divisi *Networking & IT Solution* PT. Yoshugi Putra Mandiri dan Captive Portal OpenWrt, dapat disimpulkan sebagai berikut:

1. Dengan adanya sistem keamanan RADIUS *server* yang menggunakan otentikasi captive portal, hanya *user* yang terdaftar saja yang bisa terkoneksi ke jaringan *wireless*.
2. Terdapat permasalahan yang berhasil ditemukan pada jaringan *wireless* seperti pencurian *password* dan *username*, akses ilegal, serta man in the middle *attack*.
3. Teknik MAC *filtering* pun bisa dikelabui dnegan mudah, karena MAC *address* dapat diubah secara *virtual* menggunakan *tool* macchanger.
4. WPA2-PSK memiliki enkripsi yang cukup kuat, namun apabila menggunakan *passphrase* yang lemah masih memungkinkan untuk dilakukan proses *cracking password* menggunakan *dictionary attack*.
5. Sistem keamanan RADIUS *server* dengan captive portal menggunakan OpenWRT ini menawarkan alternatif keamanan pada jaringan *wireless* LAN yang kuat, dan juga manajemen *user* yang terkontrol. Dari hasil pengujian menunjukkan bahwa sistem ini sangat sulit untuk dijebol menggunakan teknik serangan ARP *Spoofing*, *brute force* dan *sniffing to eavesdrop*.

6. Keamanan data pada WPA2-PSK masih tergolong rendah karena data sensitif seperti *username* dan *password* dapat di ketahui dengan melakukan sniffing pada jaringan. Sedangkan pada captive portal keamanan data terjamin karena berdasarkan hasil pengujian *sniffing* gagal dilakukan pada captive portal.

5.2 Saran

1. Apabila masih menggunakan enkripsi WPA2-PSK, sebaiknya gunakan *passphrase* yang tidak ada di dalam *dictionary* file. Sebagai contoh gunakan *passphrase* 5t_]d10A1 atau $3cU12eP45$w0rD. Penggunaan *passphrase* yang kuat merupakan jaminan keamanan untuk sebuah jaringan *wireless*, karena satu-satunya cara yang paling gampang yang sering digunakan oleh *hacker* untuk mendapatkan WPA2-PSK *key* adalah dengan melakukan serangan *brute force* menggunakan *dictionary file*, karena itu hindari menggunakan *passphrase* yang ada di dalam *dictionary file* bahasa manapun.
2. Untuk mendapatkan jaringan *wireless* yang lebih aman, gunakan RADIUS *server* dengan otentikasi Captive Portal yang bisa mengurangi resiko-resiko yang tidak diinginkan.