BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang membandingkan sistem keamanan WPA2-PSK dengan RADIUS *server* mikrotik di PT. Intan Pariwara, maka dapat diambil kesimpulan sebagai berikut :

1. Berdasarkan masalah-masalah kerentanan yang ditemukan dan hasil pengujian yang dilakukan, maka sistem keamanan jaringan *wireless* WPA2-PSK di PT. Intan Pariwara sudah tidak aman untuk diterapkan.
2. Walaupun WPA2-PSK menggunakan enkripsi yang cukup kuat, namun serangan *brute force* menggunkan *dictionary file* masih mungkin dilakukan dan berhasil menemukan *password* yang tergolong lemah.
3. RADIUS *server* menggunakan sistem keamanan yang berbeda yaitu *user* dan *password* yang menggunakan web *browser* untuk *login*. Dimana serangan *brute force* yang dilancarkan gagal, karena pada sistem keamanan RADIUS *server* tidak ada proses *handshake*.
4. Dalam beberapa pengujian yang dilakukan pada *access point* yang menggunakan sistem keamanan WPA2-PSK di PT. Intan Pariwara. Serangan *brute force* berhasil di lakukan, namun tidak semua berhasil menemukan *password* yang digunakan. Hal tersebut terjadi karena *password* yang digunakan tidak terdapat pada *dictionary file*.
5. Serangan *ping of death* pada keamanan RADIUS *server* gagal karena *user* belum mendapat akses sebagai pengguna yang sah. Pada perintah **Ifconfig**

yang dilakukan di terminal, dapat dilihat bahwa *user* mendapatkan alamat IP DHCP saat melakukan koneksi. Akan tetapi *user* belum mendapatkan hak akses dan tidak bisa menggunakan fasilitas pada jaringan. Pada saat serangan *brute force* pada RADIUS *server* gagal, yang berarti tidak mendapatkan akun *user* dan *password* sebagai pengguna yang sah.

5.2 Saran

Adapaun saran-saran sebagai berikut :

1. Untuk mengurangi resiko yang tidak diinginkan, gunakan sistem keamanan RADIUS *server* untuk keamanan jaringan *wireless* yang lebih baik.
2. Jika masih menerapkan sistem keamanan WPA2-PSK, sebaiknya mengganti *password* secara berkala dan menggunakan kombinasi *password* yang kuat seperti "P4S5w0rD1Nt4n" atau "H0tSpoT+1nt4N". Karena salah satu cara untuk mendapatkan *password* pada sistem keamanan WPA2-PSK adalah serangan *brute force* menggunakan *dictionary file*. Dimana dalam *dictionary file* tersebut terdapat kumpulan *passphrase* yang mungkin digunakan untuk *password*.