BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari analisis data dan percobaan penyerangan yang dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Jaringan wireless pada SAS CENTER MAGELANG telah menggunakan sistem keamanan jaringan dengan WPA2-PSK, namun menggunakan passphrase yang lemah sehingga memungkinkan untuk dilakukan proses cracking password menggunakan dictionary attack.
2. Sistem keamanan jaringan wireless yang hanya menggunakan satu sistem keamanan jaringan memungkinkan jaringan tersebut lebih mudah untuk diserang oleh pihak luar.
3. Aplikasi Aircrack-ng berhasil mendapatkan kata sandi.
4. Peyerangan packet sniffing dengan aplikasi Bettercap dapat merekam dan menampilkan informasi ip, akses DNS yang dituju target dan informasi account.

5.2 Saran

Berdasarkan uraian dari kesimpulan, maka kelebihan dan kekurangan di atas dapat menjadi pelajaran serta referensi untuk ke depannya. Saran-saran yang dapat dipertimbangkan untuk ke depan antara lain:

1. Ketika menggunakan WPA atau WPA2-PSK, gunakan passphrase yang tidak ada dalam kamus atau informasi pribadi seperti nama pemilik, tanggal lahir

atau nomor penting lainnya. Kombinasi antara huruf dan angka dan symbol lainnya juga penting, dengan minimal 8 karakter. Penggunaan passphrase yang kuat merupakan jaminan untuk sebuah jaringan wireless, karena attacker hanya dapat menggunakan serangan brute force dengan file kamus untuk memecahkan kata sandi WPA/WPA2, karena itu jangan menggunakan passphrase yang ada dalam kamus.

2. Memasang mikrotik, mikrotik mempunyai fitur yang lebih lengkap seperti system login yang berbeda dibandingkan dengan sistem router access point.
3. Selalu update aplikasi browser.
4. Pada penelitian selanjutya, dapat dilakukan upaya untuk peningkatan sistem keamanan jaringan di SAS CENTER MAGELANG.