

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Dari hasil penelitian yang dilakukan pada perpustakaan Universitas Gadjah Mada, dapat disimpulkan sebagai berikut:

1. Dengan adanya sistem autentikasi RADIUS *server*, hanya yang *user* terdaftar saja yang bisa terkoneksi ke jaringan *wireless*.
2. Untuk mengetahui celah keamanan *wireless* penulis menggunakan aplikasi *air-cracking* untuk menembus sistem keamanan yang lama dan masih terdapat celah kelemahan. Sistem enkripsi yang menggunakan WPA memiliki kelemahan terhadap engkripsinya. Sehingga seorang *user* yang tidak memiliki hak akses dapat melakukan pengaksesan ke dalam jaringan secara ilegal. Penggunaan sistem otentikasi RADIUS *server* memberikan *level* keamanan yang lebih baik, karena seorang *user* harus terdaftar terlebih dahulu ke dalam sistem untuk dapat menggunakan jaringan *internet*.
3. Dengan adanya sistem RADIUS *server* ini, admin dapat melakukan monitoring terhadap *user* (mahasiswa, tamu, dan staff) yang terkoneksi ke jaringan Hotspot perpustakaan Universitas Gadjah Mada.
4. Dengan adanya sistem RADIUS *server* sistem keamanan jaringan *wireless* pada perpustakaan Universitas Gadjah Mada menjadi lebih aman karena sistem tersebut tidak bisa ditembus dengan serangan *air-*

*cracking* dan *user* yang terkoneksi terhadap jaringan adalah *user* yang *valid* atau terdaftar pada jaringan.

## 5.2 Saran

Saran yang diberikan sebagai berikut:

1. Sebaiknya karyawan atau staff perpustakaan UGM memiliki *user* autentikasi sendiri apabila ingin mengakses ke dalam jaringan *wireless* dan dibuatkan *user* khusus buat karyawan atau staff guna untuk dapat dimonitoring oleh administrator.
2. Apabila masih menggunakan keamanan enkripsi WPA/WPA2 gunakan *passkey* yang tidak ada dalam kamus yang digunakan pada *brute force*. Gunakann *passkey* yang panjang dan berkrakter seperti contoh "@#\$SDF%^FG45". Penggunaan *passkey* yang kuat merupakan jaminan untuk sebuah jaringan *wireless*, karena satu-satunya cara bisa digunakan oleh *hacker* untuk mendapatkan WPA/WPA2 *key* adalah dengan melakukan serangan *brute force* dengan *file* kamus, karena itu jangan menggunakan *passkey* yang lemah.