

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penulisan laporan skripsi ini antara lain sebagai berikut :

1. Langkah metode pengujian keamanan file server yang terhubung dengan perangkat wireless adalah dimulai dengan pengujian fitur keamanan perangkat wireless, pemetaan perangkat komputer yang terkoneksi, deteksi port dan service yang bekerja, deteksi kelemahan sistem, dan percobaan *exploitasi* kelemahan sistem.
2. Perangkat lunak yang efektif untuk digunakan adalah Kismet, airodump-ng, Pyrit, Nmap, Nessus, dan Armitage.
3. Fitur – fitur keamanan yang diterapkan tetap memiliki celah keamanan yang dapat ditemukan dikemudian hari, sehingga perlu adanya kombinasi penggunaan fitur keamanan guna meningkatkan kualitas keamanan sistem.
4. Keamanan merupakan proses yang berkelanjutan dan bukan merupakan produk jadi, dengan demikian penerapan usulan kebijakan keamanan pada CV. Brainesia bersifat dinamis dan menyesuaikan dengan perkembangan teknologi dan informasi.

## 5.2 Saran

Saran yang dapat diberikan dengan adanya penulisan laporan skripsi ini antara lain sebagai berikut :

1. Perlu adanya usaha membudayakan "*security aware*" guna mencegah tindakan-tindakan merugikan yang mungkin terjadi.
2. Perlu adanya penelitian lebih lanjut mengenai pencegahan serangan deauthenticasi pada perangkat *wireless* serta penelitian mengenai pengaturan seberapa jauh sinyal *wireless* dapat dipancarkan yang mungkin dapat diterapkan sebagai alternatif pengamanan.
3. Perlu adanya penelitian lanjut mengenai langkah-langkah pengujian keamanan jaringan yang mungkin dapat lebih dieksplorasi kembali, misalnya pengujian keamanan WPA pada jaringan *wireless* tanpa ada client sah yang terkoneksi.
4. Perlu adanya penelitian lebih lanjut mengenai *vulnerability research* pada sistem operasi maupun program aplikasi guna mengetahui kemungkinan adanya celah keamanan baru sehingga dapat dilakukan usaha pencegahan.