BAB V
PENUTUP

5.1. Kesimpulan

Kesimpulan yang dapat diambil setelah analisa data dan percobaan serangan yang dilakukan sebagai berikut:

1. Sistem keamanan wireless captive portal pada Warnet Fortran pada umumnya sudah cukup baik. Hal ini dibuktikan dengan percobaan metode Man In The Middle Attack tidak didapat informasi penting seperti username dan password utuk mengakses jaringan wireless.
2. Celah keamanan pada sistem wireless Warnet Fortran masih memberikan kemungkinan untuk melakukan kegiatan MAC Address Spoofing, sehingga dibutuhkan konfigurasi atau sistem tambahan untuk mengantisipanya.
3. Sistem atau konfigurasi tambahan yang diperlukan untuk memperbaiki celah keamanan yang ada, diantaranya dengan menggunakan software decaffeinatID sebagai software monitoring dan metode isolasi user. DecaffeinatID memberikan peringkatan kepada Administrator saat terjadi MAC Address Spoofing dan metode isolasi user mencegah penyerang pada saat melakukan scanning.

5.2. Saran

Berdasarkan kesimpulan di atas, saran – saran yang dapat dipertimbangkan untuk kedepannya antara lain :

1. Administrator Warnet sebaiknya ikut memperhatikan perkembangan sistem yang ada. Walau pun menggunakan hardware dengan sistem keamanan yang baik dan sudah memproteksi sistem wirelessnya. Administrator harus tetap memperhatikan keamanan yang ada, karena sebaik apapun sistem keamanan pasti masih terdapat celah. Faktor maintenance yang dilakukan administrator untuk menangani celah tersebut sangatlah penting.
2. Penanganan untuk dapat meminimalisir terjadinya serangan MAC Address Spoofing dapat dilakukan dengan memantau aktivitas client yang terhubung ke dalam jaringa untuk mengetahui perubahan yang terjadi, jika ada aktivitas yang dianggap mencurigakan seperti serangan administrator dapat langsung memutus client yang melakukan aktivitas tersebut.
3. Pengecekan jaringan secara berkala diperlukan utuk menghindari terjadinya permasalahan/eror pada jaringan yang bisa mengakibatkan terganggunya kinerja jaringan.