BAB 5
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan dari penelitian yang sudah dilakukan dan melakukan analisis yang mendalam dalam penelitian ini, ditemukan kesimpulan yang dapat diuraikan sebagai berikut :

1. Dalam penerapan keamanan dan manajemen jaringan *Wireless Local Area Network* (WLAN), penggunaan teknologi keamanan WLAN dengan protokol otentikasi EAP PEAP-MSCHAPv2 yang dikombinasikan dengan teknologi model protokol *Authentication*, *Authorization*, *Accounting* (AAA) secara terpusat di *User Manager* v7 *Radius Server* MikroTik terbukti dapat mencegah serangan *Random* MAC *Address*. Metode ini telah berhasil dilakukan melalui beberapa langkah yang diambil. Pertama, penggunaan protokol otentikasi EAP PEAP-MSCHAPv2 bahwa hanya perangkat dengan kredensial yang valid yang diizinkan mengakses jaringan WLAN. Proses otentikasi yang kuat dan enkripsi komunikasi antara klien dan *Radius Server usermanager* versi 7 menggunakan SSL dan *shared secret* yang melindungi antara Akses point *authenticator* dan *Radius Server usermanager* versi 7 dalam menjaga keamanan, dalam satu akun kredensial hanya mendapatkan satu IP *Address* saja.
2. Selanjutnya, teknologi model protokol AAA secara terpusat di *User Manager* versi 7 *Radius Server* MikroTik menyediakan solusi yang baik dalam *Authentication, Authorization, Accounting* (AAA). Dengan pengelolaan yang terpusat, kebijakan akses, bandwitdh manajemen, dan monitoring serta mengatur sumber daya jaringan pada jaringan *Wireless* tersebut dapat diterapkan secara konsisten dan deteksi serangan *Random* MAC *Address* telah dapat dilakukan dengan cepat, ditambah pengambilan tindakan pencegahan yang tepat. layanan yang diberikan dengan sistem keamanan EAP PEAP-MSCHAPV2 tetap lebih baik dibanding dengan WPA2PSK setelah dampak dari serangan *Random*

MAC *Address*. Penerapan keamanan ini terbukti telah dapat mencegah serangan *Random* MAC *Address*. Protokol otentikasi EAP PEAP-MSCHAPv2 memberikan tingkat keamanan yang tinggi, sementara pengelolaan terpusat melalui *User Manager* v7 *Radius Server* MikroTik telah dapat mencegah serangan dengan cepat dan mudah.

5.2 Saran

Saran yang dapat diusulkan untuk penelitian selanjutnya guna memperluas dan memperbaiki temuan dari penelitian Pengamanan Jaringan *Wireless* LAN Dengan Menggunakan *Authentication*, *Authorization*, *Accounting* (AAA) Dalam Mencegah Serangan *Random* MAC *Address* ini:

1. Dalam penelitian ini, dapat melihat bahwa penting untuk menjelajahi metode keamanan alternatif sebagai langkah lanjutan. Meskipun metode keamanan yang digunakan, seperti protokol otentikasi EAP PEAP-MSCHAPv2 dan teknologi model protokol AAA di *User Manager* v7 *Radius Server* MikroTik, terbukti dapat mencegah serangan *Random* MAC *Address*, namun ada manfaat yang besar dalam menggali dan membandingkan metode keamanan alternatif. Untuk itu, penelitian berikutnya dapat dilakukan untuk mempelajari protokol otentikasi lainnya dan teknologi keamanan jaringan WLAN yang sedang dikembangkan atau baru muncul.
2. Selain itu, evaluasi performa keamanan yang komprehensif juga menjadi hal penting. Dalam penelitian selanjutnya, dapat melakukan pengujian dan pemantauan yang lebih mendalam terhadap kerentanan keamanan yang mungkin masih ada, dan mengevaluasi sejauh mana metode keamanan yang digunakan mampu melindungi jaringan WLAN dari serangan yang lebih kompleks.
3. Terkait dengan faktor keamanan pada skala yang lebih besar, penelitian ini saat ini berfokus pada keamanan dan manajemen jaringan WLAN dalam skala yang terbatas. Namun, disarankan untuk melakukan penelitian yang melibatkan jaringan WLAN pada skala yang lebih besar, misalnya di perusahaan yang lebih kompleks. Langkah ini akan membantu memahami tantangan keamanan yang mungkin muncul pada

skala yang lebih luas dan memperluas pemahaman tentang penerapan metode keamanan dalam konteks yang lebih realistis terhadap serangan yang tidak terduga.