BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan oleh penulis dengan judul "Analisis Vulnerability Keamanan Jaringan Wireless Pada Protokol WPA dan WPA2 terhadap serangan Aircrack/Hashcat Menggunakan Metode 4-Way Handshake dan Pairwise Master Key Identifier" dapat diimplementasikan dan diuji sesuai dengan perencanaan. Kesimpulan yang bisa diambil dari penelitian ini adalah sebagai berikut:

1. Setelah melakukan implementasi dan pengujian serangan 4-*way handshake*, maka didapatkan kerentanan pada bagian *frame* manajemen yang tidak terenkripsi oleh protokol WPA/WPA2 PSK.
2. Setelah melakukan implementasi dan pengujian serangan PMKID, maka didapatkan kerentanan pada bagian opsional 802.1x yang memasukkan PMKID pada elemen informasi RSN.
3. Penggunaan fitur PMKID pada lingkungan WPA/WPA2 PSK menimbulkan dampak penyalahgunaan fitur tersebut oleh penyerang yang digunakan untuk melakukan serangan *password cracking*.
4. Serangan *deauthentication* pada saat proses 4-*way handshake* menimbulkan klien secara paksa melakukan otentikasi ulang yang

menyebabkan penyerang mendapatkan WPA *handshake* untuk digunakan pada serangan *password cracking* ataupun serangan lain.

5. Dengan mengimplementasikan standar fitur 802.11 w, maka *frame* manajemen akan terenkripsi sehingga penyerang tidak dapat melakukan serangan pada saat proses 4-*way handshake* antara *access point* dan klien.
6. Serangan PMKID lebih efisien dibandingkan dengan serangan 4-*way handshake* yang selanjutnya akan dilakukan serangan *password cracking* dikarenakan serangan PMKID tidak memerlukan klien dan hanya membutuhkan satu pesan dari 4-*way handshake*, namun keberhasilan dari serangan ini tergantung dari vendor *access point* apakah menyematkan PMKID pada pesan pertama saat proses 4-*way handshake*.
7. Serangan 4-*way handshake* lebih efektif dibandingkan dengan serangan PMKID yang selanjutnya akan dilakukan serangan *password cracking* dikarenakan serangan ini menyerang *frame* manajemen yang menjadi dasar proses otentikasi dari protokol nirkabel 802.11.

5.2 Saran

Saran untuk pengembangan lebih lanjut antara lain:

1. Pada saat penulis melakukan penelitian, protokol WPA3 telah dirilis namun masih terdapat beberapa *bug*. Implementasi protokol WPA3 pada jaringan nirkabel secara *default* akan mengenkripsi *frame*

manajemen sehingga penyerang tidak dapat melakukan serangan *deauthentication* guna mendapatkan *handshake*.

2. Ditambahkannya fitur *management frame protection* (802.11w) pada jaringan nirkabel protokol WPA/WPA2 PSK yang berfungsi untuk mengenkripsi *frame* manajemen, namun harus dilihat apakah perangkat klien mendapatkan dukungan untuk fitur tersebut.
3. Menonaktifkannya fitur PMKID pada lingkungan protokol WPA/WPA2 PSK yang tidak menggunakan mode *roaming* tidak akan menimbulkan dampak kerugian kinerja sehingga kemanan jaringan masih tetap aman untuk digunakan.
4. Dalam perancangan dan implementasi pengujian ini disadari masih banyak kekurangan ataupun dari segi pembuatan laporan. Sebagai penutup, harapannya semoga skripsi ini bisa bermanfaat bagi semua orang khususnya yang sedang mempelajari atau mendalami ilmu keamanan jaringan komputer khususnya mengenai protokol WPA/WPA2 PSK.