BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan mengenai analisis dan implementasi serangan *deauther* esp8266 terhadap jaringan wifi router, maka dapat disimpulkan hasilnya sebagai berikut :

1. Deauther Esp8266 menggunakan *hardware Microcontroller* Nodemcu Esp8266 yang sudah dikonfigurasi flashing firmware deauther menunjukan ancaman dalam keamanan jaringan, penyerangan dapat melakukan scan terhadap jaringan wifi yang ada di sekitar dan melakukan serangan terhadap jaringan wifi.

2. Hasil evaluasi kelemahan dan ancaman Serangan deauther esp8266 ini memanfaatkan celah pada management frame WLAN standar 802.11 yang tidak di enkripsi dengan melakukan pengiriman paket-paket palsu kepada frame deautentikasi, membuat router dan client terputus secara paksa serta memblokade kedua akses jaringan. Kelemahan serangan deauther eps8266 dengan memilih router yang berstandar 802.11w (2009), pada router yang berstandar ini sudah terdapat fitur enkripsi pada manajement frame yaitu PMF (Protected Management Frame). Cara kerjanya dengan melakukan enkripsi pada manajement frame tersebut client dan router tetap bisa saling mendengar dan mengerti manajement frame nya, namun proteksi akan berlaku efektif jika client yang terhubung dengan router tersebut juga memiliki proteksi management frame yang serupa. Serangan deauther eps8266 untuk saat ini hanya bisa dilakukan dan tersedia hanya pada frekuensi 2.4 Ghz. Dikarenakan cara kerja alat ini Penyerang akan membangkitkan satu frekuensi yang sama dengan frekuensi pada wireless LAN, jadi hanya menyandingkan frekuensi yang sama tidak membangkitkan frekuensi yang lebih tinggi pada target seperti jamming.

5.2 Saran

Berdasarkan kesimpulan yang telah diuraikan diatas, maka adapun saran dari penulis sebagai pertimbangan penelitian selanjutnya :

1. Diharapkan penelitian selanjutnya dapat membuat alat pencegahan terhadap serangan deauther esp8266 ini dikarenakannya untuk saat ini frekuensi 2.4 Ghz ini banyak digunakan diberbagai semua perangkat nirkabel khususnya pada perangkat iot.

2. Untuk Penyerang yang menggunakan Phising SSID menggunakan evil twin ini memiliki ancaman Penyerang dapat mengelabui korban agar menginstal ulang kunci yang sudah digunakan. Dapat ditanggulangi dengan melakukan hide SSID pada router. Jarak penyebaran akses palsu ini hanya mencapai 50 meter jika tidak ditambahkan dengan antena.

3. Penanggulangan dengan melakukan hide SSID seperti pada Gambar 4. 23 menunjukan tidak terdeteksinya Wifi jaringan dalam web penyerangan membuat router tidak dapat dilakukan penyerangan deauther.