BAB V
PENUTUP

5.1 Kesimpulan

Kesimpulan dari Analisis Kerentanan Jaringan Wifi wpa & wpa2 Terhadap Serangan Menggunakan Airgeddon adalah sebagai berikut :

1. Protokol keamanan yang lemah atau usang, seperti WEP (Wired Equivalent Privacy), rentan terhadap serangan dan mudah ditembus. WPA (Wi-Fi Protected Access) dan WPA2 telah menjadi standar yang lebih kuat, tetapi juga bisa memiliki kerentanan tertentu.
2. Penggunaan password yang lemah atau mudah ditebak adalah kerentanan umum pada jaringan Wi-Fi. Password yang kuat dan kompleks harus digunakan untuk mengurangi risiko serangan.
3. Ada kerentanan dalam metode enkripsi yang digunakan dalam jaringan Wi-Fi, yang bisa memungkinkan serangan untuk mendekripsi lalu lintas data. Salah satu contohnya adalah serangan Krack (Key Reinstallation Attack) yang memanfaatkan celah dalam protokol WPA2.
4. Perangkat keras (router, access point) dan firmware yang tidak diperbarui secara teratur bisa menjadi kerentanan keamanan. Produsen dan pengguna harus menjaga perangkat mereka tetap diperbarui dengan versi firmware terbaru yang mengatasi kerentanan yang diketahui.

Kerentanan keamanan pada jaringan Wi-Fi adalah realitas yang harus diwaspadai. Penting bagi pengguna dan pemilik jaringan untuk mengadopsi praktik keamanan terbaik, seperti menggunakan protokol keamanan yang kuat, menggunakan password yang kuat, mengatur firewall, memperbarui perangkat dan firmware secara teratur, serta memantau dan melindungi jaringan mereka dengan solusi keamanan yang tepat.

5.2 Saran

Sebagai bahan pertimbangan peneliti memberikan saran untuk pengembangan kemanan jaringan wifi selanjutnya sebagai berikut :

1. Gunakan protokol keamanan WPA2 atau yang lebih baru, seperti WPA3, untuk mengenkripsi lalu lintas data. Hindari menggunakan protokol keamanan yang sudah usang, seperti WEP.
2. Buat password yang kuat dan kompleks untuk jaringan Wi-Fi. Gunakan kombinasi huruf (huruf besar dan huruf kecil), angka, dan simbol. Pastikan password memiliki panjang yang mencukupi dan tidak mudah ditebak. Ganti password secara teratur.
3. Pastikan perangkat Wi-Fi memiliki versi firmware terbaru. Firmware yang diperbarui seringkali mencakup perbaikan keamanan yang penting. Pantau situs web produsen untuk pembaruan firmware terbaru dan terapkan segera.
4. Nyalakan fitur firewall pada router untuk melindungi jaringan Wi-Fi dari serangan yang berpotensi. Ini dapat membantu melindungi perangkat dari serangan yang berasal dari internet.
5. Aktifkan fitur filtering MAC address pada router. Dengan ini, hanya perangkat yang memiliki alamat MAC yang ditentukan sebelumnya yang diperbolehkan terhubung ke jaringan Wi-Fi.
6. Gunakan perangkat lunak pemantau jaringan untuk melacak dan memeriksa aktivitas yang mencurigakan dalam jaringan Wi-Fi. Ini dapat membantu mendeteksi serangan dan langkah-langkah yang perlu diambil untuk melindungi jaringan.