BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil penelitian yang dilakukan melalui metode *penetration testing* terhadap jaringan Wi-Fi di lingkungan PT *Evergrown Technology*, dapat disimpulkan beberapa hal sebagai berikut:

1. Penelitian berhasil mengidentifikasi celah keamanan pada jaringan Wi-Fi dengan pendekatan praktis menggunakan tools seperti *Wifite, Airodump-ng, Wireshark, dan Aircrack-ng*. Proses *monitoring* dan penangkapan *handshake* menunjukkan bahwa jaringan masih rentan terhadap serangan, khususnya jika terdapat klien yang aktif terhubung. Analisis menggunakan *Wireshark* membuktikan bahwa paket *handshake* yang ditangkap *valid* dan dapat digunakan untuk proses dekripsi. Dengan menggunakan *wordlist*, password jaringan Wi-Fi berhasil ditemukan melalui teknik *dictionary attack*. Hal ini menunjukkan bahwa kata sandi yang digunakan masih tergolong lemah dan rentan terhadap serangan berbasis *wordlist*.
2. Efektivitas *Aircrack-ng* terbukti dalam mengidentifikasi kelemahan jaringan, terutama jika jaringan menggunakan kata sandi yang lemah. Dalam penelitian ini, password Wi-Fi berhasil ditemukan menggunakan *wordlist rockyou.txt,* yang menunjukkan bahwa jaringan masih rentan terhadap serangan *brute force* dan *dictionary attack* apabila tidak dilindungi dengan kata sandi yang kuat.

3. Strategi mitigasi seperti penonaktifan fitur *WPS*, penggunaan kata sandi yang kompleks, serta implementasi *MAC filtering*, merupakan langkah-langkah penting yang perlu diterapkan untuk meningkatkan keamanan jaringan nirkabel dan mengurangi potensi risiko terhadap serangan seperti *dictionary attack*.

5.2 Saran

Adapun saran-saran yang dapat diberikan berdasarkan hasil penelitian ini adalah sebagai berikut:

1. Administrator jaringan disarankan untuk menonaktifkan fitur *WPS (Wifi Protected Setup)*, karena fitur ini dapat menjadi celah keamanan yang memungkinkan akses tidak sah ke jaringan tanpa perlu mengetahui kata sandi secara langsung. Penggunaan kata sandi yang kompleks sangat dianjurkan, dengan kombinasi huruf besar, huruf kecil, angka, dan simbol, serta tidak menggunakan kata atau frasa umum yang mudah ditebak maupun terdapat dalam *wordlist* publik. Implementasi *MAC filtering* sebaiknya diterapkan untuk membatasi akses hanya pada perangkat-perangkat tertentu yang telah terdaftar, sehingga mencegah perangkat asing masuk meskipun mengetahui kata sandi jaringan.
2. Untuk penelitian selanjutnya, disarankan untuk memperluas cakupan pengujian pada jaringan dengan konfigurasi keamanan yang berbeda, serta menguji efektivitas mitigasi lainnya seperti *WPA3, captive portal, dan* segmentasi jaringan.