BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terhadap jaringan Wi-Fi pada lingkungan kos menggunakan metode *penetration testing*, maka dapat disimpulkan sebagai berikut:

1. Hasil penelitian menunjukkan bahwa serangan brute force cukup efektif dalam membobol jaringan Wi-Fi WPA2 di lingkungan kost, khususnya apabila kata sandi yang digunakan memiliki tingkat kompleksitas yang rendah. Semakin pendek dan sederhana kombinasi karakter dalam kata sandi, semakin cepat proses pembobolan dapat dilakukan. Di sisi lain, tingkat kerentanan jaringan Wi-Fi kost terhadap serangan packet sniffing juga terbilang tinggi, terutama karena lalu lintas data yang tidak dilindungi oleh enkripsi tambahan. Hal ini memungkinkan pihak tidak berwenang untuk memperoleh informasi sensitif seperti *username, password*, alamat IP, DNS, serta aktivitas pengguna jaringan dengan relatif mudah.

2. Hasil penetration testing menunjukkan adanya beberapa celah keamanan pada jaringan Wi-Fi kos, di antaranya penggunaan kata sandi yang mudah ditebak, dan tidak diterapkannya segmentasi atau isolasi antar pengguna jaringan.

3. Untuk memitigasi serangan *brute force* dan *packet sniffing*, diperlukan penerapan kebijakan keamanan yang lebih ketat, seperti penerapan sistem enkripsi yang lebih kuat dengan WPA3, penggunaan kata sandi yang kompleks dan diperbarui secara berkala, implementasi penggunaan protokol HTTPS dan enkripsi tambahan seperti VPN untuk mengakses Web, menerapkan segmentasi atau isolasi antar pengguna jaringan, dan melakukan pemantauan aktivitas jaringan secara berkala.

5.2 Saran

Berdasarkan hasil penelitian terhadap keamanan jaringan Wi-Fi lokal yang dilakukan melalui metode *penetration testing*, diperoleh temuan adanya kerentanan terhadap serangan brute force dan packet sniffing. Berdasarkan hasil tersebut, peneliti memberikan beberapa saran dan rekomendasi teknis untuk meningkatkan proteksi jaringan. Berikut adalah saran dan rekomendasi yang dapat diterapkan.

1. Penerapan Sistem Enkripsi yang Lebih Kuat

   Pengelola jaringan disarankan untuk menggunakan protokol keamanan WPA3, sesuai dengan rekomendasi NIST SP 800-97, yang menawarkan perlindungan lebih baik dibandingkan WPA2, terutama terhadap serangan brute force. Jika perangkat belum mendukung WPA3, maka pengaturan WPA2 dengan enkripsi AES harus dipastikan aktif, dan penggunaan TKIP sebaiknya dihindari.

2. Penguatan Kebijakan Kata Sandi (*Password Policy*)

   Mengacu pada NIST SP 800-63B, pengguna disarankan untuk menggunakan kata sandi dengan tingkat kompleksitas tinggi, minimal 8 karakter, serta memuat kombinasi huruf besar, huruf kecil, angka, dan simbol. Penggunaan kata sandi umum atau mudah ditebak harus dihindari, dan penggunaan *passphrase* juga dapat dipertimbangkan sebagai alternatif yang lebih aman dan mudah diingat.

3. Penggunaan HTTPS untuk Akses Web

   Untuk mencegah penyadapan data melalui serangan sniffing, penggunaan protokol HTTPS sangat disarankan, khususnya dalam proses autentikasi akun atau pertukaran informasi sensitif. Hal ini selaras dengan pedoman NIST SP 800-52 Rev.2 terkait penggunaan *Transport Layer Security* (TLS) dalam sistem komunikasi.

4. Segmentasi Jaringan dan Pembatasan Akses

   Disarankan agar jaringan Wi-Fi dibagi menjadi beberapa segmen, misalnya jaringan utama dan jaringan tamu, guna meminimalkan risiko penyebaran

serangan. Prinsip *least privilege* seperti yang diatur dalam NIST SP 800-53 perlu diterapkan, yaitu memberikan hak akses seminimal mungkin sesuai kebutuhan pengguna.

5. Pemantauan Aktivitas Jaringan secara Berkala

   Mengacu pada NIST SP 800-137, pengelola jaringan disarankan untuk melakukan pemantauan lalu lintas jaringan secara berkala menggunakan tools seperti IDS (*Intrusion Detection System*) atau *packet analyzer*. Hal ini bertujuan untuk mendeteksi aktivitas mencurigakan secara dini dan mencegah potensi serangan yang lebih luas.