BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan yang sudah dipaparkan dalam penelitian ini yang berjudul Analisis Perbandingan Keamanan Protokol Wifi WPA2 Dan WPA3 Melalui Penetrasi Aktif Dan Pasif, serta melakukan pengujian terhadap protokol WPA2 dan WPA3 mengunakan teknik *Aircrack-ng dan Brute Force Attack* total sebanyak 20 kali percobaan maka dapat disimpulkan sebagai berikut :

1. Perbandingan Keamanan melalui Penetrasi Aktif

   Berdasarkan hasil uji coba menggunakan teknik penetrasi aktif ditemukan bahwa protokol keamanan WPA2 rentan terhadap serangan dengan tingkat keberhasilan yang signifikan. Dengan percobaan masing-masing protokol sebanyak 5 kali percobaan pengujian menghasilkan 5 percobaan mendapatkan kata sandi untuk protokol WPA2 dan 5 kali percobaan tidak mendapatkan kata sandi pada protokol WPA3. Hal ini disebabkan oleh adanya fitur *Protected Management Frames* (PMF) dan SAE (*Simultaneous Authentication of Equals*) pada WPA3 yang dapat mengurangi risiko serangan aktif. Teknik seperti *Aircrack-ng dan Brute Force* Attack mampu dengan relatif mudah memperoleh akses ke jaringan yang menggunakan WPA2. Di sisi lain, protokol keamanan WPA3 menunjukkan ketahanan yang lebih tinggi terhadap serangan, dengan tidak ada percobaan yang berhasil memperoleh password dalam uji coba yang dilakukan.

2. Perbandingan Keamanan melalui Penetrasi Pasif

   Dari hasil analisis lalu lintas jaringan menggunakan pendekatan penetrasi pasif tidak ditemukan kelemahan yang signifikan pada protokol WPA3. Dengan percobaan masing-masing protokol sebanyak 5 kali percobaan pengujian menghasilkan 5 percobaan mendapatkan kata sandi untuk protokol WPA2 dan 5 kali percobaan tidak mendapatkan kata sandi pada protokol WPA3. Keunggulan ini dikarenakan WPA3 menggunakan enkripsi yang lebih kuat dan pengaturan autentikasi yang lebih baik sehingga

mempersulit serangan pasif untuk mendapatkan informasi penting dari jaringan.

Walaupun protokol WPA2 menunjukkan beberapa potensi kerentanan yang dapat dieksploitasi, seperti penggunaan handshake yang rentan terhadap serangan offline, namun hal ini tidak berlaku pada protokol WPA3. Pengamatan secara pasif tidak mengungkapkan kelemahan yang serupa pada WPA3.

Kesimpulan ini menunjukkan bahwa dalam aspek penetrasi aktif maupun pasif, protokol WPA3 lebih unggul dalam memberikan perlindungan keamanan yang lebih efektif dibandingkan dengan WPA2.

Tabel 5.1 Hasil berbandingan protokol WPA2 dan WPA3

Protokol	Penetrasi aktif	Penetrasi pasif	Hasil
WPA2	berhasil	berhasil	2
WPA3	gagal	gagal	-

Dari tabel hasil di atas penulis mendapati bahwa perbandingan keamanan jaringan WPA2 dan WPA3 lebih aman protokol WPA3 dari pada protokol WPA2 dengan perpandingan 2 kali lebih aman dari protokol jaringan WPA2.

5.2 Saran

Berdasarkan kesimpulan di atas, penelitian ini memberikan beberapa saran untuk pengembangan keamanan jaringan WiFi di masa depan, beberapa saran yang dapat kami berikan diantaranya sebagai berikut:

1. Prioritaskan Implementasi Protokol WPA3
   Mengingat tingkat keamanan yang lebih tinggi dari protokol WPA3, disarankan untuk memprioritaskan migrasi keamanan jaringan WiFi ke

protokol ini. Hal ini dapat dilakukan dengan mengupgrade perangkat keras dan perangkat lunak yang terlibat dalam jaringan.

2. Perbarui Keamanan secara Berkala

   Penting untuk secara berkala memperbarui perangkat lunak dan firmware perangkat keras yang terhubung ke jaringan WiFi, termasuk router dan perangkat pengguna akhir. Ini akan membantu dalam mengatasi kerentanan yang baru ditemukan dan meningkatkan keamanan secara keseluruhan.