# BAB V
# PENUTUP

## 5.1. Kesimpulan

Berdasarkan Rumusan masalah dan hasil penelitian yang telah dilakukan mengenai Analisis Risiko Keamanan Jaringan *Smart Home* dengan Penerapan Metode *OCTAVE* dan Simulasi *Packet Tracer*, maka dapat ditarik beberapa kesimpulan sebagai berikut:

5.1.1. Penelitian ini membuktikan bahwa metode *OCTAVE* dapat diadaptasi secara efektif untuk lingkungan Smart Home berbasis IoT, yang umumnya belum memiliki kerangka standar keamanan yang baku. Melalui identifikasi aset, ancaman, dan kerentanan, metode ini menghasilkan pemetaan risiko yang terukur terhadap aspek *Confidentiality, Integrity, dan Availability* (CIA Triad). Temuan bahwa serangan *Unauthorized Access dan Denial of Service* (DoS) memiliki tingkat risiko tinggi memberikan kontribusi konseptual terhadap pemahaman pola risiko dominan dalam jaringan IoT rumah tangga. Hal ini dapat menjadi acuan bagi penelitian lanjutan dalam pengembangan model penilaian risiko yang lebih spesifik untuk IoT, termasuk integrasi dengan metode kuantitatif seperti *ISO/IEC 27005*.

5.1.2. Dari sisi implementasi, hasil simulasi pada *Cisco Packet Tracer* menunjukkan bahwa kombinasi langkah mitigasi seperti *Hide SSID, WPA2-Personal, Access Control List (ACL), dan MAC Filtering* mampu menurunkan dampak serangan terhadap jaringan secara signifikan. Meskipun tidak sepenuhnya menghilangkan ancaman, penerapan mekanisme tersebut dapat menjadi rekomendasi dasar bagi pengembang dan pengguna sistem *Smart Home* untuk memperkuat keamanan jaringan lokal. Selain itu, disarankan penggunaan perangkat *Smart Home* yang mendukung autentikasi dua faktor, segmentasi *VLAN*, serta monitoring berbasis *IDS/IPS*, agar keamanan dapat ditingkatkan hingga mendekati kondisi nyata di lapangan.

## 5.2. Saran

Berdasarkan hasil penelitian yang telah diperoleh, maka beberapa saran yang dapat diberikan adalah sebagai berikut:

5.2.1. Agar memaksimalkan pertahanan terhadap serangan, disarankan untuk menambahkan mekanisme keamanan yang lebih baru, seperti *WPA3*, *Intrusion Detection System* (IDS), atau *VPN*.

5.2.2. Agar hasilnya lebih valid dan aplikatif, penelitian selanjutnya harus dilakukan pada perangkat IoT nyata karena penelitian ini masih berbasis simulasi di *Cisco Packet Tracer*.

5.2.3. Untuk memperluas cakupan analisis risiko, pengujian harus dilakukan dengan menambahkan serangan yang lebih kompleks, seperti serangan *Man-in-the-Middle* (MITM), serangan *Replay*, atau *Brute Force*.