ABSTRAK

Penelitian ini menganalisis keamanan jaringan *Wi-Fi* XL Home terhadap serangan *Evil Twin* dan mengukur performa jaringan menggunakan parameter *Quality of Service* (QoS), yaitu *Delay*, *Jitter*, *Throughput*, dan *Packet loss*. Jaringan *Wi-Fi* rentan terhadap serangan ini karena menggunakan gelombang radio yang mudah dieksploitasi. Serangan *Evil Twin* memungkinkan penyerang menciptakan jaringan palsu untuk mencuri data pengguna melalui teknik *Deauthentication* dan *Captive Portal*. Dengan meningkatnya jumlah pengguna internet di Indonesia, yang mencapai 215 juta pada tahun 2023, ancaman serangan siber terus meningkat, termasuk upaya kejahatan yang mencapai 495 juta pada tahun 2020. Hasil penelitian menunjukkan bahwa serangan *Evil Twin* dapat secara signifikan menurunkan *Throughput* dan meningkatkan *Delay*, khususnya pada aplikasi berbasis dokumen. Meskipun layanan XL Home mampu mempertahankan performa untuk aplikasi streaming, kelemahan keamanan terhadap serangan berbasis *Man in the Middle* (MITM) memerlukan perhatian serius. Penelitian ini juga memberikan rekomendasi, seperti penerapan protokol WPA3 dan edukasi pengguna untuk meningkatkan kesadaran terhadap ancaman serangan siber. Kontribusi penelitian ini meliputi pemahaman lebih dalam tentang kerentanan jaringan *Wi-Fi* XL Home, dampak serangan *Evil Twin* terhadap performa jaringan, dan wawasan untuk meningkatkan keamanan serta kualitas layanan jaringan di Indonesia.

Kata Kunci: Keamanan Jaringan, *Wi-Fi*, XL Home, *Evil Twin*, *Quality of Service* (QoS).