ABSTRACT

This research analyzes the security of XL Home Wi-Fi Network against Evil Twin Attacks and measures Network performance using Quality of Service (QoS) parameters, namely Delay, Jitter, Throughput, and Packet loss. Loss. Wi-Fi Networks are vulnerable to this attack because they use radio waves that are easily exploited. radio waves that are easy to exploit. Evil Twin Attacks allow attackers to create a fake Network to steal User data through Deauthentication and Captive Portal techniques. With the increasing number of internet Users in Indonesia, which reached 215 million in 2023, the threat of cyberattacks continues to increase, including malicious attempts that reached 495 million in 2020. The results show that Evil Twin Attacks can significantly significantly reduce Throughput and increase Delay, especially in document-based applications. document-based applications. Although XL Home service is able to maintain performance for streaming applications, security weaknesses against Man in the Middle (MITM) based Man in the Middle (MITM) attacks require serious attention. This research also provides recommendations, such as the implementation of the WPA3 protocol and educating to increase awareness of the threat of cyber-attacks. The contributions of this research include a deeper understanding of the vulnerability of XL Home's Wi-Fi XL Home Wi-Fi Network, the impact of Evil Twin Attacks on Network performance, and insights to improve Network security and Quality of Service in Indonesia.

***Keywords**: Network Security, Wi-Fi, XL Home, Evil Twin, Quality of Service (QoS).*