ABSTRACT

The rapid development of wireless network technology has significantly improved internet accessibility for users in various locations. However, this progress also increases security risks that can be exploited by malicious actors. Wireless network security is a crucial issue, especially in academic environments where sensitive data and information are frequently exchanged over the internet. Therefore, this study aims to analyze the security level of wireless networks at Universitas Pembangunan Nasional "Veteran" Yogyakarta.

This study compares the security of three types of network infrastructures: integrated wi-fi networks, local wi-fi networks, and public wi-fi networks using the Penetration Testing method. The testing process utilizes seven attack parameters: deauthentication, cracking the encryption, dictionary attack, man-in-the-middle attack, sniffing, traffic control network, and evil twin attack.

The results indicate that the integrated wi-fi network, managed by the university's Information and Communication Technology Unit, has a higher level of security compared to local and public wi-fi networks, which are more vulnerable to security threats. Several attack methods were successfully executed, particularly on networks with weaker security configurations or default settings. To enhance network security, this study recommends several measures, including the implementation of stronger security protocols, the enforcement of stricter access policies, and regular network monitoring to detect potential threats. Additionally, educating network users about cybersecurity best practices is essential to prevent social engineering-based attacks.

This research is expected to serve as a reference for the university in strengthening its wireless network security, ensuring better data protection and privacy for the academic community, and creating a safer digital environment.

Keywords: *Penetration Testing, Network Security, Wi-Fi, Cyber Attacks,* UPN "Veteran" Yogyakarta.