

## ABSTRAK

Di era digital yang berkembang pesat, internet telah menjadi kebutuhan vital bagi masyarakat Indonesia, dengan 215,63 juta pengguna pada periode 2022-2023 menurut APJII. Akses mudah melalui jaringan Wireless Fidelity (Wi-Fi) sangat umum digunakan di fasilitas publik. Namun, kemudahan ini membawa risiko, karena koneksi Wi-Fi publik rentan terhadap serangan siber, seperti phishing dan sniffing. Badan Siber dan Sandi Negara (BSSN) mencatat 279,84 juta serangan siber di Indonesia pada tahun 2023. Dengan indeks keamanan digital terendah pada tahun 2022 (3,12), penerapan metode Penetration Testing Execution Standard (PTES) untuk analisis keamanan jaringan menjadi penting, terutama di lingkungan akademik yang sering digunakan oleh banyak pengguna. Evaluasi jaringan wireless UPNVYK diperlukan untuk melindungi data sensitif pengguna dan memastikan keberlangsungan kegiatan pembelajaran serta penelitian.

Penelitian ini bertujuan untuk menganalisis keamanan jaringan Wi-Fi di Universitas Pembangunan Nasional Veteran Yogyakarta (UPNVYK) menggunakan metode PTES. Dengan meningkatnya penggunaan internet dan kerentanan terhadap serangan siber, keamanan jaringan Wi-Fi menjadi sangat penting, terutama di lingkungan akademik. Metodologi penelitian menggunakan pendekatan studi kasus dengan menerapkan PTES dan NIST SP 800-42 sebagai panduan. Pengujian dilakukan pada lima fakultas di UPNVYK, meliputi parameter Cracking The Encryption, Deauthentication/DoS, ARP Spoofing, Sniffing, dan Traffic Control Network. Tools yang digunakan termasuk Aircrack-ng, Bettercap, Wireshark, dan Evillimiter.

Hasil penelitian mengindikasikan bahwa jaringan Wi-Fi di UPNVYK memiliki tingkat keamanan yang tinggi, meskipun masih terdapat peluang untuk perbaikan. Serangan Deauthentication/DoS berhasil dilakukan, namun dampaknya terhadap operasional jaringan tergolong minimal. Untuk meningkatkan keamanan, disarankan melakukan pemantauan secara berkelanjutan dan memperkuat mitigasi serangan DoS. Penelitian ini menekankan pentingnya keamanan jaringan Wi-Fi di lingkungan akademik dan dapat menjadi acuan bagi institusi pendidikan lain dalam memperkuat sistem keamanan jaringan mereka.

**Kata kunci:** Keamanan Jaringan, Wi-Fi, *Penetration Testing*, *PTES*, Universitas

## ABSTRACT

*In this rapidly evolving digital era, the internet has become a vital necessity for Indonesian society, with 215.63 million users reported by APJII for the 2022-2023 period. Easy access through Wireless Fidelity (Wi-Fi) networks is commonly used in public facilities. However, this convenience comes with risks, as public Wi-Fi connections are vulnerable to cyber attacks such as phishing and sniffing. The National Cyber and Crypto Agency (BSSN) recorded 279.84 million cyber attacks in Indonesia in 2023. With the lowest digital security index in 2022 (3.12), the implementation of the Penetration Testing Execution Standard (PTES) for network security analysis is essential, especially in academic environments that are frequently used by many users. Evaluating UPNVYK's wireless network is necessary to protect sensitive user data and ensure the continuity of learning and research activities.*

*This study aims to analyze the security of the Wi-Fi network at the Universitas Pembangunan Nasional Veteran Yogyakarta (UPNVYK) using the PTES method. With the increasing use of the internet and vulnerability to cyber attacks, the security of Wi-Fi networks is crucial, especially in academic settings. The research methodology employs a case study approach by applying PTES and NIST SP 800-42 as guidelines. Testing was conducted across five faculties at UPNVYK, focusing on parameters such as Cracking The Encryption, Deauthentication/DoS, ARP Spoofing, Sniffing, and Traffic Control Network. Tools used include Aircrack-ng, Bettercap, Wireshark, and Evillimiter.*

*The results indicate that the Wi-Fi network at UPNVYK has a high level of security, although there are still opportunities for improvement. The Deauthentication/DoS attacks were successfully executed, but their impact on network operations was minimal. To enhance security, it is recommended to implement continuous monitoring and strengthen DoS attack mitigation. This study emphasizes the importance of Wi-Fi network security in academic environments and can serve as a reference for other educational institutions to strengthen their network security systems.*

**Keywords:** *Network Security, Wi-Fi, Penetration Testing, PTES, University*