EVALUASI KEAMANAN JARINGAN NIRKABEL SSID UNDIKSHA EVENT MENGGUNAKAN METODE PENETRATION TESTING BERBASIS PENETRATION TESTING EXECUTION STANDARD (PTES)

Oleh

Junaidi, NIM 1915101041

Program Studi S1 Ilmu Komputer

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi keamanan jaringan nirkabel SSID Undiksha Event Universitas Pendidikan Ganesha menggunakan metode *Penetration Testing Execution Standard* (PTES). Penelitian menggunakan pendekatan deskriptif dengan tahapan PTES yang meliputi *pre-engagement, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation,* dan *reporting*. Teknik pengumpulan data dilakukan melalui wawancara, observasi, dan dokumentasi, sedangkan tahap eksploitasi menggunakan teknik *Cracking the Encryption* dan *Evil Twin Attack*. Hasil penelitian menunjukkan bahwa proses penangkapan *four-way handshake* berhasil dilakukan, namun *dictionary attack* menggunakan *wordlist* rockyou.txt tidak berhasil menemukan kata sandi jaringan. Selain itu, *access point* palsu berhasil dibuat sehingga perangkat pengguna dapat terhubung ke jaringan palsu pada beberapa lokasi pengujian. Hasil evaluasi mengidentifikasi empat kerentanan dengan tingkat risiko kritis, yaitu intersepsi *four-way handshake*, tidak adanya *mutual authentication*, tidak tersedianya mekanisme deteksi *rogue access point*, serta kerentanan pengguna terhadap *evil twin attack*. Berdasarkan hasil tersebut, direkomendasikan penerapan WPA2/WPA3 Enterprise berbasis IEEE 802.1X, implementasi *Wireless Intrusion Detection System* (WIDS) atau *Wireless Intrusion Prevention System* (WIPS), serta peningkatan edukasi pengguna untuk memperkuat keamanan jaringan nirkabel SSID Undiksha Event.

Kata kunci: keamanan jaringan nirkabel, *penetration testing*, PTES, *cracking the encryption*, *evil twin attack*.

SECURITY EVALUATION OF THE UNDIKSHA EVENT SSID WIRELESS NETWORK USING THE PENETRATION TESTING EXECUTION STANDARD (PTES) METHOD

By
Junaidi, Student ID 1915101041
Bachelor of Computer Science Study Program

ABSTRACT

This study aims to evaluate the security of the Undiksha Event SSID wireless network at Universitas Pendidikan Ganesha using the Penetration Testing Execution Standard (PTES) methodology. The research employed a descriptive approach based on the PTES phases, including pre-engagement, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation, and reporting. Data were collected through interviews, observations, and documentation, while the exploitation phase applied Cracking the Encryption and Evil Twin Attack techniques. The results indicate that the four-way handshake was successfully captured; however, the dictionary attack using the rockyou.txt wordlist failed to recover the wireless network password. In addition, a rogue access point was successfully created, allowing user devices to connect to the fake network at several testing locations. The evaluation identified four critical-risk vulnerabilities: interception of the four-way handshake, the absence of mutual authentication, the lack of a rogue access point detection mechanism, and users' susceptibility to Evil Twin attacks. Based on these findings, the study recommends implementing WPA2/WPA3 Enterprise based on the IEEE 802.1X standard, deploying a Wireless Intrusion Detection System (WIDS) or Wireless Intrusion Prevention System (WIPS), and enhancing user security awareness to strengthen the security of the Undiksha Event SSID wireless network.

Keywords: *wireless network security, penetration testing, PTES, cracking the encryption, evil twin attack.*