INTISARI

Keamanan jaringan wi-fi menjadi perhatian utama dalam dunia teknologi informasi, terutama terhadap ancaman serangan packet sniffing yang dapat mencuri data sensitif pengguna salah satunya seperti username dan password. Penelitian ini bertujuan untuk menganalisis tingkat keamanan jaringan wi-fi di Universitas Perwira Purbalingga terhadap potensi serangan packet sniffing. Pengujian dilakukan menggunakan metode eksperimen dengan teknik penetration testing menggunakan beberapa tools, seperti InSSIDer untuk pemindaian jaringan wi-fi, Ettercap untuk serangan arp spoofing, Nmap untuk pemindaian port terbuka, Low Orbit Ion Cannon (LOIC) untuk serangan DDoS, serta Wireshark untuk analisis lalu lintas data. Hasil penelitian menunjukkan bahwa serangan arp spoofing tidak berhasil menangkap aktivitas target, mengindikasikan adanya perlindungan dalam jaringan. Pengujian port scanning menemukan beberapa port terbuka yang berpotensi menjadi titik masuk bagi penyerang. Pengujian DDoS attack menunjukkan bahwa sistem mengalami gangguan yang ditandai dengan penurunan responsivitas layanan.

Kata kunci: Keamanan Jaringan, Wi-fi, Packet Sniffing, Penetration Testing.

ABSTRACT

Wi-fi network security is a major concern in the world of information technology, especially against the threat of packet sniffing attacks that can steal sensitive user data, one of which is username and password. This research aims to analyze the security level of the wi-fi network at Perwira Purbalingga University against potential packet sniffing attacks. Tests were conducted using experimental methods with penetration testing techniques using several tools, such as InSSIDer for wi-fi network scanning, Ettercap for arp spoofing attacks, Nmap for open port scanning, Low Orbit Ion Cannon (LOIC) for DDoS attacks, and Wireshark for data traffic analysis. The results showed that the arp spoofing attack was unsuccessful in capturing the target activity, indicating the presence of protection in the network. Port scanning tests found several open ports that could potentially be entry points for attackers. DDoS attack testing showed that the system experienced a disruption characterized by a decrease in service responsiveness.

Keywords: Network Security, Wi-fi, Packet Sniffing, Penetration Testing.