INTISARI

Pengujian Konfigurasi Keamanan Jaringan Wi-Fi terhadap Ancaman Deauthentication dan Evil Twin: Studi Eksperimen Berbasis ESP8266

Nayaka Iman Wiraputra
21/482203/SV/19910

Perkembangan teknologi jaringan nirkabel (*wireless*) telah memberikan kemudahan akses komunikasi data, namun juga menimbulkan tantangan baru dalam aspek keamanan. Salah satu ancaman yang umum terjadi adalah serangan *Deauthentication* dan *Evil Twin* yang memanfaatkan kelemahan pada protokol IEEE 802.11. Penelitian ini bertujuan untuk menguji dan menganalisis efektivitas kedua jenis serangan tersebut dengan memanfaatkan modul ESP8266 sebagai perangkat utama, *Access Point* TP-Link WR840N sebagai target, serta adaptor TP-Link TL-WN722N untuk memantau lalu lintas jaringan menggunakan Wireshark pada sistem operasi Kali Linux. Metodologi penelitian meliputi perancangan skenario serangan, implementasi skrip *Deauther* dan *Evil Twin* pada ESP8266, pengujian fungsionalitas, serta evaluasi performa berdasarkan parameter kuantitatif seperti tingkat keberhasilan pemutusan koneksi klien, waktu respon serangan, tingkat keberhasilan pencurian kredensial, dan pengaruh jarak terhadap efektivitas serangan. Hasil pengujian menunjukkan bahwa serangan *Deauthentication* memiliki efektivitas tertinggi pada jarak dekat dengan tingkat pemutusan koneksi mencapai 100%, sedangkan serangan *Evil Twin* berhasil mencuri kredensial korban dengan tingkat keberhasilan bergantung pada kesadaran pengguna.

Kata kunci*: Deauther, Evil Twin, ESP8266,* Jaringan Nirkabel

ABSTRACT

Wi-Fi Network Security Configuration Testing against Deauthentication and Evil Twin Threats: An Experimental Study Based on ESP8266

Nayaka Iman Wiraputra
21/482203/SV/19910

The development of wireless network technology has provided ease of access to data communication but has also introduced new challenges in terms of security. One common threat is the Deauthentication and Evil Twin attack, which exploits vulnerabilities in the IEEE 802.11 protocol. This research aims to test and analyze the effectiveness of these two types of attacks by utilizing the ESP8266 module as the main device, a TP-Link WR840N Access Point as the target, and a TP-Link TL-WN722N adapter to monitor network traffic using Wireshark on the Kali Linux operating system. The research methodology includes designing attack scenarios, implementing Deauther and Evil Twin scripts on the ESP8266, conducting functionality testing, and evaluating performance based on quantitative parameters such as client disconnection success rate, attack response time, credential theft success rate, and the effect of distance on attack effectiveness. The results show that the Deauthentication attack is most effective at close range, with a client disconnection success rate of up to 100%, while the Evil Twin attack successfully captured victim credentials with a success rate highly dependent on user awareness

Keywords: Deauther, Evil Twin, ESP8266, Wireless Network