RANCANG BANGUN *REMOTE-EVIL-TWIN-ATTACK* BERBASIS OPENWRT DAN TAILSCALE UNTUK ANALISIS PAKET DATA JARINGAN WI-FI MENGGUNAKAN ARKIME

Yuha Nazhif Zuhair[1], Dedy Hariyadi[2]

INTISARI

Latar Belakang: Jaringan Wi-Fi berkembang pesat pada era saat ini yang dapat meningkatkan risiko terhadap serangan siber yaitu serangan *Man in the Middle* (MitM) dengan teknik *Evil Twin Attack* yang dapat mencuri paket data korban. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan alat uji keamanan jaringan Wi-Fi dengan mensimulasikan *Evil Twin Attack* berbasis OpenWRT yang dapat diakses secara *remote* menggunakan Tailscale dan menangkap paket data dalam format .pcap untuk dianalisis menggunakan Arkime.

Tujuan: Penelitian ini bertujuan untuk mengembangkan alat uji jaringan Wi-Fi berbasis OpenWRT dan Tailscale untuk mensimulasikan *Evil Twin Attack* serta analisis paket data jaringan Wi-Fi menggunakan Arkime.

Metode Penelitian: Penelitian ini mengadopsi metode *Cyber Kill Chain* (CKC) yang terdiri dari *Reconnaissance* (Pengintaian), *Weaponization* (Persiapan Alat Uji dan Sistem Pengujian), *Exploitation* (Eksploitasi atau Pengujian Sistem), dan *Actions on Objectives* (Tindakan untuk Tujuan Akhir).

Hasil: Pengembangan alat uji keamanan jaringan Wi-Fi berbasis OpenWRT dan Tailscale berhasil mensimulasikan *Evil Twin Attack* dan mendapatkan hasil paket data dalam format .pcap menggunakan *tools tcpdump*. Analisis paket data dalam format .pcap menggunakan Arkime mampu mengidentifikasi jumlah korban, sesi komunikasi yang diakses, dan data sensitif yang dikirimkan oleh korban melalui *port* 80. Namun, tidak ditemukan data sensitif korban pada hasil analisis.

Kesimpulan: Hasil pengujian menunjukkan pengembangan alat uji berhasil mensimulasikan *Evil Twin Attack* secara *remote* dan mendapatkan hasil paket data dalam format .pcap untuk dianalisis menggunakan Arkime.

Kata-kunci: Jaringan Wi-Fi, *Man in the Middle* (MitM), *Evil Twin Attack*, OpenWRT, Tailscale, Arkime, *Cyber Kill Chain* (CKC), *remote*, *tcpdump*, .pcap

1 Mahasiswa Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta

2 Dosen Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta

DESIGN OF REMOTE-EVIL-TWIN-ATTACK BASED ON OPENWRT AND TAILSCALE FOR WI-FI NETWORK DATA PACKET ANAYSIS USING ARKIME

Yuha Nazhif Zuhair[1], Dedy Hariyadi[2]

ABSTRACT

***Background**: Wi-Fi networks are growing rapidly in the current era which can increase the risk of cyber attacks, namely Man in the Middle (MitM) attacks with Evil Twin Attack techniques that can steal victim data packets. Therefore, this study aims to develop a Wi-Fi network security testing tool by simulating an OpenWRT-based Evil Twin Attack that can be accessed remotely using Tailscale and capturing data packets in .pcap format for analysis using Arkime.*

***Objective**: This research aims to develop a Wi-Fi network test tool based on OpenWRT and Tailscale to simulate Evil Twin Attack and analyze Wi-Fi network data packets using Arkime.*

***Method**: This research adopts the Cyber Kill Chain (CKC) method which consists of Reconnaissance, Weaponization (Preparation of Test Equipment and Testing Systems), Exploitation (Exploitation or System Testing), and Actions on Objectives (Actions for the Final Goal).*

***Result**: The development of a Wi-Fi network security testing tool based on OpenWRT and Tailscale successfully simulated the Evil Twin Attack and obtained the results of data packets in .pcap format using the tcpdump tool. Analysis of data packets in .pcap format using Arkime was able to identify the number of victims, communication sessions accessed, and sensitive data sent by the victim via port 80. However, no sensitive victim data was found in the analysis results.*

***Conclusion**: The test results show that the development of the test tool successfully simulated the Evil Twin Attack remotely and obtained data packet results in .pcap format for analysis using Arkime.*

***Keywords**: Wi-Fi network, Man in the Middle (MitM), Evil Twin Attack, OpenWRT, Tailscale, Arkime, Cyber Kill Chain (CKC), remote, tcpdump, .pcap*

1 *Undergraduate Student of Information Technology Study Program, Faculty of Engineering and Information Technology, General Achmad Yani University, Yogyakarta*

2 *Lecturer of the Bachelor of Information Technology Study Program, Faculty of Engineering and Information Technology, General Achmad Yani University, Yogyakarta*