BAB 1
PENDAHULUAN

1.1 Latar Belakang

Jaringan nirkabel adalah jenis jaringan komputer dengan perangkat yang saling terhubung dan berkomunikasi menggunakan teknologi gelombang elektromagnetik. Gelombang elektromagnetik merupakan gelombang yang dapat merambat tanpa memerlukan medium perantara, tetapi gelombang elektromagnetik dapat membawa medan magnet dan energi listrik. Gelombang elektromagnetik digunakan untuk media transmisi jaringan nirkabel, seperti *Infrared*, *Bluetooth*, *Wireless Fidelity* (Wi-Fi), WiMax, Seluler, Satelit, dan Balon Google. Wi-Fi adalah teknologi yang dapat menghubungkan dua atau lebih perangkat dalam satu jaringan dengan jangkauan sekitar 30 meter dari *Access Point* (AP). AP adalah perangkat yang memancarkan sinyal atau jaringan dengan teknologi Wi-Fi. Dengan memanfaatkan AP, Wi-Fi menjadi salah satu teknologi yang digunakan dalam jaringan nirkabel berdasarkan standar *Institute of Electrical and Electronics Engineers* (IEEE) 802.11. Pada standar IEEE 802.11, frekuensi Wi-Fi yang digunakan adalah 2,4GHz dan 5GHz (Wibowo dkk., 2022).

Jaringan nirkabel dengan teknologi Wi-Fi meningkat pesat di era saat ini dan digunakan berbagai bidang maupun instansi untuk mengirim dan menerima data tanpa media kabel. Dengan berkembang pesatnya jaringan Wi-Fi, terdapat kerentanan pada sistem komunikasi dan perangkat (Faishol dkk., 2024). Salah satu bentuk kerentanan jaringan Wi-Fi adalah serangan *Man in the Middle* (MitM) (Aman, 2023). Serangan MitM adalah jenis serangan siber yang dilakukan oleh

penyerang saat dua pihak yang sedang berinteraksi atau berkomunikasi. Serangan MitM bertujuan untuk menyusup, menyadap, hingga mengambil paket data yang sedang ditransmisikan. Dampak dari serangan MitM meliputi kebocoran data, kehilangan privasi, dan pencurian identitas (Auliafitri dkk., 2024).

Serangan MitM merupakan ancaman serius yang dapat merugikan individu maupun instansi, di mana penyerang dapat menyadap atau mencuri paket data seperti video, audio, gambar, dan dokumen. Teknik yang digunakan dalam serangan MitM meliputi *Sniffing*, ARP *Spoofing*, DNS *Spoofing*, SSL *Stripping*, dan *Evil Twin Attack*, yang memungkinkan penyerang mendapatkan akses tidak sah terhadap komunikasi pengguna. Serangan MitM dapat dijadikan sebagai indikator pengujian kerentanan keamanan siber (Auliafitri dkk., 2024). Penelitian yang dilakukan di Universitas Sriwijaya membahas tentang pengujian serangan MitM sebagai indikator pengujian kerentanan keamanan siber, yaitu melakukan deteksi pola serangan MitM pada jaringan *Supervisory Control and Data Acquisition* (SCADA) menggunakan algoritma *decision tree* dan deteksi serangan MitM pada *Smart Home* menggunakan metode algoritma *K-Nearest Neighbor* (Farhan, 2021; Sadifatiasmi, 2024).

Sebagai indikator pengujian kerentanan keamanan siber pada jaringan Wi-Fi, serangan MitM diimplementasikan menggunakan teknik *Evil Twin Attack*. *Evil Twin Attack* adalah teknik serangan MitM dengan membuat *Service Set Identifier* (SSID) palsu yang meniru jaringan Wi-Fi asli. Perangkat pengguna yang berada di dekat jaringan dari *Evil Twin Attack* secara tidak sengaja akan terhubung pada jaringan *Evil Twin Attack* dengan asumsi bahwa perangkat pengguna terhubung ke jaringan Wi-Fi asli (Aman, 2023). Menurut penelitian yang dilakukan di Universitas Jenderal Achmad Yani Yogyakarta membahas tentang pengujian keamanan jaringan Wi-Fi menggunakan *Evil Twin Attack* dengan membuat SSID palsu yang meniru jaringan Wi-Fi asli. Dampak dari *Evil Twin Attack* yang dibuat

meliputi pencurian informasi data pengguna. Penelitian tersebut menggunakan Raspberry Pi 3 dengan sistem pengoperasian Linux (Ubuntu 20.04) dan *tools* Wi-Fi Pumpkin untuk pengujian serangan *Evil Twin Attack* dan analisis jaringan Wi-Fi. Namun, pada penelitian ini perlu mempertimbangkan *hardware*, sistem pengoperasian, dan *tools* yang dapat melakukan analisis dengan skala yang besar serta alat pengujian yang lebih kompleks dan fleksibel (Sadewo, 2023).

Pada penelitian sebelumnya masih diperlukan solusi yang lebih optimal untuk mengembangkan alat uji keamanan jaringan Wi-Fi yang mampu menangkap dan menganalisis paket data jaringan dengan skalabilitas yang besar. Berdasarkan permasalahan dari penelitian sebelumnya, maka penelitian ini bertujuan untuk mengembangkan alat uji keamanan jaringan Wi-Fi dengan menerapkan teknik *Evil Twin Attack* yang lebih kompleks berbasis *Single Board Computer* berupa Raspberry Pi dan OpenWRT yang dikonfigurasi untuk dapat diakses jarak jauh secara *remote* melalui Mesh *Virtual Private Network* (VPN) menggunakan Tailscale. Penelitian yang diusulkan juga menggunakan *tools* Arkime untuk analisis paket data jaringan Wi-Fi dengan skalabilitas yang besar. Raspberry Pi dan OpenWRT diusulkan untuk saling terintegrasi agar sistem pengoperasian yang dirancang sebagai perangkat jaringan Wi-Fi dan menangkap paket data jaringan Wi-Fi dalam format .pcap secara *remote* menggunakan Tailscale, selanjutnya menggunakan *tools* Arkime untuk analisis paket data jaringan Wi-Fi dalam format .pcap.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, penelitian sebelumnya masih memerlukan solusi yang lebih optimal dalam mengembangkan alat uji keamanan jaringan Wi-Fi yang dapat dirancang dan diintegrasikan untuk melakukan pengujian dan penangkapan paket data yang dapat dikendalikan secara *remote* menggunakan teknologi Mesh VPN agar alat uji dapat diakses dimana saja

menggunakan internet, yang selanjutnya dilakukan analisis paket data jaringan Wi-Fi dengan skalabilitas yang besar

1.3 Batasan Penelitian

Batasan penelitain bertujuan unutk memperjelas ruang lingkup penelitian agar tidak melebar. Berikut batasan penelitian dari penelitian ini:

1. Pengembangan alat uji menggunakan Raspberry Pi 4 Model B yang dikonfigurasi dengan sistem pengoperasian OpenWRT.
2. Layanan integrasi keamanan komunikasi menggunakan Tailscale untuk melakukan *remote* alat uji penelitian.
3. Penangkapan paket data jaringan Wi-Fi disimpan melalui *mounting Secure Shell File System* (SSHFS) yang diintegrasikan dengan Server Arkime.
4. Analisis paket data jaringan Wi-Fi menggunakan Arkime.
5. Pengujian dilakukan selama sumber daya habis di setiap masing – masing lokasi, dikarenakan perangkat alat uji yang digunkan dalam penelitian ini menggunakan Baterai sebagai sumber daya utama.

1.4 Pertanyaan Penelitian

Berdasarkan perumusan masalah, maka dapat diuraikan sebagai pertanyaan penelitian, diantaranya:

1. Bagaimana cara mengembangkan alat uji *remote Evil Twin Attack* berbasis Raspberry Pi dan OpenWRT yang terintegrasi untuk pengujian dan penangkapan paket data jaringan Wi-Fi yang dapat dikendalikan jarak jauh melalui jaringan internet menggunakan Tailscale, serta analisis paket data jaringan Wi-Fi menggunakan Arkime?
2. Bagaimana cara melakukan pengujian keamanan jaringan Wi-Fi dengan mensimulasikan serangan MitM dengan menggunakan teknik *Evil Twin Attack*?

1.5 Tujuan Penelitian

Berdasarkan penelitian yang diusulkan, penelitian ini bertujuan, sebagai berikut:

1. Mengembangkan alat uji *remote Evil Twin Attack* berbasis Raspberry Pi dan OpenWRT yang terintegrasi untuk pengujian dan penangkapan paket data jaringan Wi-Fi yang dapat dikendalikan jarak jauh melalui jaringan internet menggunakan Tailscale, serta analisis paket data jaringan Wi-Fi menggunakan Arkime.
2. Melakukan pengujian keamanan jaringan Wi-Fi dengan mensimulasikan serangan MitM dengan menggunakan teknik *Evil Twin Attack*.

1.6 Manfaat Hasil Penelitian

Pada penelitian ini diharapkan dapat memberikan manfaat dalam perancangan alat uji keamanan jaringan Wi-Fi dengan menarapkan teknik *Evil Twin Attack* berbasis OpenWRT dan Tailscale yang terintegrasi dan Arkime untuk analisis paket data jaringan Wi-Fi dengan skala besar, diantaranya:

1. Menghasilkan peralatan pengujian keamanan jaringan Wi-Fi yang dapat dikendalikan secara jarak jauh atau *remote* melalui jaringan internet dengan teknologi Mesh VPN.
2. Memberikan edukasi kepada pengguna jaringan Wi-Fi tentang bahaya serangan MitM dengan teknik *Evil Twin Attack* pada jaringan Wi-Fi.
3. Menghasilkan analisis dari pengujian keamanan jaringan Wi-Fi dengan skalabilitas yang besar.