BAB 1
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan aspek krusial dalam teknologi informasi, terutama pada sistem komunikasi nirkabel yang semakin banyak digunakan di berbagai sektor seperti pendidikan, bisnis, dan rumah tangga. Kemudahan akses jaringan WiFi publik sering kali tidak diimbangi dengan kesadaran pengguna akan risiko keamanan yang ada. Salah satu bentuk ancaman nyata yang sering terjadi adalah *Evil Twin attack*, yakni serangan yang menciptakan *access point* palsu dengan nama dan tampilan yang menyerupai jaringan asli. Pengguna yang tidak waspada akan secara otomatis terhubung ke jaringan palsu tersebut, membuka peluang terjadinya pencurian data melalui serangan *Man-in-the-Middle* (MITM).

Salah satu kasus nyata dilaporkan oleh *BleepingComputer*, (2024) di mana seorang pria di Australia menjalankan jaringan *Evil Twin* selama penerbangan domestik untuk mencuri kredensial *email* dan media sosial penumpang. Fenomena ini menandakan pentingnya pengujian keamanan terhadap jaringan WiFi publik guna memahami seberapa mudah serangan semacam ini dilakukan dan dampak yang ditimbulkannya.

Penelitian terdahulu oleh (Sigit dkk., 2024) menunjukkan bahwa simulasi *Evil Twin* dapat diimplementasikan menggunakan perangkat berbiaya rendah seperti ESP8266 dengan memanfaatkan *deauthentication attack* dan *captive portal* sebagai media simulasi serangan terhadap jaringan nirkabel. Implementasi tersebut menunjukkan bahwa perangkat mikrokontroler mampu digunakan sebagai media *penetration testing* pada jaringan WiFi. Namun, berdasarkan hasil eksplorasi terhadap implementasi tersebut dan beberapa *firmware Evil Twin* yang tersedia, diketahui adanya kendala teknis yang mendasar pada arsitektur perangkat kerasnya. Berdasarkan spesifikasi fisik pabrikan, mikrokontroler tunggal seri ESP hanya dilengkapi dengan satu buah antarmuka *radio transceiver* Wi-Fi. Modul radio tunggal ini memiliki keterbatasan karena tidak dapat memproses mode *Monitor* (untuk menyuntikkan paket *deauthentication*) dan mode *Access Point* (untuk memancarkan *captive portal*) secara simultan dan stabil tanpa memicu kelebihan

beban sistem. Kondisi tersebut menjadi kendala ketika sistem dikembangkan agar proses pemutusan koneksi target terhadap *access point* asli tetap berlangsung selama proses pengalihan koneksi menuju *access point* palsu.

Berdasarkan permasalahan keterbatasan fisik modul radio tersebut, pada penelitian ini diimplementasikan sistem *Evil Twin* menggunakan dua mikrokontroler ESP32 yang memiliki pembagian fungsi. ESP32-S3 difungsikan sebagai pengendali utama yang menangani antarmuka pengguna, pemindaian jaringan (*scanning*), pemancaran *access point* palsu (*Evil Twin*), serta penyediaan *web server* untuk *captive portal*. Sedangkan ESP32 difungsikan secara khusus untuk menjalankan operasi radio tingkat rendah, meliputi *deauthentication attack*, *packet sniffing*, dan *WPA handshake capture*. Kedua mikrokontroler dihubungkan melalui komunikasi serial UART dengan protokol komunikasi yang dirancang untuk mendukung pertukaran perintah dan data. Melalui pendekatan arsitektural tersebut, proses *deauthentication attack* dapat terus dipertahankan oleh modul radio pendamping selama *access point* palsu dan *captive portal* tetap beroperasi pada modul utama, sehingga skenario pengujian keamanan dapat diimplementasikan sesuai dengan kebutuhan operasional.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

1) Bagaimana mengimplementasikan simulasi serangan *Evil Twin* menggunakan arsitektur mikrokontroler ganda berbasis ESP32?
2) Bagaimana efektivitas serangan *deauthentication* dalam memutus koneksi perangkat target dari jaringan asli?
3) Bagaimana efektivitas implementasi *captive portal* dalam menangkap kredensial target?
4) Bagaimana fitur *packet sniffing* dapat diimplementasikan untuk menghasilkan berkas PCAP yang dapat dianalisis menggunakan perangkat lunak Wireshark?

1.3 Batasan Masalah

Adapun batasan masalah dalam pembuatan proyek akhir ini adalah:

1) Perangkat keras yang digunakan terdiri dari dua buah mikrokontroler, yaitu ESP32-S3 yang berfungsi sebagai pengendali utama, pemancar *Evil Twin*, dan penyedia *web server* untuk *captive portal*, serta ESP32 yang berfungsi sebagai unit pemrosesan radio untuk *deauthentication attack*, *packet sniffing*, dan penangkapan *WPA handshake*. Kedua perangkat terhubung melalui komunikasi serial UART.
2) Sistem beroperasi secara *standalone*. Proses penyimpanan dan pengunduhan luaran pengujian berupa kredensial pengguna serta data tangkapan dalam format PCAP dan HCCAPX dikelola melalui *web server* internal perangkat tanpa memerlukan koneksi internet selama proses pengujian.
3) Fitur *packet sniffing* dirancang untuk menangkap paket data nirkabel dan menyusunnya ke dalam format standar PCAP.
4) Ruang lingkup target pengujian terbatas pada perangkat jaringan nirkabel yang beroperasi di frekuensi 2.4 GHz serta menggunakan protokol keamanan WPA (*Wi-Fi Protected Access*) dan WPA2, menyesuaikan dengan spesifikasi modul radio bawaan *chip* ESP32 dan batasan kemampuan eksploitasi sistem.
5) Pengujian alat wajib dilakukan pada lingkungan laboratorium tertutup atau terhadap jaringan yang telah memiliki izin sah, guna mematuhi etika pengujian keamanan (*penetration testing*).
6) Fokus penelitian dibatasi pada implementasi dan pengujian teknik *Evil Twin* beserta fitur pendukungnya tanpa membahas mekanisme pertahanan jaringan secara mendalam.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan dari penelitian ini adalah:

1) Mengimplementasikan sistem *Evil Twin* berbasis arsitektur dua mikrokontroler ESP32.
2) Menguji efektivitas serangan *deauthentication* dalam memutus dan mengarahkan perangkat target beralih ke *access point* palsu.
3) Menerapkan sistem *captive portal* yang dirancang untuk menangkap kredensial akses jaringan secara otomatis.

4) Mengimplementasikan fitur *packet sniffing* untuk menghasilkan berkas PCAP yang dapat dianalisis menggunakan perangkat lunak Wireshark.

1.4.2 Manfaat

Adapun manfaat dari penelitian ini adalah:

1. Memberikan pemahaman teknis yang komprehensif mengenai mekanisme serangan *Evil Twin* dan metode penangkapan paket data (*sniffing*) menggunakan komponen mikrokontroler berbiaya rendah.
2. Menjadi referensi dalam pengembangan perangkat *penetration testing* jaringan nirkabel berbasis ESP32 yang menerapkan pembagian fungsi menggunakan dua mikrokontroler dan komunikasi serial UART.
3. Membantu meningkatkan kesadaran pengguna dan administrator jaringan mengenai bahaya akses jaringan WiFi publik dan pentingnya penerapan protokol keamanan nirkabel yang lebih mutakhir.