BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan Wi-Fi telah menjadi solusi utama dalam menyediakan konektivitas yang cepat dan fleksibel. Namun, di balik manfaatnya, Wi-Fi juga memiliki sejumlah tantangan keamanan yang perlu mendapatkan perhatian serius. Salah satu kerentanan utama pada protokol IEEE 802.11, yang menjadi standar jaringan Wi-Fi, adalah serangan deauthentication frame.

Serangan ini memanfaatkan kerentanan pada manajemen frame Wi-Fi, di mana frame yang tidak terenkripsi dapat dimanipulasi atau dipalsukan oleh pihak tidak bertanggung jawab. Dalam serangan ini, penyerang mengirimkan frame deauthentication palsu ke *Access Point* (AP) atau klien untuk memutus koneksi perangkat dari jaringan Wi-Fi. Akibatnya, pengguna kehilangan akses jaringan, yang dapat mengganggu produktivitas, menciptakan peluang untuk serangan lebih lanjut, atau bahkan menyebabkan gangguan pada layanan publik yang rentan [2].

Sebuah sistem IDS (Intrusion Detection System) berbasis NodeMCU ESP8266 untuk mendeteksi frame Deauthentication dan frame Disassociation. Dengan mengandalkan teknik algoritma threshold-based detection yang bekerja dengan dua lapis pengecekan threshold, yaitu filter paket WiFi berdasarkan tipe frame (0xA0 = deauthentication, 0xC0 = disassociation) dan jika jumlah paket deauthentication/disassociation melebihi 5 paket/de tik (PKT_RATE), sistem mendeteksi adanya serangan.

Peneliti menilai bahwa perlindungan standar seperti WPA2 tidak cukup memadai untuk menangani serangan ini. Walaupun protokol WPA3 dengan *Protected Management Frames* (PMF) memberikan solusi potensial, adopsi teknologi ini masih lambat karena keterbatasan kompatibilitas perangkat dan kurangnya kesadaran pengguna. Akibatnya, jaringan publik dan perangkat IoT terus berada dalam risiko [2].

Peneliti menganggap bahwa ketersediaan Akses Poin yang mendukung WPA3 sangat terbatas dan sangat jarang sekali ditemukan di Café, Halte, atau tempat umum lainnya. Selain itu harga dari router yang mendukung fitur WPA3 serta PMF cenderung mahal, ini membuat kekhawatiran kepada pengusaha yang berpotensi terdampak serangan deauthentication ini dikarenakan pengetahuan yang terbatas, belum lagi penyedia layanan provider tidak langsung memberikan akses poin yang lebih aman ketika pertama kali memasang Wi-Fi disuatu tempat tanpa memikirkan keamanan jaringan publik [22].

1.2 Rumusan Masalah

1. Seberapa efektif deteksi NodeMCU ESP8266 sebagai Intrusion Detection System dalam mendeteksi serangan deauthentication frame?
2. Seberapa penting keamanan Proteksi Manajemen Frame pada ESP32 NAT Router dalam jaringan lokal?

1.3 Batasan Masalah

1. Penelitian menggunakan Access Point Pribadi TL-WA855RE.
2. ESP32 NAT Router menggunakan frekuensi 2.4Ghz.
3. Jarak deteksi dari Nodemcu ESP8266 5-6 meter.
4. Wemos D1 ESP8266 hanya berperan sebagai Penetration Tools.
5. Nodemcu hanya sebagai detector, tidak memberikan detail IP/MAC serta Destination.
6. Nodemcu ESP8266 hanya dapat menangkap paket dalam format 802.11 Wi-Fi frames, tidak mencakup alamat IP.

1.4 Tujuan Penelitian

Peneliti bertujuan memberikan kesadaran terhadap pengguna jaringan bahwa keamanan jaringan publik sangatlah penting meski dianggap remeh atau kurang diperhatikan, sekaligus bertujuan meningkatkan keamanan transmisi data secara nirkabel dengan biaya yang lebih murah dan efisien pada lalu lintas jaringan.

1.5 Manfaat Penelitian

1. Bagi Penyedia Layanan (*Public Space*): Memudahkan Penyedia layanan untuk menjaga kualitas jaringan yang stabil, aman, dan terjamin.
2. Bagi Peneliti dan Akademisi: Memberikan referensi dalam bidang Teknologi khususnya IoT sekaligus tambahan dan kemajuan penelitian kedepan agar banyak peneliti terutama cyber security untuk bisa mendevelop atau mengembangkan keamanan jaringan di ruang publik.
3. Bagi Masyartakat Umum: Memberikan pemahaman tentang bagaimana jaringan internet khususnya WLAN memiliki kerentanan terhadap serangan dan menjadikan ini untuk meningkatkan kewaspadaan masyarakat luas tentang bahaya nya *cyber attack* pada skala kecil maupun besar terhadap jaringan publik.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN, bagian ini menjelaskan latar belakang penelitian, menyoroti pentingnya keamanan jaringan di ruang publik dengan meningkatkan kewaspadaan ke masyarakat ataupun pengguna jaringan publik. Adapun rumusan masalah, batasan penelitian, serta tujuan utama, yaitu mengukur efektivitas dan waktu respon sistem dalam mendeteksi Deauthentication Frame. Selain itu, manfaat penelitian dibahas dari segi akademik dan praktis untuk menunjukkan kontribusinya dalam bidang Internet of Things dan Cyber Security.

BAB II TINJAUAN PUSTAKA, tinjauan pustaka berisi berbagai referensi dan teori dasar yang mendukung penelitian, termasuk penelitian terdahulu yang relevan dengan penelitian ini. Konsep Frame Detection, IDS (*Intrusion Detection System)*, serta NAT Router dalam menghubungkan banyak client ke dalam satu jaringan juga memperdalam pengetahuan dan pemahaman mengenai protokol keamanan atau jaringan yang digunakan.

BAB III METODE PENELITIAN, bagian ini menjelaskan tahapan penelitian yang dilakukan, mencakup identifikasi objek penelitian, perancangan alur penelitian, analisis kebutuhan sistem, serta pemilihan alat dan bahan yang digunakan. Setiap tahapan disusun secara sistematis untuk memastikan pengembangan Wi-Fi alternatif ESP32 NAT Router dan detektor frame NodeMCU ESP8266 berjalan sesuai dengan tujuan penelitian.

BAB IV HASIL DAN PEMBAHASAN, hasil pengembangan dan pengujian aplikasi disajikan dalam bab ini, mencakup model deteksi dengan berbagai Reason Code Deauthentication Frame serta implementasi ESP32 NAT Router. Proses pengujian dilakukan untuk mengukur efektivitas deteksi dan akurasi waktu respon ketika serangan terjadi. Data yang diperoleh dianalisis untuk menilai efektivitas metode yang digunakan serta mengidentifikasi potensi peningkatan di masa mendatang. Disaat bersamaan mengajak masyarakat untuk berpindah ke jaringan yang lebih aman.

BAB V PENUTUP, kesimpulan dari penelitian dirangkum berdasarkan tujuan yang telah ditetapkan, termasuk performa sistem dalam mendeteksi Deauthentication framed dan ESP32 NAT Router sebagai NAT Router. Hasil pengujian mengenai efektivitas dan akurasi waktu respon dipaparkan, sementara saran diberikan untuk pengembangan lebih lanjut, seperti peningkatan akurasi melalui teknik Intrusion Detection System atau pengembangan fitur tambahan guna meningkatkan sistem keamanan jaringan publik (WLAN).