BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang semakin pesat dalam era transformasi digital telah mengubah hampir seluruh aktivitas manusia, termasuk dalam dunia pendidikan. Saat ini, internet bukan lagi sekadar fasilitas tambahan, melainkan sudah menjadi kebutuhan utama yang sangat menentukan kelancaran kegiatan akademik. Mahasiswa dan dosen memanfaatkan jaringan internet untuk berbagai aktivitas seperti praktikum, riset, pengembangan sistem informasi, pembelajaran berbasis digital, akses jurnal ilmiah, pengumpulan tugas melalui *Learning Management System* (LMS), hingga komunikasi dan kolaborasi melalui platform daring. [1] Perkembangan teknologi informasi menuntut kebutuhan akan perancangan keamanan jaringan yang efektif guna melindungi infrastruktur komunikasi, khususnya router, dari serangan *brute force*. Serangan *brute force* merupakan metode yang umum digunakan oleh penyerang untuk mencoba kombinasi *password* secara berulang hingga berhasil masuk ke dalam sistem.

Dalam kondisi tersebut, ketersediaan jaringan yang stabil, cepat, dan dapat diandalkan menjadi salah satu faktor penting dalam menunjang kualitas layanan pendidikan. Salah satu infrastruktur yang paling banyak digunakan adalah *Wireless Local Area Network* (WLAN) atau jaringan WiFi. WLAN dipilih karena sifatnya yang fleksibel, mudah diakses, dan mampu mendukung mobilitas pengguna tanpa harus bergantung pada kabel jaringan. Namun, di balik kemudahan tersebut, WiFi juga memiliki tantangan yang cukup besar terutama pada aspek keamanan, karena aksesnya yang terbuka memungkinkan siapa saja mencoba untuk terhubung. [2] *Wireless Local Area Network* (WLAN) menggunakan akses *tethering* tidak cukup aman untuk digunakan. Perihal ini dibuktikan dari hasil pengujian tersebut berupa data yang didapatkan dari dampak serangan itu berupa *Username, Password*, dan situs yang diakses oleh target menunjukkan bahwa keamanan jaringan *Wireless*

Local Area Network (WLAN) menggunakan akses tethering tidak aman dan perlu untuk di tingkatkan.

Di lingkungan Laboratorium Teknik Informatika Politeknik Negeri Bengkalis, WiFi merupakan sarana utama yang mendukung kegiatan belajar mengajar serta aktivitas praktikum. Hampir seluruh perangkat mahasiswa maupun dosen terhubung melalui jaringan nirkabel, mulai dari laptop, *smartphone*, hingga perangkat pendukung lain seperti IoT dan alat uji jaringan. Tingginya jumlah perangkat yang terhubung setiap harinya membuat jaringan WiFi laboratorium menjadi salah satu komponen vital yang harus dijaga kualitas dan keamanannya. Apabila jaringan mengalami gangguan atau disalahgunakan, maka proses praktikum dan kegiatan akademik lainnya akan terganggu, bahkan dapat menyebabkan kerugian baik secara teknis maupun operasional.

Permasalahan yang sering muncul pada jaringan WiFi laboratorium adalah sulitnya mengidentifikasi siapa pengguna sebenarnya yang sedang terhubung. Dalam banyak kasus, perangkat dapat terkoneksi tanpa identitas pengguna yang jelas, sehingga aktivitas di jaringan menjadi sulit dilacak. Kondisi ini membuka peluang terjadinya berbagai bentuk penyalahgunaan jaringan, seperti penggunaan *bandwidth* secara berlebihan, akses ke layanan internal tanpa izin, serta potensi tindakan ilegal yang dilakukan oleh pihak yang tidak bertanggung jawab. Ketika tidak ada sistem autentikasi pengguna yang kuat, administrator jaringan juga akan kesulitan menentukan langkah penanganan jika terjadi insiden keamanan.

Selain itu, jaringan WiFi yang tidak memiliki pengamanan optimal sangat rentan terhadap serangan jaringan. Beberapa ancaman yang umum terjadi di jaringan nirkabel antara lain *brute force attack* untuk menebak kata sandi WiFi, *sniffing* untuk menyadap lalu lintas data, hingga serangan *rogue access point* yaitu pembuatan WiFi palsu yang meniru jaringan resmi agar pengguna terkecoh dan memasukkan kredensial mereka. Serangan seperti ini dapat menyebabkan kebocoran data, pencurian akses, hingga mengganggu performa jaringan secara keseluruhan. Jika dibiarkan, kondisi ini akan menjadi masalah serius karena laboratorium merupakan lingkungan yang menyimpan berbagai data penting, termasuk data akademik dan sistem internal.

WPA (*Wi-Fi Protected Access*) dan WPA2 merupakan standar keamanan jaringan nirkabel yang dikembangkan untuk meningkatkan perlindungan terhadap akses tidak sah. Sistem ini menggunakan metode enkripsi dan otentikasi yang lebih kuat dibandingkan pendahulunya, yaitu WEP (*Wired Equivalent Privacy*). WPA2-PSK (*Pre-Shared Key*) menggunakan sandi yang sama untuk semua pengguna dan sangat umum diterapkan pada jaringan rumah maupun jaringan kantor kecil. Meskipun mudah diimplementasikan, sistem ini memiliki kelemahan dalam skenario dengan banyak pengguna karena sulit dilakukan pengendalian individual.[3] Namun, secara umum WPA/WPA2-PSK tetap menjadi pilihan dasar.Saat ini, sebagian besar jaringan WiFi masih mengandalkan metode keamanan tradisional seperti WPA2-PSK (*Pre-Shared Key*), yaitu sistem yang menggunakan satu kata sandi bersama untuk semua pengguna. Walaupun metode ini mudah diterapkan, namun memiliki kelemahan yang cukup besar. Kata sandi yang digunakan bisa saja bocor atau dibagikan secara bebas, sehingga pengguna di luar lingkungan laboratorium tetap dapat mengakses jaringan. Selain itu, WPA2-PSK tidak dapat membedakan siapa pengguna yang sedang terhubung, karena semua orang memakai kunci yang sama. Hal ini membuat kontrol akses menjadi lemah, dan apabila terjadi pelanggaran, sulit untuk mengetahui pelakunya secara spesifik.

Sebagai upaya meningkatkan keamanan, standar terbaru yaitu WPA3-SAE (*Simultaneous Authentication of Equals*) hadir sebagai solusi yang lebih kuat dibandingkan WPA2. WPA3-SAE dirancang untuk memberikan perlindungan yang lebih baik terhadap serangan *offline dictionary attack*, serta meningkatkan keamanan proses autentikasi WiFi. Dengan mekanisme yang lebih modern, WPA3 membuat jaringan nirkabel menjadi lebih sulit untuk ditembus hanya dengan menebak kata sandi, sehingga risiko pembobolan dapat ditekan. Walaupun demikian, penerapan WPA3-SAE saja belum sepenuhnya menyelesaikan masalah utama, yaitu identitas pengguna. Sebagai solusi, *Wi-Fi Alliance* memperkenalkan WPA3 dengan mekanisme autentikasi *Simultaneous Authentication of Equals* (SAE) yang berbasis *Password Authentication Key Exchange*, WPA3-SAE dirancang untuk meningkatkan perlindungan terhadap serangan kamus,

penyadapan, serta memberikan *forward secrecy*. Secara teknis, WPA3-SAE menawarkan tingkat keamanan yang lebih tinggi dibandingkan WPA2. [4]

Oleh karena itu, dibutuhkan pendekatan keamanan yang lebih modern dan relevan dengan kondisi saat ini, yaitu konsep *Zero-Trust Security*. *Zero-Trust* adalah pendekatan keamanan yang menekankan prinsip bahwa tidak ada perangkat atau pengguna yang secara otomatis dipercaya, meskipun mereka berada di dalam jaringan internal. Konsep ini dirangkum dalam prinsip utama: *"Never trust, always verify"*. Artinya, setiap permintaan akses harus diverifikasi terlebih dahulu, dan setiap pengguna harus melewati proses autentikasi yang jelas sebelum diberi izin untuk menggunakan layanan jaringan.

Penerapan *Zero-Trust* pada jaringan WiFi laboratorium dapat dilakukan dengan menggabungkan beberapa teknologi keamanan agar tercipta sistem yang berlapis dan lebih terkontrol. Salah satu kombinasi yang efektif adalah penggunaan WPA3-SAE, RADIUS, dan *Captive Portal*. WPA3-SAE berperan sebagai perlindungan pada lapisan fisik/link agar koneksi WiFi lebih aman. Kemudian, RADIUS (*Remote Authentication Dial-In User Service*) digunakan untuk melakukan autentikasi pengguna secara individual menggunakan kredensial yang terdaftar, sehingga setiap pengguna memiliki identitas yang jelas. Selanjutnya, *Captive Portal* dapat berfungsi sebagai kontrol akses berbasis web yang memaksa pengguna melakukan login terlebih dahulu sebelum dapat mengakses internet, sekaligus menjadi sarana monitoring aktivitas pengguna.

Dengan menggabungkan ketiga mekanisme tersebut, sistem keamanan jaringan WiFi laboratorium akan menjadi lebih kuat karena menerapkan autentikasi berlapis. Setiap perangkat harus berhasil terkoneksi secara aman menggunakan WPA3, kemudian setiap pengguna tetap harus diverifikasi melalui sistem login berbasis akun. Pendekatan ini membuat administrator lebih mudah mengatur siapa saja yang berhak menggunakan jaringan, membatasi akses pengguna tertentu, serta melakukan pencatatan aktivitas untuk kebutuhan audit dan penanganan insiden.

Berdasarkan permasalahan dan kebutuhan tersebut, penerapan *Zero-Trust* WiFi *Access* berbasis WPA3-SAE, RADIUS, dan *Captive Portal* menjadi langkah strategis untuk meningkatkan keamanan WLAN di Laboratorium Teknik

Informatika Politeknik Negeri Bengkalis. Sistem ini diharapkan mampu mencegah akses ilegal, mengurangi risiko serangan jaringan, menjaga kualitas layanan internet, serta menciptakan lingkungan akademik yang lebih aman dan terkendali. Dengan jaringan yang aman dan stabil, kegiatan praktikum, pembelajaran, serta pengembangan sistem dapat berjalan lebih efektif dan mendukung kemajuan institusi dalam menghadapi era digital yang terus berkembang.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, maka rumusan masalah dalam penelitian ini adalah:

1. Apa saja masalah keamanan yang terjadi pada jaringan WiFi di Laboratorium Teknik Informatika Politeknik Negeri Bengkalis?
2. Siapa saja yang dapat menggunakan jaringan WiFi tersebut, dan siapa yang bisa saja menyalahgunakan atau menyerang jaringan?
3. Di mana letak kelemahan sistem keamanan jaringan yang sedang digunakan saat ini?
4. Kapan risiko serangan seperti pembobolan *password* (*brute force*), penyadapan data (*sniffing*), atau WiFi palsu (*rogue access point*) bisa terjadi?
5. Bagaimana cara meningkatkan keamanan jaringan WiFi laboratorium dengan menerapkan sistem *Zero-Trust* yang menggabungkan WPA3-SAE, RADIUS, dan *Captive Portal*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Menganalisis kelemahan sistem keamanan jaringan WiFi (WLAN) yang masih menggunakan metode WPA2-PSK di Laboratorium Teknik Informatika Politeknik Negeri Bengkalis.
2. Mengidentifikasi potensi ancaman dan serangan jaringan seperti *brute force*, *sniffing*, dan *rogue access point* yang dapat mengganggu keamanan serta kestabilan jaringan.

3. Merancang dan mengimplementasikan sistem keamanan jaringan berbasis konsep *Zero-Trust* dengan mengintegrasikan WPA3-SAE, RADIUS, dan *Captive Portal*.

1.4 Batasan Masalah

Agar penelitian tetap fokus, beberapa batasan diterapkan, yaitu:

1. Ruang lingkup penelitian hanya difokuskan pada jaringan WiFi (WLAN) di Laboratorium Teknik Informatika Politeknik Negeri Bengkalis, sehingga tidak mencakup jaringan di gedung atau unit lain.
2. Teknologi yang diterapkan dibatasi pada integrasi WPA3-SAE, RADIUS, dan *Captive Portal* berbasis konsep *Zero-Trust* untuk meningkatkan autentikasi dan kontrol akses pengguna.
3. Pengujian keamanan hanya mencakup simulasi serangan umum seperti *brute force attack, sniffing, dan rogue access point* untuk melihat efektivitas sistem yang dirancang.

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1.5.1 Bagi Penulis

1. Menambah wawasan dan pemahaman tentang perancangan serta implementasi keamanan jaringan berbasis konsep *Zero-Trust*.
2. Meningkatkan keterampilan teknis dalam konfigurasi WPA3-SAE, RADIUS, dan *Captive Portal.*
3. Mengembangkan kemampuan analisis dalam mengidentifikasi serta mengatasi permasalahan keamanan jaringan WiFi.
4. Menjadi sarana penerapan ilmu yang telah diperoleh selama perkuliahan ke dalam bentuk implementasi nyata.

1.5.2 Bagi Institusi

1. Memberikan rekomendasi peningkatan sistem keamanan jaringan WiFi di Laboratorium Teknik Informatika.
2. Membantu meningkatkan keamanan, stabilitas, dan kualitas layanan internet untuk mendukung kegiatan akademik.

3. Menjadi referensi dalam pengembangan kebijakan keamanan jaringan berbasis autentikasi terpusat dan terkontrol.
4. Mendukung terciptanya lingkungan pembelajaran yang lebih aman dan kondusif.

1.5.3 Bagi Bidang Ilmu

1. Menambah referensi ilmiah dalam pengembangan keamanan jaringan nirkabel berbasis *Zero-Trust*.
2. Memberikan gambaran implementasi integrasi WPA3-SAE, RADIUS, dan *Captive Portal* dalam lingkungan pendidikan.
3. Menjadi bahan kajian atau rujukan untuk penelitian selanjutnya di bidang keamanan jaringan komputer.