BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi jaringan telah menjadi salah satu komponen utama dalam mendukung masyarakat untuk memperoleh dan mengelola informasi. Jaringan internet, khususnya yang berbasis nirkabel (*wireless*), semakin dibutuhkan oleh berbagai kalangan, mulai dari siswa, mahasiswa, tenaga pendidik, hingga pekerja di lingkungan perkantoran (Anam & Fachri, 2025). Berdasarkan laporan *Digital 2022 October Global Statshot Report* yang diterbitkan oleh We Are Social dan Hootsuite, jumlah pengguna internet di seluruh dunia pada Oktober 2022 tercatat mencapai 5,07 miliar orang atau sekitar 63,45% dari total populasi global, meningkat sebesar 3,89% dibandingkan periode yang sama pada tahun sebelumnya (Simon Kemp, 2022). Pesatnya perkembangan teknologi informasi di bidang siber, khususnya pada infrastruktur jaringan nirkabel, turut meningkatkan potensi ancaman pencurian data dan informasi sehingga diperlukan penilaian keamanan sistem secara menyeluruh sebagai langkah pencegahan (Astrida et al., 2022).

Jaringan nirkabel (*wireless*) merupakan bentuk hubungan telekomunikasi yang memanfaatkan gelombang elektromagnetik sebagai media transmisi data tanpa menggunakan kabel fisik(’Sastya Hendri Wibowo, 2022). Kemudahan yang ditawarkan oleh teknologi *Wireless Local Area Network* (WLAN) menjadikannya sebagai pilihan utama dalam mengakses jaringan di berbagai lingkungan, seperti institusi pendidikan, perkantoran, dan fasilitas umum (Yudi mulyanto, 2022). Namun, karakteristik media transmisi nirkabel yang menggunakan gelombang radio menyebabkan proses pengiriman data lebih rentan terhadap penyadapan

dibandingkan jaringan berbasis kabel(’Sastya Hendri Wibowo, 2022). Kondisi ini menjadikan jaringan WLAN berpotensi menjadi sasaran berbagai jenis serangan siber yang dapat mengancam kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data, sehingga penerapan mekanisme keamanan yang memadai pada jaringan nirkabel merupakan suatu kebutuhan yang tidak dapat diabaikan (Muhana Nur & Aditya, n.d.)

Universitas Pendidikan Ganesha sebagai salah satu institusi pendidikan tinggi yang memanfaatkan teknologi informasi dalam mendukung kegiatan akademik dan administrasi memiliki infrastruktur jaringan nirkabel yang cukup luas. Salah satu jaringan yang digunakan adalah SSID Undiksha Event, yaitu jaringan Wi-Fi yang disediakan khusus untuk mendukung berbagai kegiatan seperti seminar, konferensi, pelatihan, rapat resmi, serta kegiatan akademik yang melibatkan banyak peserta. Pada saat kegiatan berlangsung, jaringan ini diakses secara bersamaan oleh banyak pengguna menggunakan berbagai perangkat seperti *laptop* dan *smartphone*, sehingga lalu lintas jaringan menjadi cukup tinggi dan kompleksitas pengelolaan jaringan pun meningkat. Tingginya intensitas penggunaan jaringan berpotensi memperbesar celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang, baik melalui penyadapan lalu lintas data, pemalsuan identitas jaringan, maupun upaya *cracking* terhadap mekanisme enkripsi yang digunakan (Muhana Nur & Aditya, n.d.).

Hingga saat ini, belum pernah dilakukan evaluasi keamanan secara sistematis terhadap jaringan SSID Undiksha Event, sehingga kondisi keamanan jaringan tersebut belum dapat diketahui secara menyeluruh. Tanpa adanya evaluasi yang terstruktur, pengelola jaringan tidak memiliki gambaran yang jelas mengenai

kerentanan yang ada, sehingga langkah perbaikan dan kebijakan keamanan yang tepat belum dapat diterapkan. Kondisi ini menunjukkan perlunya dilakukan pengujian keamanan yang komprehensif terhadap jaringan SSID Undiksha Event sebagai upaya proaktif dalam melindungi sistem informasi di lingkungan Universitas Pendidikan Ganesha.

Salah satu metode yang dapat digunakan untuk melakukan evaluasi keamanan jaringan secara sistematis adalah *penetration testing*, yaitu metode pengujian keamanan dengan cara mensimulasikan serangan yang dilakukan oleh pihak tidak berwenang untuk mengidentifikasi kelemahan pada sistem jaringan (Galang Saputra & Parga Zen, 2023). Dalam pelaksanaannya, *penetration testing* memerlukan kerangka kerja yang terstruktur agar pengujian dapat dilakukan secara terarah, menyeluruh, dan dapat dipertanggungjawabkan. Kerangka kerja yang digunakan dalam *penetration testing* adalah *Penetration Testing Execution Standard* (PTES), yaitu standar yang memberikan panduan sistematis dalam pelaksanaan *penetration testing* mulai dari tahap persiapan hingga pelaporan hasil pengujian (Dasmen et al., 2023). PTES dipilih karena mencakup tujuh tahapan yang komprehensif, yaitu *pre-engagement*, *intelligence gathering*, *threat modelling*, *vulnerability analysis*, *exploitation*, *post exploitation*, dan *reporting*, sehingga seluruh aspek keamanan jaringan dapat dievaluasi secara menyeluruh (Astrida et al., 2022).

Berdasarkan uraian tersebut, penelitian ini dilakukan untuk mengevaluasi tingkat keamanan jaringan nirkabel SSID Undiksha Event di Universitas Pendidikan Ganesha menggunakan metode *penetration testing* berbasis *Penetration Testing Execution Standard* (PTES). Hasil penelitian ini diharapkan

dapat memberikan gambaran yang komprehensif mengenai kondisi keamanan jaringan SSID Undiksha Event, mengidentifikasi kerentanan yang ada, serta memberikan rekomendasi perbaikan yang dapat diterapkan oleh pengelola jaringan dalam meningkatkan keamanan jaringan nirkabel di lingkungan Universitas Pendidikan Ganesha.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat diidentifikasi beberapa permasalahan sebagai berikut:

1. Jaringan nirkabel SSID Undiksha Event diakses oleh banyak pengguna secara bersamaan menggunakan berbagai perangkat pada saat kegiatan berlangsung, sehingga meningkatkan kompleksitas pengelolaan jaringan dan memperbesar potensi celah keamanan yang dapat dieksploitasi oleh pihak yang tidak berwenang.
2. Karakteristik media transmisi jaringan nirkabel yang menggunakan gelombang radio bersifat lebih terbuka dibandingkan jaringan berbasis kabel, sehingga rentan terhadap berbagai ancaman siber seperti penyadapan lalu lintas data, pemalsuan identitas jaringan, serangan pemutusan koneksi, dan upaya *cracking* terhadap mekanisme enkripsi yang digunakan.
3. Belum pernah dilakukan evaluasi keamanan secara sistematis terhadap jaringan nirkabel SSID Undiksha Event, sehingga kondisi keamanan jaringan tersebut belum dapat diketahui secara menyeluruh oleh pihak pengelola jaringan Universitas Pendidikan Ganesha.

4. Pengelola jaringan belum memiliki gambaran yang jelas mengenai kerentanan yang terdapat pada jaringan SSID Undiksha Event, sehingga langkah perbaikan dan kebijakan keamanan yang tepat belum dapat dirumuskan dan diterapkan.

1.3 Batasan Penelitian

Agar penelitian ini lebih terarah dan terfokus, maka ditetapkan batasan-batasan penelitian sebagai berikut:

1. Pengujian keamanan jaringan hanya dilakukan pada jaringan nirkabel dengan SSID Undiksha Event yang berada di lingkungan Universitas Pendidikan Ganesha, dan tidak mencakup jaringan atau SSID lain yang terdapat di lingkungan universitas tersebut.
2. Metode yang digunakan dalam penelitian ini adalah *penetration testing* dengan mengacu pada kerangka *Penetration Testing Execution Standard* (PTES).
3. Pengujian dilakukan secara langsung pada jaringan nyata setelah mendapatkan izin resmi dari pihak pengelola jaringan Universitas Pendidikan Ganesha, sehingga tidak melanggar ketentuan hukum dan etika yang berlaku.
4. Hasil penelitian berupa temuan kerentanan beserta rekomendasi perbaikan, dan tidak mencakup implementasi langsung dari solusi keamanan yang disarankan.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan maka ditemukan rumusan masalah sebagai berikut:

1. Bagaimana proses pengujian keamanan jaringan nirkabel SSID Undiksha Event menggunakan metode *penetration testing* berbasis *Penetration Testing Execution Standard* (PTES)?

2. Bagaimana hasil evaluasi keamanan jaringan nirkabel SSID Undiksha Event berdasarkan pengujian yang telah dilakukan menggunakan metode *penetration testing* berbasis *Penetration Testing Execution Standard* (PTES)?

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui proses pengujian keamanan jaringan nirkabel SSID Undiksha Event menggunakan metode *penetration testing* berbasis *Penetration Testing Execution Standard* (PTES).
2. Mengetahui hasil evaluasi keamanan jaringan nirkabel SSID Undiksha Event berdasarkan pengujian yang telah dilakukan menggunakan metode *penetration testing* berbasis *Penetration Testing Execution Standard* (PTES).

1.6 Manfaat Penelitian

Mengacu pada tujuan penelitian ini, maka diharapkan memberikan manfaat dari segi teoritis maupun praktis, yaitu:

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat menambah serta memperluas wawasan keilmuan dalam bidang keamanan jaringan komputer, khususnya terkait dengan penerapan metode *penetration testing* dalam mengevaluasi keamanan jaringan nirkabel.

2. Manfaat Praktis

   a. Bagi Pengelola Jaringan

   Hasil penelitian ini diharapkan dapat memberikan informasi mengenai kondisi keamanan jaringan nirkabel di Universitas Pendidikan Ganesha, khususnya

pada jaringan SSID Undiksha Event. Informasi mengenai celah keamanan yang ditemukan dapat dijadikan sebagai bahan pertimbangan bagi pengelola jaringan dalam melakukan perbaikan sistem keamanan serta penerapan kebijakan yang tepat untuk meningkatkan keamanan jaringan.

b. Bagi Peneliti

Penelitian ini diharapkan dapat memberikan pengalaman serta pemahaman praktis dalam menerapkan metode *penetration testing* untuk mengevaluasi keamanan jaringan nirkabel. Selain itu, penelitian ini juga dapat menjadi referensi dan bahan pembelajaran bagi peneliti dalam mengembangkan kemampuan analisis keamanan jaringan serta menjadi dasar bagi penelitian selanjutnya yang berkaitan dengan evaluasi keamanan jaringan.