BAB I

PENDAHULUAN

1.1 Latar belakang

Di zaman teknologi yang terus berkembang, model jaringan kabel atau jaringan komputer yang menggunakan kabel sebagai media distribusi informasi masih umum digunakan, tetapi lebih cenderung digunakan dalam lingkup lokal, seperti dalam satu gedung atau ruangan.(Al Farizi & Sugiantoro, 2022).

Koneksi jaringan dengan internet memiliki risiko keamanan yang intrinsik dan dapat dipantau oleh pihak yang tidak diinginkan, baik melalui jaringan *LAN* berbasis kabel maupun nirkabel. Oleh karena itu, keamanan jaringan menjadi aspek yang sangat penting. Keamanan jaringan harus menjadi perhatian utama karena pengguna atau peretas potensial dapat mencuri atau memodifikasi data ketika file atau informasi melewati berbagai terminal di jaringan. Untuk itu, diperlukan perencanaan dan pemahaman yang matang dalam membangun sistem keamanan jaringan yang terhubung ke internet. Tujuannya adalah melindungi sumber daya seperti file atau data secara efektif dan aman, serta mengurangi risiko serangan dari pihak yang tidak sah.

Fasilitas *WiFi* menjadi salah satu teknologi umum yang digunakan dalam jaringan komputer saat ini. Teknologi *WiFi* memungkinkan pengguna untuk terhubung ke jaringan secara nirkabel dan mengakses internet tanpa perlu menggunakan kabel. Meskipun memberikan kenyamanan, sifat nirkabel dari jaringan *WiFi* membuatnya rentan terhadap serangan *sniffing*. *Sniffing* adalah

metode yang digunakan untuk menangkap dan memonitor lalu lintas data yang melewati jaringan. (Hidayat et al., 2018).

Sniffer adalah sebuah aplikasi perangkat lunak ataupun perangkat keras yang digunakan untuk melaksanakan *sniffing*, yaitu memonitor lalu lintas data yang dikirimkan dan diterima melalui jaringan. Informasi yang dapat diakses melalui *Sniffer* meliputi *username*, *password*, dan data pribadi lainnya. Keberadaan serangan *sniffing* dapat menimbulkan risiko terhadap keamanan jaringan dan privasi pengguna. Penjahat siber dapat menggunakan *sniffing* untuk mencuri informasi pribadi seperti *username*, *password*, dan bahkan data kartu kredit. Selain itu, pengguna jaringan yang tidak sah juga dapat memanfaatkan serangan *sniffing* untuk memonitor aktivitas pengguna lainnya.(Hidayat et al., 2018).

Analisis keamanan jaringan diperlukan sebagai Langkah preventif untuk mencegah potensi serangan *sniffing* pada jaringan *WiFi*. Proses analisis keamanan jaringan mencakup pemeriksaan sistem keamanan jaringan, identifikasi potensi celah keamanan, dan perumusan strategi keamanan yang sesuai untuk melindungi jaringan dari serangan *sniffing.*

Wireshark merupakan alat pemantau paket yang digunakan untuk menganalisis protokol jaringan dan melakukan audit keamanan jaringan. Kemampuan Wireshark tidak hanya terbatas pada memblokir lalu lintas di jaringan lokal (*LAN*), namun juga mencakup akses terhadap kata sandi, serta penyadapan pada protokol-protokol umum yang aktif. Kehadiran *Wireshark* dapat membantu dalam penyelesaian masalah yang muncul dan mencegah terjadinya

insiden keamanan. Dengan demikian, *Wireshark* dapat dianggap sebagai aplikasi atau perangkat lunak untuk mengidentifikasi aktivitas yang mencurigakan.(Jaya et al., 2022)

PT ALFA SCORPII Tembesi telah menerapkan jaringan *LAN* dan W*LAN* sebagai sarana untuk berbagi data dan informasi terkait personel, layanan komersial atau publik, serta informasi penting lainnya. Setiap kamar dilengkapi dengan jaringan terpasang, walaupun *WiFi* di setiap kamar kerap kali rentan terhadap peretas atau orang yang tidak sengaja. Banyak pengguna jaringan *WiFi* yang tidak menyadari risiko terkait penggunaan titik akses nirkabel (WPA).

Ketika menangani kebutuhan jaringan komputer pribadi, kepentingan ini menjadi semakin vital dalam lingkup pekerjaan, pendidikan, serta kegiatan hiburan. Namun, dalam mengelola keamanan jaringan komputer pribadi, pengguna harus memahami bahwa dengan banyaknya akses masuk ke dalam jaringan, terdapat peluang besar bagi para peretas untuk melakukan tindakan kejahatan. Contohnya, peretas dapat mencuri data atau informasi penting yang berada dalam jaringan, atau bahkan menyebabkan gangguan dengan sengaja mematikan sumber daya jaringan. (Hidayat et al., 2018)

Untuk mengimplementasikan sistem keamanan jaringan yang handal, diperlukan analisis menyeluruh terhadap sistem keamanan yang ada. Hasil dari analisis tersebut dapat menjadi dasar untuk mengevaluasi efektivitas sistem keamanan jaringan. PT ALFA SCORPII Tembesi, terutama di divisi YAMAHA, telah menyediakan fasilitas jaringan nirkabel sebagai media pendukung untuk memenuhi kebutuhan informasi. Berdasarkan konteks ini, peneliti mengambil

judul penelitian. “**ANALISIS KEAMANAN JARINGAN PADA FASILITAS *WIFI* TERHADAP SERANGAN *SNIFFING*”**

1.2 Identifikasi masalah

Tingkat kegaga*LAN* merupakan isu yang terus menerus dihadapi dan menjadi fokus perhatian YAMAHA, PT ALFA SCORPII Tembesi. Beberapa permasalahan yang telah diidentifikasi antara lain:

1. Terdapat berbagai macam serangan yang dapat mengancam keamanan jaringan nirkabel (*Wi-Fi*).
2. Pada jaringan komputer atau internet nirkabel (*Wi-Fi*) dengan tingkat keamanan yang masih rendah, terdapat potensi kerentanan.
3. Belum adanya pendeteksi serangan di YAMAHA, PT ALFA SCORPII Tembesi

1.3 Batasan Masalah

Dalam penulisan skripsi ini, penulis memfokuskan analisis pada beberapa permasalahan, yakni:

1. Menganalisis keamanan jaringan nirkabel di YAMAHA, PT ALFA SCORPII Tembesi.
2. Melaksanakan pengujian terhadap keamanan jaringan nirkabel di YAMAHA, PT ALFA SCORPII Tembesi.
3. Melakukan pengujian dengan menggunakan perangkat Wireshark terhadap serangan *sniffing* pada paket data..

1.4 Rumusan Masalah

Dari hasil analisis masalah, rumusan permasalahan dapat diuraikan sebagai berikut:

1. Bagaimana cara menganalisis paket data dalam jaringan *WiFi* di YAMAHA, PT ALFA SCORPII Tembesi terkait dengan serangan *sniffing*?
2. Bagaimana mengevaluasi tingkat keamanan jaringan *WiFi* di YAMAHA, PT ALFA SCORPII Tembesi terhadap serangan *sniffing*??

1.5 Tujuan penelitian

1. Untuk mengetahui bagaimana metode analisis paket data pada jaringan *WiFi* di YAMAHA, PT ALFA SCORPII Tembesi terhadap serangan *sniffing*?
2. Untuk mengetahui bagaimana melakukan evaluasi terhadap tingkat keamanan jaringan *WiFi* di YAMAHA, PT ALFA SCORPII Tembesi terhadap serangan *sniffing*?

1.6 Manfaat penelitian

Keberhasilan penelitian ini terletak pada analisis keamanan jaringan pada fasilitas *Wi-Fi* terhadap serangan *sniffing* di YAMAHA, PT ALFA SCORPII Tembesi, yang memberikan manfaat yang signifikan.x

1.6.1 Secara teoritis

1. Sebagai informasi bagi karyawan atau pengguna layanan internet, terutama untuk pengguna umum, tentang potensi risiko dalam jaringan *LAN* yang tidak memiliki keamanan yang kuat.
2. Sebagai tambahan informasi untuk para peneliti dan sebagai upaya mendapatkan pemahaman praktis dalam menganalisis keamanan jaringan

pada fasilitas *Wi-Fi* terhadap serangan *sniffing* di YAMAHA, PT ALFA SCORPII Tembesi.

1.6.2 Secara praktis

Membantu mahasiswa memahami keamanan sistem pada jaringan *Wi-Fi* dan teknik analisis serta evaluasi kondisi keamanan, dengan tujuan agar mereka dapat lebih efisien dalam mengelola serta menjaga keamanan koneksi *Wi-Fi*.