# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Kemajuan teknologi informasi saat ini semakin pesat, dan teknologi ini telah menjadi hal yang biasa di kalangan masyarakat. Teknologi terus berkembang, yang mempermudah pekerjaan lembaga yang mengandalkan jaringan. Oleh karena itu, diperlukan alat yang mendukung perkembangan ini, seperti internet yang stabil. Namun, masalah keamanan sering menjadi perhatian utama dan harus diperiksa secara rutin. Informasi data yang diolah menjadi sangat berharga bagi penerima karena memberikan nilai penuh berupa keakuratan, ketepatan waktu, dan relevansi. (Tekino, 2020).

Internet adalah jaringan komunikasi yang menghubungkan jutaan orang yang terpisah oleh jarak dan waktu di seluruh dunia. Ini adalah jaringan publik dan global yang menyediakan koneksi langsung kepada siapa saja melalui Jaringan Area Lokal (LAN) dan Penyedia Layanan Internet (ISP).

Keamanan jaringan harus dikembangkan dan dijaga agar tidak ada yang membobol sebuah data-data di dalam server. Kegunaan keamanan jaringan berasal dari kebutuhan untuk melindungi data. Yang menjadi utama kehilangan data dan kerusakan, beberapa pihak tidak berwenang untuk mengakses atau mengubah data. penggunaan data.

PT. Pupuk Sriwidjaja Palembang adalah salah satu pabrik terbesar yang terletak di Pulau Sumatera. Saat ini, perusahaan memproduksi Ammoniak, Urea, dan NPK. Peralatan utama yang mereka gunakan memiliki fungsi untuk mendukung berbagai aspek kinerja, termasuk di antaranya komputer dan jaringan.

*Sniffing* dalam arti salah satu jenis kejahatan siber dengan cara memantau atau menangkap paket data yang melewati jaringan tertentu. Tujuan dari tindak kejahatan ini adalah mencuri data pribadi, seperti password, informasi akun, dan lainnya.

*Sniffing* terjadi ketika data ditransmisikan antara klien dan server (atau sebaliknya), di mana pihak yang tidak berwenang memperoleh nama pengguna dan kata sandi milik orang lain, baik dengan sengaja maupun tidak. Pelaku dapat memanfaatkan akun korban untuk melakukan tindakan penipuan atau merusak/menghapus data korban. Oleh karena itu, ketika Anda mengirim atau menerima data melalui koneksi internet, sangat penting untuk tetap waspada terhadap potensi adanya proses transmisi yang tidak aman atau keberadaan sniffer yang berusaha mencuri data (Pos et al. 2020).

Salah satu metode untuk melindungi data dari serangan sniffing adalah dengan menggunakan IPSec Tunnel melalui VPN yang diimplementasikan dengan autentikasi dan enkripsi. IPSec memiliki *Internet Key Exchange*(IKE) yang berfungsi sebagai mekanisme untuk membentuk IPSec tunnel.

Sebelum tunnel ini terbentuk, dilakukan peering dengan cara bernegosiasi mengenai metode keamanan yang digunakan oleh inisiator dan responden.

Beberapa penelitian sebelumnya mengenai keamanan siber mencakup studi oleh (H. Supriyono, J. A. Widjaya, dan A. Suparmi 2013) tentang penerapan *Virtual Private Network* (VPN) untuk mengamankan komunikasi data di PT Mega Besar Alami. Dengan cara ini, komunikasi data antara kantor pusat dan cabang dapat terhubung secara aman dari penyadapan.

Penelitian selanjutnya oleh (Sugiyatno dan Dina Atika 2018) mengkaji VPN SSTP menggunakan Raspberry Pi. Dalam penelitian ini, dilakukan pengujian keamanan yang menunjukkan bahwa VPN PPTP aman terhadap serangan *sniffing*. Hasil penelitian menunjukkan bahwa nama pengguna dan kata sandi yang digunakan untuk login tidak dapat diketahui oleh penyerang.

Berdasarkan uraian tersebut, penulis tertarik untuk meneliti masalah keamanan jaringan dari serangan sniffing. Oleh karena itu, penulismengambil judul **"PENERAPAN KEAMANAN JARINGAN DARI SERANGAN SNIFFING DI DEPARTEMEN LAYANAN TI PT. PUPUK SRIWIDJAJA (PUSRI) PALEMBANG."**

## 1.2 Rumusan Masalah

Dalam penelitian ini, terdapat perumusan masalah utama yaitu, "Bagaimana penerapan keamanan jaringan terhadap serangan *sniffing* di Departemen Layanan TI PT. Pupuk Sriwidjaja (Pusri) Palembang?"

## 1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah:

1. Keamanan jaringan yang dibahas yaitu menggunakan koneksi VPN IPSec
2. Menganalisis keamanan data VPN IPSec dari serangan *sniffing* pada sistem keamanan jaringan Departemen Layanan TI PT. Pupuk Sriwidjaja (Pusri) Palembang.

## 1.4 Tujuan Penelitian

Dari Penjelasan latar belakang serta rumusan masalah yang dipaparkan diatas, tujuan yang dilakukan penelitian ini unuk menganalisis kinerja keamanan data informasi yang dilakukan secara teratur jika pengguna menerapkan jaringan VPN IPSec dari beberapa ancaman *sniffing* yang ada pada jaringan internet.

## 1.5 Manfaat Penelitian

Beberapa manfaat yang akan diperoleh dalam penyusunan tugas akhir ini yaitu terdiri dari:

1. Dapat menunjang kinerja Departemen Layanan TI PUSRI pada keamanan jaringan.

2. Dapat melakukan pengecekan terhadapt kualitas sistem keamnaan jaringan yang diterapkan dari ancaman serangan *sniffing* yang ada pada jaringan internet.
3. Untuk peneiti bermanfaat untuk menambah ilmu pengetahuan dan mengasah skill menggunakan teknologi jaringan.
4. Untuk pembaca dapat dijadikan acuan untuk membuat analisis kinerja keamanan jaringan dari serangan *sniffing*

## 1.6 Penelitian Terdahulu

Penelitian terdahulu berfungsi sebagai upaya untuk mencari pembanding dan menemukan inspirasi baru bagi penelitian selanjutnya. Selain itu, penelitian sebelumnya juga berperan dalam mempromosikan penelitian yang akan dilakukan.

Penelitian sebelumnya yang dilakukan oleh Hidayat S (2022) bertujuan untuk mengoptimalkan RouterOS perusahaan agar dapat berfungsi sebagai jaringan Tunnel yang menghubungkan komunikasi data antara jaringan publik (internet) dan jaringan LAN kantor. Hal ini memungkinkan karyawan untuk mengakses sumber daya kantor tanpa terbatas oleh ruang dan waktu, sejalan dengan regulasi pemerintah dan kebijakan perusahaan.

Penelitian lain yang dilakukan oleh M. Novriansyah (2021) mengimplementasikan VPN Tunnel untuk mencegah Packet Sniffing menggunakan metode LP2TP/IPSec. Dalam penggunaan IPSec untuk

mengamankan paket data yang dikirim, proses pengiriman data menjadi lebih aman karena data yang terenkripsi dengan baik akan terlindungi dari gangguan.

Dalam penelitian yang dilakukan oleh Amarudin (2018), dilakukan analisis dan implementasi keamanan jaringan pada MikroTik RouterOS menggunakan metode port knocking. Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan dari penerapan keamanan jaringan pada perangkat router yang dikembangkan di Universitas Teknokrat Indonesia. Hasil penelitian menunjukkan bahwa sistem dapat beroperasi dengan baik dan mampu meningkatkan keamanan jaringan yang dibangun dibandingkan dengan jaringan yang tidak menerapkan metode *port knocking*. Keberhasilan ini ditunjukkan melalui autentikasi yang tepat saat mengaksesrouter, sesuai dengan peran yang telah ditentukan.

Dalam penelitian sebelumnya oleh Dina Olivia (2021), dilakukan analisis quality of service (QoS) pada jaringan Virtual Private Network (VPN) dengan menggunakan protokol IPSec di SMK Negeri 3 Pariaman. Penelitian ini bertujuan untuk mengevaluasi kualitas layanan jaringan VPN di sekolah menengah kejuruan tersebut, dengan mempertimbangkan parameter QoS seperti delay, packet loss, throughput, jitter, dan bandwidth. Hasil penelitian menunjukkan bahwa kualitas layanan jaringan VPN di SMK Negeri 3 Pariaman tergolong baik, sebagaimana dibuktikan dengan hasil pengukuran rata-rata yang memuaskan untuk parameter QoS tersebut.

Dengan demikian, jaringan VPN di SMK Negeri 3 Pariaman menunjukkan kualitas yang memuaskan.

Dalam penelitian yang dilakukan oleh R. Andriani (2022), dilakukan implementasi VPN pada Proxy Router menggunakan metode *Point to Point Tunneling Protocol* (PPTP) untuk memungkinkan karyawan tetap dapat mengakses jaringan lokal kantor dari jaringan eksternal secara aman dan lancar. Sebelum penerapan server VPN, keamanan dalam akses internet rentan terhadap penyadapan dan serangan, seperti login halaman *website, login router,* dan informasi saat transmisi data dapat dengan mudah diakses. Namun, dengan menggunakan server VPN menggunakan metode *Point to Point Tunneling Protocol* (PPTP), karyawan yang bekerja secara *Work From Home (WFH)* dapat terhubung dengan baik tanpa risiko akses tidak sah.

Pemilihan solusi yang sesuai terhadap tantangan di atas menjadi fokus utama dan topik pembahasan dalam penelitian ini, yakni melakukan Analisis Kinerja Keamanan Jaringan Dari Serangan Sniffing Di Departemen Layanan TI PT. Pupuk Sriwidjaja (Pusri) Palembang. Dalam penelitian sebelumnya ini, penulis menerapkan metode action research. Sesuai dengan Prasetyo, Hasanah, dan Wijaya (2022), metode ini terdiri dari lima tahapan yang membentuk siklus dari *action research* yaitu :

1. Diagnosa (Diagnosing).
2. Perencanaan tindakan (Action Planning).
3. Pelaksanaan tindakan (Action Taking).

4. Evaluasi (Evaluating).

5. Pembelajaran (Learning).