BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi semakin pesat khususnya di era modern seperti sekarang ini, seiring dengan berkembangnya teknologi. Dengan berkembangnya teknologi informasi saat ini, kebutuhan akan informasi semakin meningkat. Dimana setiap masyarakat membutuhkan informasi dalam waktu yang cepat, singkat, dan akurat. Oleh karena itu, diperlukan suatu alat yang dapat mendukung hal tersebut. Salah satunya adalah internet yang cepat dan stabil. Namun permasalahan yang sering muncul adalah faktor keamanan saat ini menjadi menjadi perhatian yang sangat penting. Sehingga diperlukan suatu metode untuk dapat memperoleh suatu informasi data , pertukaran data, dilakukan dengan aman dan stabil (Normah *et al*. 2022).

Internet merupakan sebuah jaringan komunikasi yang menghubungkan jutaan orang yang dipisahkan oleh jarak dan waktu dari seluruh belahan dunia. Internet adalah sebuah jaringan komunikasi public dan global yang menyediakan koneksi langsung kepada siapa saja melalui *Local Area Network (LAN)* dan *Internet Service Provider (ISP)*.

Keamanan database harus dikembangkan dan diutamakan agar tidak ada yang membobol sebuah data penting yang ada di dalam server.

Kebutuhan akan keamanan database berasal dari kebutuhan untuk melindungi data. Pertama, kehilangan data dan kerusakan data. Kedua, beberapa pihak tidak berwenang untuk mengakses atau mengubah data. Masalah lain termasuk melindungi data dari penundaan yang tidak semestinya dalam akses atau penggunan data, atau menyelesaikan masalah penolak layanan

PT. Pupuk Sriwidjaja merupakan salah satu perusahaan yang bergerak dalam industri manufacture berupa pupuk urea sebagai bahan bakunya. Departemen TI PT Pupuk Sriwidjaja (PUSRI) yang berada di Jl. Mayor Zen, Kalidoni Palembang adalah instansi milik negara yang menproduksi dan mengelola Pupuk urea Di Indonesia, instansi ini menggunakan *Storage Area Network (SAN)* sebagai penyimpanan data-data, Instansi tersebut menggunakan internet kabel dan *wireless* untuk mengolah data dan menginputnya ke *website* perusahaan. Bahaya yang tidak diharapakan bisa terjadi kapanpun tanpa sepengetahuan Pegawai/Staff ketika menggunakan jaringan *wireless*. Bahkan *Wifi* instansi tersebut bisa saja diretas oleh hacker. Berdasarkan hal tersebut, dengan maraknya kejahatan pada keamanan database salah satunya adalah *website* yang harus dikembangkan dan diutamakan agar tidak ada yang membobol sebuah data penting yang ada di dalam *website* server.

Sniffing dalam artian mengendus, sedangkan dalam ilmu keamanan siber, mengendus adalah tindakan menangkap paket data yang melewati jaringan. Sniffing attack berbahaya jika penyadap mengambil tindakan

atau memodifikasi paket data di jaringan, karena data dapat dicuri (Idi, Leiwakabessy, *and* Tentua 2023) Pencurian data tersebut dapat berdampak pada pihak tertentu. Data didapatkan penyerang dengan menggunakan serangan *sniffing* saat ada data yang dikirim melalui jaringan *wifi,hotspot*, server dan lain-lain. Agar tidak terjadi hal-hal tersebut, maka harus diterapkan keamanan database pada *storage area network.*

Sniffing dapat terjadi saat mengirim data dari *client* ke server (atau sebaliknya) , dimana pelaku mencuri username dan password orang lain secara sengaja maupun tidak sengaja. Pelaku kemudian dapat memakai akun korban untuk melakukan penipuan atas nama korban atau merusak/menghapus data milik korban. Karena itu, ketika Anda mengirim data atau menerima data melalui koneksi internet, Anda harus selalu waspada, tidak peduli apakah ada proses transmisi, apakah ada *sniffer* yang mencoba mencuri data (Pos *et al*. 2020).

Salah satu cara untuk mengamankan data dari serangan Sniffing tersebut menggunakan Ipsec Tunnel yang harus memakai VPN yang diimplementasikan sesuai otentikasi dan enkripsi. Pada IPSec terdapat *Internet Key Excharge* (IKE) yang befungsi sebagai mekanisme yang mana sebelum terbentuk sebuah IPSec tunnel maka akan dilakukan peering dengan melakukan negoisasi metode keamanan yang digunakan disisi intiator maupun responder.

Beberapa penelitian sebelumnya tetang keamanan siber antara lain penelitian (H. Supriyono, J A Widjaya, A. Suparmi 2013) tentang penerapan *Virtual Private Network* (VPN) untuk mengamankan komunikasi data pada PT Mega Besar Alami. Dengan demikian, komunikasi data antara kantor pusat dan cabang dapat terhubung dengan aman terhadap penyadapan.

Penelitian selanjutnya (Sugiyatno and Dina Atika 2018) *VPN* SSTP Menggunakan Raspberry Pi. Pada penelitiannya telah dilaukan pengujian keamanan yang menunjukkan VPN PPTP aman terhadap serangan *sniffing*, hal itu ditunjukkan pada hasil yang diperoleh bahwa *username* dan *password* yang digunakan untuk login tidak dapat diketahui oleh *attacker*.

Berdasarkan uraian tersebut maka dalam penulisan ini penulis tertarik untuk meneliti mengenai permasalahan keamanan database dari *packet sniffing*. Oleh karena itu penulis mengambil judul ***"IMPLEMENTASI KEAMANAN DATABASE DARI SERANGAN PACKET SNIFFING PADA DEPARTEMEN TI PT PUPUK SRIWIDJAJA"***

1.2 Rumusan Masalah

Pada penelitian ini terdapat rumusan permasalahan yang menjadi titik utama yaitu "Bagaimana menerapkan Keamanan Database dari Serangan *Packet Sniffing* pada Departemen TI PT Pupuk Sriwidjaja?".

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah :

1. Keamanan jaringan yang dibahas yaitu menggunakan koneksi VPN IPSec.
2. Menerapkan keamanan data VPN IPSec dari serangan *packet sniffing* pada sistem keamanan jaringan Departemen TI PT Pupuk Sriwidjaja.

1.4. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penilitian ini yaitu untuk Menerapkan keamanan data informasi yang dilakukan secara *real time* jika *user* menerapkan keamanan jaringan menggunakan VPN IPSec dari beberapa ancaman *packet sniffing* yang ada pada jaringan internet.

1.5 Manfaat Penelitian

Adapun manfaat hasil dari penilitian tersebut yaitu :

a. Bagi Penulis

   Menambah wawasan menerapkan keamanan data dan menerapkan ilmu yang telah diperoleh selama kuliah.

b. Bagi Instansi Perusahaan

   Supaya bisa melakukan pengecekan terhadap kualitas sistem keamanan jaringan yang diterapkan dari ancaman serangan *packet sniffing* yang ada pada jaringan internet.

c. Bagi Akademik

Sebagai referensi bagi para penulis lainnya untuk dijadikan sebagai Studi perbandingan dalam menysusun penelitian yang sejenis.

1.6 Penelitian Terdahulu

Penelitian terdahulu merupakan upaya penelitian untuk mencari pembanding kemudian menemukan inspirasi baru untuk penelitian selanjutnya. Selain itu penelitian sebelumnya membantu mempromosikan penelitian dan menunjukkan *orisinalitas* penelitian.

Adapun penelitian sebelumnya juga telah dilakukan oleh (Hidayat S : 2022) yaitu mengoptimalkan RouterOS yang dimiliki perusahaan agar dapat menjadi jaringan Tunnel yang dapat menjembatani komunikasi data antara jaringan publik (internet) dengan jaringan LAN kantor, sehingga karyawan dapat mengakses *resource* kantor tanpa batasan ruang dan waktu akibat regulasi pemerintah dan kebijakan perusahaan.

Penelitian lain juga dilakukan oleh (M Novriansyah : 2021) juga menerapkan VPN Tunnel untuk mencegah *Packet Sniffing* dengan metode LP2TP/IPSec. Untuk mengamankan paket data yang dikirim digunakan IPSec, sedangkan dengan IPSec VPN proses pengiriman data akan lebih aman tanpa adanya gangguan karena data yang telah dikirim telah dienkripsi dengan baik.

Pada peneltian yang dilakukan oleh (Amarudin : 2018) yaitu analisis dan implementasi keamanan jaringan pada mikrotik router OS menggunakan metode *port knocking,* yang bertujuan untuk mengetahui tingkah keamanan atas implementasi keamanan jaringan pada perangkat router yang telah dibangun di Universitas Teknoikrat Indonesia. Sehingga didapatkan hasil bahwa sistem dapat berjalan dengan baik dan dapat meningkatkan keamanan sistem jaringan yang dibangun dibandingkan pada jaringan yang tidak menerapkan keamanan *port knocking*. Hal ini dibuktikan dengan adanya autentikasi yang tepat saat mengakses router. Yaitu autentikasi yang sesuai dengan role yang telah dibangun.

Pada penelitian sebelumnya yang dilakukan oleh (Dina Olivia : 2021) yaitu Analisis *quality of service* (QoS) jaringan *Virtual Private Network* (VPN) dengan menggunakan protokol IPSec (Studi kasus : SMK Negeri 3 Pariaman), yang bertujuan untuk mengetahui, kualitas layanan jaringan VPN dengan memakai protokol IPSec di sekolah menengah kejuruan (SMK) Negeri 3 pariaman, dengan parameter QoS untuk mengetahui besar hasil pengukuran dari parameter *delay, packet loss,*

throughput, jitter, dan *bandwith.* Sehingga didapatkan hasil bahwa kualitas layanan jaringan VPN di SMK Negeri 3 Pariaman termasuk kedalam kategori jaringan yang berkualitas baik dibuktikan dengan hasil pengukuran penelitian memiliki nilai rata-rata memuaskan menggunakan parameter QoS *delay , packet loss, throughput, jitter* dan *bandwith* yang mana jaringan VPN di SMK Negeri 3 Pariaman memiliki kualitas yang memuaskan.

Pada penelitian yang dilakukan oleh (R Andriani : 2022) yaitu mengimplementasikan VPN pada Proxy Router dengan metode *Point to Point Tunneling Protocol* (PPTP) sehingga karyawan tetap dapat mengakses jaringan lokal kantor dari jaringan eksternal dengan aman dan lancar, dimana sebelum menerapkan server VPN keamanan dalam akses internet masih rentan terhadap penyadapan dan serangan, baik informasi berupa login halaman *website, login router*, maupun informasi saat transmisi data sangat mudah didapatkan. Sangat berbeda, ketika *user* menggunakan konerksi server VPN tindakan tersebut tidak dapat dilakukan lagi, dengan metode *Point to Point Tunneling Protocol* (PPTP) karyawan yang bekerja secara *Work From Home* (WFH) dapat saling terhubung dengan baik.

Pemilihan solusi yang tepat terhadap persoalan di atas menjadi tujuan dan pembahasan penulis dalam penelitian ini, yaitu diperlukan sebuah langkah Implementasi Keamanan Database Dari Serangan *Packet Sniffing* Pada Departemen TI PT Pupuk Sriwidjaja. Pada penelitian

terdahulu ini penulis menggunakan sebuah metode *action research.* Menurut (Prasetyo, Hasanah, dan Wijaya 2022)) ada lima tahapan dalam penelitian yang merupakan siklus dari *action research* yaitu:

1. Melakukan Diagnosa (*Diagnosing).*
2. Membuat Rencana Tindakan (*Action Planning).*
3. Melakukan Tindakan (*Action Tacking).*
4. Melakukan Evaluasi (*Evaluating).*
5. Pembelajaran (*Learning).*