**Tugas Individu**

**E-Commerce dan Pengembangan Web**

**Diaz Adha Asri Prakoso**

**0102518007**

* **Definisi Transport Layer Security**

Transport Layer Security (TLS) adalah protokol enkripsi yang digunakan untuk transmisi data di Internet. Protokol ini menjelaskan standar umum yang dapat diimplementasikan di lingkungan tertentu. Transport Layer Security adalah salah satu protokol enkripsi yang paling banyak digunakan. Selain mengangkut data antara browser dan server web, seperti halnya HTTPS, TLS juga digunakan untuk mengirim email, koneksi FTP dan VPN, serta pesan instan dan voice over IP. TLS digunakan terutama di daerah-daerah di mana data sensitif diperhatikan, seperti perbankan online, penyimpanan data pelanggan, kata sandi, dan komunikasi digital. Tujuannya adalah memastikan transmisi data yang aman dan untuk memastikan tingkat integritas pengguna komunikasi yang tinggi.

* **Adapun tujuan dari dibuatnya TLS ini diantaranya:**

1. Criptographic security
2. Interoperability
3. Extensibility
4. Relative Efficiency

* **Proses Kerjanya.**
  1. **TLS Record Protocol** – Tugas dari TLS Record Protocol ini adalah melakukan negoisasi koneksi antara client dan server. Meskipun protokol ini bisa digunakan tanpa menggunakan enkripsi namun protokol ini tetap menggunakan enkripsi dengan kunci kriptografi simetris untuk memastikan koneksi yang terjalin aman. Pengamanan koneksi ini menggunakan fungsi hash yaitu Message Authentication Code.
  2. **TLS Handshake Protocol** – Protokol ini akan mengijinkan adanya komunikasi antara client dan server apabila sudah ter-otentikasi. Sebelum adanya pengiriman data ada proses untuk menyamakan algoritma enkripsi dan kunci yang digunakan. Cara kerja dari proses handshake pada TLS ini sama dengan yang terjadi pada SSL.