Nama : Dominggus Louk

Nim : 20230801125

UJIAN TENGAH SEMESTER

Mata Kuliah : Keamanan Informasi

Kelas : KJ003

Hari tanggal : 20 Mei 2025

Laporan ESSAY

1. Jelaskan menurut anda apa itu keamanan informasi !

- Keamanan informasi adalah praktik **melindungi informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah.** Tujuannya adalah menjaga **kerahasiaan** (hanya diakses pihak berwenang), **integritas** (akurat dan tidak diubah), serta **ketersediaan** (selalu bisa diakses saat dibutuhkan) informasi. Ini penting untuk melindungi aset berharga, menghindari kerugian, dan menjaga reputasi di era digital.

2. Jelaskan menurut anda apa itu Confidentiality, Integrity dan Availability !

Confidentiality, Integrity, dan Availability (CIA Triad) adalah tiga prinsip inti keamanan informasi:

- **Confidentiality (Kerahasiaan)**

Memastikan informasi hanya diakses oleh pihak yang berwenang. Ini seperti kunci untuk brankas, menjaga data sensitif dari mata yang tidak berhak (misalnya, enkripsi data, *password*).

- **Integrity (Integritas)**

Memastikan informasi akurat, lengkap, dan tidak diubah tanpa izin. Ini tentang keaslian dan keandalan data (misalnya, *checksums*, tanda tangan digital).

- **Availability (Ketersediaan)**

Memastikan informasi dan sistem selalu bisa diakses dan digunakan saat dibutuhkan oleh pihak yang berwenang. Ini tentang kelancaran operasional (misalnya, *server* cadangan, rencana pemulihan bencana).

3. Sebutkan jenis-jenis kerentanan keamanan yang anda ketahui !

Kerentanan keamanan adalah **kelemahan** dalam sistem, *software*, *hardware*, atau proses yang bisa dieksploitasi penyerang.

Berikut jenis-jenis umumnya:

- **Kerentanan Aplikasi:** Cacat pada kode atau desain aplikasi (contoh: SQL Injection, XSS).
- **Kerentanan Sistem Operasi:** Celah pada OS itu sendiri (contoh: *buffer overflow*, *misconfiguration*).
- **Kerentanan Jaringan:** Kelemahan pada infrastruktur atau protokol jaringan (contoh: *weak encryption*, *open ports*).
- **Kerentanan Perangkat Keras:** Cacat pada desain *hardware* (contoh: *firmware vulnerabilities*).
- ***Misconfiguration*:** Pengaturan yang tidak aman.
- ***Weak Passwords*:** Penggunaan *password* yang mudah ditebak.
- ***Outdated Software/Firmware*:** Tidak memperbarui sistem dengan *patch* keamanan terbaru.
- ***Zero-Day Vulnerability*:** Kerentanan baru yang belum diketahui atau diperbaiki vendor.
- ***Human Error*:** Kesalahan atau kelalaian pengguna (contoh: *phishing*).

4. Pengamanan data bisa menggunakan hash dan encryption. Jelaskan apa yang anda ketahui terkait hash dan encryption !

Hash

***Hash* adalah fungsi satu arah yang mengubah data (teks, *file*) menjadi kode unik dengan panjang tetap, disebut *hash value* atau *digest*.**

- **Satu arah:** Anda tidak bisa mengembalikan *hash value* menjadi data aslinya.
- **Unik:** Perubahan sekecil apa pun pada data asli akan menghasilkan *hash value* yang sama sekali berbeda.

Fungsi utama: Memastikan integritas data. Jika *hash value* dari data yang diterima sama dengan *hash value* data aslinya, berarti data tidak diubah.

Contoh: Sidik jari digital untuk *file* atau untuk menyimpan *password* (yang disimpan adalah *hash* dari *password*, bukan *password* itu sendiri).

Encryption (Enkripsi)

***Encryption* adalah proses mengubah data asli (*plaintext*) menjadi bentuk yang tidak terbaca (*ciphertext*) menggunakan algoritma dan kunci.**

- **Dua arah:** Data terenkripsi bisa dikembalikan menjadi data asli dengan menggunakan kunci yang benar (proses dekripsi).
- **Kerahasiaan:** Tujuan utamanya adalah menjaga kerahasiaan data dari akses tidak sah.

Fungsi utama: Menjaga kerahasiaan data. Hanya pihak yang memiliki kunci yang bisa membaca data.

Contoh: Mengirim pesan rahasia yang hanya bisa dibaca oleh penerima yang punya kunci, atau mengunci *file* di komputer Anda sehingga hanya Anda yang bisa membukanya.

5. Jelaskan menurut anda apa itu session dan authentication !

Authentication (Autentikasi)

Autentikasi adalah proses verifikasi identitas pengguna. Ini adalah langkah pertama untuk memastikan siapa Anda sebenarnya.

- **Tujuan:** Memastikan Anda adalah orang yang Anda klaim.
- **Cara kerja:** Biasanya melibatkan kombinasi sesuatu yang Anda **tahu** (misal: *password*), **miliki** (misal: token keamanan), atau **adalah** Anda (misal: sidik jari).
- **Contoh:** Saat Anda memasukkan *username* dan *password* untuk masuk ke *email* atau akun media sosial.

Session (Sesi)

Sesi adalah periode waktu ketika pengguna yang sudah diautentikasi dapat terus berinteraksi dengan sistem tanpa perlu *login* ulang setiap kali.

- **Tujuan:** Memberikan kenyamanan dan efisiensi setelah pengguna berhasil diautentikasi.
- **Cara kerja:** Setelah berhasil *login* (autentikasi), sistem akan membuat "sesi" untuk Anda, seringkali dengan memberikan *token* sesi (misal: *cookie*) ke *browser* Anda. *Browser* akan mengirimkan *token* ini setiap kali Anda berinteraksi dengan situs, memberitahu situs bahwa Anda masih aktif dan sudah terautentikasi.
- **Contoh:** Setelah Anda *login* ke Facebook, Anda bisa menjelajah berbagai halaman tanpa perlu memasukkan *password* lagi sampai sesi Anda berakhir (misal: *logout* atau sesi *timeout*).

5. Jelaskan menurut anda apa itu privacy dan ISO !

Privacy (Privasi)

Privasi adalah hak individu untuk mengontrol informasi pribadi mereka dan bagaimana informasi tersebut dikumpulkan, digunakan, dan dibagikan. Ini tentang siapa yang boleh melihat dan melakukan apa dengan data Anda.

- **Tujuan:** Melindungi data pribadi dari akses atau penyalahgunaan yang tidak diinginkan.
- **Contoh:** Hak Anda agar nomor telepon, alamat rumah, atau riwayat medis Anda tidak dibagikan tanpa izin Anda.

ISO (International Organization for Standardization)

ISO adalah organisasi independen dan non-pemerintah yang mengembangkan standar internasional. Standar ini berlaku untuk berbagai industri dan membantu memastikan kualitas, keamanan, dan efisiensi produk, layanan, dan sistem.

- **Tujuan:** Menciptakan standar yang diakui secara global untuk konsistensi dan praktik terbaik.
- **Contoh: ISO 27001** adalah standar khusus untuk **Sistem Manajemen Keamanan Informasi (ISMS)**. Ini membantu organisasi mengelola keamanan informasi mereka secara sistematis, mencakup orang, proses, dan teknologi. Organisasi yang mengimplementasikan ISO 27001 menunjukkan komitmen terhadap keamanan informasi yang kuat.