JAWABAN UJIAN TENGAH SEMESTER KEMANAN INFORMASI KJ003

Dosen Pengampu:

HANI DEWI ARIESSANTI , S.Kom, M.Kom

Disusun Oleh:

Alfianita Ingsiany - 20210801173

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS ESA UNGGUL
TAHUN 2025

1. Jelaskan menurut anda apa itu keamanan informasi!

   Jawab:

   Keamanan informasi adalah cara untuk melindungi informasi dari berbagai ancaman agar tetap aman, terjaga kerahasiaannya, utuh, dan dapat diakses oleh pihak yang berwenang. Tujuan utama dari keamanan informasi yaitu memastikan bahwa data tidak disalahgunakan, diubah, atau diakses tanpa izin oleh pihak yang tidak berwenang.

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

   Jawab:

   Ketiga konsep ini dikenal sebagai CIA Triad, yaitu pilar utama dalam keamanan informasi:

   - Confidentiality (Kerahasiaan): Menjamin bahwa informasi hanya dapat diakses oleh pihak yang memiliki hak. Contohnya penggunaan password, enkripsi, dan otorisasi akses.
   - Integrity (Integritas): Menjamin bahwa informasi tidak diubah atau dimodifikasi tanpa izin. Data harus tetap konsisten dan akurat dari sumber hingga tujuan.
   - Availability (Ketersediaan): Menjamin bahwa informasi tersedia dan dapat diakses saat dibutuhkan oleh pihak yang berwenang. Contohnya seperti backup data dan sistem redundansi.

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

   Jawab:

   Beberapa jenis kerentanan keamanan informasi antara lain:

   - Phishing: Penipuan untuk mencuri data pribadi melalui email atau pesan palsu.
   - Malware: Program berbahaya seperti virus, worm, ransomware, atau trojan.
   - SQL Injection: Serangan terhadap database melalui celah input aplikasi.
   - Man-in-the-Middle Attack: Penyadapan komunikasi antara dua pihak.
   - Brute Force Attack: Upaya menebak password dengan mencoba semua kemungkinan.
   - Zero-Day Exploit: Serangan terhadap celah keamanan yang belum diketahui atau ditambal.

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

   Jawab:

   - Hash: Proses mengubah data menjadi rangkaian karakter tetap (biasanya dalam bentuk string hex) menggunakan algoritma tertentu seperti SHA-256. Hash bersifat satu arah, artinya hasil hash tidak bisa diubah kembali menjadi data aslinya. Digunakan untuk memastikan integritas data.
   - Encryption (Enkripsi): Proses mengubah data asli (plaintext) menjadi bentuk tidak terbaca (ciphertext) agar tidak bisa dimengerti oleh pihak yang tidak memiliki kunci. Enkripsi bisa bersifat simetris (menggunakan satu kunci) atau asimetris (menggunakan pasangan kunci publik dan privat).

5. Jelaskan menurut anda apa itu session dan authentication!

   Jawab:

   - Session: Merupakan periode interaksi aktif antara pengguna dan sistem, biasanya setelah pengguna berhasil login. Session memungkinkan sistem untuk mengenali pengguna selama waktu tertentu dan menyimpan status interaksi tersebut.
   - Authentication (Otentikasi): Proses untuk memastikan bahwa seseorang adalah benar-benar dirinya. Biasanya menggunakan kombinasi dari sesuatu yang diketahui (password), dimiliki (token), atau melekat (sidik jari, wajah).

6. Jelaskan menurut anda apa itu privacy dan ISO!

   Jawab:

   - Privacy (Privasi): Hak individu untuk mengontrol data pribadi mereka, termasuk siapa yang boleh mengakses, menggunakan, dan membagikan data tersebut. Dalam konteks digital, privasi penting untuk melindungi informasi sensitif dari penyalahgunaan.
   - ISO (International Organization for Standardization): Organisasi internasional yang mengembangkan standar-standar global, termasuk di bidang keamanan informasi. Contoh standar penting adalah ISO 27001, yang memberikan kerangka kerja untuk sistem manajemen keamanan informasi (ISMS).