Nama : Dhini Febrasari

Mata Kuliah : UTS (CIE406 – Keamanan Informasi)

ESSAY

1. Jelaskan menurut anda apa itu keamanan informasi!

   Ans :

   Keamanan informasi adalah upaya sistematis untuk melindungi data dan informasi dari berbagai ancaman, seperti akses tidak sah, perusakan, pencurian, atau manipulasi, dengan menerapkan kebijakan, prosedur, dan teknologi guna menjamin kerahasiaan, integritas, dan ketersediaan informasi bagi pihak yang berwenang.

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

   Ans :

   - *Confidentiality* memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang dan tidak bocor kepada pihak yang tidak berhak.
   - *Integrity* menjamin bahwa informasi tetap akurat, konsisten, dan tidak diubah secara tidak sah.
   - *Availability* memastikan bahwa informasi dan sistem selalu tersedia serta dapat diakses saat dibutuhkan oleh pengguna yang sah.

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

   Ans :

   - SQL Injection – Serangan yang memanfaatkan celah dalam input database untuk menjalankan perintah SQL berbahaya.
   - Cross-Site Scripting (XSS) – Menyisipkan skrip berbahaya ke dalam halaman web yang dilihat oleh pengguna lain.
   - Cross-Site Request Forgery (CSRF) – Memanfaatkan sesi login pengguna untuk melakukan aksi tanpa sepengetahuan mereka.
   - Buffer Overflow – Terjadi ketika program menulis data melebihi batas buffer, sehingga memungkinkan eksekusi kode berbahaya.
   - Broken Authentication – Cacat pada sistem otentikasi yang memungkinkan peretas mengambil alih akun pengguna.

- Sensitive Data Exposure – Data penting seperti kata sandi atau informasi kartu kredit tidak diamankan dengan baik.
- Misconfiguration Security – Pengaturan keamanan sistem atau aplikasi yang salah atau tidak lengkap.
- Malware – Perangkat lunak berbahaya seperti virus, worm, trojan, ransomware, dan spyware.
- Zero-Day Vulnerabilities – Kerentanan yang belum diketahui atau belum diperbaiki oleh vendor perangkat lunak.
- Phishing – Teknik manipulasi sosial untuk mencuri informasi sensitif dengan menyamar sebagai entitas tepercaya.

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

   Ans :

   Hash dan encryption adalah dua teknik penting dalam pengamanan data, namun memiliki fungsi dan cara kerja yang berbeda:

   - *Hash* adalah proses mengubah data menjadi nilai tetap (disebut hash value atau digest) menggunakan algoritma tertentu seperti SHA-256 atau MD5, di mana hasilnya bersifat satu arah (tidak bisa dikembalikan ke data aslinya) dan biasanya digunakan untuk verifikasi integritas data, seperti menyimpan password secara aman atau memverifikasi keaslian file.

   - *Encryption* adalah proses mengubah data asli (plaintext) menjadi bentuk tidak terbaca (ciphertext) menggunakan algoritma dan kunci tertentu, dengan tujuan agar data hanya bisa dibaca kembali oleh pihak yang memiliki kunci dekripsi yang sesuai; teknik ini digunakan untuk menjaga kerahasiaan data dalam komunikasi atau penyimpanan.

5. Jelaskan menurut anda apa itu *session* dan *authentication*!

   Ans :

   - *Session* adalah mekanisme yang digunakan dalam aplikasi web untuk menyimpan informasi pengguna sementara selama interaksi atau kunjungan (sesi) berlangsung, seperti status login, preferensi, atau aktivitas, sehingga

pengguna tidak perlu melakukan otentikasi ulang di setiap permintaan ke server selama sesi masih aktif.

- *Authentication* adalah proses verifikasi identitas pengguna, biasanya dilakukan dengan mencocokkan kredensial seperti username dan password, guna memastikan bahwa orang yang mencoba mengakses sistem benar-benar memiliki hak akses yang sah.

6. Jelaskan menurut anda apa itu privacy dan ISO!

   Ans :

   - *Privacy (privasi)* adalah hak individu atau entitas untuk mengontrol informasi pribadinya, termasuk bagaimana data tersebut dikumpulkan, digunakan, disimpan, dan dibagikan, serta memastikan bahwa informasi sensitif tidak diakses atau disalahgunakan oleh pihak yang tidak berwenang.

   - *ISO (International Organization for Standardization)* adalah organisasi internasional yang mengembangkan dan menerbitkan standar global di berbagai bidang, termasuk keamanan informasi, seperti ISO/IEC 27001, yang merupakan standar internasional untuk sistem manajemen keamanan informasi (ISMS) guna membantu organisasi melindungi data secara sistematis dan berkelanjutan.