UTS KEAMANAN INFORMASI KJ002

Nama : Fayza Azzahra

NIM : 20230801329

Dosen Pengampu : HANI DEWI ARIESSANTI , S.Kom, M.Kom

Soal:

1. Jelaskan menurut anda apa itu keamanan informasi!
2. Jelaskan menurut anda apa itu Confidentiality, Integrity dan Availability!
3. Sebutkan jenis-jenis kerentanan keamanan yang anda ketahui!
4. Pengamanan data bisa menggunakan hash dan encryption. Jelaskan apa yang anda ketahui terkait hash dan encryption!
5. Jelaskan menurut anda apa itu session dan authentication!
6. Jelaskan menurut anda apa itu privacy dan ISO!

Jawab:

1. Keamanan informasi adalah cara atau upaya melindungi data supaya tidak dicuri, diubah, atau diakses oleh orang yang tidak berhak. Tujuannya adalah agar data tetap rahasia, tidak rusak atau diubah tanpa izin, dan selalu bisa diakses saat dibutuhkan. Ini penting supaya data pribadi, data perusahaan, atau sistem tetap aman dan tidak disalahgunakan.

2.
   - Confidentiality (Kerahasiaan) artinya data hanya boleh diakses oleh orang yang punya hak. Contohnya, pesan yang dikirim lewat internet biasanya dienkripsi supaya orang lain tidak bisa membacanya.
   - Integrity (Integritas) berarti data harus tetap benar dan tidak boleh diubah tanpa izin. Misalnya, sistem menggunakan cara khusus untuk mengecek apakah data sudah diubah.
   - Availability (Ketersediaan) artinya data atau layanan harus bisa diakses kapan saja oleh orang yang berhak. Misalnya, server harus tetap hidup dan punya cadangan supaya tidak hilang.

3. Di dunia sistem komputer, ada banyak celah atau titik lemah yang sering dimanfaatkan oleh orang jahat. Contohnya, ada serangan yang namanya SQL Injection, di mana hacker masuk lewat celah input data supaya bisa ngacak-acak database secara ilegal. Terus ada juga yang namanya Cross-Site Scripting (XSS), yaitu hacker nyelipin kode jahat ke website supaya bisa nyolong data pengunjungnya. Kadang karena kesalahan coding, terjadi Buffer Overflow—ini semacam memori kebocoran yang bisa dipakai buat jalanin program berbahaya. Selain itu, ada malware kayak virus, worm, dan trojan yang suka bikin kerusakan atau maling data di komputer kita. Ada juga trik penipuan seperti phishing dan social engineering yang bikin orang nggak sadar kasih data pribadi atau passwordnya. Nah, kalau sistemnya salah setting, misalnya masih pakai password bawaan yang gampang ditebak, itu juga jadi celah besar buat orang yang nggak bertanggung jawab masuk.

4.
   - Hash adalah proses mengubah data jadi kode unik yang tidak bisa dibalik lagi. Hash dipakai untuk memastikan data tidak berubah, misalnya menyimpan password secara aman. Contoh algoritma hash: SHA-256 dan MD5 (meski MD5 sekarang kurang aman).

- Encryption: dalah proses menyandikan data supaya tidak bisa dibaca sembarangan, tapi bisa dikembalikan ke bentuk asli dengan kunci tertentu. Ada dua jenis enkripsi, simetris, pakai satu kunci untuk enkripsi dan dekripsi (contoh: AES) dan Asimetris, pakai pasangan kunci publik dan privat (contoh: RSA).

5.

- Session adalah cara sistem menyimpan info sementara tentang pengguna yang sedang aktif, misalnya setelah login supaya tidak perlu masuk ulang terus-menerus.
- Authentication adalah proses memastikan seseorang benar-benar siapa yang dia klaim, biasanya dengan username dan password, sidik jari, atau token supaya hanya orang yang berhak yang bisa masuk.

6.

- Privacy (Privasi) adalah hak seseorang atau organisasi untuk mengontrol data pribadinya, termasuk bagaimana data itu dikumpulkan, digunakan, dan dibagikan. Privasi penting supaya data tidak disalahgunakan dan pengguna merasa aman.
- ISO (International Organization for Standardization) adalah organisasi internasional yang membuat standar, termasuk soal keamanan informasi. Contohnya, standar ISO/IEC 27001 memberikan aturan bagaimana cara mengelola keamanan informasi secara sistematis supaya data terlindungi dengan baik.