UJIAN TENGAH SEMESTER

Dosen : Hani Dewi Ariessanti

Mata Kuliah : CIE406- Keamanan Informasi

Disusun Oleh :

Agustinus Djumhani Wagolebo 20230801340

PRODI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS ESA UNGGUL

2025

ESSAY :

1. **Apa itu keamanan informasi menurut Anda?**

   Menurut saya, Keamanan Informasi itu segala usaha buat melindungi data dan sistem komputer dari berbagai macam ancaman yang bisa merusak atau mencuri informasi yang ada di dalamnya. Jadi, intinya adalah kita memastikan informasi yang ada di komputer atau dalam jaringan tetap aman, nggak bisa diakses orang yang tidak berhak, dan tidak rusak.

2. **Apa itu Confidentiality, Integrity, dan Availability?**

- **Confidentiality (Kerahasiaan):** Ini artinya menjaga agar informasi hanya bisa diakses oleh orang yang berhak saja. Misalnya, hanya orang yang punya izin yang bisa melihat informasi pribadi atau data sensitif.
- **Integrity (Integritas):** Ini berarti memastikan data tetap dalam kondisi yang benar dan tidak ada yang merusaknya atau mengubahnya tanpa izin. Jadi, kalau ada data, pastikan datanya tetap sama seperti saat pertama kali dimasukkan dan tidak ada yang diubah-ubah tanpa sepengetahuan.
- **Availability (Ketersediaan):** Ini artinya memastikan informasi bisa diakses kapan saja oleh orang yang butuh. Jadi, saat kita butuh data atau informasi, sistem harus memastikan data itu tersedia dan bisa langsung diakses tanpa masalah.

3. Kerentanan itu adalah titik lemah yang bisa dimanfaatkan oleh orang jahat. Beberapa kerentanan yang saya ketahui dan sering terjadi antara lain:

   ## 1. Malware (Perangkat Lunak Jahat)

   Malware adalah program jahat yang dirancang untuk merusak komputer atau mencuri informasi penting kita. Misalnya, ada virus atau trojan yang bisa masuk ke komputer lewat email atau unduhan file yang tidak kita sadari berbahaya. Begitu terinfeksi, malware bisa merusak data, mencuri informasi pribadi, atau bahkan mengunci data kita dan meminta tebusan untuk membukanya (ransomware).
   Contoh: Bayangkan kamu dapat email dari orang yang tidak dikenal, lalu kamu mengunduh lampiran yang terlihat biasa saja, tetapi setelah itu komputer kamu terinfeksi virus yang merusak data.

2. Phishing (Penipuan Online)
Phishing itu penipuan di internet, di mana orang jahat mencoba mengambil data pribadi kita, seperti password atau nomor kartu kredit, dengan cara menyamar sebagai orang atau organisasi yang kita percayai. Mereka biasanya mengirim email yang terlihat seperti dari bank atau perusahaan lain yang kita gunakan, meminta kita klik link dan masukkan data pribadi. Padahal, itu cuma website palsu yang dirancang untuk mencuri informasi.
Contoh: Kamu dapat email yang seolah-olah dari bank, yang mengharuskan kamu untuk klik link dan masuk ke akun kamu, padahal link itu membawa kamu ke situs palsu yang didesain mirip situs bank asli.

3. SQL Injection
SQL Injection itu ketika hacker memanfaatkan celah di sistem aplikasi, misalnya aplikasi web, untuk menyisipkan kode berbahaya ke dalam database. Ini bisa terjadi jika aplikasi tidak memeriksa input dengan baik. Dengan menyuntikkan perintah ke dalam sistem, hacker bisa mendapatkan akses ke data pribadi, atau merusak data yang ada di database.
Contoh: Misalnya, ada form login di sebuah website yang tidak memeriksa data dengan benar. Hacker bisa memasukkan kode yang memungkinkan mereka masuk tanpa perlu tahu password.

4. Man-in-the-Middle (MITM)
Serangan Man-in-the-Middle (MITM) itu terjadi saat seorang hacker diam-diam mengawasi percakapan atau komunikasi antara dua pihak. Ini sering terjadi di jaringan yang tidak aman, seperti Wi-Fi publik. Hacker bisa mencuri informasi yang dikirimkan atau bahkan mengubah data yang sedang dipertukarkan tanpa diketahui oleh pengirim atau penerima.
Contoh: Kamu sedang menggunakan Wi-Fi gratis di kafe dan hacker menyadap komunikasi antara kamu dan website yang kamu akses, mencuri data login atau informasi pribadi yang kamu kirimkan.

5. Password Cracking (Pemecahan Kata Sandi)
Password cracking adalah cara hacker mencoba menebak kata sandi kita. Mereka bisa memakai program khusus untuk mencoba berbagai kombinasi kata sandi sampai menemukan yang benar. Kalau kita pakai kata sandi yang lemah atau gampang ditebak, misalnya “123456” atau “password,” akun kita jadi gampang diretas.
Contoh: Hacker menggunakan program untuk menebak kata sandi kamu dengan mencoba banyak kombinasi, seperti "admin123" atau "password123," dan akhirnya mereka bisa masuk ke akun kamu.

4. **Apa yang Anda ketahui tentang hash dan encryption dalam pengamanan data?**
   Yang saya ketahui tentang hash dan encryption yaitu :

- **Hash:** Hash itu seperti cara mengubah data asli jadi angka atau kode yang unik dan tidak bisa dibalik lagi ke bentuk aslinya. Biasanya dipakai buat ngecek apakah data yang kita terima atau simpan sudah benar dan nggak diubah-ubah.
- **Encryption (Enkripsi):** Enkripsi adalah cara mengacak data agar tidak bisa dibaca oleh orang lain yang nggak punya kunci. Jadi, kalau kita kirim pesan lewat aplikasi, pesan itu dienkripsi supaya hanya orang yang kita tuju yang bisa baca, sementara orang lain yang mencoba mengakses pesan tersebut tidak bisa membacanya

5. **Apa yang dimaksud dengan session dan authentication menurut Anda?**

1. Session

Session itu kayak waktu atau periode ketika kita sedang aktif menggunakan sebuah aplikasi atau situs web. Misalnya, ketika kita login ke dalam sebuah aplikasi, aplikasi tersebut akan "mengingat" bahwa kita sudah login dan akan terus menyimpan status itu sampai kita selesai menggunakan aplikasi tersebut. Selama sesi ini, kita nggak perlu terus-terusan login karena sistem sudah tahu kita adalah orang yang sama yang sedang menggunakan aplikasi itu.

Contoh: Bayangin kamu login ke aplikasi belanja online. Selama sesi ini, kamu bisa menambahkan barang ke keranjang dan melanjutkan belanja tanpa harus login ulang setiap kali membuka aplikasi. Begitu kamu logout atau aplikasi ditutup dalam waktu yang lama, sesi tersebut berakhir, dan kamu perlu login lagi jika ingin melanjutkan.

2. Authentication (Autentikasi)

Autentikasi itu adalah proses untuk memastikan bahwa kita benar-benar orang yang kita klaim. Ketika kita ingin mengakses sesuatu yang bersifat pribadi atau sensitif, seperti akun media sosial atau aplikasi perbankan, sistem akan meminta kita untuk memverifikasi identitas kita terlebih dahulu. Biasanya, kita diminta untuk memasukkan **username** dan **password**. Dengan cara ini, sistem bisa memastikan bahwa hanya kita yang berhak mengakses akun atau data tersebut, bukan orang lain yang mencoba masuk dengan cara yang tidak sah.

Contoh: Saat kamu membuka akun email, sistem akan meminta username dan password untuk memastikan bahwa kamu adalah pemilik akun tersebut. Jika kamu

memasukkan password yang salah, kamu nggak bisa masuk ke akun, dan itu menunjukkan bahwa autentikasi tidak berhasil.

6.

1. Privacy (Privasi)

Privasi yang saya ketahui itu adalah hak kita untuk mengendalikan siapa saja yang boleh mengakses informasi pribadi kita. Misalnya, kita punya hak untuk menentukan siapa yang boleh tahu alamat rumah kita, nomor telepon, atau informasi sensitif lainnya. Di dunia digital, privasi menjadi sangat penting karena data pribadi kita bisa saja disalahgunakan jika jatuh ke tangan yang salah.

Saat kita menggunakan aplikasi atau situs web, kita sering diminta untuk memberikan informasi pribadi. Jika informasi itu tidak dilindungi dengan baik, orang lain bisa mencurinya dan menggunakannya untuk tujuan yang merugikan, seperti penipuan atau pencurian identitas. Privasi penting agar kita merasa aman dan tidak khawatir tentang siapa yang bisa mengakses data kita.

Contoh: Ketika kamu membuat akun di media sosial, kamu biasanya diminta untuk mengisi data pribadi seperti nama, alamat email, atau tanggal lahir. Privasi memastikan data ini hanya bisa diakses oleh orang yang berhak dan bukan oleh pihak yang tidak sah.

2. ISO (International Organization for Standardization)

Dan untuk ISO yaitu organisasi internasional yang membuat standar atau pedoman untuk berbagai bidang, termasuk teknologi informasi dan keamanan data. Jadi, ISO berfungsi seperti aturan main yang diakui secara global untuk memastikan setiap organisasi atau perusahaan melindungi data dengan cara yang benar dan sesuai prosedur.

Salah satu standar yang terkenal dalam hal keamanan data adalah **ISO/IEC 27001**. Standar ini memberikan pedoman kepada organisasi tentang cara mengelola, melindungi, dan menjaga keamanan informasi dengan cara yang sistematis. Jadi, kalau sebuah organisasi mengikuti standar ini, mereka akan tahu langkah-langkah apa yang perlu diambil untuk memastikan bahwa data mereka aman dari ancaman dan tidak disalahgunakan.

Contoh: Misalnya, jika sebuah perusahaan ingin melindungi data pelanggannya, mereka bisa mengikuti standar ISO/IEC 27001 untuk memastikan sistem mereka aman. Dengan mengikuti pedoman ini, perusahaan bisa menjaga data pelanggan dengan cara yang diakui dan sesuai standar internasional, sehingga pelanggan merasa lebih percaya dan aman.