NAMA : Arrauuf Reza Firmansyah
NIM : 20210801188

UTS

Keamanan Informasi

1. Apa itu keamanan informasi?

Keamanan informasi itu intinya adalah bagaimana caranya kita menjaga agar data atau informasi yang kita miliki tetap aman dan nggak jatuh ke tangan orang yang nggak berhak. Jadi, bukan cuma soal ngejaga dari hacker aja, tapi juga memastikan bahwa data itu nggak rusak, nggak berubah tanpa izin, dan bisa diakses oleh orang yang memang punya hak akses. Dalam dunia digital sekarang, keamanan informasi itu penting banget, karena hampir semua aktivitas pakai data—mulai dari transaksi online, data pelanggan, sampai data pribadi. Kalau nggak dijaga, bisa bocor dan disalahgunakan.

2. Apa itu Confidentiality, Integrity, dan Availability?

Tiga istilah ini sering disebut sebagai prinsip dasar keamanan informasi, dan dikenal juga dengan singkatan CIA. Confidentiality (kerahasiaan) itu soal menjaga supaya data nggak bisa diakses sembarangan. Misalnya, data pelanggan di web hanya bisa diakses oleh admin yang punya hak. Lalu Integrity (integritas) itu menjaga agar data tetap utuh, nggak diubah-ubah tanpa izin. Bayangin kalau data transaksi diubah diam-diam, itu bisa bahaya. Dan Availability (ketersediaan) artinya data harus selalu bisa diakses saat dibutuhkan. Jadi walaupun aman, tapi kalau sistemnya sering down atau error terus, itu juga jadi masalah.

3. Jenis-jenis kerentanan keamanan yang saya ketahui:

Kerentanan atau celah keamanan itu banyak jenisnya. Salah satunya adalah SQL Injection, yaitu teknik di mana penyerang bisa menyisipkan perintah SQL ke dalam input form untuk mencuri data. Ada juga Cross Site Scripting (XSS), di mana penyerang menyisipkan script berbahaya ke dalam halaman web. Terus ada juga Brute Force Attack, yaitu upaya menebak password dengan mencoba banyak kombinasi secara terus-menerus. Selain itu, phishing juga termasuk serangan

yang cukup sering, yaitu memancing user agar memberikan data penting lewat tampilan yang seolah-olah resmi.

4. Hash vs Encryption

Hash dan encryption itu dua teknik buat mengamankan data, tapi cara kerjanya beda. Hash itu proses satu arah. Artinya, data asli (misalnya password) diubah jadi kode acak (hash), dan kode itu nggak bisa diubah balik ke data aslinya. Biasanya dipakai buat nyimpan password. Sementara encryption itu dua arah, jadi data bisa di-encode jadi bentuk terenkripsi, tapi juga bisa didekripsi lagi jadi data asli dengan kunci tertentu. Encryption biasanya dipakai buat melindungi data penting saat dikirim, misalnya data login atau transaksi di internet. Intinya, hash buat cek keaslian, encryption buat nyembunyiin isi data.

5. Apa itu session dan authentication?

Session itu ibarat identitas sementara yang disimpan di server saat pengguna login. Jadi selama pengguna aktif, server tahu siapa dia. Ini berguna banget buat nyimpen status login atau aktivitas pengguna tanpa harus login ulang terus. Sedangkan authentication adalah proses buat memastikan bahwa seseorang adalah benar dirinya, biasanya dengan login pakai username dan password. Jadi authentication itu tahap awal buat ngecek identitas, sedangkan session dipakai buat nyimpen status pengguna setelah lolos proses tersebut.

6. Apa itu privacy dan ISO?

Privacy itu soal hak seseorang untuk ngatur data pribadinya—siapa aja yang boleh tahu, ngakses, atau pakai data itu. Misalnya, data KTP, alamat, atau riwayat transaksi, itu semua termasuk data pribadi yang harusnya nggak bisa diakses sembarangan. Nah, di sinilah pentingnya standar seperti ISO. ISO (International Organization for Standardization) adalah lembaga internasional yang bikin standar termasuk buat keamanan informasi. Salah satu yang terkenal adalah ISO 27001, yaitu standar untuk sistem manajemen keamanan informasi. Tujuannya biar organisasi bisa punya pedoman jelas buat ngelola dan ngamanin data.