**Jawaban Latihan Komputer dan Jaringan**

Nama : Mufadhal

NIM : 0110223299

Rombel : TI03

1. Cara mengamankan aplikasi dan database STT NF dari serangan dalam dan luar :
2. Firewall dan IDS/IPS

Gunakan firewall dan Intrusion Detection/Prevention System untuk memantau serta menyaring lalu lintas jaringan.

1. Enkripsi

Terapkan enkripsi pada data saat disimpan (at rest) dan saat dikirimkan (in transit).

1. Akses Terbatas: Terapkan prinsip least privilege, yaitu hanya memberikan akses kepada pihak yang membutuhkan.
2. Tugas masing-masing kelompok:
3. Roles and Responsibility : Menentukan siapa yang bertanggung jawab dalam proses manajemen risiko, mulai dari penilai risiko hingga eksekutor mitigasi.
4. Risk Analysis : Menganalisis kemungkinan dan dampak dari risiko yang teridentifikasi untuk mengetahui tingkat bahayanya.
5. Asset & Threat Identification : Mengidentifikasi aset penting dan potensi ancaman terhadap aset tersebut.
6. Risk Prioritization : Mengurutkan risiko berdasarkan tingkat keparahan dan kemungkinan terjadinya untuk fokus pada risiko paling kritis.
7. Mitigasi Risiko : Menentukan dan menerapkan langkah untuk mengurangi kemungkinan atau dampak dari risiko.
8. Akses kontrol dan autentikasi saling berkaitan karena autentikasi adalah proses untuk memverifikasi identitas pengguna, sedangkan akses kontrol menentukan hak akses pengguna berdasarkan hasil autentikasi tersebut. Tanpa autentikasi, sistem tidak dapat menerapkan kontrol akses yang tepat.
9. Dalam keamanan komputer dan jaringan, threat (ancaman) adalah potensi bahaya yang dapat mengeksploitasi vulnerability (kerentanan), yaitu kelemahan dalam sistem. Jika ancaman berhasil memanfaatkan kerentanan, akan timbul impact (dampak) seperti kerusakan atau kehilangan data. Risk (risiko) adalah gabungan dari ancaman, kerentanan, dan dampak yang menunjukkan kemungkinan dan besarnya kerugian yang bisa terjadi.
10. Security attack dengan metode passive attack dan active attack beserta contoh :
11. Passive Attack: Serangan yang bertujuan untuk mengintai atau mencuri informasi tanpa mengubah data.

Contoh: Sniffing, eavesdropping.

1. Active Attack: Serangan yang berusaha mengubah atau merusak data/sistem. Contoh: DoS attack, man-in-the-middle, penggantian pesan.