M. Yusril helmi Setyawan, S.Kom., M.Kom., SFPC., CCNA.
KEAMANAN SISTEM INFORMASI

Nama : Muhammad Rafli Alfarisi/714220008

Kelas : 3A D4 TI

PRE-TEST

1. Apa yang dimaksud dengan prinsip Kerahasiaan (Confidentiality) dalam keamanan informasi?
2. Apa tujuan utama dari pemodelan ancaman (threat modelling)?
3. Sebutkan tiga langkah utama dalam proses manajemen risiko.
4. Apa yang dimaksud dengan serangan DDoS dan bagaimana cara mencegahnya?
5. Sebutkan satu ancaman umum terhadap sistem operasi Windows dan langkah pencegahannya.
6. Apa itu serangan SQL Injection dan bagaimana cara melindungi aplikasi web darinya?
7. Apa tantangan keamanan utama dalam penggunaan layanan cloud?
8. Apa tujuan dari pengujian penetrasi (penetration testing)?
9. Apa fungsi utama dari Security Operation Center (SOC)?
10. Apa yang dimaksud dengan ISO 27001?

Jawaban

1. Dalam keamanan informasi, prinsip kerahasiaan (kerahasiaan) adalah ide yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan tidak boleh dibagikan kepada pihak yang tidak berhak. Tujuannya adalah untuk mencegah data sensitif jatuh ke tangan yang salah, baik secara sengaja maupun tidak sengaja.
2. Tujuan utama pemodelan ancaman (threat modelling) adalah untuk mengidentifikasi, memahami, dan mengevaluasi potensi ancaman terhadap sistem atau aplikasi sehingga dapat mengambil tindakan mitigasi yang tepat untuk melindungi aset-aset penting.
3. - Identifikasi Risiko : Langkah ini melibatkan proses mengidentifikasi berbagai potensi risiko yang dapat mempengaruhi tujuan atau operasi organisasi.
   - Penilaian dan Analisis Risiko : Setelah risiko diidentifikasi, langkah ini melibatkan penilaian tingkat keparahan risiko dengan memperkirakan dampak dan kemungkinan terjadinya. Analisis risiko membantu dalam menentukan prioritas risiko mana yang harus segera ditangani.
   - Mitigasi dan Pengendalian Risiko : Langkah ini melibatkan pengembangan dan implementasi strategi untuk mengurangi atau mengendalikan risiko yang telah dinilai.
4. Serangan DDoS (Distributed Denial of Service) adalah jenis serangan siber di mana sejumlah besar permintaan palsu dikirim ke server, layanan, atau jaringan dengan tujuan membanjiri sistem sehingga tidak dapat menangani permintaan yang sah. Serangan ini biasanya menggunakan botnet, sekumpulan perangkat yang telah terinfeksi malware, yang dapat dikendalikan oleh penyerang untuk menyerang target secara bersamaan. Layanan menjadi tidak tersedia karena overload atau crash sebagai akibat dari serangan ini.
   Cara mencegahnya :
   - Gunakan CDN (Content Delivery Network)
   - Implementasi Firewall dan Sistem Deteksi Intrusi
   - Rate Limiting

5. Salah satu ancaman umum terhadap sistem operasi Windows adalah malware (misalnya, virus, trojan, ransomware).
   Cara pencegahannya seperti berikut :
   - Menggunakan antivirus yang terpercaya.
   - Aktifkan Windows Defender.
   - Memperbarui system secara berkala.
   - Gunakan Firewall.
   - Hindari mengklik tautan yang mencurigakan..
6. SQL injection merupakan salah satu metode eksploitasi yang memanfaatkan celah keamanan pada sistem basis data aplikasi. Teknik ini memanfaatkan kelemahan dalam proses validasi input, yang mengakibatkan adanya peluang bagi penyerang untuk menyisipkan perintah SQL berbahaya. Dengan adanya kesalahan dalam pemfilteran input, penyerang dapat menyusupkan kode yang mengeksploitasi celah keamanan di database, baik pada website maupun aplikasi.
   Salah Satu Cara penanggulangan sql injection:
   1. Pengaturan Format input data sesuaikan karakter nya
   2. Penerapan validasi data
   3. Pemanfaatan parameterized sql query
   4. Pemanfaatan sql escape string
   5. Menonaktifkan log error pada console
7. A. Pertama kerentanan terhadap penyerangan sistem dari pihak luar
   B. Kekhawatiran terhadapat privasi data dari penyedia layanan cloud
   C. Hacking Interface dan API
   D. tidak memiliki akses penuh terhadap sistem
8. A. Untuk melakukan pengecekan serta evaluasi terhadap keamanan sebuat sistem jaringan dan informasi
   B. mengetahui kelemahan dari suatu sistem informasi dari kemungkinan serangan hacker.
   C. Dapat Memperkirakan kerugian yang terjadi oleh suatu perusahaan
9. Fungsinya untuk menjadi perlindungan dan keamanan server perusahaan dari serangan siber yang dapat mengancam aset, reputasi hingga kelangsungan bisnis.
10. ISO 27001 adalah standar internasional yang menetapkan spesifikasi untuk sistem manajemen keamanan informasi (ISMS).