**LAPORAN PRAKTIKUM**

Information Security Overview



**Institut Teknologi Del**

**T.P. 2021/2022**

Disusun Oleh :

Nama: Santo L Harianja

Nim: 11419027

Kelas : 43 TRPL 1

1. What is the OSI security architecture?( Apa arsitektur keamanan OSI?)

* Arsitektur Keamanan OSI adalah kerangka kerja yang menyediakan cara sistematis untuk mendefinisikan persyaratan untuk keamanan dan mengkarakterisasi pendekatan untuk memenuhi persyaratan tersebut. Dokumen ini mendefinisikan serangan keamanan, mekanisme, dan layanan, dan hubungan di antara kategori-kategori ini.

1. Serangan Keamanan

Setiap tindakan yang membahayakan keamanan informasi yang dimiliki oleh sebuah organisasi .

1. Mekanisme Keamanan

Sebuah proses ( atau perangkat menggabungkan proses tersebut ) yang dirancang untuk mendeteksi , mencegah , atau memulihkan dari serangan keamanan.

1. Servis Keamanan

Sebuah layanan pemrosesan atau komunikasi yang meningkatkan keamanan pengolahan data sistem dan transfer informasi dari sebuah organisasi. Layanan tersebut adalah dimaksudkan untuk melawan serangan keamanan, dan mereka menggunakan satu atau lebih mekanisme servis untuk memberikan keamanan.

1. Ancaman

Sebuah potensi pelanggaran keamanan, yang ada ketika terdapat keadaan, kemampuan, tindakan, atau peristiwa yang dapat melanggar keamanan dan menyebabkan bahaya. Artinya, ancaman bahaya yang mungkin mengeksploitasi kerentanan.

1. Serangan

Serangan terhadap sistem keamanan yang berasal dari ancaman yang cerdas, yaitu, suatu tindakan yang cerdas yang merupakan upaya yang disengaja (terutama dalam arti metode atau teknik) untuk menghindari layanan keamanan dan melanggar kebijakan sistem keamanan.

1. Apa perbedaan antara ancaman keamanan pasif dan aktif? (What is the difference between passive and active security threats?)

* Serangan pasif harus dilakukan dengan memantau atau transmisi. Surat elektronik, transfer file, dan pertukaran klien / server adalah contoh transmisi yang dapat dipantau. Serangan pasif adalah jenis serangan yang tidak membahayakan terhadap sebuah sistem jaringan. Serangan aktif meliputi modifikasi data yang dikirimkan dan upaya untuk mendapatkan akses tidak sah ke sistem komputer.

1. Buat daftar dan tentukan secara singkat kategori serangan keamanan pasif dan aktif? (List and briefly define categories of passive and active security attacks?)

* - **Serangan pasif:** pelepasan konten pesan dan analisis lalu lintas.
* **Serangan aktif**: Mencoba mengubah sumber daya sistem atau memengaruhi

operasi. Dengan modifikasi aliran data menjadi:

+ penyamaran satu entitas sebagai entitas lain

+ putar ulang pesan sebelumnya

+ ubah pesan dalam perjalanan

+ penolakan layanan

1. Daftar dan tentukan secara singkat kategori layanan keamanan (List and briefly define categories of security services?)

* a**. Authentication**

Jaminan bahwa entitas yang berkomunikasi adalah yang diklaimnya.

b. **Access Control**

Pencegahan penggunaan sumber daya secara tidak sah (Misal : Layanan ini mengontrol siapa yang dapat memiliki akses ke sumber daya, dalam kondisi apa akses dapat terjadi, dan apa yang dilakukan oleh orang yang mengakses sumber daya).

c. **Data Confidentiality**

Perlindungan data dari pengungkapan yang tidak sah.

d. **Data Integrity**

Jaminan bahwa data yang diterima persis seperti yang dikirim oleh entitas yang berwenang (Misal : Tidak mengandung modifikasi, penyisipan, penghapusan, atau pemutaran ulang).

e**. Non-Repudiation**

Memberikan perlindungan terhadap penolakan oleh salah satu entitas yang terlibat dalam komunikasi yang telah berpartisipasi dalam semua atau sebagian dari komunikasi.

1. Daftar dan tentukan secara singkat kategori-kategori mekanisme keamanan? (List and briefly define categories of security mechanisms ?
   1. **Encipherment :** Penggunaan algoritma matematika untuk mengubah data menjadi bentuk yang tidak mudah dipahami. Transformasi dan pemulihan data selanjutnya bergantung pada suatu algoritma dan nol atau lebih kunci enkripsi.
   2. **Digital Signature** (Tanda Tangan Digital): Data ditambahkan ke, atau transformasi kriptografi dari, unit data yang memungkinkan penerima unit data untuk membuktikan sumber dan integritas unit data dan melindungi terhadap pemalsuan.
   3. **Access Control** (Kontrol Akses) : Berbagai mekanisme yang menegakkan hak akses ke Sumber Daya.
   4. **Data Integrity** (Integritas Data) : Berbagai mekanisme yang digunakan untuk memastikan integritas unit data atau aliran unit data.
   5. **Authentication Exchange** (Pertukaran Otentikasi) : Suatu mekanisme yang dimaksudkan untuk memastikan identitas suatu entitas melalui pertukaran informasi.
   6. **Traffic Padding:** Penyisipan bit ke celah dalam aliran data untuk Frustrate traffic analysis analysis.
   7. **Routing Control** (Kontrol Routing) : Memungkinkan pemilihan Rute yang aman secara fisik tertentu untuk data tertentu dan memungkinkan perubahan rute, terutama ketika pelanggaran keamanan diduga terjadi.
   8. **Notarization**  (Notaris) : Penggunaan pihak ketiga yang tepercaya untuk memastikan Properti tertentu dari pertukaran data.

**PROBLEM**

1. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement
2. **Confidentiality** : Personal Identification Number (PIN) adalah aset yang kerahasiaannya dianggap sangat penting oleh seorang individu. Informasi PIN hanya boleh tersedia untuk individu. Tingkat Pentingnya: TINGGI
3. **Integrity :** Seseorang harus dapat mempercayai bahwa kartu yang disediakan untuk akses akun adalah benar dan terkini. Dan seorang individu harus dapat menarik jumlah yang dia inginkan dari akunnya yang tersedia. Sekarang anggaplah staf bank yang berwenang untuk melihat dan memperbarui rekening individu dengan sengaja memalsukan data di dalamnya, Integritas hilang. Database perlu dipulihkan ke basis tepercaya dengan cepat, dan harus dimungkinkan untuk melacak kesalahan kembali ke orang yang bertanggung jawab. Tingkat Pentingnya: Tinggi.
4. **Availability :** Anjungan Tunai Mandiri (ATM) menyediakan cara bagi individu untuk menarik uang kapan saja dan dari mana saja mereka inginkan. Oleh karena itu, seseorang harus dapat menarik uang dari ATM (mis. ATM harus selalu tersedia untuk penarikan) asalkan ia memiliki PIN dan Kartu untuk akses akun. Namun, ini adalah fasilitas yang disediakan oleh bank untuk memfasilitasi pelanggannya untuk memudahkan akses ke rekening bank mereka. Ini bukan komponen penting dari sistem informasi bank, tetapi tidak tersedianya layanan ini akan menimbulkan rasa malu bagi pelanggan. Tingkat Pentingnya: Sedang
5. Repeat Problem 1 for a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller

* **Confidentially** : Pelanggan harus mengharapkan privasi dalam komunikasi.

Tingkat pentingnya kerahasiaan : Menjamin kerahasiaan individu

CIA dalam sistem telepon yang merutekan panggilan melalui perpindahan jaringan berdasarkan nomor telepon yang diminta oleh penelepon. Confidentiality → Penelepon harus memastikan privasi dalam komunikasi mereka. Integrity → Penelopon yang dapat menentukan nomor yang akan di hubungi. Availability → Penelepon dapat melakukan panggilan terhadap nomor yang dihubungi dimana pun dan kapan pu jika nomor yang dihubungi tersedia.

1. Consider a desktop publishing system used to produce documents for various organizations.

1. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.

2. Give an example of a type of publication in which data integrity is the most important requirement.

3. Give an example in which system availability is the most important requirement.

* 1. Dalam jenis publikasi ini adalah materi milik perusahaan maka kerahasiaan data yang disediakan adalah yang paling penting. Karena materi yang dipatenkan berisi informasi rahasia, rahasia harus dipastikan untuk data yang tersimpan terkait dengan pekerjaan.

2. Dalam jenis publikasi ini terkait dengan hukum dan mengatur integritas data yang disediakan adalah yang paling penting. Di sini kita memiliki undang-undang dan peraturan yang sedikit berbeda dari masing-masing organisasi, tepatnya hukum dan peraturan yang disediakan oleh organisasi disimpan. Dokumen integritas sangat penting.

3. Dalam jenis publikasi ini dikaitkan dengan tampilan harian diperbarui misalnya majalah berita harian. Ketersediaan data ini sangat penting. Seperti majalah berita harian diperbarui dan dirilis ke pasar dengan yang paling diperlukan.

1. For each of the following assets, assign a low, moderate, or high impact level

for the loss of confidentiality, availability, and integrity, respectively. Justify

your answers.

a. An organization managing public information on its Web server.

b. A law enforcement organization managing extremely sensitive

investigative information.

c. A financial organization managing routine administrative information

(not privacy-related information).

d. An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

e. A power plant contains a SCADA (supervisory control and data acquisition)

f. system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

1. Confidentiality = Not Applicable

Integrity = Moderate

Availability = Moderate

1. Confidentiality = High

Integrity = Moderate

Availability = Moderate

1. Confidentiality = Low

Integrity = Low

Availability = Low

1. Security Category of Contract Information

Confidentiality = Moderate

Integrity = Moderate

Availability = Low

Security Category of administrative Information

Confidentiality = Low

Integrity = Low

Availability = Low

Security Category of Acquisition Information

Confidentiality = Moderate

Integrity = Moderate

Availability = Low

1. Security Category of Sensor Data

Confidentiality

Integrity

Availability

Security Category of administrative Information

Confidentiality = Low

Integrity = Low

Availability = Low

Security Category of SCADA system

Confidentiality = Low

Integrity = Low

Availability = Low