TUGAS 1

“RESUME KEAMANAN SISTEM KOMPUTER”

DI SUSUN OLEH :

NAMA : ANDI AMANDA ANDI T.

NIM : F551 22 034

KELAS : TI A

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS TADULAKO

PALU

2023

A. Computer Security

Di dalam computer Security terdapat perlindungan yang diberikan kepada system informasi untuk mencapai tujuan untuk menjaga integritas, ketersediaan serta rahasia dimana terdapat beberapa pembahasan dalam computer security diantaranya adalah:

1. Konsep Keamanan Sistem Komputer

- **Availability** : berfungsi untuk memastikan bahwa data pada sistem tersedia saat dibutuhkan oleh pengguna yang memiliki hak akses
- **Confidentality** : terdapat dua hal yang diterapkan pada konsep ini yang pertama adalah kerahasiaan data dimana memastikan informasi yang sifatnya rahasia dan tidak dapat diungkap oleh seseorang yang tidak berwenang, lalu terdapat juga privasi pengguna dimana masing-masing pengguna daoat mengatur informasi yang bisa menjadi asupan publik atau private
- **Integrity** : terdapat beberapa hal yang diterapkan pada konsep ini yaitu, integritas data dimana yang dapat mengubah informasi hanya pihak yang berwenang dalam mengubah informasi, lalu terdapat integritas system dimana system harus dapat bekerja tanpa ada intefensi atau gangguan dari pihak luar yang tidak memiliki wewenang dalam system, lalu yang terakhir adalah Autencity dimana metode yang memberikan informasi adalah pengguna yang betul-betul dimaksud atau server yang digunakakan adalah server yang asli

2. Konsep Threat asset dan Attack

- **Threat and Attack**

  Berdasarkan RFC 4949 terdapat 4 macam dari Threat consequences dan beberapa macam, dari serangan

  1. Unauthorized Disclosure
     a. Exposure, atau yang disebut pengungkapan contohnya seprti orang yang sengaja merilos informasi sensitif, seperti nomor kartu kredit kepada orang luar, hal ini juga dapat disebebabkan oleh kesalahan manusia, perngakat keras, perangkat lunak yang error, hal itu mengaknatkan entitas memperoleh pengetahuan yang tidak sah tentang data sensitif
     b. Intereception, entitas yang tidak berwenang dalam mengakses data yang bersifat sensitif yang sedang memproses anatar sumber dan tujuan

c. Inference, contoh dari inference dikenal sebagai analisis lalu lintas dimana musuh ini dapat memperoleh informasi dengan mengamati pola dari lalu lintas suatu jaringan, contohnya seperti inferensi informasi rinci dari database oleh pengguna yang hanya memiliki akses terbatas
d. Intrusion, contoh dari intrusion adalah musuh yang mendapatkan izin tanpa akses ke data sensitif dengan mengatasi perlindungan kontrol akses sistem

2. Deception
   a. Masquerde salah satu contohnya dalah upaya yang tidak sah bagi pengguna untuk mendaptkan akses ke suatu sistem yang menyamar sebagai pengguna yang berwenang ini bisa terjadi ketika pengguna yang tidak sah mengetahui ID masuk dan kata sandi
   b. Falsification, ini mengacu pada perubahan atau penggantian data valid atau memasukkan data palsu ke dalam file atau database, contohnya siswa mungkin berubah nilainya di database sekolah
   c. Repudiation, pada kasus ini seorang pengguna menolak mengirim data atau pengguna menolak menerima atau memiliki data
3. Disruption
   a. Incapacitation, ini merupakan penyerangan pada sistem yang tersedia, hal ini dapat terjadi sebagai akibat kenacuran fisk atau kerusakan pada perangkat keras sistem. Contohnya seprti pada perangkat lunak berbahaya seperti trojan horse, virus atau worm yang beroprasi untuk menonaktifkan sistem atau beberapa layanannya
   b. Corruption, ini merupakan serangan dalam pada integritas sistem, perangkat lunak yang berbahaya dapat beroprasi sehingga sumber daya atau sisteam atau layanan berfungsi dengan cara yang tidak disengaja, atau pengguna bisa mendapatkan akses tidak sah ke sistem dan memodifikasi beberapa fungsinya, contohnya adalah penemptana pengguna logika bintu belakang dalam sistem untuk menyediakan akses selanjutnya ke sistem sumber daya dengan cara yang berbeda dari prosedur biasanya
   c. Obstruction, terdapat satu cara untuk menghalangi pengorasian sistem adalah dengan mengganggu komuniasi

dengan menonajtifkan tautan komunikasi atau mengubah komunikasi menjadi mengendalikan komunikasi

4. Usurpation
    a. Misappropriation, hal ini mencakup dalam pencurian layanan, contohnya adalah distribusi serangan penolakan layanan, ketika perangkat lunak bebrahaya diinstal pada sejumlah host untuk digunakan sebagai platform untuk meluncurkan lalu lintas pada host target
    b. Misuse, hal ini dapat terjadi melalui logika jahat atau peretas dapat memperoleh akses yang tidak sah ke suatu sistem, dalam kassu ini fungsi kemanan dapat dinonaktifka atau digagalkan

- **Threats and Assets**

    Aset sistem komputer dapat dikategorikan sebagai perangkat keras, perangkat keras, perangkat lunak, data dan jalur dan jaringan komuikasi

    a. Hardware, ancaman utam terhadap perangkat keras sistem komputer adalah ancaman terhdap ketersediaan, perangkat keras adalah yang paling rentan terjadi serangan dan paling tidak rentan terhadap serangan kontrol otomatis, ancaman juga mencakup kerusakan peralatan yang tidak disengaja dan disengaja serta pencurian. Dalam perkembangan komputer pribadi dan workstation dan meluasnya penggunaan LAN meningkatkan potensi kerugian di area ini contohnya CD-ROM dan DVD dapat menyebabkan hilangnya kerahasiaan
    b. Software, perangkat lunak menackup sistem operasi, utulitas dan aplikasi program, ancaman utamanya adalah serangan terhadap ketersediaan, pada perangkat lunak aplikasi seringkali mudah dihapus
    c. Data, keamanan perangkat keras dan perangkat lunak biasaya menjadi perhatian pusat komputasi profesional atau kekhawatiran individu pengguna komputer pribadi, masalah yang paling luas adalag keamanan data, yang melibatkan file dan bentuk data lainnya yangdikendalikan oleh individu, kelompok dan organisasi bisnis
    d. Communication Lines And Network

        Serangan keamanan jaringan dapat diklasifikasikan seperti serangan pasif dan serangan aktif, serangan pasif mencoba untuk belajar atau membuat penggunaan informasi dari sistem tetapi tidak mempenagruhi sumber daya sistem

3. **Persyaratan fungsional keamanan**

   Persyaratan fungsional keamanan adalah kriteria atau spesifikasi fungsional yang herus dipenuhi oleh sistem atau perangkat untuk memastikan bahwa keamanan informasi data terjaga, pada pembahasan ini terdapat FIPS 300 yang yang di dalamnya terdapat Acces Control, Identification and Autentication, System and Communication Protection, System and Information Integrity semisal pada confidentiality yang memberikan contoh pada informasi nilai siswa yang dimana kerahasiaan datanya sangat tinggi, lalu pada integrity yang memberikan contoh data hasil survey online anonym yang memiliki integritas data yang renda, dan juga availability yang memberikan contoh mekanisme autentikasi oada aplikasi atau komponen system yang kruses memiliki kebutuhan yang keterdediaannya tinggi.

4. **Prinsip Dasar Desain Keamanan**

   Ada beberapa prinsip dasar pada desain keamanan yaitu:

   - **Economy Of Mecganism** : keamanan yang harus seserdahan dan sekecil mungkin agar dapat diakses
   - **Fail-safe Default**: ketika gagal mengakses maka user memiliki alternatif lainnya
   - **Complete Mediation** : setiap askes harus melaui pengecekkan melalui mekanisme contol system
   - **Open design** : mekanisme dari desain harus terbuka dan tidak berisfat rahasia agar algoritma dapat diperbaiki
   - **Separation privilege** :beberapa atribut menjadi bentuk praktik yang memeiliki hak istimewa untuk mencapai akses ke sumber daya yang dibatasi
   - **Least privilege** :proses dan pengguna harus mengoprasikan dengan menggunakan hak istemwa yang diperlukan
   - **Least Common Mechanism** : meminimalkan fungsi yang dimiliki oleh semua pengguna
   - **PsycologicalAcceptability** : dalam pembentukam mekanisme keamanan tidak boleh terlalu mengganggu user sehimgga memenuhi standar keamanan yang ditetapkan
   - **Isolation** : mekanisme keamanan harus terisolasi
   - **Encapsulation**: objek data harus dikenali oleh di domainnya sendiri
   - **Modularity** : system keamana harush modular yang berarti dalam prosedurnya harus dapat disubstitusikan

- **Layering** : system kemanan harus dengan pendekatan berlapis-lapis

5. Konsep Attack Surface dan Attack Tree
   - **Attack Surface**, merupakan akumulasi kerentanan yang mudah dijangkau dan disalahgunakan dalam system seperti port yang terbuka, layanan di luar firewall, konsep ini terbagi dalam 3 kategori yaitu:
     – Network Attack Surface; Contoh : Kerentanan Jaringan.
     – Software Attack Surface; Contoh : Kerentanan Perangkat Lunak.
     – Human / Phisical Access Attack Surface; Contoh : Social Engineering
   - **Attack Tree**, konseptual diagram yang memperlihatkan bagaimana asset atau target dapat diserang yang tujuannya adalah lebih mudah dalam mengeksploitasi pada pola serangan

6. Strategi Pengamana Komputer

- **Kebijakan**, dalam pengamanan sebuah system harus memiliki kebijakan bahwa keamanan seperti apa yang dilakukan dengan cara mengidentifikasi asset dan nilainya, menggunakan acaman yang potensial, kemudahan pengguna dan hubungannya dengan kemanan serta biaya pengadaan system keamana dan recovery
- **Implementasi**, dalam pengamanan system harus menerapkan implementasi seperti pencegahan, mendeteksi, respon, serta perbaikan dalam sebuah keamanan systen
- **Evaluasi**, dimana tiap system keamanan harus bekerja dengan baik dengan menerapkan evaluasi pada strategi dengan cari memvalidasi dan mereview tiap kegiatan yang dilakukan pada system keamanan