# MENGEVALUASI SISTEM KEAMANAN JARINGAN

# A. PRINSIP DAN ANCAMAN KEAMANAN JARINGAN

Keamanan jaringan computer merupakan bagian dari sebuah system informasi yang sangat penting dalam menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya.

## 1. Prinsip keamanan jaringan

Prinsip keamanan jaringan dikatagorika menjadi 6 sebagai berikut:

### a. Kerahasiaan (Secrecy)

Secrecy berhubungan dengan hak akses untuk membaca data ,informasi dan suatu sistem computer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat dibaca oleh pihak yang telah diberi wewenang secara legal

### b. Integritas (Integrity)

Integrity berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem komputer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat diubah oleh pihak yang telah diberi hak.

### c. Ketersediaan (Availability)

Availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi yang terdapat pada sistem komputer dapat diakses dan dimanfaatkan oleh pihak yang berhak.

### d. Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses dan memberikan informasi adalah benar orang yang dimaksud, atau server yang kita hubungi adalah server yang asli.

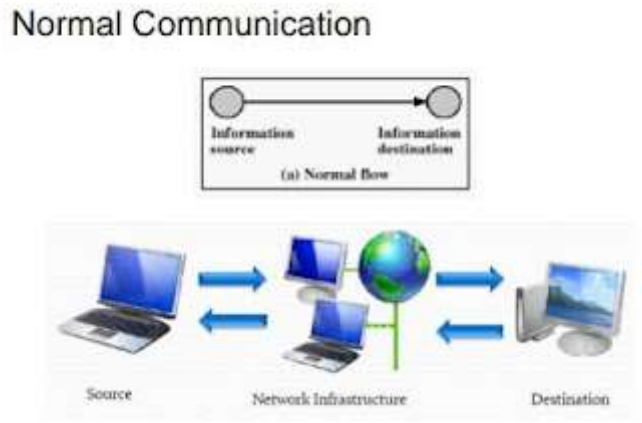
**e. Akses control**

Aspek kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana user berkomunikasi dengan sistem.Akses kontrol melindungi sistem dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkapi.

**f. Non repudation**

Non Repudiation adalah merupakan sebuah identifikasi yang bersifat individual atau devais yang diakses oleh user yang dikirim melalui jalur komunikasi melalui sebuah rekaman (systemlog). Rekaman itu akan digunakan sebagai bukti aksesibilitas user sehingga user tidak dapat menyangkal.

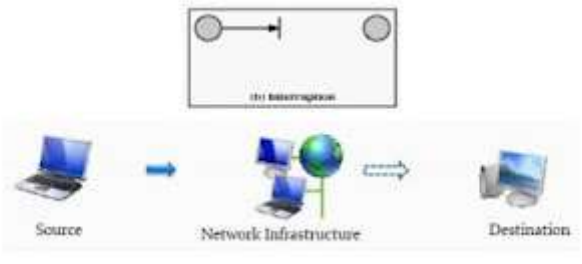
**2. Jenis gangguan, serangan dan ancaman keamanan jaringan**




Serangan terhadap keamanan system informasi security attack menjadi penyebab utama terjadinya kejahatan computer pada dunia maya yang dilakukan oleh kelompok orang yang inin menembus sesuatu keamanan sebauah system.

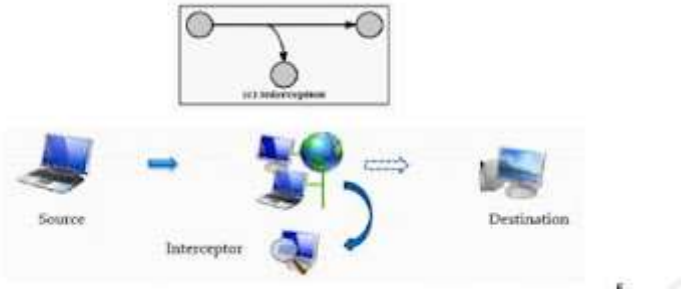
**Tipe serangan terhadap security attack:**

**a.) Interruption (interupsi layanan)**



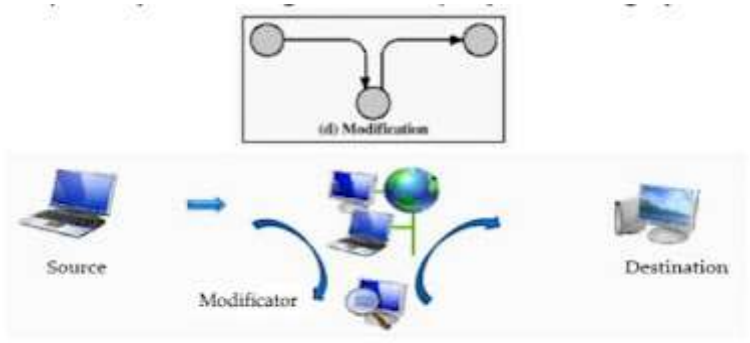

Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem.
Misalnya : perusakan terhadap suatu item hardware, pemutusan jalur komunikasi, disable sistem manajemen file

**b.) Interception (pengalihan layanan)**




Pengaksesan asset informasi oleh orang yang tidak berhak.
Misalnya oleh seseorang, program, atau komputer.
Contoh serangan ini pencurian data pengguna kartu kredit Pengerangan terhadap layanan confidentiality

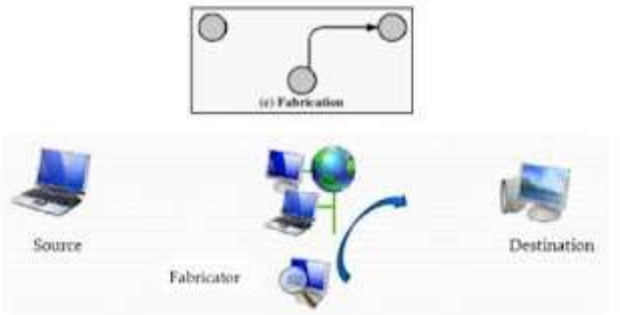
**c.) Modification (pengubahan)**




Pengaksesan data oleh orang yang tidak berhak, kemudian ditambah, dikurangi, atau diubah setelah itu baru dikirimkan pada jalur komunikasi

Contoh pengubahan suatu nilai file data Merupakan jenis serangan terhadap layanan integrity

**d.) Fabrication (produksi - pemalsuan)**




Seorang user yang tidak berhak mengambil data, kemudian menambahkannya dengan tujuan untuk dipalsukan Merupakan serangan terhadap layanan authentication

## A. Gangguan

Jenis gangguan keamanan jaringan diantara lain:

### 1. Carding

Pencurian data terhadap identitas perbankan seseorang. Misalnya pencurian nomor kartu kredit yang dimanfaatkan untuk berbelanja online.

### 2. Physing

Pemalsuan data resmi

### 3. Deface

Perubahan terhadap bentuk atau tampilan website.

### 4. Hacking

Perusakan pada infrastruktur jaringan komputer yang sudah ada.

## B. Serangan

Pada dasarnya serangan terhadap suatu data dalam suatu jaringan menurut jenisnya dapat dikatagorikan menjadi dua sebagai berikut:

1. **Serangan aktif**

Serangan aktif adalah serangan di mana penyerang mencoba mengubah informasi atau membuat pesan palsu. Pencegahan serangan ini cukup sulit karena berbagai potensi kerentanan fisik, jaringan, dan perangkat lunak. Alih-alih pencegahan, ia menekankan pada deteksi serangan dan pemulihan dari gangguan atau keterlambatan yang disebabkan olehnya.

Serangan aktif biasanya membutuhkan lebih banyak upaya dan implikasi sering kali lebih berbahaya. Ketika peretas mencoba menyerang, korban menyadarinya.

2. **Serangan Pasif**

Serangan pasif adalah serangan di mana penyerang memanjakan diri dalam menguping yang tidak sah, hanya memantau transmisi atau mengumpulkan informasi. Eavesdropper tidak membuat perubahan apa pun pada data atau sistem. Tidak seperti serangan aktif, serangan pasif sulit dideteksi karena tidak melibatkan perubahan dalam sumber daya sistem atau data. Dengan demikian, entitas yang diserang tidak mendapatkan petunjuk tentang serangan itu. Meskipun, itu dapat dicegah dengan menggunakan metode enkripsi di mana data pertama kali dikodekan dalam bahasa yang tidak dapat dipahami di ujung pengirim dan kemudian pada penerima ujung itu lagi dikonversi menjadi bahasa yang dapat dimengerti manusia.

## C. Ancaman

Bentuk ancaman pada keamanan jaringan memiliki 7 ancaman sebagai berikut:

### a) Sniffer

Peralatan yang dapat memonitor proses yang sedang berlangsung

### b) Spoofing

Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP.

**c) Remote Attack**

Segala bentuk serangan terhadap suatu sistem/komputer dimana penyerangnya memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jauh diluar sistem jaringan atau media transmisi

**d) Hole**

Kondisi dari software atau hardware yang bisa diakses oleh pemakai yang tidak memiliki hak / otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses otorisasi

**e) Phreaking**

Perilaku menjadikan sistem pengamanan telepon melemah

**f) Hacker**

Orang yang secara diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan men-share hasil ujicoba yang dilakukannya. Hacker tidak merusak sistem

**g) Craker**

Orang yang secara diam-diam mempelajari sistem dengan maksud jahat. Muncul karena sifat dasar manusia yang selalu ingin membangun (salah satunya merusak)