PRINSIP DASAR KEAMANAN KOMPUTER

PERTEMUAN 2

SECURITY ATTACK

- Segala bentuk pola, cara, metode yang dapat menimbulkan gangguan terhadap suatu sistem komputer atau jaringan

SECURITY ATTACK MODELS

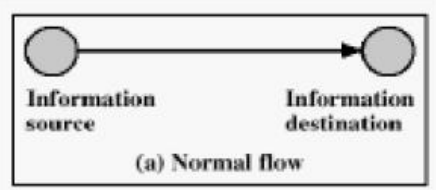
Interruption

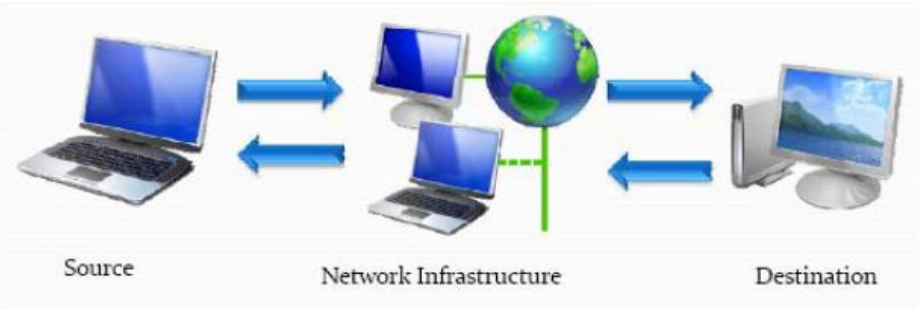
Interception

Modification

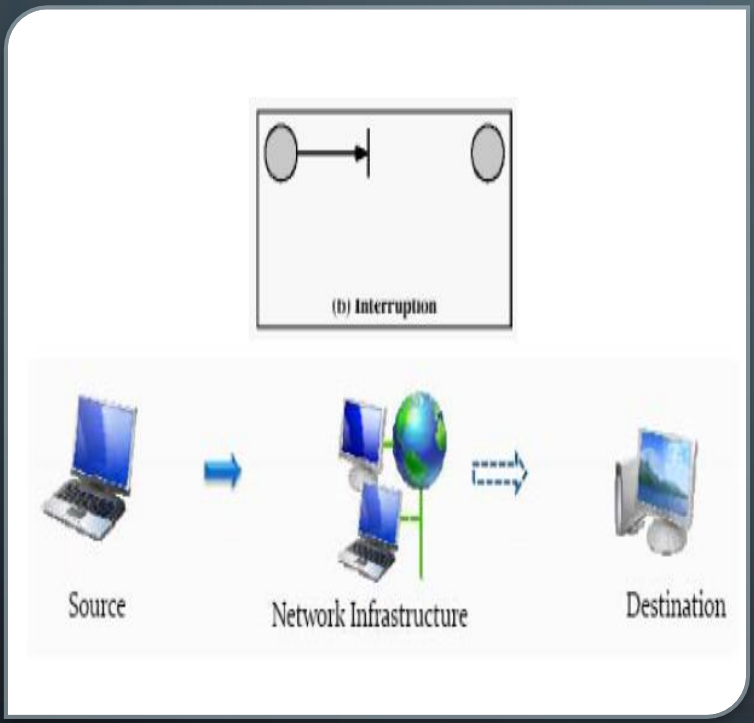
Fabrication

NORMAL COMMUNICATION



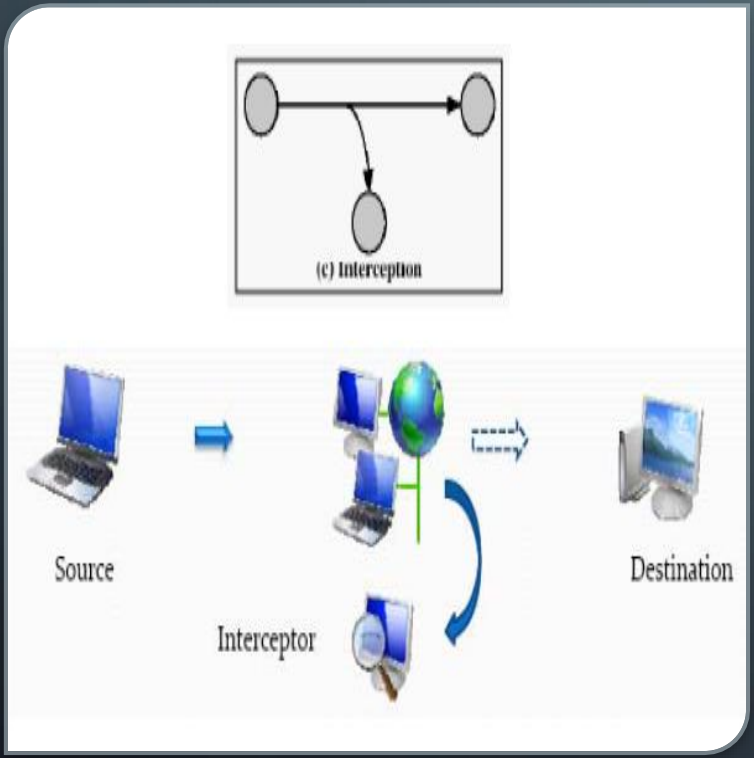


INTERRUPTION



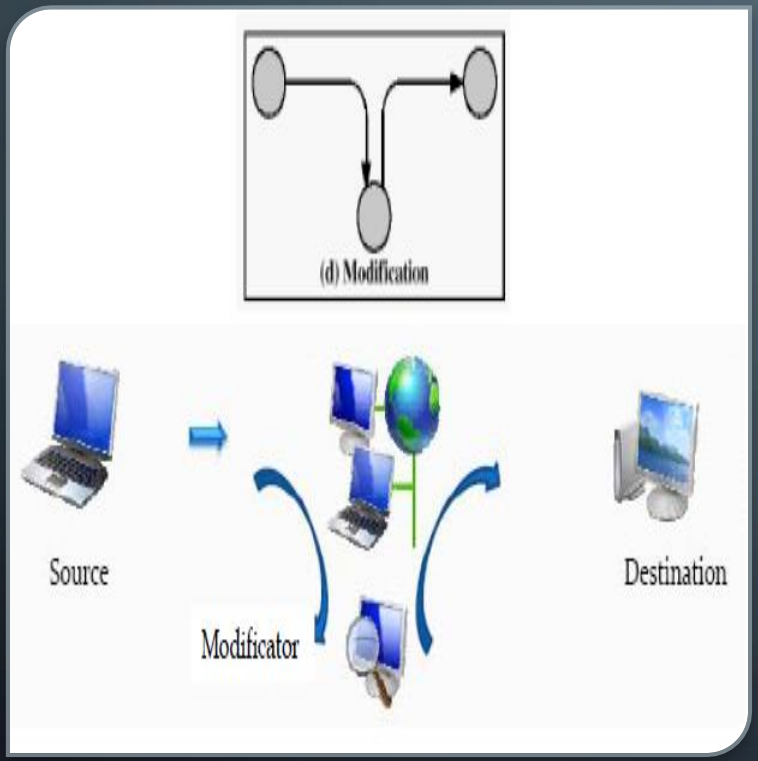
- Perangkat sistem menjadi rusak atau tidak tersedia
- Serangan ditujukan kepada ketersediaan (availability) dari sistem
- Misalnya : perusakan terhadap suatu item hardware, pemutusan jalur komunikasi, Menonaktifkan sistem manajemen file

INTERCEPTION



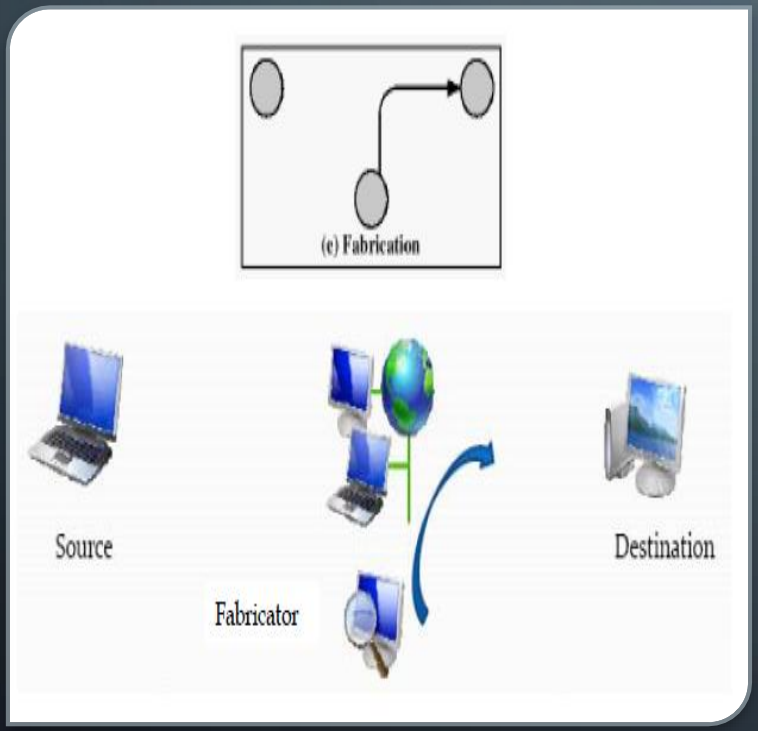
- Pengaksesan asset informasi oleh orang yang tidak berhak
- Penyerangan terhadap layanan confidentiality
- Contoh serangan ini adalah pencurian data pengguna kartu kredit

MODIFICATION

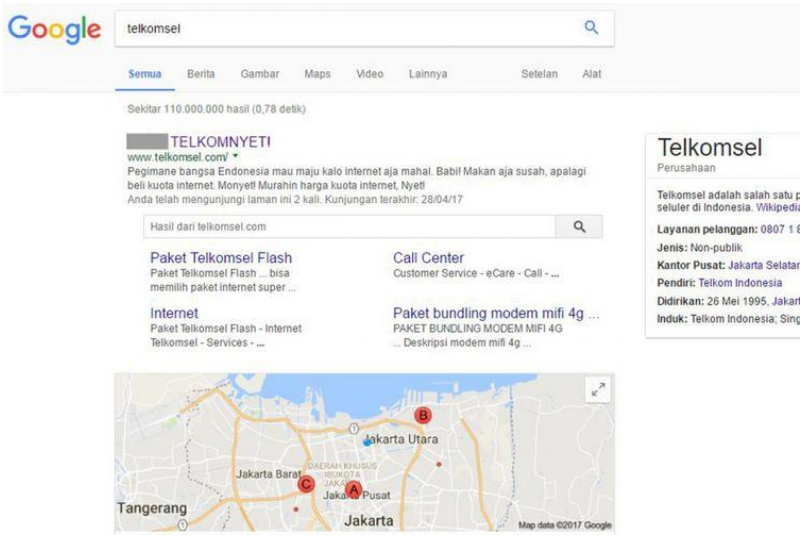


- Pengaksesan data oleh orang yang tidak berhak, kemudian ditambah, dikurangi, atau diubah setelah itu baru dikirimkan pada jalur komunikasi
- Merupakan jenis serangan terhadap layanan integrity
- Contoh pengubahan suatu nilai file data

FABRICATION



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



KASUS KEAMANAN KOMPUTER

2017

KASUS KEAMANAN KOMPUTER

- 2020

Pegiat media sosial Denny Siregar melaporkan dugaan kebocoran data dirinya ke Polda Metro Jaya, belum lama ini. Dalam pelaporannya, Denny membawa barang bukti berupa tangkapan layar pemilik akun yang menyebarkan data pribadinya. Dengan tersebarnya data pribadinya, Denny mengaku, ia dan keluarganya mendapatkan teror dari orang tidak dikenal, sehingga ia meminta polisi mengusut pihak yang menyebarkan data pribadinya ke media sosial. Kasus itupun ditanggapi Telkomsel sebagai operator selular yang digunakan denny. Andi Agus Akbar, Senior Vice President Corporate Secretary Telkomsel mengatakan.. "Kami sangat menyayangkan ketidaknyamanan sodara denny siregar sebagai pelanggan atas keluhan yang disampaikan terkait adanya dugaan penyalahgunaan data pelanggan". "Saat ini, kami terus melakukan koordinasi secara intensif dengan aparat penegak hukum, guna membantu kelancaran proses lanjutan atas pelaporan yang telah diajukan, serta mempercayakan sepenuhnya pada proses hukum yang sudah berjalan, sesuai aturan yang berlaku". Setelah dilakukan penyelidikan, pelaku pembobolan Data Pribadi Denny berhasil ditangkap. Ia merupakan karyawan Outsourcing Telkomsel Surabaya. Tersangka nekat membobol dan menyebarkan data pribadi karena tidak suka kepada Denny Siregar.

Sumber KompasTV, 13 Juli 2020

MEMAHAMI HACKER BEKERJA

- Secara umum Hacker bekerja melalui tahapan-tahapan sebagai berikut:
  - Mencari tahu sistem komputer yang menjadi sasaran
  - Penyusupan
  - Penjelajahan
  - Keluar dan menghilangkan jejak

PRINSIP DASAR PERANCANGAN SISTEM YANG AMAN

- Mencegah hilangnya data
- Mencegah masuknya penyusup

LAPISAN KEAMANAN

- Keamanan Fisik
- Keamanan Lokal
- Keamanan File dan Sistem File
- Keamanan Password dan Enkripsi
- Keamanan Kernel
- Keamanan Jaringan

LAPISAN FISIK

- Membatasi akses fisik ke mesin :
  - Akses masuk ke ruangan komputer
  - Penguncian komputer secara hardware
  - Keamanan BIOS
  - Keamanan Bootloader
- Back-up data :
  - Pemilihan piranti back-up
  - Penjadwalan back-up
- Mendeteksi gangguan fisik :
  - Log file : Log pendek atau tidak lengkap, Log yang berisikan waktu yang aneh, Log dengan permisi atau kepemilikan yang tidak tepat, Catatan pelayanan reboot atau restart, Log yang hilang, masukan su atau login dari tempat yang janggal
  - Mengontrol akses sumber daya.

KEAMANAN LOKAL

- Berkaitan dengan user dan hak-haknya :
  - Beri mereka fasilitas minimal yang diperlukan.
  - Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
  - Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses (biasanya berhubungan dengan transaksi).

KEAMANAN ROOT

- Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu, terutama perintah yang menggunakan globbing: contoh, anda ingin melakukan "rm foo*.bak", pertama coba dulu: "ls foo*.bak" dan pastikan anda ingin menghapus file-file yang anda pikirkan.
- Beberapa orang merasa terbantu ketika melakukan "touch /-i" pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : "rm -fr *" menanyakan apakah anda benar-benar ingin menghapus seluruh file. (Shell anda menguraikan "-i" dulu, dan memberlakukannya sebagai option -i ke rm).
- Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga anda yakin apa yang perlu dilakukan oleh root.
- Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokal yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan '.', yang berarti 'direktori saat ini', dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.
- Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.
- File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian 'su' jika anda butuh (mudah-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.
- Selalu perlahan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

KEAMANAN FILE DAN SISTEM FILE

- Directory home user tidak boleh mengakses perintah mengubah system seperti partisi, perubahan device dan lain-lain.
- Lakukan setting limit system file.
- Atur akses dan permission file : read, write, execute bagi user maupun group.
- Selalu cek program-program yang tidak dikenal

KEAMANAN PASSWORD DAN ENKRIPSI

- Hati-hati terhadap bruto force attack dengan membuat password yang baik.
- Selalu mengenkripsi file yang dipertukarkan.
- Lakukan pengamanan pada level tampilan, seperti screen saver.

KEAMANAN KERNEL

- Selalu update kernel system operasi.
- Ikuti review bugs dan kekurang-kekurangan pada sistem operasi.

KEAMANAN JARINGAN

- Waspadai paket sniffer yang sering menyadap port Ethernet
- Lakukan prosedur untuk mengecek integritas data
- Verifikasi informasi DNS
- Lindungi network file system
- Gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal