KEAMANAN SISTEM OPERASI

PERTEMUAN 11

ACCESS CONTROL

- Access control pada sistem operasi mengatur kemampuan akses user dalam suatu jaringan, komputer atau aplikasi.
- Sistem access control pada jaringan data umumnya menggunakan firewall. Firewall akan bertindak sebagai pembatas terhadap orang-orang yang tidak berhak mengakses jaringan.

KEMAMPUAN-KEMAMPUAN FIREWALL :

IP Hiding/Mapping

- Kemampuan ini mengakibatkan IP address dalam jaringan ditransalasikan ke suatu IP address yang baru. Dengan demikian, IP address dalam jaringan tidak akan dikenali di internet.

Privilege Limitation

- Dengan kemampuan ini, kita juga bisa membatasi para user jaringan sesuai dengan otorisasi atau hak-hak yang diberikan kepadanya.

Outside Limitation

- Kemampuan ini, dapat membatasi para user dalam jaringan untuk mengakses ke alamat-alamat tertentu di luar jangkauan kita.

Inside Limitation

- Kita memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu computer dalam jaringan kita. Selain itu, tidak diperbolehkan untuk mengakses seluruh komputer yang terhubung ke jaringan kita

Password dan Encrypted Authentication

- Beberapa user di luar jaringan memang diizinkan untuk masuk ke jaringan kita untuk mengakses data, dengan terlebih dahulu harus memasukkan password khusus yang sudah terenkripsi.

ADA 3 MACAM PEMBAGIAN FIREWALL BERDASARKAN CARA KERJANYA:

Internet firewalls

- Merupakan sistem atau grup sistem yang memberikan kebijakan keamanan pada hubungan antara jaringan korporasi dan internet. Firewall mengatur layanan-layanan apa yang bisa di akses dari luar sistem. Internet firewall dapat berupa perangkat fisik atau software yang menyaring header paket bergantung pada kebijakan keamanan.

Packet filtering firewalls

- Merupakan tipe firewall yang melakukan control akses ke dalam maupun keluar jaringan. Packet filter firewalls dapat berupa router maupun switch yang dapat dikonfigurasi dengan access list. Izin maupun penolakan akses didasarkan pada protocol, port asal maupun port tujuan alamat IP asal maupun tujuan.

Application/proxy firewalls

- Perangkat atau software ini menjamin bahwa resource yang terlindungi tidak bisa diakses oleh sembarang user. Pada saat ini ada beberapa aplikasi firewall yang dapat dipasang di PC diantaranya adalah : McAfee, Personal Firewall, Symantec Norton Personal Firewall 2000, Network ICE Blackice Defender, dll.

FUNGSI ACCESS CONTROL

- Memberikan ijin kepada user yang berhak (authorized) agar dapat mengakses sistem/sumber data/proses sistem.
- Memberikan hak (Grant) atau menghapus hak (Deny) sesuai dengan security yang telah di tentukan, yang mempunyai ijin (permission) untuk mengakses sumber data.
- Sekumpulan prosedur yang dibentuk oleh hardware, software dan administrator, untuk memonitor akses, mengidentifikasi user yang meminta akses, merecord yang diakses dan memberikan akses grant atau deny berdasarkan aturan yang sudah ditetapkan.

KLASIFIKASI ASET INFORMASI

- Siapa yang mempunyai hak akses dan untuk apa ?
- Level akses yang diberikan
- Siapa yang bertanggungjawab untuk menentukan hak akses dan level akses
- Persetujuan apa yang diperlukan untuk melakukan akses?

KENDALI ACCESS CONTROL

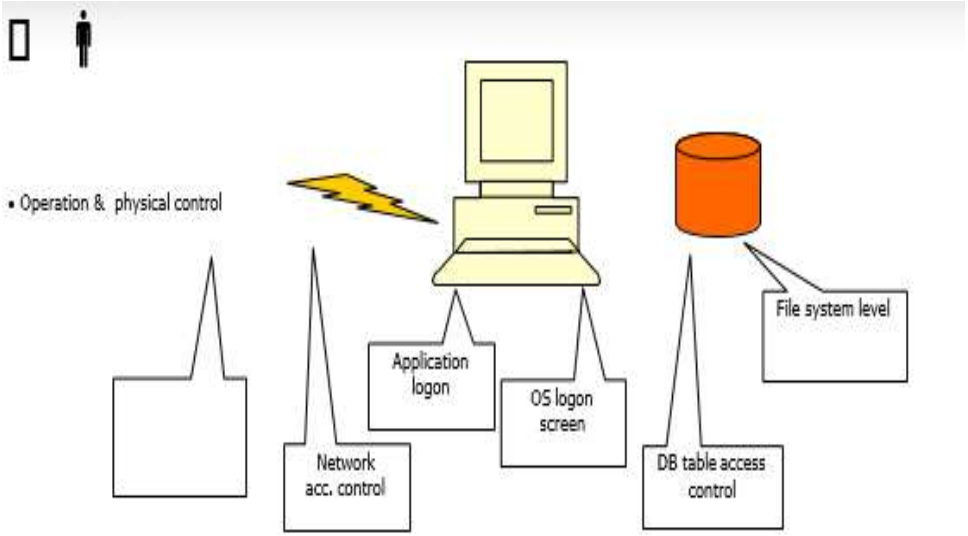
Tujuan untuk mengurangi resiko

- Administrative Control: policies, prosedur, security awareness/training, supervisi, dll.
- Logical/Technical Control: pembatasan akses ke sistem dan teknik proteksi yang digunakan, mis. Smart cards, enkripsi dll.
- Physical Control: penjagaan fisik, mis. Biometric door lock, secured area utk server, deadman door dll.

SECURITY ARCHITECTURE & MODELS (1)

- Arsitektur keamanan merupakan informasi mendasar mengenai penyelengaraan terkait sistem informasi, oleh karna itu hal ini menjadi sangat penting bagi profesional keamanan dalam mengerti arsitektur komputer, mekanisme proteksi dan masalah distributed environment security.
- model-model formal yang menyediakan framework untuk kebijakan keamanan. Sebagai tambahan, para profesional harus mempunyai pengetahuan mengenai assurance evaluation, sertifikasi, dan petunjuk akreditasi dan standar

SECURITY ARCHITECTURE & MODELS (2)



- Mempelajari konsep, prinsip, standar unutk merancang dan mengimplentasikan aplikasi, sistem operasi dan sistem yang aman

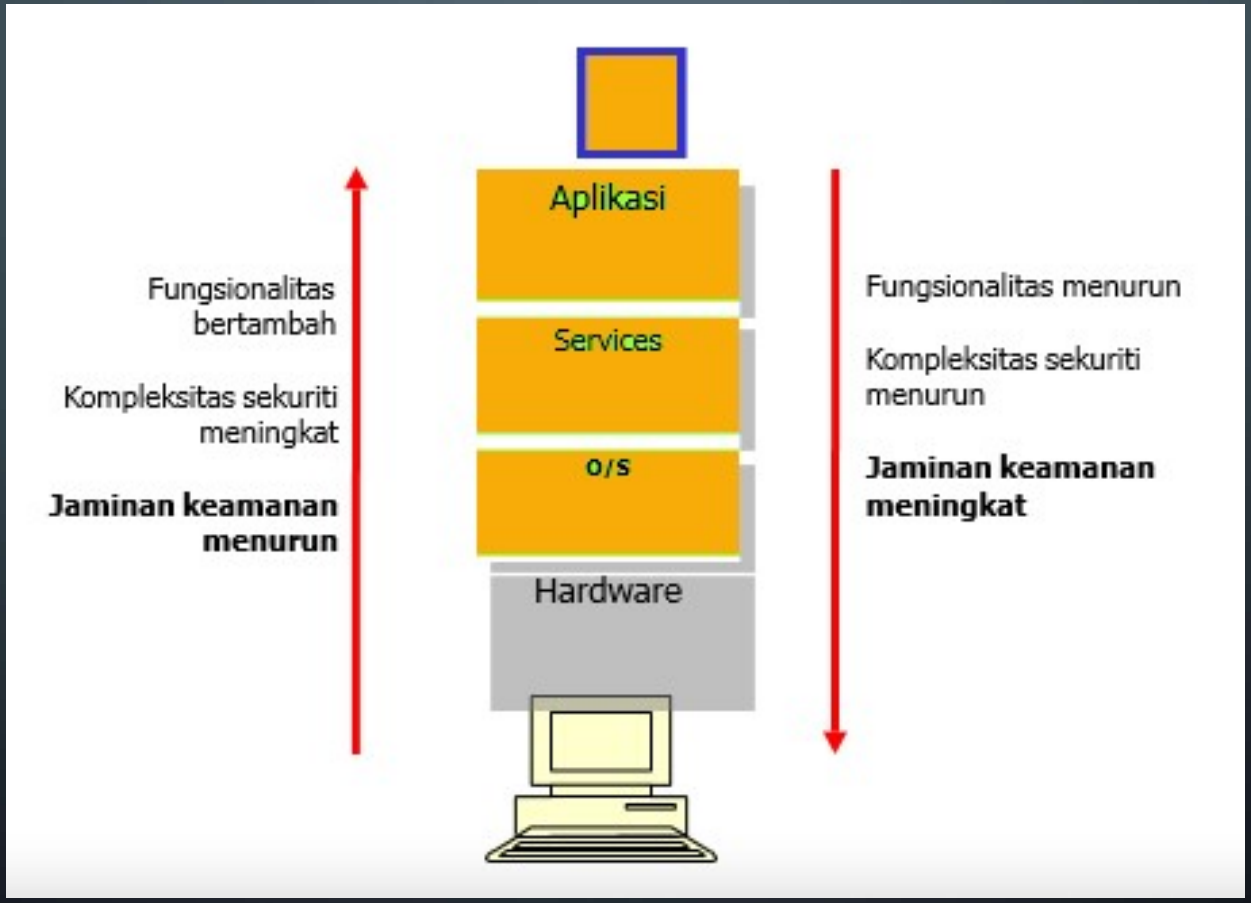
PRINSIP-PRINSIP KEAMANAN (1)

- Least Previlage: pemberian akses sesuai kebutuhan
    - Contoh: Seorang admin TU sekolah hanya berhak menginput data dan memeriksa datanya tidak dapat mengubah nilai pembayaran dan biaya keterlambatan dan memeriksa keuangan sekolah.
- Defence in Depth: berbagai perangkat keamanan untuk saling membackup
    - Contoh: Sebuah Divisi / Departemen harus selalu membackup datanya pagi dan sore hari dan menyiapkan double peyimpanan atau misalnya dua cd peyimpanan agar jika salah satu mengalami kerusakan maka masih ada backup satunya.
- Choke Point: semua keluar masuk lewat gerbang satu gerbang tidak diperkenankan melalui jalur lain
- Weakst Link: mengetahui kelemahan sekuriti sistem didalam organisasi, kelemahan didalam jaringan harus selalu diawasi dan dimonitor agar jika ada virus baru segera terdeteksi, Pentingnya mengupdate antivirus baik di server maupun di client

PRINSIP-PRINSIP KEAMANAN (2)

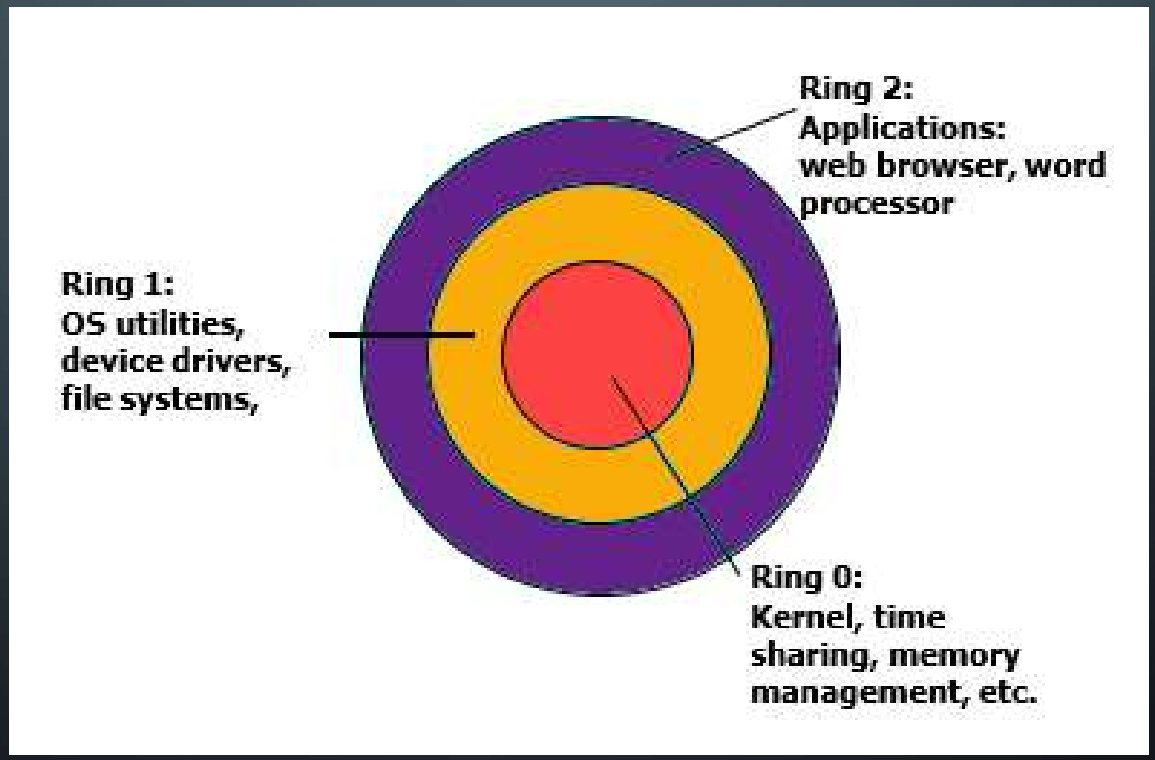
- Fail-Safe Stance: jika suatu perangkat rusak, maka secara default perangkat disetting ke settingan paling aman
    - Contoh : Jika sebuah kapal selam diudara mengalami kegagalan / kerusakan didalam air maka secara otomatis sistem akan memuat setingan mengapung dan pinutnya akan Unlock secara otomatis
    - Contoh :packet filtering kalau rusak akan mencegah semua paket keluar-masuk. Bila packet filtering pada firewall modem router ADSL rusak maka semua paket keluar-masuk akan dicegah
- Unversal participation: semua orang dalam organisasi harus terlibat dalam security, dan dilakukan pelatihan setiap 3 bulan sekali unutk menyegarkan ingatan pentingya menggunakan dan menerapkan keamanan komputer dalam proses kerja agar lebih efisien
- Diversity of defence: penggunaan sistem yang berbeda untuk keamanan agar jika penyerang sudah melumpuhkan sistem kemanana yang satu masih ada sistem kemamana yang berbeda yang membuat penyerang harus belajar kembali untuk melumpuhkan sistem.
- Simplicity: sistem jangan terlalu kompleks karena akan sangat sulit mencari bugs jika terlalu sulit dipahami.

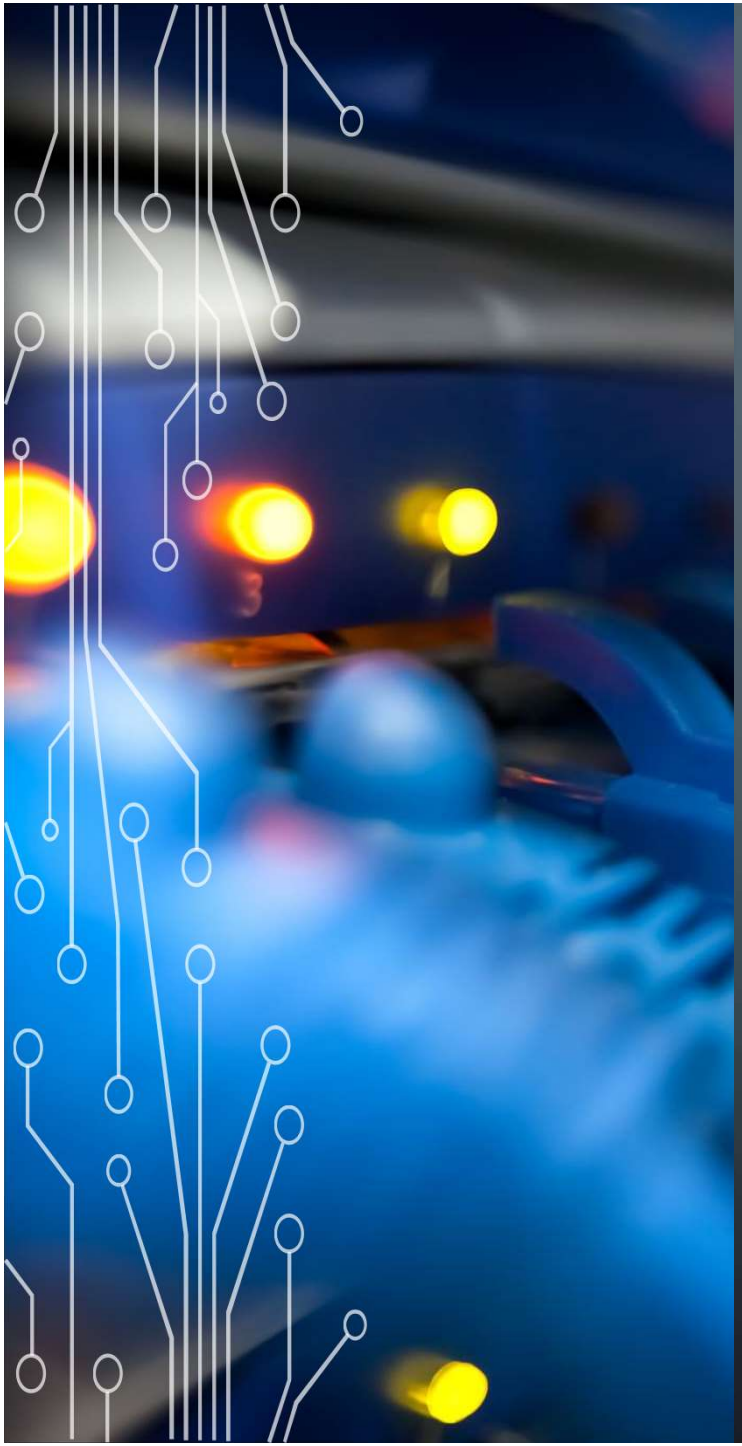
TINGKATAN JAMINAN KEAMANAN



SYSTEM ARCHITECTURE SECURITY

Contoh pada Sistem Operasi





KEAMANAN SISTEM OPERASI LINUX

Komponen arsitektur keamanan Linux:

- Account pemakai
- Kontrol akses secara diskresi (Discretionary Access Control)
- Kontrol akses jaringan (Network Access Control)
- Enkripsi
- Logging Deteksi Penyusupan (Intrusion Detection)

KEAMANAN SISTEM OPERASI LINUX ACCOUNT PEMAKAI

Kelebihan atau keuntungan yang didapat dalam hal ini :

- Pengendalaian dalam satu account yaitu ROOT memudahkan pengendalian administrasi sistem
- Kesalahan yang di buat user tidak berpengaruh terhadap sistem secara keseluruhan
- setiap account pemakai memeiliki privacy yang ketat

Macam User dalam linux:

- Root : kontrol system file, user, sumber daya (devices) dan akses jaringan
- User : account dengan kekuasaan yang diatur oleh root dalam melakukan aktifitas dalam sistem.
- Group : kumpulan user yang memiliki hak sharing yang sejenis terhadap suatu devices tertentu.

DISCRETIONARY ACESS CONTROL

DAC adalah metode pembatasan yang ketat, yang meliputi:

- Setiap account memiliki username dan password sendiri
- Setiap file/device memiliki atribut (read/write/execution) kepemilikan, group, dan user umum

PENERAPAN DAC

-	rw-	r--	r--	9	Goh	hack	318	mar	30	09:05	Borg.dea d. letter
1	2	3	4	5	6	7	8	9		10	11

Keterangan :

1 = tipe dari file ; tanda dash (-) berarti file biasa, d berarti directory, l berarti file link, dsb
2 = Izin akses untuk owner (pemilik), r=read/baca, w=write/tulis, x=execute/eksekusi
3 = Izin akses untuk group
4 = Izin akses untuk other (user lain yang berada di luar group yang didefinisikan sebelumnya)
5 = Jumlah link file
6 = Nama pemilik (owner)
7 = Nama Group
8 = Besar file dalam byte
9 = Bulan dan tanggal update terakhir
10 = Waktu update terakhir
11 = Nama file/device

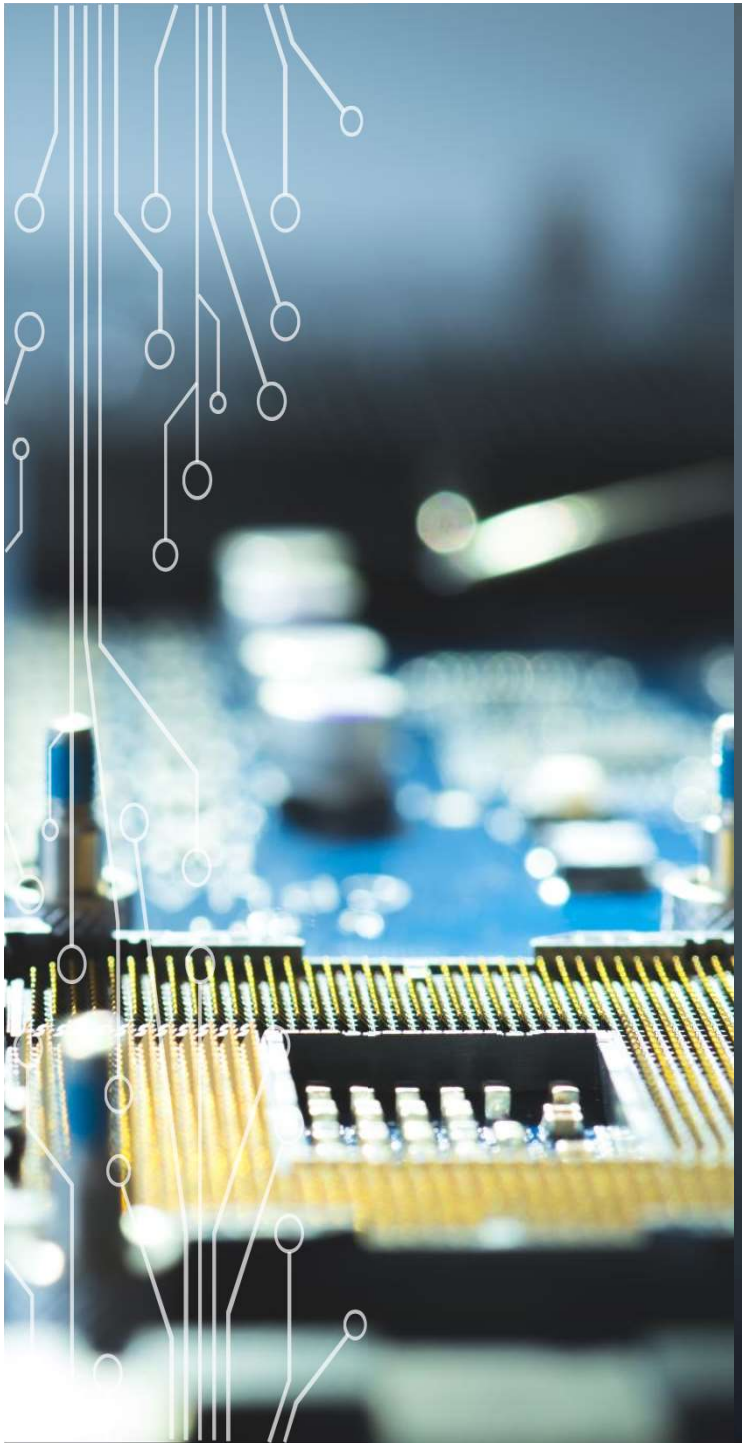
PERINTAH-PERINTAH PENTING DAC (1)

Mengubah izin akses file:

- chmod < u | g | o > < + | - > < r | w | x > nama file, contoh : chmod u+x g+w o-r borg.dead.letter ; tambahkan akses eksekusi (x) untuk user (u), tambahkan juga akses write (w) untuk group (g) dan kurangi izin akses read (r) untuk other (o) user.
- chmod metode octal, chmod - - - namafile , digit dash (-) pertama untuk izin akses user, digit ke-2 untuk izin akses group dan digit k e-3 untuk izin akses other, berlaku ketentuan : r(read) = 4, w(write) = 2, x (execute) = 1 dan tanpa izin akses = 0.
    - Contoh :
        - Chmod 740 borg.dead.letter
        - Berarti : bagi file borg.dead.letter berlaku
        - digit ke-1 -> 7=4+2+1=izin akses r,w,x penuh untuk user. digit ke-2 -> 4=4+0+0=izin akses r untuk group
        - digit ke-3 -> 0=0+0+0=tanpa izin akses untuk other user.

PERINTAH-PERINTAH PENTING DAC (2)

- Mengubah kepemilikan : chown <owner><nama file>
- Mengubah kepemilikan group: chgrp<group owner><nama file>
- Menggunakan account root untuk sementara:
  - ~$su; sistem akan meminta password Password: ****;prompt akan berubah jadi pagar,tanda login sebagai root
- Mengaktifkan shadow password, yaitu membuat file /etc/passwd menjadi dapat dibaca (readable) tetapi tidak lagi berisi password, karena sudah dipindahkan ke /etc/shadow.
- Perlunya Pro Aktif Password, Linux menggunakan metode DES (Data Encription Standart) untuk passwordnya.
- User harus training dalam memilih password supaya tidak mudah ditebak dengan program crack password.
- Perlu adanya program bantu cek keamanan password seperti:
  - Passwd+ :meningkatkan loging dan mengingatkan user jika mengisi password yang mudah ditebak
  - Anlpasswd: dapat membuat aturan standar pengisian password seperti batas minimum, gabungan huruf besar kecil, dsb.



NETWORK ACCESS CONTROL

Firewall linux

- Fungsinya: analisis dan filtering paket, blocking content dan protocol, autentikasi koneksi dan enkripsi.
- Tipenya: Application-proxy firewall/ application gateways, Network Level Firewall

PENERAPAN ENKRIPSI DI LINUX

- Password : DES (Data Encryption Standard)
- Komunikasi data:
  - Secure Shell
  - (SSH) Program yang melakukan loging terhadap komputer lain dalam jaringan, mengeksekusi perintah lewat mes in secara remote dan memindahkan file dari satu mesin k e mesin lainnya
- Secure Socket Layer
  - (SSL) mengenkripsi data yang dikirimkan lewat port http. Konfigurasi dilakukan di : web server APACHE dengan ditambah PATCH SSL

LOGGING

- Prosedur dari Sistem Operasi atau aplikasi merekam setiap kejadian dan menyimpan rekaman tersebut untuk dapat dianalisa.
- Semua file log linux disimpan di directory /var/log, antara lain :
  - Lastlog : rekaman user login terakhir kali
  - last : rekaman user yang pernah login dengan mencarinya pada file /var/log/wtmp
  - xferlog : rekaman informasi login di ftp daemon berupa data wktu akses, durasi transfer file, ip dan dns host yang mengakses, jumlah/nama file, tipe transfer(b inary/ASCII), arah transfer(incoming/outgoing), modus akses(anonymous/guest/ user resmi), nama/id/layanan user dan metode otentikasi.
  - Access_log : rekaman layanan http / webserver.
  - Error_log : rekaman pesan kesalahan atas service http / webserver berupa data ja m dan waktu, tipe/alasan kesalahan
  - Messages : rekaman kejadian pada kernel ditangani oleh dua daemon :
  - Syslog : merekam semua program yang dijalankan, konfigurasi pada syslog.conf
  - Klog :menerima dan merekam semua pesan kernel

DETEKSI PENYUSUPAN (INTRUSION DETECTION)

aktivitas mendeteksi penyusupan secara cepat dengan menggunakan program khusus secara otomatis yang disebut Intrusion Detection System

Tipe dasar IDS:

- Ruled based system: mencatat lalu lintas data jika sesuai dengan database dari tanda penyusupan yang telah dikenal, maka langsung dikategorikan penyusupan.
    - Pendekatan Ruled based system :
        - Preemptory (pencegahan) ; IDS akan memperhatikan semua lalu lintas jaringan, dan langsung bertindak jika dicurigai ada penyusupan.
        - Reactionary (reaksi) ; IDS hanya mengamati file log saja.
            - Adptive system: Penerapan expert system dalam mengamati lalu lintas jaringan.

Program IDS:

- Chkwtmp: program pengecekan terhadap entry kosong.
- Tcplogd: program pendeteksi stealth scan (scanning yang dilakukan tanpa membuat sesi Tcp)
- Host entry: program pendeteksi login anomaly (perilaku aneh)

KEAMANAN SISTEM OPERASI WINDOWS NT

Komponen Arsitektur Keamanan NT:

Account

- Jenis account user (admin, guest, user)
- Jenis account group (admin, guest,user,operator back up, power user, operator server, operator account, operator printer
- Hak akses user/group
- Hak basic dan Hak advance

KOMPONEN ARSITEKTUR KEAMANAN NT:

- Keamanan Sistem File
  - NTFS :
    - Cepat dalam operasi standar file (read – write – search)
    - Terdapat system file recovery, access control dan permission.
    - Memandang obyek sebagai kumpulan atribut, termasuk permission access.
  - Proteksi untuk integritas data
    - Transaction logging: merupakan system file yang dapat di-recovery untuk dapat mencatat semua perubahan terakhir pada directory dan file secara otomatis.
    - Sector sparing: Teknik dynamic data recovery yang hanya terdapat pada disk SCSI dengan cara memanfaatkan teknologi fault-tolerant volume untuk membuat duplikat data dari sector yang mengalami error. Metodenya adalah dengan merekalkulasi dari stripe set with parity atau dengan membaca sector dari mirror drive dan menulis data tersebut ke sektor baru.
    - Cluster remapping: Jika ada kegagalan dalam transaksi I/O pada disk , secara otomatis akan mencari cluster baru yang tidak rusak, lalu menandai alamat cluster yang mengandung bad sector tersebut.
    - Fault Tolerance: Kemampuan untuk menyediakan data secara realtime yang akan memberi tindakan penyelematan bila terjadi kegagalan perangkat keras, korupsi perangkat lunak dan lainnya, teknologi RAID (Redudant Arrays of Inexpensive Disk)

KOMPONEN ARSITEKTUR KEAMANAN NT:

- Model Keamanan Window NT
  - Beberapa komponen yang bekerja sama untuk memberikan keamanan logon dan acces control list (ACL) dalam NT:
    - LSA (Local Security Authority) : menjamin user memiliki hak untuk mengakses system. Inti keamanan yang menciptakan akses token, mengadministrasi kebijakan keamanan local dan memberikan layanan otentikasi user.
    - Proses Logon : menerima permintaan logon dari user (logon interaktif dan logon remote), menanti masukan username dan password yang benar. Dibantu oleh Netlogon service.
    - Security Account Manager (SAM) : dikenal juga sebagai directory service database, yang memelihara database untuk account user dan memberikan layan validasi untuk proses LSA.
    - Security Reference Monitor (SRM) : memeriksa status izin user dalam mengakses, dan hak user untuk memanipulasi obyek serta membuat pesan-pesan audit.

KOMPONEN ARSITEKTUR KEAMANAN NT:

- Keamanan Sumber Daya Lokal
  - Objek Security Descriptor:
  - Security ID Owner
  - Security ID Group
  - Discretionary ACL
  - System ACL
- Keamanan Jaringan
  - Jenis keamanan jaringan windows NT:
    - Model Keamanan user level : account user akan mendapatkan akses untuk pemakaian bersama dengan menciptakan share atas directory atau printer.
      - Keunggulan : kemampuan untuk memberikan user tertentu akses ke sumberdaya yang di-share dan menentukan jenis akses apa yang diberikan.
      - Kelemahan : proses setup yang kompleks karena administrator harus memberitahu set iap user dan menjaga policy system keamanan tetap dapat dibawah kendalinya dengan baik.
    - Model Keamanan share level : dikaitkan dengan jaringan peer to peer, dimana user manapun membagi sumber daya dan memutuskan apakaha diperlukan password untuk suatu akses tertentu.
      - Keuntungan : kesederhanaannya yang membuat keamanan share-level tidak membutuhkan account user untuk mendapatkan akses.
      - Kelemahan : sekali izin akses / password diberikan, tidak ada kendali atas siap yang menakses sumber daya.

Cara NT menangani keamanan jaringan:

- Memberikan permission
  - Permision NTFS LOCAL
  - Permision Shere
- Keamanan RAS (Remote Access Server)
  - Melakukan remote access user menggunakan dial-up :
    - Otentikasi user name dan password yang valid dengan dial-in permission.
    - Callback security : pengecekan nomor telepon yang valid.
    - Auditing : menggunakan auditing trails untuk melacak ke/dari siapa, kapan user memiliki akses ke server dan sumberdaya apa yang diakses.
- Pengamanan Layanan Internet
  - Firewall terbatas pada Internet Information server (IIS).
  - Menginstal tambahan proxy seperti Microsoft Proxy server.
- Share administrative
  - memungkin administrator mendapatkan akses ke server windows NT atau workstation melalui jaringan

KOMPONEN ARSITEKTUR KEAMANAN NT:

- Keamanan Pada Printer
  - Dilakukan dengan setting properties printer:
    - Menentukan permission: full control (admin), manage document (owner), print (semua user).
    - Mengontrol print job (setting waktu cetak, prioritas, notifikasi)
    - Set auditing information
- Keamanan Pada Registry
  - Tools yang disediakan untuk akses registry:
    - System policy editor
    - Registry editor (regedit32.exe)
    - Windows NT diagnostics (winmsd.exe)
  - Tools backup untuk registry:
    - Regback.exe
      - Regback.exe memanfaatkan command line / remote session untuk membackupr registry.
    - Ntbackup.exe : otomatisasi backup HANYA pada Tape drive, termasuk sebuah kopi dari file backup registry local.
    - Emergency repair disk (rdisk.exe) : memback-up hive system dan software dalam registry.

KOMPONEN ARSITEKTUR KEAMANAN NT:

- Audit Dan Pencatatan LOG
  - Pencatatan logon dan logoff termasuk pencatatan dalam multi entry login
  - Object access (pencatatan akses obyek dan file)
  - Privilege Use (paencatatan pemakaian hak user)
  - Account Management (manajemen user dan group)
  - Policy change (Pencatatan perubahan kebijakan keamanan)
  - System event (pencatatan proses restart, shutdown dan pesan system)
  - Detailed tracking (pencatatan proses dalam system secara detail)