BAB IX
KEAMANAN SISTEM OPERASI KOMPUTER

9.1 Access Control

Kontrol akses adalah suatu proses dimana user diberikan akses dan hak untuk melihat sistem, sumber atau informasi. Untuk keamanan komputer, access control meliputi otorisasi, otentikasi, dan audit dari suatu kesatuan untuk memperoleh akses. Access control memiliki subjek dan objek. User (manusia), adalah subjek yang mencoba untuk mendapatkan akses dari objek, Software. Dalam sistem komputer, daftar access control berisi perizinan dan data kemana user memberikan izin tersebut. Data yang telah memiliki izin hanya dapat dilihat oleh beberapa orang dan ini tentunya sudah dikontrol oleh *access control.* Hal ini memungkinkan administrator untuk mengamankan informasi dan mengatur hak atas informasi apa saja yang boleh diakses, siapa yang bisa mengakses informasi tersebut, dan kapan informasi tersebut bisa diakses. (Prameswari 2018)

Kontrol akses mendukung baik kerahasiaan dan integritas dari sebuah sistem yang aman. Kerahasiaan melindungi informasi dari orang yang tidak berhak.[14]

Mekanisme kontrol akses akan melakukan pengecekan hak dari pengguna, berdasarkan otorisasi yang telah ditetapkan. Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.[4]

Tantangan dalam Access Control, yaitu :

1. Berbagai macam tipe user membutuhkan level akses yang berbeda
2. Berbagai macam sumber memiliki klasifikasi level yang berbeda
3. Bermacam-macam data identitas harus disimpan di tipe user berbeda
4. Lingkungan perusahaan berubah secara kontinuitas

Tipe – tipe Access Control, yaitu :

1. **Preventative** : Menghindari munculnya hal-hal yang tidak diinginkan
2. **Detective** : Mengidentifikasi kejadian tidak diinginkan yang sudah muncul
3. **Corrective** : Membenahi kejadian tidak diinginkan yang sudah muncul
4. **Deterrent** : Menghalangi pelanggaran keamanan
5. **Recovery** : Mengembalikan sumber dan kemampuan
6. **Compensative** : Menyediakan alternatif ke kontrol lainnya

Implementasi :

- Administrative Control : Policies,Prosedur,Security awareness\training supervisi dll

- Logical\Technical : Pembatatsan acces ke sistem dan teknik proteksi yang di gunakan, mis,Smart Cards,enkripsi dll
- Physical Control : Penjagaan fisik,mis,Biometric door lock,secured area untuk serever, deadman door dll

Logical Acces Control

Akses Kontrol Infastruktur TI dapat di lakukan pada berbagai tingkat, yaitu :

1. Front end (user) and Back end (server)
2. Bagaimana jaringan terbagi dan perlindungan akses ke sumber informasi
   - ➢ Paths of logical Acces
     - ✓ Point umum dari Entry
       - Network Connectivity
       - Remote acces
       - Operator Con sole
       - Online Workstation or terminals

Logical Acces Control : Protection

Tujuan:

1. Cegah akses dan modifikasi data sensitif organisasi dari orang yang tidak mempunyai otorisasi dan penggunaan fungsi sistem kritis.
2. Semua layar ,network,operating system,data bases dan application system

Fungsi Software

1. Identifikasi dan otentikasi
2. Otorisasi akses
3. Monitor : Login aktifitas user,reporting

Implementasi Paling efekif : Tingkat Networks dan operating system (membatasi priveleges pada low level)

Logical Acces Control : Software

Secara umum fungsi akses kontrol sistem operasi meliputi :

1. Mekanisasi identifikasi dan otentikasi user
2. Restriced logon IDS
3. Aturan akses untuk sumber informasi yang spesifik
4. Create Individual account ility and Auditability
5. Create or change user profile
6. Log events
7. Log user activities
8. Report Capabilities

Fungsi akses kontrol basis data dan aplikasi meliputi :

1. Create of change data files and database profiles
2. Verify user authorization at the application and transaction levels
3. Verify user authorization within the applicationn
4. Verify subsystem authorization fot the user at the file level

5. Log database\data communication access activities for monitoring access violations

9.2 Access Control Matrix

Transaksi yang aman tetap di pertanyakan karena tidak yakin apakah e-mail purchase order yang diterima benar-benar otentik, apakah transfer bonus anggota tidak diubah-ubah.

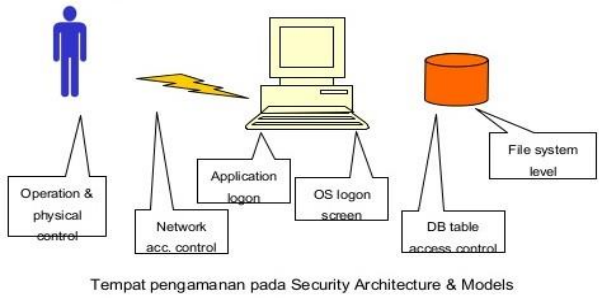
- Bagaimana Caranya supaya wibsate saya tidak di Hack orang?
- Bagaimana Caranya agar kita yakin bahwa e-mail purchase order yang kita terima benar-benar otentik?
- Bagaimana caranya agar yakin bahwa nilai 100 juta dalam fund transfer tidak di ubah-ubah?

Untuk meyakinkan hal ini maka di pelajari Security Architecture & Models.

9.3 Security Architecture dan Models

Tujuannya :

1. Mempelajari berbagai konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi, sistem operasi, dan sistem yang aman.

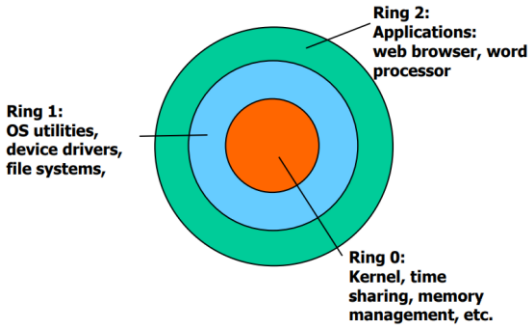


Gambar 9.1 Konsep pengamanan security Architecture & Models

Bagian ini akan menjelaskan teknik teknik keamanan sebuah informasi pada sebuah sistem. Model-model ini untuk memformalkan kebijakan-kebijakan yang telah dibuat. Model keamanan informasi ini dibagi dalam tiga kelompok menurut fungsinya, Access Control Models, Integrity Models, dan Information Flow Models. Untuk memperdalam pemahaman tentang Security Architecture and Models, tulisan akan membahas penerapan teori yang sudah dijelaskan dengan ilustrasi penerapannya pada usaha kecil dan menengah.

9.3.1 Rings

Satu perencanaan yang mendukung daerah wewenang proteksi merupakan kegunaan dari cincin proteksi. Cincin-cincin ini dikelompokkan pada daerah tersembunyi di tengah-tengah cincin dan pada ujung lokasi yang paling besar pada bagian cincin tersebut. Pendekatan ini ditunjukkan pada gambar 42.



Gambar 9.2 Contoh Operating System Kernel

Operating system security kernel biasanya terletak pada cincin dan memiliki akses pada seluruh daerah sistem. Security kernel disimpulkan sebagai hard ware, software, dan firmware pada dasar komputerisasi yang legal yang mengimplementasikan konsep layar referensi.

Layar referensi adalah sebuah komponen sistem yang menekankan kontrol akses ke sebuah objek. Layar referensi merupakan sebuah mesin abstrak yang menjadi perantara seluruh akses pada sasarannya.

Security kernel harus :

1. menjadi perantara semua akses
2. terlindung dari segala bentuk modifikasi • telah diverikasi dengan baik dan benar dalam konsep cincin, wewenang akses berkurang apabila jumlah cincin bertambah. Karena proses legal kebanyakan terletak padar pusat cincin. Komponen sistem ditempatkan pada cincin yang layak sehubungan pada prinsip-prinsip tertentu. Proses hanya memiliki kegunaan minimum yang dibutuhkan untuk menjalankan fungsi-fungsinya. Mekanisme proteksi cincin diimplementasikan dalam MIT's MULTICs yang ditingkatkan untuk aplikasi aman melalui Honeywell Corporation. MULTICS awalnya ditargetkan untuk kegunaan media perangkat keras karena beberapa kegunaannya bisa diimplementasikan melalui perangkat keras yang didesain untuk menopang sebanyak 64 cincin, tapi dalam prakteknya, hanya delapan cincin yang bisa ditopang.

Berikut juga merupakan pendekatan-pendekatan kernel yang berkaitan pada proteksi :

- menggunakan perangkat keras yang terpisah yang menerangkan berlakunya masa seluruh refernsi dalam sistem tersebut
- mengimplementasikan layar mesin secara virtual, yang menetapkan jumlah dari mesin virtual yang terpisah dari bagian lainnya dimana sistem komputer dijalankan sesungguhnya. Mesin virtual ini meniru arsitektur dari wujud mesin yang sesungguhnya dalam pembentukan suatu lingkungan pengamanan bertingkat, dimana tiap mesin virtual dapat berjalan pada tingkat pengamanan yang berbeda.
- Menggunakan kernel pengamanan software yang beroperasi pada daerah kekuasaan proteksi perangkat kerasnya.

9.3.2 Security Labels

Label keamanan ditujukan pada suatu sumber untuk menunjukkan sebuah tipe pengelompokan atau perencanaan. Label ini dapat menunjukkan penanganan keamanan khusus, yang dapat digunakan untuk mengakses kontrol. Sekali label diberikan, maka label tersebut biasanya tidak dapat digantikan karena label-label ini merupakan mekanisme kontrol akses yang efektif. Label yang ada harus dibandingkan, diuji dan dievaluasi terlebih dahulu melalui aturan pengamanan yang ada, karena dapat mendatangkan dampak buruk setelah proses berlangsung apabila tidak dievaluasi dulu.

9.3.3 Security Modes

Sebuah sistem informasi beroperasi dalam mode keamanan yang berbeda yang ditentukan oleh level klasifikasi sistem informasi dan penjelasan dari semua pengguna sistem. Bagaimanapun juga, tidak semua user memiliki kemampuan untuk mengetahui semua data. Mode bertingkat pada pengguna suport operasi yang memiliki perbedaan media pembersih dan data pada tingkat klasifikasi yang bertingkat.

Mode tambahan pada sistem operasi yaitu :

1. **Dedikasi**. Semua pengguna memiliki media pembersih atau semacam wewenang untuk mengetahui segala macam informasi yang diproses oleh sistem informasi; sistem yang bisa menangani level klasifikasi yang beraneka ragam
2. **Compartmented**. Semua user memiliki media pembersih untuk level tertinggi pada klasifikasi informasi, tapi mereka tidak memiliki wewenang yang diperlukan untuk mengetahui semua data yang ditempatkan secara legal dalam hubungannya pada tingkat informasi dapat diproses.
3. **Akses terbatas**. Merupakan tipe akses sistem dimana hanya dapat digunakan user tertentu dan klasifikasi data maksimum tidak disusun, tetapi cukup sensitif.
4. **Keamanan Multi-level**. Sebuah sistem informasi pada usaha kecil dan menengah sebaiknya menggunakan mode keamanan multi- level mode of operation karena pada usaha kecil dan menengah diperlukan keluesan terhadap informasi yang ada pada organisasi. Informasi harus mengalir dengan aman tanpa proses yang rumit, sesuai dengan sifat usaha kecil dan menengah yang harus cepat dan tangkas. Pada mode keamanan multi-level mode of operation, user memiliki level klasifikasi yanng berbeda. Penggunaan mode keamanan system high mode of operation pada usaha kecil dan menengah akan membuat komunikasi dan alur informasi pada organisasi menjadi rumit dan tidak tangkas. Karena setiap user terkesan sendiri-sendiri dalam berkerja dan dalam kepemilikan inforrmasi. Tapi penggunaan mode keamanan multi-level mode of operation ini bisa menjadi birokrasi yang rumit karena tingkatan-tingkatan yang ada, untuk itu diperlukan klasifikasi level yang pendek.

9.3.4 Additional Security Considerations

Vulnerabilitas pada arsitektur keamanan sistem dapat menghasilkan pelanggaran ketentuan keamanan sistem. Vulnerabilitas digambarkan sebagai

berikut : • Channel yang tersembunyi. Langkah komunikasi yang tidak disengaja diantara dua atau lebih subjek membagi secara umum, dimana mendukung pemindahan informasi menjadi semacam cara yang melanggar ketentuan keamanan sistem. Pemindahan biasanya membutuhkan tempat melalui area penyimpanan umum atau melalui akses menuju bagian tertentu yang dapat menggunakan chanel waktu untuk komunikasi yang tidak terencana.

1. Kurangnya pemeriksaan parameter. Kegagalan mengecek ukuran stream input yang ditetapkan oleh parameter.
2. Maintenance Hook. Mekasnisme perangkat keras maupun perangkat lunak diinstal untuk mengizinkan maintenance sistem dan untuk melewati perlindungan keamanan sistem.
3. Time of Check to Time of Use (TOC/TOU) Attack. Perlawanan yang merusak perbedaan waktu kontrol keamanan dipasang dan waktu servis resmi digunakan.

9.3.5 Recovery Procedures

Pada saat komponen sebuah perangkat keras atau perangkat lunak dari suatu sistem yang diakui mengalami kegagalan atau gangguan, sangat penting diketahui bahwa gangguan tersebut tidak memiliki ketergantungan pada kelengkapan aturan keamanan pada sistem tersebut. Sebagai tambahan, prosedur recovery tidak memberikan perlawanan terhadap pelanggaran aturan ketentuan keamanan sistem. Jika sebuah sistem yang dimulai diperlukan, sistem tersebut harus dimulai dengan aman. Awal harus terjadi dalam mode pemelihaaran yang mengizinkan akses hanya dari pengguna yang dipercaya dari terminal yang diyakini juga. Mode ini mendukung penggunaan sistem dan keamanan.

Pada saat komputer atau komponen jaringan gagal namun komputer/jaringan tetap berfungsi, hal tersebut dikenal dengan system toleransi kesalahan. Dalam toleransi ksalahan beroperasi, sistem harus mampu mendeteksi bahwa kesalahan tersebut memang telah terjadi itu, dan sistem harus mampu untuk mengoreksi kesalahan atau operasi di sekitarnya. Dalam sistem perbaikan kesalahan ini, eksekusi program terbatas dan sistem terlindung dari pengaruh kompromi tertentu pada saat kegagalan hardware atau software terjadi dan terdeteksi. Komputer atau jaringan berlanjut pada fungsi dalam tingkat yang lebih rendah. Kegagalan akhir pada masa tertentu pada sistem lalu dihubungkan pada komponen duplikat back up dalam waktu nyata pada saat hardware atau software tejadi, dimana sistem mampu melanjutkan proses. Prosedur pemulihan sistem pada usaha kecil menengah tidak menjadi suatu yang kritis. Pada saat system usaha kecil dan menengah mati atau gagal, system dapat direstart atau diperbaiki dengan mode default yang aman. System dapat diperbaiki oleh pihak yang diberi kewenangan langsung ke system yang bermasalah tanpa membutuhkan terminal khusus. Penggunaan backup system bisa sangat membantu untuk mengalihkan fungsi sistem agar bisa berjalan kembali.[15]

9.4 Prinsip-prinsip Keamanan Komputer

a. **Least previlage** , Artinya setiap orang hanya diberi hak akses tidak lebih dari yang di butuh kan untuk menjalankan tugasnya. Seorang staf umum

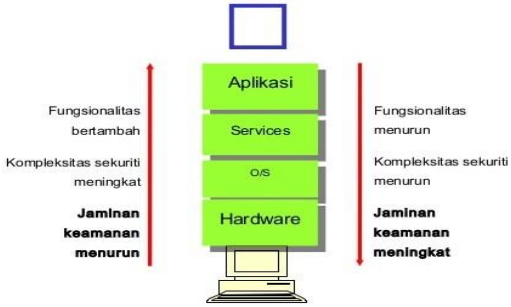
dan gudang hanya mendapat hak akses untuk menjalankan aplikasi administrasi gudang. Seorang staf penanganan anggota hanya mendapat hak akses untuk menjalankan aplikasi administrasi seorang staf pemasaran hanya mendapat hak akses untuk mejalankan aplikasi administrasi pemasaran dan penjualan. Seorang direktur dapat memonitor seluruh pekerjaan yang di lakukan oleh manejer yang ada di bawahnya.

b. **Defense in Depth** , Gunakan berbgai perangkat keamanan untuk saling mencakup . Misalnya dapat di pergunakan multipe sccrening router,mirroring hardisk pada server, dua CDRW untuk satu kali Backup Data yaitu dua kali sehari (setiap pagi dan sore) pada masing-masing departement sehingga kalau satu di jebol, maka yang satu lagi berfungsi.
c. **Choke Point,** Semua keluar masuk lewat satu (atau sedikit) gerbang. Syaratnya tidak ada cara lain keluar masuk selain lewat gerbang
d. **Weakest Link,** "A Chain in only as strong as its weekest link". Oleh karena itu kita harus persis dimana weakes link dalam sistem sekuriti organisasi kira. Kelemahan jaringan di dalam sistem sekuriti organisasi yang perlu di awasi adalah bila ada virus baru yang tidak terdeksi. Oleh karena itu Update Anti Virus pada Server dan Client harus selalu di lakukan dan tidak boleh di abaikan.
e. **Fall-safe Stance,**Maksudnya kalau suatu perangkat keamanan rusak , Maka secara Defult perangkat setingnya akan ke seting yang paling aman.
f. **Universal Participation,** Semua orang dalam organisasi harus terlibat dalam proses sekuriti. Setiap tiga bulan sekali di lakukan pelatihan untuk menyyegarkan kembali ingatan akan pentingnya mengamankan perangkat keamanan komputer. Di dalamnya di lakukan evaluasi untuk peningkatan efisien keamanan komputer.
g. **Deveraity Od Defense,**Mempergunakan beberapa jenis sistem yang berbeda untuk pertahanan. Maksudnya, kalau penerangan sudah menyerang suatu jenis sistem pertahanan, maka dia tetap akan perlu belajar sistem jenis lainnya.
h. **Simpllcity,** Jangan terlalu kompleks, Karena sulit sekali mengetahui salah nya ada di mana kalau sistem terlalu kompleks untuk di pahami. Untuk mempermudah mengetahui bila terjadi kesalahan maka setiap data yang di simpan dalam server akan teridentivikasi siapa yang menimpan berdasarkan username dan password nya, kapan tanggal dan waktu nya, dari workstation yang mana, dan apa aksi yang di lakukan.

9.5 Tingkatan Jaminan Keamanan

- Proteksi Lapis Bawah (Low Level)
  1. Pengamanan yang lebih ke arah Hardware
  2. Lebih Sederhana
  3. Melebar
  4. Tidak Fleksibel
  5. Misalnya : Write-protect pada USB drive, IP restriction
- Proteksi Lapis Atas (High Level)
  1. Lebih rumit atau kompleks
  2. Bisa pada aplikasi atau sistem prosedur

3. Lebih fleksibel dan lebih detail kendalinya
4. Mengakibatkan menurunnya jaminan nekanisme keamanan
5. Karena butuh ekstra untuk install,Testing/pengujian dan pemeliharaan
6. Misalnya : Akses kontrol tabel dtabase dan aplikasi



Gambar 9.3 Contoh Operating System

9.6 System Architecture Security

Contoh pada Operating System

- **Trusted Computing Base (TCB)**
  - Kombinasi keseluruhan dari mekanisme pengamanan dalam sebuah sistem komputer
  - Mencakup : Hardware,Software, dan Firmware
  - Komponen yang masuk TCB harus teridentifikasi dan kemampuan terdefenisi dengan jelas.
  - TCB mengikuti standar security rating tertentu seperti Orange Book (akan di jelaskan)
  - Perihal tingkat kepercayaan (Bukan keamanan)

- **Security Perimeter**
  1. Semua komponen yang tidak masuk dalam TCB
  2. Harus ada standar komunikasi, akni melalui interface yang sudah defined.
     Contoh :
     Anda membuat program dengan bahasa Java, belum tentu anda berhak mendapatkan hak akses untuk menipulasi data di lakukan melalui objek-objek dan Interface Java Virtual Machine.

- **Security Models**

Security Models adalah representasi simbolik dari kebijakan, yang harus di laksana kan oleh sistem komputer, apa yang boleh dan tidak secara teknis .

Tujuannya :

1. Untuk memformalkan kebijakan keamanan organisasi
2. Representasi Simbolik dari kebijakan , yang harus di laksanakan oleh sistem komputer.

3. Security policy sifatnya lebih abstrak dan lebar, Security model adalah apa yang boleh dan tidak secara teknis
4. Analogi : Kalau dokter bilang kita harus sehat.

Bagian Security Models

1. Acces Control Matrix Models
2. Bell-LaPadula Model
3. Biba
4. Clar-Wilson Model
5. Information Flow Model

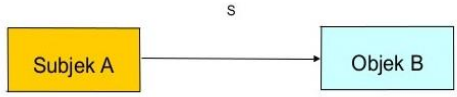
Access Matrix Model :

	File: Income	File: Salaries	Process: Deductions	Print Server
Joe	R	R/W	X	W
Jane	R/W	R	-	W
Checking prog.	R	R	X	-
Tax Prog.	R/W	R/W	X	W

Gambar 9.4 Contoh Access Matrix Model

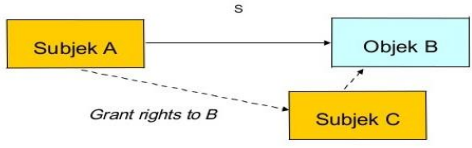
Take-Grant Model

- Menggunaka derected graph untuk mentransfer hak ke subjek lain
- Misalnya A punya hak S,termasuk untuk hak mentransfer , pada objek B



Gambar 9.5 Contoh Take Grant Model Subjek A dan Objek B

- Subjek A bisa memberikan hak nya kepad subjek C, sehingga memiliki hak atas objek B



Gambar 9.6. Contoh Take Grant Model Subjek A,C dan Objek B

9.7 Keamanan Sistem operasi Linux

9.7.1 Account Pemakai (user account)

Keuntungan : Kekuasaan dalam satu account yaitu root, sehingga mudah dalam administrasi system.\ Kecerobohan salah satu user tidak berpengaruh kepada system secara keseluruhan. Masing-masing user memiliki privacy yang ketat.

Macam bagian User :

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

9.7.2 Kontrol Akses secara Diskresi

Discretionary Access control (DAC) adalah metode pembatasan yang ketat, yang meliputi :

1. Setiap account memiliki username dan password sendiri.
2. Setiap file/device memiliki atribut(read/write/execution) kepemilikan, group, dan user umum.
3. Virus tidak akan mencapai file system, jika sebuah user terkena, maka akan berpengaruh pada file-file yang dimiliki oleh user yang mengeksekusi file tersebut.

9.7.3 Discretionary Acces Control (DAC)

Jika kita lakukan list secara detail menggunakan $ls –l, kita dapat melihat penerapan DAC pada file system linux :

Tabel 9.1 Penerapan DAC di Linux

-	Rw-	r--	r--	9	goh	hack	318	mar	30	90:05	Borg.dead.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 pada DAC :

- Mengubah izin Akses File
  - bu : chmod < u | g | o >< + | - >< r | w | e > nama file,

contoh : chmod u+x g+w o-r borg.dead.letter ; tambahkan akses eksekusi(e) untuk user (u), tambahkan juga akses write(w) untuk group (g) dan kurangi izin akses read(r) untuk other(o) user.

- chmod metode octal, bu: chmod - - - namafile , digit dash (-) pertama untuk izin akses user, digit ke-2 untuk izin akses group dan digit ke-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.
- Mengubah kepemilikan : crown <owner/pemilik><nama file>
- Mengubah kepemilikan group : chgrp<group owner><nama file>
- Menggunakan account root untuk sementara :
    - ~$su ; System akan meminta Password
    - Password : ****; Prompt akan berubah jadi pagar, tanda login sebagai root ~#
- Mengaktifkan shadow password, yaitu membuat file /etc/passwd menjadi Readable (dapat dibaca) tetapi tidak lagi berisi password, karena sudah dipindah ke /etc/shadow.

Perlunya Pro-aktif password Linux

menggunakan metode DES (Data Encription Standart) untuk password-nya. User harus di training dalam memilih password yang akan digunakannya agar tidak mudah ditebak dengan program-program crack password dalam ancaman bruto force attack. Dan perlu pula ditambah dengan program Bantu cek keamanan password seperti:

- Passwd+ : meningkatkan loging dan mengingatkan user jika mengisi password yang mudah ditebak, ftp://ftp.dartmouth.edu/pub/security
- Anlpasswd : dapat membuat aturan standar pengisian password seperti batas minimum, gabungan huruf besar dengan huruf kecil, gabungan angka dan huruf dsb, ftp://coast.rs.purdue.edu/pub/tools/unix/

9.7.3.1 Kontrol akses jaringan (Network Access Control)

Firewall linux Adalah alat pengontrolan akses antar jaringan yang membuat linux dapat memilih host yang berhak / tidak berhak mengaksesnya.

Fungsi Firewall linux :

1. Memeriksa paket TCP, lalu diperlakukan dengan kondisi yang sudah ditentukan, contoh paket A lakukan tindakan B
2. Blocking isi pake seperti applet java, active, Vbscript, Cookie
3. Menjalankan enkripsi dalam identitas user, integritas satu session dan melapisi data dengan algoritma enkripsi seperti : DES, triple DES, Blowfish, IPSec, SHA, MD5, IDEA, dsb.

Tipe Firewall Linux:

1. Application-proxy firewall/Application Gateways
2. Network Level Firewall

Enkripsi (encryption)

Penerapan Enkripsi di linux :

1. Enkripsi password ?menggunakan DES (Data Encryption Standard)
2. Enkripsi komunikasi data :
    a. **Secure Shell (SSH)** : Program yang melakukan loging terhadap komputer lain dalam jaringan, mengeksekusi perintah lewat mesin

secara remote dan memindahkan file dari satu mesin ke mesin lainnya. Enkripsi dalam bentuk Blowfish, IDEA, RSA, Triple DES.

Isi SSH Suite :

a) scp (secure shell copy) : mengamankan penggandaan data ?
b) ssh (secure shell client) : model client ssh seperti telnet terenkripsi.
c) ssh-agent : otentikasi lewat jaringan dengan model RSA.
d) sshd (secure shell server) : di port 22
e) ssh-keygen : pembuat kunci (key generator) untuk ssh

Konfigurasi dilakukan di :

a) /etc/sshd_config (file konfigurasi server)
b) /etc/ssh_config (file konfigurasi client)

b. **Secure socket Layer (SSL)** : mengenkripsi data yang dikirimkan lewat port http. Konfigurasi dilakukan di : web server APACHE dengan ditambah PATCH SSL.

9.7.3.2 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 :

1. **Lastlog** : rekaman user login terakhir kali ? last : rekaman user yang pernah login dengan mencarinya pada file /var/log/wtmp
2. **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(binary/ASCII), arah transfer(incoming/outgoing), modus akses(anonymous/guest/user resmi), nama/id/layanan user dan metode otentikasi.
3. **Access_log** : rekaman layanan http / webserver. ? Error_log : rekaman pesan kesalahan atas service http / webserver berupa data jam dan waktu, tipe/alasan kesalahan
4. **Messages** : rekaman kejadian pada kernel ditangani oleh dua daemon :
   a. Syslog : merekam semua program yang dijalankan, konfigurasi pada syslog.conf
   b. Klog : menerima dan merekam semua pesan kernel 6

9.7.3.3 Deteksi Penyusupan (Intrusion Detection)

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

Tipe dasar IDS :

1. 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 :

a. Preemptory (pencegahan) ; IDS akan memperhatikan semua lalu lintas jaringan, dan langsung bertindak jika dicurigai ada penyusupan.
b. Reactionary (reaksi) ; IDS hanya mengamati file log saja.

2. Adaptive system : penerapan expert system dalam mengamati lalu lintas jaringan.

Program IDS:

1. **Chkwtmp** : program pengecekan terhadap entry kosong
2. **Tcplogd** : program pendeteksi stealth scan (scanning yang dilakukan tanpa membuat sesi tcp)
3. **Host entry** : program pendeteksi login anomaly (perilaku aneh) : bizarre behaviour (perilaku aneh), time anomalies (anomaly waktu), local anomaly.[16]

9.8 Model Arsitektur Keamanan NT

Komponen Arsitektur Keamanan NT :

1. Adminisrasi User dan Group

Jenis Account User :

a. Administrator
b. Guest
c. User

Jenis Account Gorup :

a. Administrator
b. Guest
c. User
d. Operator back-up
e. Power user
f. Operator server
g. Operator account
h. Operator printer

Hak User / Grup :

a. Hak basic : acces computer from network, back-up files/directory, change system time, logon locally, manage auditing and security, log (event viewer), restore files and directory, shutdown system, take ownership files or other object, dll.
b. Hak advance : access service and kernel untuk kebutuhan pengembangan system.

Keamanan untuk system File

1. **NTFS :**
   a. Cepat dalam operasi standar file (read – write – search)
   b. Terdapat system file recovery, access control dan permission.

c. Memandang obyek sebagai kumpulan atribut, termasuk permission access.

2. Proteksi untuk integritas data

a. **Transaction logging** : merupakan system file yang dapat di-recovery untuk dapat mencatat semua perubahan terakhir pada directory dan file secara otomatis.
   a) Jika transaksi system berhasil NT akan melakukan pembaharuan pada file.
   b) Jika transaksi gagal, NT akan melalui :
      1) Tahap analisis : mengukur kerusakan dan menentukan lokasi cluster yang harus diperbarui per informasi dalam file log.
      2) Tahap redo : melakukan semua tahapan transaksi yang dicatat pada titik periksa terakhir
      3) Tahap undo : mengembalikan ke kondisi semula untuk semua transaksi yang belum selesai dikerjakan.

b. **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.

c. **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.

3. Fault tolerance

Kemampuan untuk menyediakan redudansi data secara realtime yang akan memberikan tindakan penyelamatan bila terjadi kegagalan perangkat keras, korupsi perangkat lunak dan kemungkinan masalah lainnya.

a. RAID (Redudant Arrays of inexpensive Disk) : sebuah array disk dimana dalam sebuah media penyimpanan terdapat informasi redudan tentang data yang disimpan di sisa media tersebut.

Kelebihan RAID :

1. Meningkatkan kinerja I/O
2. meningkatkan reabilitas media penyimpanan

Ada 2 bentuk fault tolerance :

1. Disk mirroring (RAID 1) : meliputi penulisan data secara simultan kedua media penyimpanan yang secara fisik terpisah.
2. Disk stripping dengan Parity (RAID 5) : data ditulis dalam strip-strip lewat satu array disk yang didalam strip-strip tersebut terdapat informasi parity yang dapat digunakan untuk meregenerasi data apabila salah satu disk device dalam strip set mengalami kegagalan.

9.8.1 Model Keamanan Windows NT

Dibuat dari beberapa komponen yang bekerja secara bersama-sama untuk memberikan keamanan logon dan access control list (ACL) dalam NT :

1. 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.
2. Proses logon : menerima permintaan logon dari user (logon interaktif dan logon remote), menanti masukan username dan password yang benar. Dibantu oleh Netlogon service.
3. Security Account Manager (SAM) : dikenal juga sebagai directory service database, yang memelihara database untuk account user dan memberikan layan validasi untuk proses LSA.
4. Security Reference Monitor (SRM) : memeriksa status izin user dalam mengakses, dan hak user untuk memanipulasi obyek serta membuat pesan-pesan audit.

9.8.2 Keamanan Sumber daya lokal

Obyek dalam NT [file, folder (directory), proses, thread, share dan device], masing-masing akan dilengkapi dengan Obyek Security Descriptor yang terdiri dari :

1. Security ID Owner : menunjukkan user/grup yang memiliki obyek tersebut, yang memiliki kekuasaan untuk mengubah akses permission terhadap obyek tersebut.
2. Security ID group : digunakan oleh subsistem POSIX saja.
3. Discretionary ACL (Access Control List) : identifikasi user dan grup yang diperbolehkan / ditolak dalam mengakses, dikendalikan oleh pemilik obyek.
4. System ACL : mengendalikan pesan auditing yang dibangkitkan oleh system, dikendalikan oleh administrator keamanan jaringan.

9.8.3 Keamanan Jaringan Windows NT

Jenis Keamanan Jaringan Windows NT :

1. 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 setiap user dan menjaga policy system keamanan tetap dapat dibawah kendalinya dengan baik.
2. 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 :

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

9.8.4 Keamanan pada printer

Dilakukan dengan mensetting properties printer :

1. Menentukan permission : full control, Manage document, print
2. Biasanya susunan permission pada NT defaulut :
   a. Adminstrator – full control
   b. Owner – Manage document
   c. Semua user – print
   d. Setting waktu cetak
   e. Prioritas
   f. Notifikasi (orang yang perlu diberi peringatan)
3. Mengontrol print job, terdiri dari :
4. Set auditing information

9.8.1 Keamanan Registry

Tools yang disediakan dalam pengaksesan registry :

- System policy editor : mengontrol akses terhadap registry editor, memungkinkan administrator mengedit dan memodifikasi value tertentu dalam registry dengan berbasis grafis.
- Registry editor (regedit32.exe) : tools untuk melakukan edit dan modifikasi value dalam registry.
- Windows NT Diagnostics (winmsd.exe) : memungkinkan user melihat setting isi registry dan valuenya tanpa harus masuk ke registry editor sendiri.

Tools backup untuk registry yaitu :

- 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.

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)

Soal

1. Apa yang di maksud dengan controls,jelaskan?
2. Tuliskan Tujuan Dari SecurityArchitecture dan Models?