KEAMANAN SISTEM OPERASI

Linux

Komponen Arsitektur Keamanan Linux :

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

2. Kontrol Akses secara Diskresi (Discretionary Access control)

Discretionary Access 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.

> Virus tidak akan mencapai file system, jika sebuah user terkena, maka akan berpengaruh pada file-file yang dimiliki oleh user yang mengeksekusi file tersebut.

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

```
d rw-  - -x  - - -  5  fade  users 1024  Feb   8 12:30 Desktop
- rw-  r - -  r - -  9 Goh  hack   318  Mar  30 09:05 borg.dead.letter
```

-	rw-	r - -	r - -	9	Goh	hack	318	Mar	30	09:05	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 :
  1. 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.
  2. 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 : chown <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 dapat dibaca (readable) tetapi tidak lagi berisi password, karena sudah dipindahkan ke **/etc/shadow**

Contoh tipikal file **/etc/passwd** setelah diaktifkan shadow:

```
…
root:x:0:0::/root:/bin/bash
fade:x:1000:103: , , , :/home/fade:/bin/bash
…
```

Lihat user fade, dapat kita baca sebagai berikut :

username	: fade
Password	: x
User ID (UID)	: 1000
Group ID (GUID)	: 103
Keterangan tambahan	: -
Home directory	: /home/fade
Shell default	: /bin/bash

Password-nya bisa dibaca (readable), tapi berupa huruf x saja, password sebenarnya disimpan di file **/etc/shadow** dalam keadaan dienkripsi :

```
…
root:pCfouljTBTX7o:10995:0:::::
fade:oiHQw6GBf4tiE:10995:0:99999:7:::
…
```

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/

3. Kontrol akses jaringan (Network Access Control)

Firewall linux [1] :
alat pengontrolan akses antar jaringan yang membuat linux dapat memilih host yang berhak / tidak berhak mengaksesnya.

Fungsi Firewall linux :
- Analisa dan filtering paket
  Memeriksa paket TCP, lalu diperlakukan dengan kondisi yang sudah ditentukan, contoh paket A lakukan tindakan B.
- Blocking content dan protocol
  Bloking isi paket seperti applet java, activeX, Vbscript, Cookies
- Autentikasi koneksi dan enkripsi
  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 :
- Application-proxy firewall/Application Gateways
  Dilakukan pada level aplikasi di layer OSI, system proxy ini meneruskan / membagi paket-paket ke dalam jaringan internal. Contoh : software TIS FWTK (Tursted Information System Firewall Toolkit)
- Network level Firewall, fungsi filter dan bloking paket dilakukan di router. Contoh : TCPWrappers, aplikasinya ada di /usr/sbin/tcpd. Cara kerjanya :
  Lihat isi file **/etc/inetd.conf** :

```
...
telnet    stream    tcp    nowait    root /usr/sbin/telnetd
shell     stream    tcp    nowait    root /usr/sbin/rshd
pop3      stream    tcp    nowait    root /usr/sbin/pop3d
…
```

  dengan diaktifkan TCPwrappers maka isi file **/etc/inetd.conf** :

```
...
telnet    stream    tcp    nowait    root /usr/sbin/tcpd in.telnetd
shell     stream    tcp    nowait    root /usr/sbin/tcpd in.rshd -L
pop3      stream    tcp    nowait    root /usr/sbin/tcpd in.pop3d
…
```

  setiap ada permintaan layanan jarak jauh, dipotong dulu dengan pencocokan rule set yang telah diatur oleh **tcp in**, jika memenuhi syarat diteruskan ke file yang akan diekseskusi, tapi jika tidak memenuhi syarat digagalkan.

  Pengaturan TCPWrapper dilakukan dengan mengkonfigurasi 2 file, yaitu :
  - /etc/host.allow → host yang diperbolehkan mengakses.
  - /etc/host.deny → host yang tidak diperbolehkan mengakses.

[1] Untuk membedakan firewall yang *built-in* di linux dengan firewall dedicated yang banyak digunakan dalam teknologi jaringan, maka digunakan istilah firewall linux.

4. Enkripsi (encryption)

Penerapan Enkripsi di linux :

- Enkripsi password → menggunakan DES (Data Encryption Standard)
- Enkripsi komunikasi data :
  1. **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 :
     - scp (secure shell copy) → mengamankan penggandaan data
     - ssh (secure shell client) → model client ssh seperti telnet terenkripsi.
     - ssh-agent → otentikasi lewat jaringan dengan model RSA.
     - sshd (secure shell server) → di port 22
     - ssh-keygen → pembuat kunci (key generator) untuk ssh

     Konfigurasi dilakukan di :
     - /etc/sshd_config (file konfigurasi server)
     - /etc/ssh_config (file konfigurasi client)
  2. **Secure socket Layer (SSL)** → mengenkripsi data yang dikirimkan lewat port http. Konfigurasi dilakukan di : web server APACHE dengan ditambah PATCH SSL.

5. Logging

Def : 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(binary/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 jam 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

6. Deteksi Penyusupan (Intrusion Detection)

Def : 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.
- Adaptive 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) → bizarre behaviour (perilaku aneh), time anomalies (anomaly waktu), local anomaly.

Windows NT

Komponen Arsitektur Keamanan NT :

1. Adminisrasi User dan Group

Jenis Account User :
- Administrator
- Guest
- User

Jenis Account Gorup :
- Administrator
- Guest
- User
- Operator back-up
- Power user
- Operator server
- Operator account
- Operator printer

Hak User / Grup :
- 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.
- Hak advance : access service and kernel untuk kebutuhan pengembangan system.

2. Keamanan untuk system File

A. 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.

B. 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.
- Jika transaksi system berhasil NT akan melakukan pembaharuan pada file.
- Jika transaksi gagal, NT akan melalui :
  - Tahap analisis : mengukur kerusakan dan menentukan lokasi cluster yang harus diperbarui per informasi dalam file log.
  - Tahap redo : melakukan semua tahapan transaksi yang dicatat pada titik periksa terakhir
  - Tahap undo : mengembalikan ke kondisi semula untuk semua transaksi yang belum selesai dikerjakan.

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.

C. 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.
Teknologinya disebut 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 :

- Meningkatkan kinerja I/O
- 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.

3. Model Keamanan Windows NT

Dibuat dari beberapa komponen yang bekerja secara bersama-sama untuk memberikan keamanan logon dan access 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.

4. 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 :

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

5. 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 setiap 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 :

1. Memberikan permission :
    - Permission NTFS local
    - Permission shere
2. 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.
3. Pengamanan Layanan internet :
    - Firewall terbatas pada Internet Information server (IIS).
    - Menginstal tambahan proxy seperti Microsoft Proxy server.
4. Share administrative :memungkin administrator mendapatkan akses ke server windows NT atau workstation melalui jaringan

6. Keamanan pada printer

Dilakukan dengan mensetting properties printer :

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

7. 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.

8. 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)