TUGAS KELOMPOK
KEAMANAN SISTEM OPERASI WINDOWS

Fathan

Mawan

Juriyah

Sugiharto

Ramlan

Windows NT dirancang untuk melindungi hardware computer beserta data yang berharga yang ada didalamnya. Kemampuan dari keamanan Windows NT tersebut tidak hanya dapat mengontrol siapa yang menggunakan komputer dan bagaimana cara menggunakannya, tetapi juga mencegah computer tertulari virus. Windows NT juga memberi kemampuan untuk memelihara salinan backup data computer dengan cara yang mudah. Dan jika menggunakan UPS, Windows NT dapat membantu mencegah hilangnya data akibat putusnya aliran listrik.

Windows NT telah dirancang untuk memberikan keamanan dan perlindungan data dengan melalui tiga fasilitas yaitu :

1. Keamanan tingkat tinggi untuk mengontrol cara mengakses data komputerWindows NT memberikan tingkat keamanan tertinggi yang diperuntukkan bagi komputer pribadi. Windows NT tidak hanya dapat mengendalikan siapa yang dapat menggunakan komputer, tetapi user juga dapat memanipulasi direktori dan file yang disimpan pada disket yang menggunakan format sistem file Windows NT (NTFS).

2. Dukungan menyeluruh bagi UPS (Uninterruptible power supply)

UPS adalah perangkat baterai cadangan yang memberikan tenaga listrik kepada komputer untuk sementara pada saat persediaan tenaga listrik utama terhenti. Dengan campur tangan manusia, UPS membantu mencegah hilangnya data yang belum tersimpan, tetapi masih berada di memori computer.

3. Utility yang mudah digunakan untuk membuat salinan backup dari data computer ke pita magnetic.

   Menyalin data computer ke pita magnetic dan menyimpan backup salinan secara terpisah memungkinkan untuk mengembalikan data jika hardisk computer rusak.

Komponen Arsitektur Keamanan windows NT

1. Adminisrasi User dan Group

Jenis Account User :

- Administrator
- Guest
- User

Komponen Arsitektur Keamanan windows NT

1. Adminisrasi User dan Group

Jenis Account Gorup :

- Administrator
- Guest
- User
- Operator back-up
- Power user
- Operator server
- Operator account
- Operator printer

Komponen Arsitektur Keamanan windows NT

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.

Keamanan untuk system File

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.

Keamanan untuk system File

- **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.

Keamanan untuk system File

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 :
  - Disk mirroring (RAID 1) : meliputi penulisan data secara simultan kedua media penyimpanan yang secara fisik terpisah.
  - 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.

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.

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.

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.

Keamanan Jaringan

Cara NT menangani keamanan jaringan :

- Memberikan permission :
- Permission NTFS local
- Permission 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

Keamanan pada printer

Dilakukan dengan mensetting properties printer :

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

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)