
AUDITING

Sasaran:

1. Dapat mengidentifikasi kelebihan dan kekurangan suatu jaringan komputer.
2. Dapat mengevaluasi sistem keamanan pada jaringan komputer.
3. Memahami konsep dasar audit jaringan komputer.
4. Memahami dasar-dasar teknik audit jaringan komputer.
5. Mengetahui dan memahami fasilitas AUDITCON pada Novell netware

5.1. Pendahuluan

Perkembangan teknologi jaringan komputer yang demikian pesat dengan kompleksitas yang semakin tinggi membutuhkan kinerja dan sistem pengamanan yang baik. Untuk mencapai hal tersebut dibutuhkan ketelitian dalam melakukan konfigurasi terhadap suatu jaringan komputer. Semakin kompleks suatu jaringan komputer, maka semakin banyak pula ancaman terhadap masalah keamanannya. Demikian juga dengan kinerja yang biasanya memiliki kecenderungan menurun. Untuk selalu dalam keadaan baik dan siaga diperlukan audit terhadap suatu jaringan komputer. Proses audit ini dapat dilakukan oleh pihak internal ataupun pihak eksternal. Terlepas dari internal ataupun eksternal, yang jelas *network auditor* harus bersikap obyektif dalam melakukan audit. Tetapi biasanya auditor eksternal akan lebih obyektif, karena yang diaudit bukan sistemnya sendiri.

5.2. Jenis Audit Jaringan Komputer

Audit jaringan komputer secara umum dapat dibagi menjadi dua bagian, yaitu *Performance Audit* dan *Security Audit*. *Performance Audit* lebih menitikberatkan pada peningkatan kinerja jaringan komputer. Sedangkan *Security Audit* lebih menitikberatkan pada sistem keamanan jaringan komputer. Pembahasan di subbab ini akan menjelaskan teknik audit dengan pendekatan secara umum yang berlaku di kedua jenis audit di atas.

5.3. Metode Audit Jaringan Komputer

Proses audit untuk jaringan komputer akan semakin kompleks jika sistemnya semakin besar dan terintegrasi satu sama lainnya. Untuk mempermudah hal tersebut, teknik audit terhadap jaringan komputer harus di *break-down* berdasarkan *layer-layer* dari *7-layer* pada *Open System Interconnection* (OSI). Pendekatan auditnya dapat dilakukan dari dua arah, yaitu pendekatan *Top-down* dan pendekatan *Bottom-up*.

5.3.1. Identifikasi Melalui *Layer* OSI

Sebelum melakukan audit, ada baiknya terlebih dulu mengetahui mengenai komponen apa saja yang terdapat di tiap-tiap *layer*. Hal ini berfungsi untuk memudahkan kita dalam menentukan target audit (obyek yang akan di audit).

5.3.1.1. *Application Layer*

Layer ini menjelaskan mengenai *user application software* berada. Seperti pengaksesan dan

pentransferan file, virtual terminal emulation, interprocess communication dan sejenisnya.

5.3.1.2. Presentation Layer

Presentation layer berbicara mengenai berbagai jenis representasi data. Sebagai contoh, UNIX *style line endings* (CR only) dikonversi ke MSDOS *style* (CR+LF), format karakter EBCDIC ke format karakter ASCII, *blinking characters, reverse video* dan *screen graphics*.

Contoh: *Failure to establish appropriate session resources, Failure to perform encryption or decryption, Security violations, Unauthorized requests or unavailable data.*

5.3.1.3. Session Layer

Layer ini mengendalikan komunikasi antar aplikasi dalam jaringan komputer. Pengujian *out-of-sequence packets, two-way communication, security, name recognition* dan *logging* ditangani oleh *layer* ini.

Contoh: *Invalid or unauthorized session requests, Security violations, Unauthorized requests or unavailable data.*

5.3.1.4. Transport Layer

Transport layer menjamin bahwa tiga *layer* dibawahnya (*layer* 3, 2 dan 1) melakukan tugasnya dengan baik dan benar. *Layer* ini juga menyediakan *logical data stream* yang transparan antara *end user* dengan *network service* yang

sedang digunakan. Selain itu, *Transport layer* juga menjamin bahwa data yang diterima memiliki format yang benar dan terurut.

Contoh: *Garbled, incomplete, or lost messages; Duplicate delivery of messages, Network security violations, Network deadlocks.*

5.3.1.5. Network Layer

Layer ini memiliki kemampuan untuk menjaga agar paket yang dikirim dari satu peralatan ke peralatan lainnya dapat tiba dengan periode waktu yang dapat diterima. Pekerjaan yang dilakukan oleh *Network layer* adalah fungsi *routing* dan *flow control*.

Contoh: *Traffic congestion, Invalid or unauthorized call setups or disconnections, Failures at network nodes.*

5.3.1.6. Datalink Layer

Datalink layer bertugas meletakkan dan mengambil paket data ke dan dari saluran transmisi, *error detection and correction* dan *retransmission*. Layer ini secara umum dibagi menjadi dua *sublayer*, yaitu LLC (*Logical Link Layer*) yang berada pada setengah bagian atas *Datalink layer* yang bertugas melakukan *error checking* dan MAC (*Medium Access Control*) yang berada pada setengah bagian bawah *Datalink layer* yang bertugas meletakkan dan mengambil data ke dan dari saluran transmisi.

Contoh: *Data bit transmission error, Faulty frame or message headers.*

5.3.1.7. Physical Layer

Layer ini bertugas mendefinisikan spesifikasi kabel, konektor dan signaling. Semua hal yang berhubungan dengan perangkat keras dan pensinyalan dibicarakan di *Physical layer*.

Contoh: *electrical circuit failure, modem problems, wire tapping or electronic eavesdropping.*

5.3.2. Pendekatan Top-down

Audit dengan pendekatan *Top-down* adalah dengan memulai melakukan identifikasi dari *layer* OSI yang tertinggi, yaitu *Application Layer* menuju ke layer yang terendah, yaitu *Physical Layer*. Berarti audit dilakukan dari perangkat lunak (*software*) aplikasi komunikasi dan berakhir di infrastruktur komunikasi.

5.3.3. Pendekatan Bottom-up

Audit dengan pendekatan *Bottom-up* adalah kebalikan dari pendekatan *Top-down*, yaitu dengan memulai melakukan identifikasi dari *layer* OSI yang terendah, yaitu *Physical Layer* menuju ke layer yang tertinggi, yaitu *Application Layer*. Dalam hal ini audit dimulai dari infrastruktur komunikasi dan berakhir di perangkat lunak (*software*) aplikasi komunikasi.

5.4. Audit Kendali Telekomunikasi

Sebagai bagian dari review of controls di data centre, audit sebaiknya mencakup *review of telecommunications controls*. Audit telekomunikasi mencakup tiga proses, yaitu:

5.4.1. Audit fungsi manajemen telekomunikasi

Fungsi manajemen telekomunikasi bertanggungjawab atas:

- *Overall management of the network* (Me-maintain inventarisasi peralatan dan men-set standar agar dimungkinkannya penambahan peralatan baru untuk dapat bergabung ke jaringan komputer)
- *Ongoing program (network usage monitoring, logging problems dan reporting)*
- *Periodic reviews of the network* (memperbaiki *balance loads*, penghematan biaya dan instalasi peralatan yang optimal)
- Berpartisipasi aktif dalam *system development*, sehingga kebutuhan dan standar telekomunikasi dapat disesuaikan dengan kebutuhan *production applications*.

Prosedur audit :

- Memeriksa apakah ada fungsi manajemen telekomunikasi yang kuat dengan otoritas untuk membuat standar dan prosedur
- Memeriksa apakah tersedia dokumen mengenai inventarisasi peralatan telekomunikasi, termasuk dokumen penggantian peralatan
- Memeriksa apakah tersedia prosedur untuk memantau *network usage* untuk keperluan

peningkatan kinerja dan penyelesaian masalah yang timbul

- Memeriksa apakah ada *control* secara aktif mengenai pelaksanaan standar untuk aplikasi-aplikasi *on-line* yang baru diimplementasikan

5.4.2. Audit *physical controls* jaringan telekomunikasi

Prosedur audit :

- Memeriksa apakah peralatan komunikasi diletakkan di tempat yang aman untuk menghindari akses oleh orang-orang yang tidak berhak
- Memeriksa apakah sambungan komunikasi telah dilapisi (*shielded*) dan dilindungi (*protected*) untuk menghindari *tapping*
- Memeriksa apakah peralatan uji komunikasi yang digunakan untuk memantau jaringan telah berada ditempat yang aman dan dibatasi hak aksesnya
- Memeriksa apakah *Disaster Recovery Planning* (DRP) telah mencakup infrastruktur telekomunikasi
- Memeriksa apakah sambungan *dial-up* telah terkendali dengan baik untuk menghindari penyalahgunaan sambungan tersebut

5.4.3. Audit *logical controls* jaringan telekomunikasi

Prosedur audit :

- Memeriksa apakah *password* dan prosedur lainnya telah ada untuk membatasi dan mendeteksi usaha-usaha dari orang-orang yang tidak berhak
- Memeriksa apakah tersedia fasilitas *error checking* untuk mendeteksi kesalahan transmisi data, serta pengiriman ulang jika memang diperlukan

- Memeriksa apakah tersedia fasilitas *automatic rerouting* untuk membatasi akses melalui *wire tap*, selain juga untuk meyakinkan bahwa transmisi hanya tertuju ke *user* yang berhak
- Memeriksa apakah seluruh aktifitas jaringan telah terekam dengan baik untuk keperluan penelusuran
- Memeriksa apakah sudah menggunakan enkripsi data

5.5. AUDITCON PADA NOVELL NETWARE

Netware 4.x mempunyai kemampuan untuk mengaudit beberapa macam aktifitas, mulai dari dibukanya sebuah file sampai ke perubahan hak akses user. Audit hanya bisa dilakukan oleh Administrator Jaringan atau oleh pihak ketiga yang berwenang melakukan audit. Netware 4.11 dapat memonitor penuh semua aspek dari keamanan jaringan.

Ada beberapa alasan kenapa suatu perusahaan harus menginstall audit pada jaringan, diantaranya :

- Untuk memonitor setiap perubahan pada konfigurasi keamanan jaringan
- Untuk mengetahui siapa saja yang mengakses file-file tertentu
- Untuk memonitor aktifitas dari sejumlah *user* jaringan
- Untuk menyimpan rekaman kegiatan *login* dan *logout* berdasarkan tanggal dan waktu

Audit pada jaringan dapat dilakukan menggunakan utilitas **AUDITCON.EXE**, yang terletak pada direktori SYS:PUBLIC pada tiap file server. Administrator jaringan yang pertama kali menyeting audit. Sekali diseting, setiap user yang mempunyai *password* audit dapat menjalankan fungsi-fungsi audit. NDS dan sistem file (audit volume) diaudit terpisah menggunakan laporan yang berbeda. Audit volume yang lain terdiri dari *management of print queues and jobs within queues, file server brought*

up and down, volume mount and dismount, dan bindery based user events.

Sebelum menyeting dan melakukan audit jaringan, harus dipikirkan dulu apa yang akan diaudit dan mengapa. AUDITCON dapat mengaudit NDS dan file sistem. Pada NDS yang dapat diaudit adalah perubahan pada partisi, ekuivalensi keamanan, hak akses user, login dan logout, dan lain lain. Pada sistem file atau yang biasa disebut *volume auditing*, yang dapat diaudit adalah membuat, menghapus, atau merubah nama dari file dan direktori, membuka serta menutup file . *Volume Auditing* lain yang bisa diaudit adalah pencetakan dan file server.

VOLUME AUDITING DAN DIRECTORY AUDITING

Hal pertama yang perlu diperhatikan adalah tipe audit apa yang akan dilakukan. Terdapat dua pilihan utama yang tersedia melalui AUDITCON : *Volume Auditing* dan *Directory Auditing*. *Volume Auditing* tersedia untuk volume individual pada struktur file/direktori dan harus diaktifkan secara terpisah tiap volumenya. Informasi yang dikumpulkan oleh *volume auditing* ditempatkan di sebuah audit log. *Audit Log* adalah file yang dimaintain pada root di tiap volume dimana audit diaktifkan. File ini disembunyikan dari semua utilitas dan disarankan untuk selalu terbuka. AUDITCON mempunyai utilitas untuk menentukan batas dari ukuran besarnya file audit.

Directory Auditing mengaudit *directory services*. Pada direktori yang dapat diaudit adalah keamanan yang terkait. Kegiatan lain yang dapat diaudit adalah kegiatan yang berhubungan pada perubahan di pohon NDS (partisi, replika, pembuatan dan modifikasi dari obyek, dan sebagainya). Data *directory auditing* disimpan di dalam NDS.

FILE-FILE AUDIT

Terdapat beberapa jenis file audit yang berbeda, seperti di bawah ini :

- **File Audit atau Audit File.** File Audit adalah file yang dimaintain untuk mendapatkan informasi audit yang sedang berjalan. Pada

kasus Volume Auditing, file audit adalah file tersembunyi yang berada pada root dari volume. Pada kasus Directory Auditing, informasi dimaintain sebagai bagian dari database NDS.

- **File Audit History atau Audit History File.** File ini adalah history dari aktifitas audit dan digunakan untuk mengaudit seorang auditor. File ini mengandung waktu ketika file audit terakhir kali direset dan waktu ketika seorang auditor masuk ke volume atau kontainer untuk mengaudit.
- **File Audit Lama atau Old Audit File.** File ini merupakan duplikat dari file audit yang dibuat ketika file audit tersebut direset. Proses reset mengcopy informasi terakhir ke dalam file yang terpisah dan mengosongkan semua informasi yang ada pada file audit. Ini berarti mereset file audit juga membuat ukuran file audit tersebut menjadi nol. Ada pilihan *Audit Files Maintenance* yang dapat digunakan untuk mengcopy Old Audit File.

PILIHAN FILE EVENT AUDITCON

Auditcon mempunyai tiga pilihan *file events* yang dapat dipilih untuk menentukan berapa banyak data audit yang akan dikumpulkan. Tiga pilihan tersebut adalah :

- Global
- User or File/Directory
- User and File/Directory

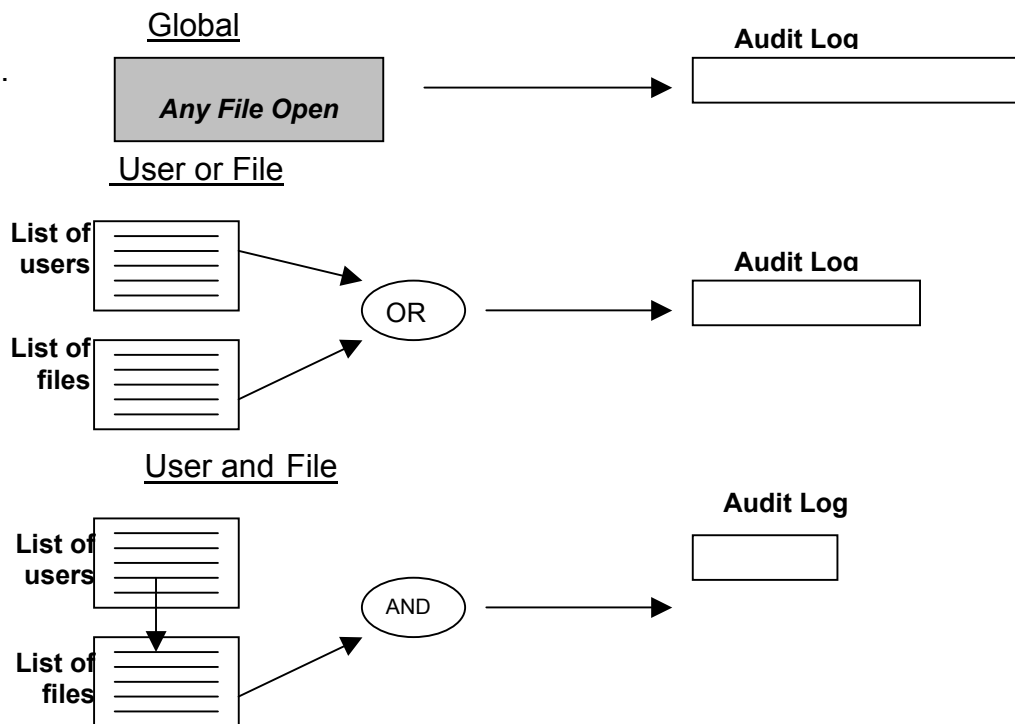
Global mengumpulkan semua data mengenai file event yang dipilih. Pilih file event **File Open – Global** (dari menu utama AUDITCON pilih login volume Auditor, Auditing Configuration, Audit by Event, Audit by File Event), data yang terdapat dalam volume log audit adalah semua hal dari semua user yang membuka file pada volume tersebut.

User or File/Directory lebih selektif karena pilihan ini mengumpulkan data tentang events yang dilakukan oleh daftar user yang dipilih, atau data tentang events dari daftar file (atau direktori) yang dipilih.

Pilih file event **File Open – User or File**, terdapat dalam volume log audit adalah file yang dibuka oleh daftar user yang dipilih, atau daftar user yang membuka file yang dipilih.

User and File/Directory yang paling selektif dari semua pilihan, karena pilihan ini mengumpulkan data hanya seorang user dari daftar yang dipilih membuka file yang juga telah dipilih. Pilih file event **File Open – User and File**, terdapat dalam volume log audit hanya file yang sudah dipilih dan dibuka oleh user dari daftar user yang dipilih.

Pilihan auditing yang lain, seperti Server Events atau NDS tidak menggunakan tiga pilihan tadi, mereka hanya menggunakan *on* atau *off*. Sebagai contoh, ketika login dan logout akan dimonitor, rubah kondisi dari *off* ke *on* (dari menu utama AUDITCON, pilih Audit directory service – Audit directory tree, pilih container to audit – Auditing configuration – audit by ds event, lalu pilih login user dan logout user)



Gambar 1. Pilihan File Event AUDITCON

AUDITING REPORTS

Setelah diputuskan informasi apa saja yang akan diaudit, baru pikirkan informasi apa saja yang akan ditampilkan di dalam laporan (*report*). Sebelumnya sudah dibahas bagaimana mendapatkan data audit dalam jumlah yang besar atau dalam jumlah yang dibatasi. Setelah data dikumpulkan, dapat dihasilkan serangkaian penyaring laporan (*report filter*) untuk membatasi jumlah data yang akan ditampilkan di dalam laporan audit (*audit report*). *Report Filter* memungkinkan untuk menyaring data berdasarkan kriteria berikut :

- Tanggal dan Waktu
- Direktori Event yang Spesifik
- Volume Event yang Spesifik
- User yang Spesifik
- Tidak mengikutsertakan beberapa user
- File dan direktori yang spesifik
- Tidak mengikutsertakan beberapa file dan direktori

Report Filter dapat dibuat berdasarkan kebutuhan pelaporan. *Filter* tersebut dapat disimpan dan dipanggil kembali setiap saat. Pilihan pada tiap *Report Filter* berguna ketika jaringan yang diaudit sibuk, dan telah menghasilkan sangat banyak data audit.

PESAN PADA REPORT FILE

Data *report* yang dihasilkan oleh AUDITCON bukan dalam bentuk yang langsung dapat digunakan. Di bawah ini adalah contoh dari data audit yang dihasilkan dari *volume auditing* :

```
14:05:28 Open file, event 27, PUBLIC\NLS\437_UNI.001, rights RE, status
0, user NOT_LOGGED_IN, connection 2
14:05:28 Open file, event 27, PUBLIC\NLS\437_UNI.001, rights RE, status
0, user NOT_LOGGED_IN, connection 2
14:05:28 Open file, event 27, PUBLIC\NLS\ENGLISH\SCHEMA.XLT,
rights RE, status 0, user NOT_LOGGED_IN, connection 2
```

TSI Perbankan

14:05:28 Open file, event 27, PUBLIC\NLS\ENGLISH\SCHEMA.XLT, rights RE, status 0, user NOT_LOGGED_IN, connection 2
14:06:16 Active connection, event 58, address 01014088:0080c7014108, status 0, user Alee.IND.EBDB, connection 6
14:06:16 Log out user, event 23, status 0, user Alee.IND.EBDB, connection 6
14:06:20 Active connection, event 58, address 01014088:0080c7014108, status 0, user BSAUNDER, connection 6
14:06:20 Open file, event 27, NETWARE\0001b3c0.000, rights R, status 0, user BSAUNDER, connection 6

Sementara untuk merubah data di atas menjadi bentuk yang lebih dimengerti merupakan tugas dari Administrator Jaringan atau Staff MIS, tugas yang dapat diselesaikan dengan program BASIC atau dBase yang sederhana, atau dengan *spreadsheet macro*.

SIAPA YANG BERHAK MELAKUKAN AUDIT

Memutuskan siapa yang berhak melakukan audit merupakan salah satu kontroversi di dalam industri jaringan. Banyak Administrator Jaringan yang mengirim salinan data audit daripada menyewa auditor luar, yang dapat menyebabkan adanya perselisihan antara administrator jaringan dengan pihak manajemen, karena pihak manajemen terlihat tidak mempercayai administrator jaringan.

Auditor adalah user biasa yang mempunyai password audit. Auditor dapat melakukan operasi audit berdasarkan hak yang diberikan (atau diambil) oleh administrator jaringan. Seorang auditor harus merupakan user yang terdapat di dalam NDS tree dan harus mempunyai hak *browse* untuk obyek yang diaudit. Selain itu dia harus mempunyai hak *write*, *create* dan *erase* untuk menjalankan AUDITCON.EXE, karena AUDITCON membuat file sementara yang disimpan selama laporan dibuat di dalam direktori. Jika user tidak punya hak yang cukup untuk direktori tersebut maka akan tampil pesan error pada saat laporan dibuat.

SETTING AUDIT

Langkah-langkah yang perlu dilakukan untuk melakukan audit adalah :

TSI Perbankan

- Administrasi jaringan harus mengaktifkan audit pada semua volume dan kontainer yang akan diaudit
- Events yang akan diaudit harus dikonfigurasi
- Data audit dikumpulkan berdasarkan periode waktu tertentu
- *Report filter* dibuat sesuai dengan kebutuhan
- Buat laporan audit