JURNAL DASI ISSN: 1411-3201
Vol. 11 No. 3 September 2010

AUTENTIKASI, KENDALI AKSES, AUDIT SISTEM KEAMANAN JARINGAN KOMPUTER

M. Rudyanto Arief
Dosen STMIK AMIKOM Yogyakarta

Abstract

Access control, authentication, and auditing are the processes that work together to achieve the security goals. These processes provide basic security for equipment and resources in a network.

Keywords: *Regulations, policies, auditing, confidentiality, integrity*

Pendahuluan

Kendali akses, autentikasi, audit di perlukan untuk menjamin tercapainya tujuan keamanan komputer (security goal). Masing-masing metode ini (access control, authentication, auditing) memiliki konsep dan cara kerja yang berbeda-beda dalam mengamankan sistem komputer.

Pembahasan

Kendali akses (access control).

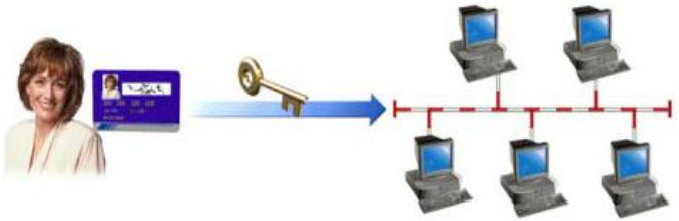
Gambar. 1 Access Control

Kendali Akses adalah sebuah kebijakan. Biasanya di implementasikan sebagai sebuah komponen hardware atau software, yang digunakan untuk membolehkan atau menolak user mengakses sumber daya yang terdapat dalam sistem komputer. Kendali akses hanya membolehkan user yang berhak saja yang dapat mengakses sumber daya dalam komputer kita. Dengan kendali akses kita dapat membatasi hak akses seorang user ke dalam sistem untuk mengerjakan tugas-tugas tertentu saja. Sehingga masing-masing user hanya dapat mengakses sumber daya yang ada dalam sistem komputer sesuai dengan hak yang di berikan kepada user tersebut.

Ada 3 jenis metode access control yang biasanya di terapkan dalam sebuah organisasi untuk mengamankan akses user atau komputer ke sumber daya yang ada dalam organisasi tersebut. Ketiganya yaitu:

1. MAC (Mandatory Access Control).
2. DAC (Discretionary Access Control).
3. RBAC (Role-Based Access Control).

Autentikasi (authentication)



Gambar. 2 Authentication

Autentikasi merupakan sebuah proses yang mem-verifikasi apakah user atau komputer yang mencoba untuk mengakses sumber daya dalam sistem komputer benar-benar user atau komputer yang sah atau tidak. User atau komputer di ijinkan untuk mengakses sebuah sistem komputer dan seluruh sumber daya di dalamnya jika sudah di autentikasi oleh komputer yang bersangkutan. Untuk mengamankan

sistem komputer dari user yang tidak berhak maka di perlukan mekanisme autentikasi yang kuat. Berikut adalah beberapa jenis autentikasi yang biasanya digunakan untuk mengamankan sistem komputer, yaitu:

- Username dan Password.
- Kerberos.
- CHAP (Challenge Handshake Authentication Protocol).
- Digital Certificates.
- Tokens.
- Multi-Factor Authentication.
- Mutual Authentication.
- Biometrics.

Audit (auditing)

Gambar. 3 Auditing

Auditing adalah sebuah proses untuk melacak kegiatan-kegiatan, kesalahan-kesalahan, dan percobaan akses dan autentikasi ke dalam sebuah sistem komputer. Dengan auditing dapat membantu kita untuk mengidentifikasi kelemahan yang ada dalam sistem komputer kita sehingga dapat menerapkan kebijakan keamanan yang tepat untuk sistem komputer kita. Audit sendiri terdiri dari berbagai macam jenis, yaitu:

- System Audit Functions.
- System Scanning Auditing.

- Logs File Auditing.
- Non-Essential Services Auditing.

Penutup

Keamanan komputer tidak dapat dilakukan hanya dari sisi keamanan hardware dan software saja, tetapi juga dilihat dari sisi kebijakan/ aturan main yang diterapkan dalam suatu organisasi dalam menerapkan sistem pengamanan komputer secara terintegrasi. Untuk mengamankan sebuah informasi dalam sebuah sistem komputer di sebuah organisasi maka diperlukan mekanisme autentikasi dan pengendalian akses yang tepat untuk masing-masing pihak dalam organisasi tersebut. Selain dari semua mekanisme pengamanan tersebut, juga diperlukan suatu kebijakan atau metode yang tepat untuk melakukan pengecekan apakah kebijakan pengamanan komputer yang selama ini telah diterapkan oleh organisasi tersebut sudah tepat atau belum. Untuk itu mekanisme audit terhadap sistem keamanan komputer sangat diperlukan.

Daftar Pustaka

CompTIA Security+, Part 1 – security concepts., www.comptia.net
Network Security Essentials., Stalling W., Prentice Hall., 2004
http://www.more.net –Network Auditing-, 2007.