NAMA : GUSWANTORO

NIM :1310651015

KELAS : TI-E

Tujuan dalama akses kontrol

• Access Control Model

• Access Control Defensive Kategori dan Jenis

• Metode Otentikasi

• Access Control Teknologi

• Menilai Access Control

Tujuan sebenarnya dalam akses control ini adalah

untuk memungkinkan pengguna berwenang akses ke data yang tepat dan menolak akses ke pengguna yang tidak sah. Kontrol akses melindungi terhadap ancaman seperti akses yang tidak sah, modifikasi yang tidak pantas data, dan hilangnya kerahasiaan.

Kerahasiaan yang dimaksud adalah Kerahasiaan berusaha untuk mencegah pengungkapan yang tidak sah informasi: itu membuat data rahasia. Dengan kata lain, kerahasiaan berusaha untuk mencegah akses tidak sah ke data membaca. Contoh dari serangan kerahasiaan akan pencurian pribadi iDEN- Informasi tifiable (PII), seperti informasi kartu kredit.

Ada 3 kinerja accses control

1. Intergritas
2. Ketersediaan memastikan bahwa informasi yang tersedia bila diperlukan.
3. Kerahasiaan

MODEL ACCESS CONTROL

model utama adalah Discretionary Access Control (DAC), Wajib Access Control (MAC), dan kontrol akses nondiscretionary.

Kontrol akses discretionary

Discretionary Access Control (DAC) memberikan pelajaran kontrol penuh dari benda-benda yang mereka telah diberi akses

Kontrol akses wajib

Wajib Access Control (MAC) adalah sistem-ditegakkan kontrol akses berdasarkan izin sub ject dan label objek. Subjek dan objek memiliki izin dan label, masing-masing, seperti rahasia, rahasia, dan rahasia

Kontrol akses nondiscretionary

RBAC adalah jenis kontrol akses nondiscretionary karena pengguna tidak memiliki kebijaksanaan mengenai kelompok benda mereka diizinkan untuk mengakses dan tidak dapat mentransfer objek untuk mata pelajaran lainnya.

Kontrol akses tugas berbasis model kontrol akses nondiscretionary lain, terkait dengan RBAC. Kontrol akses tugas berbasis didasarkan pada tugas masing-masing harus tunduk

Protokol kontrol akses dan kerangka kerja

Sejumlah protokol dan kerangka kerja dapat digunakan untuk mendukung kebutuhan ini, termasuk RADIUS, Diameter, TACACS / TACACS þ, PAP, dan CHAP.

RADIUS

Remote Authentication Dial-In Service Pengguna (RADIUS) protokol adalah sistem otentikasi pihak ketiga. RADIUS menggunakan User Datagram Protocol (UDP) port 1812 (otentikasi) dan 1813 (akuntansi). istem, yang terdiri dari tiga komponen: otentikasi, otorisasi, dan akuntansi.

Diameter

Diameter adalah RADIUS 'penerus, dirancang untuk memberikan Otentikasi ditingkatkan, Otorisasi, dan Akuntansi (AAA) kerangka.

TACACS dan TACACS1

Terminal Access Controller Access Control System (TACACS) adalah sistem kontrol akses terpusat yang mengharuskan pengguna untuk mengirim ID dan statis (reusable) password untuk otentikasi

Access Control Defensive Kategori dan Jenis 7

• Pencegahan

• Detektif

• Corrective

• Pemulihan

• Pencegah

• Kompensasi

TECHNOLOGIES ACCESS CONTROL

Single sign-on

Sign-On tunggal (SSO) memungkinkan beberapa sistem untuk menggunakan server otentikasi pusat (AS). Kerugian utama untuk SSO itu memungkinkan penyerang untuk mendapatkan akses ke beberapa sumber setelah mengorbankan salah satu metode otentikasi, seperti kata pass. SSO harus selalu digunakan dengan otentikasi multifaktor untuk alasan ini.

Manajemen identitas federasi

Federated Identity Management (FIdM) berlaku Single Sign-On pada skala yang lebih luas: mulai dari lintas organisasi untuk skala Internet.

Kerberos

Kerberos adalah layanan otentikasi pihak ketiga yang dapat digunakan untuk mendukung Single Sign-On. Kerberos menggunakan enkripsi simetris dan memberikan saling otentikasi kedua klien dan server.

SESAME

SESAME adalah Sistem Eropa Aman untuk Aplikasi di ment lingkungan multivendor, sistem single sign-on yang mendukung lingkungan yang heterogen. SESAME dapat dianggap sebagai sekuel dari jenis untuk Kerberos, "SESAME menambah Kerberos: heterogenitas, fitur kontrol akses yang canggih, skalabilitas dari sistem kunci publik, pengelolaan yang lebih baik, audit dan delegasi.

MENILAI ACCESS CONTROL

Pengujian dengan lingkup yang lebih sempit meliputi tes penetrasi, penilaian kerentanan, dan audit keamanan.

Pengujian penetrasi

Sebuah tester penetrasi adalah hacker topi putih yang menerima otorisasi untuk mencoba masuk ke perimeter fisik atau elektronik organisasi (dan kadang-kadang keduanya).

Pengujian kerentanan

Kerentanan pemindaian (juga disebut pengujian kerentanan) scan jaringan atau sistem untuk daftar kerentanan yang telah ditetapkan seperti sistem misconfiguration, perangkat lunak usang, atau kurangnya patch

Keamanan audit

Sebuah Keamanan audit adalah tes terhadap standar diterbitkan. Organisasi dapat diaudit untuk PCI-DSS (Kartu Pembayaran Standar Keamanan data Industri) kepatuhan, sebagai contoh. PCI-DSS mencakup banyak kontrol yang diperlukan, seperti firewall, akses spesifik model kendali, dan enkripsi nirkabel. Seorang auditor kemudian memverifikasi situs atau organisasi

Jadi kesimpulan tentang akses control ini adalah Jika orang berpikir tentang analogi benteng untuk keamanan, kontrol akses akan parit dan benteng dinding. Kontrol akses memastikan bahwa mekanisme perlindungan perbatasan, baik sudut pandang logis dan fisik, dijamin. Tujuan dari kontrol akses adalah untuk memungkinkan pengguna berwenang akses ke data yang tepat dan menolak akses ke users- tidak sah ini juga dikenal sebagai membatasi akses subyek ke obyek. Meskipun tugas ini adalah salah satu kompleks dan terlibat, adalah mungkin untuk menerapkan kontrol akses pro- gram yang kuat tanpa membebani pengguna yang bergantung pada akses ke sistem.

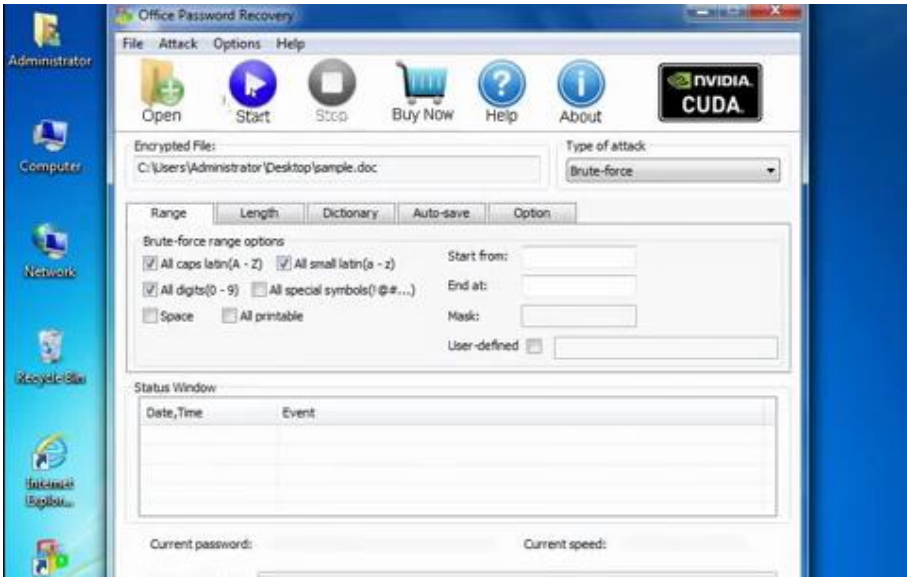
Melindungi triad CIA adalah aspek kunci lain untuk menerapkan kontrol akses. Menjaga kerahasiaan, integritas, dan ketersediaan adalah sangat penting. Menjaga keamanan selama CIA sistem berarti memberlakukan prosedur khusus untuk akses data. Prosedur ini akan berubah tergantung pada fungsi pengguna membutuhkan dan sensitivitas data yang tersimpan pada system

OFFICE PASSWORD RESCOVERY

Clik open pada toll diata

Lalu pilih document yang akan di pasword

lalu clik strart



Dan kita dapatkan password yaitu abc

Keluar dari alikasi ini laulu buka dokumen yang telah di beri password dan masukkan paswordnya