NAMA : AHMAD FARUK SAFINDI

NIM : 1310651174

KELAS : TI_A

POKOK PIKIRAN 1 : ACCES CONTROL

KONSEP CORNERSTONE KEAMANAN INFORMASI

Keamanan informasi terdiri dari 3 aspek yang harus ada yaitu kerahasiaan, integritas, dan ketersediaan.jika salah satu tidak ada maka akan bias berjalan, aspek tersebut membentuk piramida yang diberi nama “CIA Triad”.

1. Kerahasiaan : dimana kerahasiaaan ini mencoba untuk mengungkapkan suatu data yang tidak valid atau tidak sah.contohnya adalah pencurian kode kartu kredit ,atm dan lainnya.
2. Integritas : pencegahan terhadap data yang di manipulasi/modifikasi
3. Availaility : ketersediaan sebuah informasi, dimana contoh serangan yang akan terjadi seperti denial of service.

MODEL ACCES CONTROL

Beberapa model acces control yang akan diabahas terdiri dari

1. Akses Discretionary control(DAC) : memberikan control penuh terhadap data data yang diberi hak akses seperti UNIX dan Windows yang system pemberkasannya menggunakan DAC untuk mengubah beberapa atribut file yang ada.
2. Mandatory acces control (MAC) diamana control akses wajib. Dimana suatu subject tidak bias mengakses object yang tidak memiliki izin yang benar secara tertulis. Hal ini MAC biasnya digunakan untuk pelestarian kerahasiaan data
3. Kontrol akses nondiscretionary : RBAC adalah jenis control akses dimana infromasi yang diakses pada system berdasrkan peran subject dimana RBAC ini tidak memiliki kebijaksanaan mengenai kelompok benda mereke didizinkan untuk mengakses dan tidak mampu untuk mentrasfer object pada yang lainnya.

Akses kontrol berbasis aturan

Sebuah sistem kontrol akses berbasis aturan menggunakan serangkaian aturan yang ditetapkan, pembatasan,dan filter untuk mengakses objek dalam suatu sistem. Aturan-aturan dalam bentuk "Jika / kemudian" pernyataan. Contoh dari perangkat kontrol akses berbasis aturan adalah proxy firewall yang memungkinkan pengguna untuk berselancar di Web dengan konten yang disetujui yang telah ditetapkan hanya.

Kontrol akses terpusat

Kontrol akses terpusat berkonsentrasi kontrol akses di satu titik logis untuk sistem atau organisasi. Alih-alih menggunakan database kontrol akses lokal, sistem mengotentikasi melalui server otentikasi pihak ketiga. Kontrol akses terpusat dapat digunakan untuk menyediakan Single Sign-On (SSO), di mana subjek dapat mengotentikasi

Daftar kontrol akses

Daftar kontrol akses (ACL) digunakan di seluruh banyak kebijakan keamanan IT, prosedur, dan teknologi. Daftar kontrol akses adalah daftar objek; setiap entri menggambarkan mata pelajaran yang dapat mengakses objek tersebut. Akses upaya subjek untuk obyek yang tidak memiliki entri yang cocok pada ACL akan ditolak.

Diameter

Diameter adalah RADIUS 'penerus, dirancang untuk memberikan Authentication ditingkatkan, Otorisasi, dan Akuntansi (AAA) kerangka. RADIUS menyediakan terbatas akuntabilitas dan memiliki masalah dengan fleksibilitas, skalabilitas, kehandalan, dan keamanan.Diameter lebih fleksibel, yang memungkinkan dukungan bagi pengguna jarak jauh ponsel, misalnya.

TACACS dan TACACS1

Terminal Access Controller Access Control System (TACACS) adalah terpusat sistem kontrol akses yang mengharuskan pengguna untuk mengirim ID dan statis (reusable) password untuk otentikasi. TACACS menggunakan port UDP 49 (dan mungkin juga menggunakan TCP). Reusable password memiliki kerentanan keamanan: ditingkatkan TACACSþ memberikan yang lebih baik proteksi password dengan memungkinkan otentikasi dua faktor yang kuat. TACACSþ tidak kompatibel dengan TACACS. TACACSþ menggunakan TCP Port 49 untuk otentikasi dengan TACACSþserver.

PAP dan CHAP

Password Authentication Protocol (PAP) tidak aman: pengguna memasukkan password dan itu dikirim melalui jaringan dalam bentuk teks. Ketika diterima oleh server PAP, itu adalah dikonfirmasi dan divalidasi. Mengendus jaringan dapat mengungkapkan plaintext password. Tantangan-Handshake Authentication Protocol (CHAP) memberikan perlindungan terhadap pemutaran attacks.2 ini menggunakan lokasi pusat yang menantang pengguna jarak jauh. Sebagai dinyatakan dalam RFC 1994, "CHAP tergantung pada 'rahasia' yang hanya diketahui authenticator dan peer. Rahasianya tidak dikirim melalui link. Meskipun otentikasi hanya satu arah, dengan negosiasi CHAP di kedua arah set rahasia yang sama mungkin dengan mudah digunakan untuk otentikasi bersama.

ACCESS CONTROL DEFENSIVE CATEGORIES AND TYPES

Untuk memahami dan tepat menerapkan kontrol akses, pemahaman
apa manfaat setiap kontrol dapat menambah keamanan sangat penting. Pada bagian ini, setiap jenis kontrol akses akan ditentukan atas dasar bagaimana menambah keamanan sistem.
Ada enam jenis kontrol akses:

• **Pencegahan** : Control preventif mencegah tindakan dari terjadi. Ini berlaku pembatasan untuk apa Potensi pengguna, baik resmi atau tidak sah, dapat dilakukan. Contoh dari Access Control Defensive Kategori dan Jenis 7 Kontrol pencegahan administrasi adalah skrining obat pra kerja. Hal ini dirancang untuk mencegah organisasi dari mempekerjakan seorang karyawan yang menggunakan obat-obatan terlarang.

• **Detektif** : Detektif Kontrol detektif adalah kontrol yang siaga selama atau setelah serangan yang berhasil. Intrusi sistem deteksi sinyal setelah serangan sukses, kamera televisi sirkuit tertutup (CCTV) yang penjaga waspada terhadap penyusup, dan sistem bangunan alarm yang dipicu oleh penyusup merupakan contoh dari kontrol detektif.
• **Corrective** : Kontrol korektif bekerja dengan "memperbaiki" sistem atau proses rusak. The korektifkontrol akses biasanya bekerja bergandengan tangan dengan kontrol akses detektif. Anti Virus perangkat lunak memiliki kedua komponen. Pertama, perangkat lunak antivirus menjalankan scan dan kegunaanfile definisi untuk mendeteksi apakah ada software yang cocok daftar virus tersebut. Jika mendeteksi virus, kontrol korektif mengambil alih, menempatkan perangkat lunak yang mencurigakan di karantina, atau menghapusnya dari sistem.

• **Pemulihan** : Pemulihan
Setelah insiden keamanan telah terjadi, kontrol pemulihan mungkin perlu diambil dalam memesan untuk mengembalikan fungsi dari sistem dan organisasi. Pemulihan berarti bahwa sistem harus pulih: diinstal ulang dari OS Media atau gambar, data dikembalikan
dari backup, dll
• **Pencegah** : Kontrol jera mencegah pengguna dari melakukan tindakan pada sistem. Contohnya termasuk "Waspadalah terhadap anjing" tanda: pencuri menghadapi dua bangunan, satu dengan anjing penjaga dan satu tanpa, lebih mungkin untuk menyerang anjing buildingwithout penjaga. Denda besar untuk ngebut adalah pencegah untuk driver untuk tidak mempercepat. Sebuah kebijakan sanksi yang membuat pengguna memahami bahwa mereka akan dipecat jika mereka tertangkap situs Web berselancar terlarang atau ilegal adalah pencegahan.
• **Kompensasi** :Sebuah kontrol kompensasi adalah kontrol keamanan tambahan dimasukkan ke dalam tempat untuk mengkompensasi kelemahan dalam kontrol lainnya.

AUTHENTICATION METHODS

Tipe 1 otentikasi sesuatu yang harus anda tahu.

membutuhkan pengujian subjek dengan beberapa semacam tantangan dan respon dimana subjek harus merespon dengan luas menjawab. Subjek diberikan akses atas dasar sesuatu yang mereka tahu, seperti password atau PIN (Personal Identification Number, password nomor-based). Ini adalah bentuk paling mudah, dan sering lemah, otentikasi.

Password

Password telah menjadi landasan untuk kontrol akses ke sistem TI. Mereka relatif mudah dan murah untuk melaksanakan. Banyak perbankan, layanan portofolio saham online, Web mail pribadi, dan kesehatan sistem masih menggunakan nama pengguna dan password sebagai Metode kontrol akses.
Ada empat jenis password untuk dipertimbangkan ketika menerapkan kontrol akses: password statis, passphrase, satu kali password, dan password dinamis.

Tipe 2 otentikasi (sesuatu yang harus)

mengharuskan pengguna memiliki sesuatu,seperti token, yang membuktikan mereka adalah pengguna dikonfirmasi. Token adalah sebuah objek yang membantu membuktikan klaim identitas.

Token dinamis sinkron

Token dinamis sinkron menggunakan waktu atau counter untuk menyinkronkan tanda ditampilkan
kode dengan kode diharapkan oleh server otentikasi: kode disinkronisasi

Jenis kontrol biometrik

Ada sejumlah kontrol biometrik yang digunakan saat ini. Berikut ini adalah implementasi utama dan pro khusus mereka dan kontra terkait dengan mengakses kontrol keamanan.

1. **Sidik jari**
   Sidik jari adalah yang paling banyak digunakan kontrol biometrik yang tersedia saat ini. Smartcard dapat membawa informasi sidik jari. Banyak gedung perkantoran Pemerintah AS mengandalkan otentikasi sidik jari untuk akses fisik ke fasilitas. Contohnya termasuk cerdas
2. **Pemindaian retina**
   Scan retina adalah scan laser kapiler yang memberi makan retina dari belakang mata. Ini bisa mengganggu pribadi karena sinar harus langsung masukkan pupil, dan pengguna biasanya perlu menekan mata mereka hingga scanner laser
3. **iris Scan**
   Scan iris adalah kontrol biometrik pasif. Sebuah kamera mengambil gambar dari iris (yang berwarna porsi mata) dan kemudian membandingkan foto dalam database otentikasi.
4. **Geometri tangan**
   Di tangan geometri kontrol biometrik, pengukuran diambil dari titik-titik tertentu pada tangan subjek: "Perangkat menggunakan konsep yang sederhana untuk mengukur dan merekam

5. **Dinamika Keyboard**
   Dinamika Keyboard mengacu pada seberapa keras seseorang menekan setiap tombol dan irama oleh yang tombol yang ditekan.
6. Signature dinamis
   Tanda tangan dinamis mengukur proses dimana seseorang sign namanya.
7. Voiceprint
   Sebuah voiceprint mengukur nada subjek suara sementara menyatakan kalimat tertentu atau frase. Jenis kontrol akses rentan terhadap serangan replay (mengulang sebuah rekaman suara), sehingga kontrol akses lainnya harus dilaksanakan bersama dengan voiceprint tersebut.

TECHNOLOGIES ACCESS CONTROL

Ada beberapa teknologi yang digunakan untuk pelaksanaan kontrol akses. Karena setiap teknologi disajikan, penting untuk mengidentifikasi apa yang unik tentang masing-masing solusi teknis.

Single sign-on
Sign-On tunggal (SSO) memungkinkan beberapa sistem untuk menggunakan serverotentikasi pusat (AS). Hal ini memungkinkan pengguna untuk mengotentikasi sekali dan kemudian mengakses beberapa, sistem yang berbeda.

ASSESSING ACCESS CONTROL

Sejumlah proses yang ada untuk menilai efektivitas pengendalian akses. Tes dengan lingkup sempit meliputi tes penetrasi, penilaian kerentanan, dan keamananaudit. Sebuah penilaian keamanan adalah tes yang lebih luas yang mungkin termasuk tes sempit, seperti sebagai tes penetrasi, sebagai sub bagian

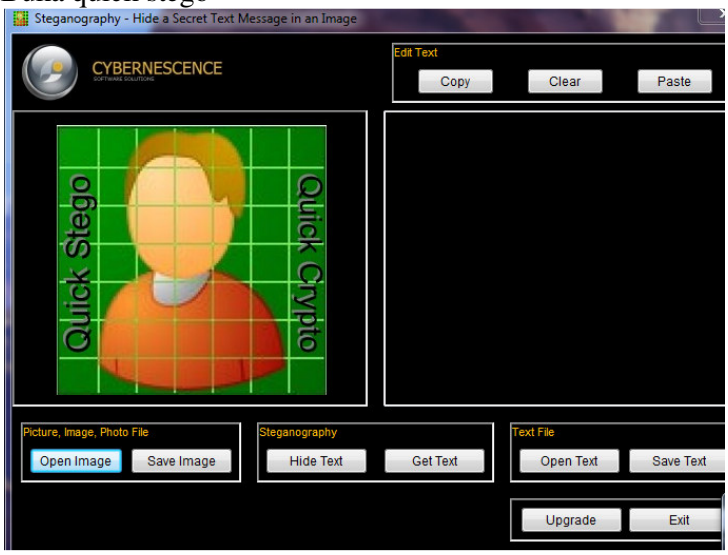
pengujian penetrasi
Sebuah tester penetrasi adalah hacker topi putih yang menerima otorisasi untuk mencoba masuk ke perimeter fisik atau elektronik organisasi (dan kadang-kadang keduanya).

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

TUGAS 2.

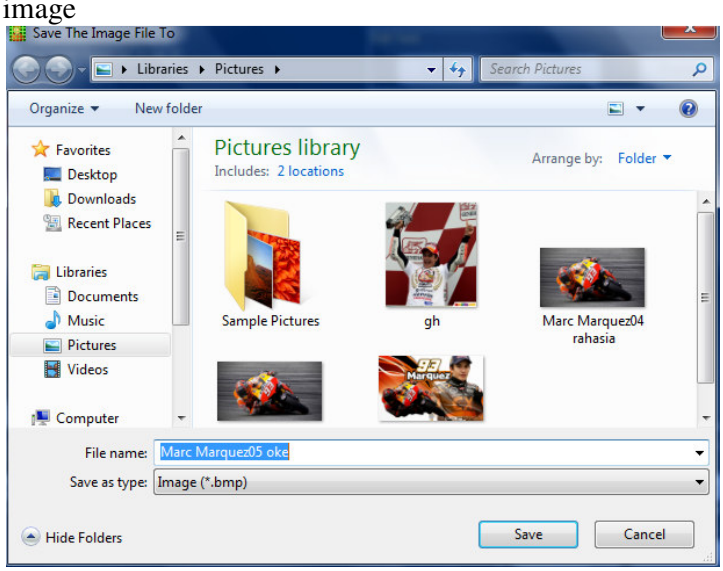
Kali ini saya menggunakan quick stego software steganography yang menyimpan pesan teks khusus yang disimpan di gambar.

1. Cara pertama instlla quick stego
2. Buka quick stego



3. Lalu klik open image cari image yang anda ingin disisipakn text

4. Setelah itu ketikkan text yang akan di sisipkan ke gambar, lalu pilih hide text dan save image



5. Untuk melihatnya buka lagi quick stego dan open image lalu get text
Ini jadinya :

TERIMA KASIH