Nama : Nurlaili

NIM : 1310651024

Kelas : D

1. Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume **tidak boleh** sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.

   Jawab :

Kontrol Akses

KONSEP KEAMANAN INFORMASI

Kerahasiaan Integritas dan Ketersediaan adalah "triad CIA," konsep landasan keamanan informasi. Urutan akronim dapat berubah (beberapa lebih "AIC," mungkin untuk menghindari hubungan dengan badan intelijen tertentu), tetapi konsep-konsep yang penting. Buku ini akan menggunakan "CIA" singkatan.

- Kerahasiaan

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

-Integritas

Integritas berusaha untuk mencegah modifikasi yang tidak sah dari informasi. Dengan kata lain, integritas berusaha untuk mencegah akses tulis tidak sah ke data.

- Ketersediaan

Ketersediaan memastikan bahwa informasi yang tersedia bila diperlukan. Sistem harus dapat digunakan (tersedia) untuk penggunaan bisnis normal. Contoh dari serangan terhadap ketersediaan akan menjadi
Denial-of-Service (DoS) serangan, yang berusaha untuk menolak layanan (atau availability) dari suatu sistem.

- Identitas dan otentikasi, otorisasi, dan akuntabilitas

Istilah "AAA" sering digunakan, menggambarkan konsep landasan
pembuktian keaslian otorisasi dan Akuntabilitas. Waktu keluar dari singkatan AAA adalah identifikasi
yang diperlukan sebelum tiga "A" dapat mengikuti.

- Identitas dan otentikasi

Identitas adalah klaim: jika nama Anda adalah "Orang X," Anda mengidentifikasi diri dengan mengatakan "Saya Orang X. "Identitas saja lemah karena tidak ada bukti. Anda juga dapat mengidentifikasi diri dengan mengatakan "Saya Orang Y." Membuktikan klaim identitas disebut authentication: Anda mengotentikasi klaim identitas, biasanya dengan menyediakan sepotong informasi atau sebuah benda yang hanya Anda dimiliki, seperti password atau paspor Anda.

- Otorisasi

Otorisasi menjelaskan tindakan yang dapat Anda lakukan pada sistem setelah Anda memiliki identified dan dikonfirmasi. Tindakan mungkin termasuk membaca, menulis, atau file eksekusi atau program.

- Akuntabilitas

Akuntabilitas memegang pengguna jawab atas tindakan mereka.Hal Ini biasanya dilakukan dengan login dan menganalisis data audit. Menegakkan akuntabilitas membantu menjaga "Orang-orang jujur jujur." Untuk beberapa pengguna, mengetahui bahwa data login tidak cukup untuk memberikan akuntabilitas: mereka harus tahu bahwa data yang dicatat dan diaudit dan Sanksi mungkin akibat dari pelanggaran polis.

- Nonrepudiation

Nonrepudiation berarti pengguna tidak dapat menyangkal (menolak) setelah dilakukan transaksi. Ini menggabungkan otentikasi dan integritas: nonrepudiation mengotentikasi identiity dari pengguna yang melakukan transaksi dan memastikan integritas transaksi itu. Anda harus memiliki kedua otentikasi dan integritas untuk memiliki nonrepudiation: membuktikan Anda menandatangani kontrak untuk membeli mobil (otentikasi identitas Anda sebagai pembeli) tidak berguna jika dealer mobil dapat mengubah harga dari $ 20.000 sampai $ 40.000 (melanggar integritas kontrak).

-Paling istimewa dan perlu tahu

Paling istimewa berarti pengguna harus diberikan jumlah minimum akses (Otorisasi) diperlukan untuk melakukan pekerjaan mereka, tapi tidak lebih. Paling istimewa diterapkan untuk kelompok benda. Perlu tahu lebih rinci dari paling istimewa: pengguna harus perlu tahu bahwa bagian tertentu dari informasi sebelum mengakses itu.

-Subyek dan obyek

subyek adalah entitas aktif pada sistem data. Sebagian contoh pelajaran melibatkan orang mengakses file data. Namun, program komputer yang menjalankan adalah subyek demikian juga.

obyek adalah data pasif dalam sistem. Objek dapat berkisar dari database ke file teks. Hal penting untuk diingat tentang obyek adalah bahwa mereka pasif dalam sistem. Mereka tidak memanipulasi benda-benda lain.

-Pertahanan-mendalam

pertahanan di kedalaman (juga disebut pertahanan berlapis) berlaku beberapa perlindungan (juga
disebut kontrol: tindakan yang diambil untuk mengurangi resiko) untuk melindungi aset. Setiap keamanan tunggal control mungkin gagal; dengan mengerahkan beberapa kontrol, Anda meningkatkan kerahasiaan, integritas, dan ketersediaan data.

Model Kontrol Akses

- Discretionary access controls (DAC)
- Mandatory access controls (MAC)
- Nondiscretionary access control /Role-Based Access Control(RBAC)
- Rule-based access controls
- Centralized access control
- Access control lists (ACLs)
- Access provisioning lifecycle
- User entitlement, access review, and audit
- Access control protocols and frameworks
- The Remote Authentication Dial-In User Service (RADIUS)
- Diameter
- TACACS and TACACS
- PAP and CHAP

2. Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

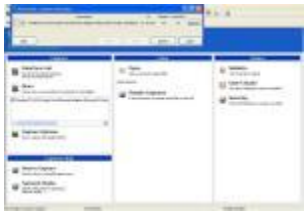
   Jawab :

Monitoring Jaringan Menggunakan Wireshark

Salah satu keunggulan dari Wireshark adalah kita bisa melihat protokol-protokol yang ada pada jaringan yang kita monitor, software ini biasanya di gunakan untuk menganalisa jaringan

untuk memulai proses monitoring menggunakan wireshark, buka aplikasinya

Klik **Interface List**, pastikan pilih interface anda yang terhubung ke jaringan



setelah muncul klik, interfacenya

lalu klik **start**, dan tunggu, kemudian wireshark akan memproses kegiatan yang terjadi pada jaringan

Terlihat pada gambar, beberapa informasi, mulai dari MAC address yang sedang melakukan komunikasi, protokol yang di gunakan, terlihat juga IP address dari sumber ke tujuan tertentu,

sebagai catatan, wireshark biasanya di gunakan untuk monitoring pada jaringan lokal, tetapi kita bisa melihat kegiatan host-host yang berada satu jaringan dengan kita, apabila mereka mengakses internet, dan wireshark hanya bisa bekerja bila komputer kita terhubung ke jaringan menggunakan perangkat fisik (ethernet atau wireless), jadi apabila menggunakan modem broadband setau saya tidak bisa.

Program ini sering juga di gunakan untuk “sniffing”, jadi bila anda menggunakan program ini maka gunakan secara bijak.