KEAMANAN INFORMASI

TUGAS UAS

Disusun oleh:

(DONI ANDRIAN)

(1410651010)

(B)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

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?

JAWABAN :

- ## Access Control

Confidentiality, integrity, and availability

Confidentiality, Integrity, and Availability are the "CIA triad," the cornerstone concept of information security. The triad, shown in Figure 1.1, forms the three-legged stool information security is built upon. The order of the acronym may change (some prefer "AIC," perhaps to avoid association with a certain intelligence agency), but the concepts are essential. This book will use the "CIA" acronym.

Confidentiality

Confidentiality seeks to prevent the unauthorized disclosure of information: it keeps data secret. In other words, confidentiality seeks to prevent unauthorized read access to data. An example of a confidentiality attack would be the theft of Personally Identifiable Information (PII), such as credit card information.

Integrity

Integrity seeks to prevent unauthorized modification of information. In other words, integrity seeks to prevent unauthorized write access to data .

Availability

Availability ensures that information is available when needed. Systems need to be usable (available) for normal businessuse. An example of attack on availability would be a Denial-of-Service (DoS) attack, which seeks to deny service (or availability) of a system.

Authentication **:** agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi.

***Integrity* :** keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan
***Authority* :** Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
***Confidentiality* :** merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.

Identity and authentication, authorization, and accountability

The term "AAA" is often used, describing cornerstone concepts Authentication,

Authorization, and Accountability. Left out of the AAA acronym is Identification,

which is required before the three "A's" can follow.

Identity and authentication

Identity is a claim: if your name is "Person X," you identify yourself by saying "I am Person X." Identity alone is weak because there is no proof. You can also identify yourself by saying "I am Person Y." Proving an identity claim is called authentication: you authenticate the identity claim, usually by supplying a piece of information or an object that only you posses, such as a password or your passport.

Authorization

Authorization describes the actions you can perform on a system once you have identified and authenticated. Actions may include reading, writing, or executing files or programs.

Accountability

Accountability holds users accountable for their actions. This is typically accomplished by logging and analyzing audit data. Enforcing accountability helps keep "honest people honest." For some users, knowing that data is logged is not enough to provide accountability: they must know that the data is logged and audited and that sanctions may result from violation of policy.

ACCESS CONTROL TECHNOLOGIES

There are several technologies used for the implementation of access controls. As each technology is presented, it is important to identify what is unique about each technical solution.

Single sign-on

Single Sign-On (SSO) allows multiple systems to use a central authentication server (AS). This allows users to authenticate once and then access multiple, different systems.

It also allows security administrators to add, change, or revoke user privileges on one central system. The primary disadvantage to SSO is it may allow an attacker to gain access to multiple resources after compromising one authentication method, such as a password. SSO should always be used with multifactor authentication for this reason.

Federated identity management

Federated Identity Management (FIdM) applies Single Sign-On at a much wider scale: ranging from cross organization to Internet scale. It is sometimes simply called Identity Management (IdM). FIdM may use OpenID or SAML (Security Association Markup Language). According to EDUCAUSE, "Identity management refers to the policies, processes, and technologies that establish user identities and enforce rules about access to digital resources. In a campus setting, many information systems—such as e-mail, learning management systems, library databases, and grid computing applications—require users to authenticate themselves (typically with a username and password). An authorization process then determines which systems an authenticated user is permitted to access. With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled. Federated identity management permits extending this approach above the enterprise level, creating a trusted authority for digital identities across multiple organizations. In a federated system, participating institutions share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and granting appropriate access to online resources. This approach streamlines access to digital assets while protecting restricted resources.

Kerberos

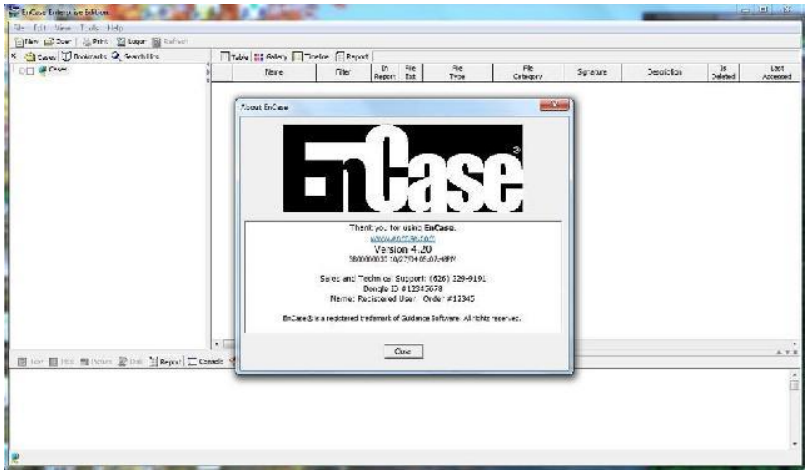
Kerberos is a third-party authentication service that may be used to support Single Sign-On. Kerberos (http://www.kerberos.org/) was the name of the threeheaded dog that guarded the entrance to Hades (also called Cerberus) in Greek mythology.

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.

JAWABAN :

- **EnCase Forensic**

  EnCase Forensic adalah Sebuah Software standar industri dalam teknologi komputer penyelidikan forensik Fungsinya untuk mengumpulakan Barang bukti. Dengan GUI yang intuitif, analisis unggul, email ditingkatkan support / Internet dan mesin scripting yang kuat, menyelimuti menyediakan peneliti dengan alat tunggal, yang mampu melakukan investigasi skala besar dan kompleks dari awal hingga akhir. Hukum aparat penegak hukum, / pemerintah perusahaan dan konsultan peneliti di seluruh dunia manfaat dari kekuatan menyelimuti Forensik dengan cara yang jauh melebihi solusi forensik lainnya.



* Memperoleh data secara forensik suara menggunakan perangkat lunak dengan rekor tak tertandingi di pengadilan di seluruh dunia.
* Memeriksa dan menganalisis beberapa platform - Windows, Linux, AIX, OS X, Solaris dan lebih - menggunakan alat tunggal.
* Simpan hari, jika tidak minggu, waktu analisis dengan mengotomatisasi tugas-tugas kompleks dan rutin dengan prebuilt enscript ® modul, seperti diinisialisasi kasus dan analisis Event Log.
* Cari informasi meskipun upaya untuk menyembunyikan, jubah atau menghapus.
* Mudah mengelola volume besar bukti komputer, melihat semua file yang relevan, termasuk "dihapus" file, slack file dan ruang yang tidak terisi.
* Bukti transfer file langsung ke penegakan hukum atau perwakilan hukum yang diperlukan.
* Review opsi ini mengizinkan non-peneliti, seperti pengacara, untuk meninjau bukti-bukti dengan

mudah.
* Pelaporan pilihan memungkinkan penyusunan laporan cepat.

EnCase merupakan software yang digunakan oleh banyak pelaksana hukum untuk mendapatkan keterangan atau kesaksian atau bukti kejahatan (yang dilakukan oleh seseorang yang dicurigai melakukan tindakan kejahatan dengan menggunakan komputer sebagai fasilitasnya) dengan melakukan scan terhadap hard drive (harddisk) komputer. Sekilas terlihat seperti program Recovery yang dapat membangkitkan file/data yang terhapus dari harddisk. Tetapi tetap ada perbedaannya, dan perbedaan tersebut akan anda ketahui setelah mencobanya. Setelah anda mendapatkan Ensetup.exe maka instalasi sudah dapat dilakukan dengan melakukan klik ganda pada ensetup.exe. Nantinya anda akan menemukan window instalasi. Untuk melanjutkan instalasi, klik tombol yang bertulisan Install Now, maka akan akan melihat proses instalasi yang berjalan. Tidak membutuhkan waktu yang sangat panjang dalam instalasi.

EnCase Forensic Persyaratan Sistem
Panduan Software merekomendasikan persyaratan perangkat keras minimum berikut untuk membungkus Forensik:

• Windows 2000, XP, atau 2003 Server
• Single 3 GHz Intel atau prosesor AMD atau lebih baik disarankan
• 1 GB RAM (2 GB atau lebih direkomendasikan)
• 1 Port USB
• oknum penyimpanan data untuk mendukung akuisisi bukti berkas yang disarankan