KEAMANAN INFORMASI

TUGAS

UJIAN AKHIR SEMESTER

Disusun oleh:

(MIFTARULLAH FIRDAUS)

(1410651012)

(B)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

Soal No. 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

The purpose of access control is to allow authorized users access to appropriate data and deny access to unauthorized users. Access controls protect against threats such as unauthorized access, inappropriate modification of data, and loss of confidentiality.

- **Confidentiality**

Confidentiality seeks to prevent the unauthorized disclosure of information: it keeps data secret. In other words, confidentiality seeks to prevent nauthorized 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 business use. An example of attack on availability would be a Denial-of-Service (DoS) attack, which seeks to deny service (or availability) of a system.

ACCESS CONTROL DEFENSIVE CATEGORIES AND TYPES

In order to understand and appropriately implement access controls, understanding what benefits each control can add to security is vital. In this section, each type of access control will be defined on the basis of how it adds to the security of the system. There are six access control types:

- **Preventive**

Preventive controls prevent actions from occurring. It applies restrictions to what a potential user, either authorized or unauthorized, can do. An example of an administrative preventive control is a preemployment drug screening. It is designed to prevent an organization from hiring an employee who is using illegal drugs.

- **Detective**

Detective controls are controls that alert during or after a successful attack. Intrusion detection systems alerting after a successful attack, closed-circuit

television cameras (CCTV) that alert guards to an intruder, and a building alarm system that is triggered by an intruder are all examples of detective controls.

- **Corrective**

Corrective controls work by “correcting” a damaged system or process. The corrective access control typically works hand in hand with detective access controls. Antivirus software has both components. First, the antivirus software runs a scan and uses its definition file to detect whether there is any software that matches its virus list. If it detects a virus, the corrective controls take over, place the suspicious software in quarantine, or delete it from the system.

- **Recovery**

After a security incident has occurred, recovery controls may need to be taken in order to restore functionality of the system and organization. Recovery means that the system must be recovered: reinstalled from OS media or image, data restored from backups, etc.

- **Deterrent**

Deterrent controls deter users from performing actions on a system. Examples include a “beware of dog” sign: a thief facing two buildings, one with guard dogs and one without,is more likely to attack the buildingwithout guard dogs. A large fine for speeding is a deterrent for drivers to not speed. A sanction policy that makes users understand that they will be fired if they are caught surfing illicit or illegal Web sites is a deterrent.

- **Compensating**

A compensating control is an additional security control put in place to compensate for weaknesses in other controls.

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.

a) **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.

b) **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).

c) 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.

SESAME

SESAME is Secure European System for Applications in a multivendor environment, a single sign-on system that supports heterogeneous environments. SESAME can be thought of as a sequel of sorts to Kerberos, "SESAME adds to Kerberos: heterogeneity, sophisticated access control features, scalability of public key systems, better manageability, audit and delegation."9 Of those improvements, the addition of public key (asymmetric) encryption is the most compelling. It addresses one of the biggest weaknesses in Kerberos: the plaintext storage of symmetric keys.
SESAME uses Privilege Attribute Certificates (PACs) in place of Kerberos' tickets. More information on SESAME is available at https://www.cosic.esat.kuleuven.be/sesame/.

ASSESSING ACCESS CONTROL

A number of processes exist to assess the effectiveness of access control. Tests with a narrower scope include penetration tests, vulnerability assessments, and security audits. A security assessment is a broader test that may include narrower tests, such as penetration tests, as subsections.

Penetration testing

A penetration tester is a white hat hacker who receives authorization to attempt to break into an organization's physical or electronic perimeter (and sometimes both). Penetration tests (called "pen tests" for short) are designed to determine whether black hat hackers could do the same. They are a arrow, but often useful, test, especially if the penetration tester is successful.
Penetration tests may include the following tests:

- Network (Internet)
- Network (internal or DMZ)
- War dialing
- Wireless
- Physical (attempt to gain entrance into a facility or room)
- Wireless

Network attacks may leverage client-side attacks, server-side attacks, or Web application attacks. See Chapter 6, "Domain 6: Security Architecture and Design" for more information on these attacks. War dialing uses modem to dial a series of phone numbers, looking for an answering modem carrier tone

(the penetration tester then attempts to access the answering system); the name derives from the 1983 movie WarGames.

Vulnerability testing
Vulnerability scanning (also called vulnerability testing) scans a network or system for a list of predefined vulnerabilities such as system misconfiguration, outdated software, or a lack of patching. A vulnerability testing tool such as Nessus (http://www.nessus.org) or OpenVAS (http://www.openvas.org) may be used to identify the vulnerabilities.

Security audits
A security audit is a test against a published standard. Organizations may be audited for PCI-DSS (Payment Card Industry Data Security Standard) compliance, for example. PCI-DSS includes many required controls, such as firewalls, specific access control models, and wireless encryption. An auditor then verifies a site or organization meets the published standard.

Security assessments
Security assessments are a holistic approach to assessing the effectiveness of access control. Instead of looking narrowly at penetration tests or vulnerability assessments, security assessments have a broader scope.

Soal No. 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 :

AirCover Security

tampilan menu

tampilan proses cleanup

Selain gratis aplikasi ini juga powerfull dengan fitur-fitur yang ada didalamnya.Seperti antivirus untuk menangani virus malware, fitur find lost device saat kalian kehilangan Smarphone Android kalian bisa menggunakan fitur ini untuk melacak Smartphone kalian dan melock dan menghapus data-data yang penting yang ada didalam Smartphone.tampilan yang nyaman dan fitur yang usefull aplikasi ini juga memenangkan penghargaan untuk kategori ***Security Protection APP for Antitheft, Antivirus and Clean.***