Nama : Samsul Arifin
Nim : 1310651082
Kelas : A

Domain 7: Operations Security

EXAM OBJECTIVES IN THIS CHAPTER
- Administrative Security
- Sensitive Information/Media Security
- Asset Management
- Continuity of Operations
- Incident Response Management

INTRODUCTION

Operations security is concerned with threats to a production operating environment. Threat agents can be internal or external actors, and operations security must account for both of these threat sources in order to be effective. Operations security is about people, data, media, hardware, and the threats associated with each of these in a production environment.

ADMINISTRATIVE SECURITY

A fundamental aspect of operations security is ensuring that controls are in place to inhibit people either inadvertently or intentionally compromising the confidentiality, integrity, or availability of data or the systems and media holding that data. Administrative security provides the means to control people's operational access to data.

Labels

Objects have labels and subjects have clearances. The object labels used by many world governments are confidential, secret, and top secret. According to Executive Order 12356—National Security Information,

• "top secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

• "secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

• "confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.[1]

Private sector companies use labels such as "Internal Use Only" and "Company Proprietary."

Clearance

A clearance is a determination concerning whether or not a user can be trusted with a specific level of information. Clearances must determine the subject's current and potential future trustworthiness; the latter is harder (and more expensive) to assess. Are there anyissues, suchasdebt or drugor alcohol abuse,whichcould leadanotherwise ethical person to violate their ethics? Is there a personal secret that could be used to blackmail this person? Some higher-level clearances include access to compartmented information. Compartmentalization is a technical method for enforcing need to know

Separation of duties

Separation of duties (also called segregation of duties) allows an organization to maintain checks and balances among the employees with privileged access. By having more than one individual perform part of a sensitive transaction, each person involved is supervising the other when access is granted and used. As the role becomes more sensitive, separation of duties should be implemented more stringently. For example, administration of a nuclear weapons system should require many people's oversight and completion of duties.

SENSITIVE INFORMATION/MEDIA SECURITY

Though security and controls related to the people within an enterprise are vitally important, so is having a regimented process for handling sensitive information, including media security. This section discusses concepts that are an important component of a strong overall information security posture.

Sensitive information

Sensitive information requires protection, and that information physically resides on some form of media. In addition to primary storage, backup storage must also be considered. It is also likely that sensitive information is transferred, whether internally or externally, for use. Wherever the data exists, there must be processes that ensure the data is not destroyed or inaccessible (a breach of availability), disclosed (a breach of confidentiality), or altered (a breach of integrity).

Labeling/marking

Perhaps the most important step in media security is the process of locating sensitive information and labeling or marking it as sensitive. How the data is labeled should correspond to the organizational data classification scheme.

Handling

People handling sensitive media should be trusted individuals who have been vetted by the organization. They must understand their role in the organization's information security posture.

Storage

When storing sensitive information, it is preferable to encrypt the data. Encryption of data at rest greatly reduces the likelihood of the data being disclosed in an unauthorized fashion due to media security issues.

Retention

Media and information have a limited useful life. Retention of sensitive information should not persist beyond the period of usefulness or legal requirement (whichever is greater), as it needlessly exposes the data to threats of disclosure when the data is no longer needed by the organization.

Media sanitization or destruction of data

While some data might not be sensitive and not warrant thorough data destruction measures, an organization will have data that must be verifiably destroyed or otherwise rendered nonusable in case the media on which it was housed is recovered by a third party.

Data remanence

Data remanence is data that persists beyond noninvasive means to delete it. Though data remanence is sometimes used specifically to refer to residual data that persists on magnetic storage, remanence concerns go beyond just that of magnetic storage media.

Wiping, overwriting, or shredding

In most file systems, if a user deletes a file, the file system merely removes metadata pointers or references to the file. The file allocation table references are removed, but

the file data itself remains. Significant amounts of "deleted data" may be recovered (undeleted); forensic tools are readily available to do so. Reformatting a file system may also leave data intact.

Degaussing

By introducing an external magnetic field through use of a degausser, the data on magnetic storage media can be made unrecoverable.

Physical destruction

Physical destruction, when carried out properly, is considered the most secure means of media sanitization. One of the reasons for the higher degree of assurance is because of the greater likelihood of errors resulting in data remanence with wiping or degaussing.

Shredding

A simple form of media sanitization is shredding, a type of physical destruction. Though this term is sometimes used in relation to overwriting of data, here shredding refers to the process of making data printed on hard copy, or on smaller objects such as floppy or optical disks, unrecoverable. Dumpster diving is a physical attack in which a person recovers trash in hopesof finding sensitive information that has not been securely erased or destroyed.

ASSET MANAGEMENT

A holistic approach to operational information security requires organizations to focus on systems as well as the people, data, and media. Systems security is another vital component to operations security, and there are specific controls that can greatly help system security throughout the system's life cycle.

Configuration management

Basic configuration management practices associated with system security will involve tasks such as disabling unnecessary services; removing extraneous programs; enabling security capabilities such as firewalls, antivirus, and intrusion detection or prevention systems; and the configurating security and audit logs.

Baselining

Security baselining is the process of capturing a point in time understanding of the current system security configuration.

Vulnerability management

Vulnerability scanning is a way to discover poor configurations and missing patches in an environment. The term vulnerability management is used rather than just vulnerability scanning to emphasize the need for management of the vulnerability information.

Zero-day vulnerabilities and zero-day exploits

A zero-day vulnerability is a vulnerability that is known before the existence of a patch. Zero-day vulnerabilities, also commonly written 0-day, are becoming increasingly important as attackers are becoming more skilled in discovery, and disclosure of zero-day vulnerabilities is being monetized.

Change management

In order to maintain consistent and known operations security, a regimented change management or change control process needs to be followed. The purpose of the change control process is to understand, communicate, and document any changes

with the primary goal of being able to understand, control, and avoid direct or indirect negative impact that the change might impose.

FAST FACTS

Because of the variability of the change management process, specific named phases have not been offered in this section. However, the general flow of the change management process includes:

- Identifying a change
- Proposing a change
- Assessing the risk associated with the change
- Testing the change
- Scheduling the change
- Notifying impacted parties of the change
- Implementing the change
- Reporting results of the change implementation

CONTINUITY OF OPERATIONS

Continuity of operations is principally concerned with the availability portion of the confidentiality, integrity, and availability triad.

Service-Level Agreements

A Service-Level Agreement (SLA) stipulates all expectations regarding the behavior of the department or organization that is responsible for providing services and the quality of the services provided.

Backup

In order for data to be able to be recovered in case of a fault, some form of backup or redundancy must be provided. Though magnetic tape media is quite an old technology, it is still the most common repository of backup data.

Incremental and differential

Incremental backups only archive files that have changed since the last backup of any kind was performed. Differential backups will archive any files that have been changed since the last full backup.

Redundant Array of Inexpensive Disks

Even if only one full backup tape is needed for recovery of a system due to a hard disk failure, the time to recover a large amount of data can easily exceed the recovery time dictated by the organization.

FAST FACTS

Three critical RAID terms are: mirroring, striping, and parity.

- Mirroring achieves full data redundancy by writing the same data to multiple hard disks.
- Striping focuses on increasing read and write performance by spreading data across multiple hard disks. Writes can be performed in parallel across multiple disks rather than serially on one disk. This parallelization provides a performance increase and does not aid in data redundancy.
- Parity achieves data redundancy without incurring the same degree of cost as that of mirroring in terms of disk usage and write performance.

RAID 0: Striped set

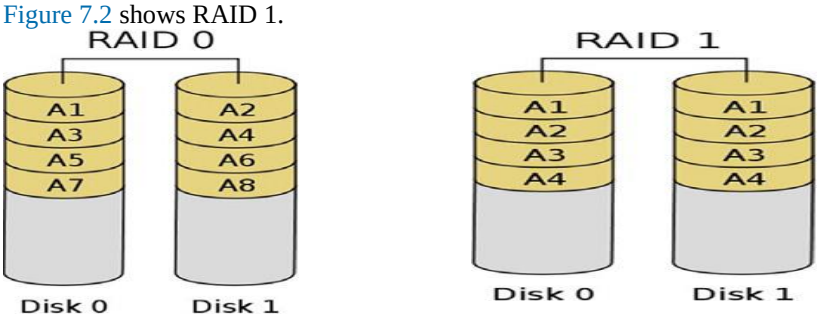
RAID 0 employs striping to increase the performance of read and writes. Striping offers no data redundancy so RAID 0 is a poor choice if recovery of data is critical.

Figure 7.1 shows RAID 0.

RAID 1: Mirrored set

RAID 1 creates/writes an exact duplicate of all data to an additional disk. The write performance is decreased, though the read performance can see an increase.

Figure 7.2 shows RAID 1.



RAID 2: Hamming code

RAID 2 is a legacy technology that requires either 14 or 39 hard disks and a specially designed hardware controller, which makes RAID 2 cost-prohibitive. RAID 2 stripes at the bit level.

RAID 3: Striped set with dedicated parity (byte level)

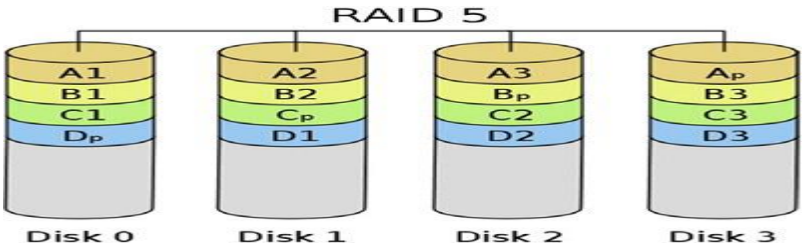
Striping is desirable due to the performance gains associated with spreading data across multiple disks. However, striping alone is not as desirable due to the lack of redundancy.

RAID 4: Striped set with dedicated parity (block level)

RAID 4 provides the same functionality as RAID 3 but stripes data at the block, rather than byte, level. Like RAID 3, RAID 4 employs a dedicated parity drive rather than having parity data distributed among all disks, as in RAID 5.

RAID 5: Striped set with distributed parity

One of the most popular RAID configurations is that of RAID 5, striped set with distributed parity. Like RAIDs 3 and 4, RAID 5 writes parity information that is used for recovery purposes. RAID 5 writes at the block level, like RAID 4. However, unlike RAIDs 3 and 4, which require a dedicated disk for parity information, RAID 5 distributes the parity information across multiple disks.



RAID 6: Striped set with dual distributed parity

While RAID 5 accommodates the loss of any one drive in the array, RAID 6 can allow for the failure of two drives and still function.

RAID 1þ0 or RAID 10

RAID 1þ0 or RAID 10 is an example of what is known as nested RAID or multi-RAID, which simply means that one standard RAID level is encapsulated within another. With RAID 10, which is also commonly written as RAID 1þ0 to explicitly indicate the nesting, the configuration is that of a striped set of mirrors.

CRUNCH TIME

Table 7.1 provides a brief description of the various RAID levels that are most commonly used.

Table 7.1 RAID Levels	
RAID Level	Description
RAID 0	Block-level striped set
RAID 1	Byte-level striping with dedicated parity
RAID 3	Block-level striping with dedicated parity
RAID 4	Block-level striping with distributed parity
RAID 5	Block-level striping with distributed parity
RAID 6	Block-level striping with dual distributed parity

System redundancy

Though redundancy and resiliency of data, provided by RAID and backup solutions, are important, further consideration needs to be given to the systems themselves that provide access to this redundant data.

Redundant hardware and redundant systems

Many systems can provide internal hardware redundancy of components that are extremely prone to failure. The most common example of this in-built redundancy is systems or devices that have redundant onboard power in the event of a power supply failure. Sometimes, systems simply have field-replaceable modular versions of commonly failing components.

High-availability clusters

A high-availability cluster (also called a failover cluster) uses multiple systems that are already installed, configured, and plugged in, such that if a failure causes one of the systems to fail then the other can be seamlessly leveraged to maintain the availability of the service or application being provided.

INCIDENT RESPONSE MANAGEMENT

A security incident is a harmful occurrence on a system or network. All organizations will experience security incidents. Incident response management is a regimented and tested methodology for identifying and responding to these incidents.

A Computer Security Incident Response Team (CSIRT) is the group tasked with monitoring, identifying, and responding to security incidents.

Methodology

Figure 7.4 is from the NIST Special Publication 800-61: Computer Security Incident Handling Guide (see http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf), which outlines the incident response life cycle in four steps:

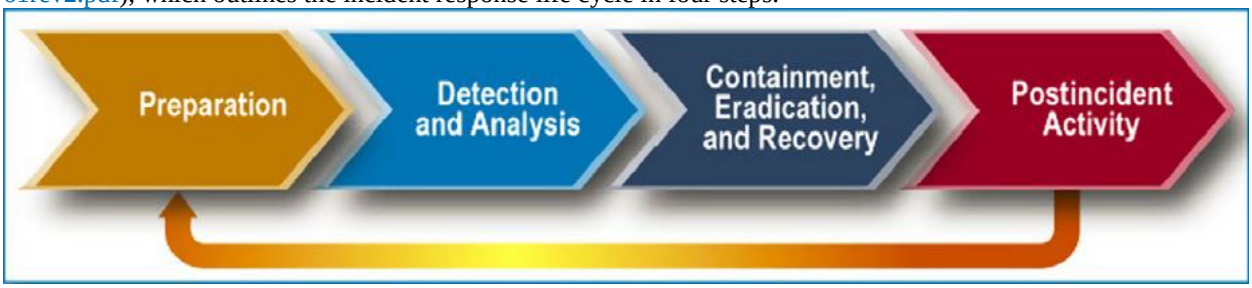


FIGURE 7.4
NIST Incident Response Life cycle.[2]

1. Preparation
2. Detection and analysis (aka identification)
3. Containment
4. Eradication

5. Recovery
6. Lessons learned (aka postincident activity, postmortem, or reporting)

Preparation

The preparation phase includes steps taken before an incident occurs. These include training, writing incident response policies and procedures, and providing tools such as laptops with sniffing software, crossover cables, original OS media, removable drives, etc.

Detection and analysis

Detection (also called identification) is the phase where events are analyzed in order to determine whether they comprise a security incident.

Containment

The containment phase is the point at which the incident response team attempts to keep further damage from occurring as a result of the incident. Containment might include taking a system off the network, isolating traffic, powering off the system, or other items to control both the scope and severity of the incident.

Eradication

The eradication phase involves two steps: removing any malicious software from a compromised system and understanding the cause of the incident so that the system can be reliably cleaned and safely restored to operational status later in the recovery phase.

Recovery

The recovery phase involves cautiously restoring the system or systems to operational status. Typically, the business unit responsible for the system will dictate when the system will go back online.

Lessons learned

Unfortunately, the lessons learned phase (also known as postincident activity, reporting, or postmortem) is likely to be neglected in immature incident response programs. This fact is unfortunate because the lessons learned phase, if done right, is the phase that has the greatest potential to effect a positive change in security posture.

Types of attacks

This section will provide basic information on the types of attacks more commonly experienced and responded to in organizations.

Session hijacking and MITM

Session hijacking compromises an existing network session, sometimes seizing control of it. A Man-in-the-Middle (MITM, also called Monkey in the Middle) attack places the attacker between the victim and another system: the attacker's goal is to be able to serve as an undiscovered proxy for either or both of two endpoints engaging in communication.

Malware

Malware, or malicious code/software, represents one of the best-known types of threats to information systems. There are numerous types of malware, some detailed in Table 7.2, that have evolved over the years to continually cause stress to operations.

Denial of Service and Distributed Denial of Service

Denial of Service (DoS) is a one-to-one availability attack; Distributed Denial of Service (DDoS) is a many-to-one availability attack. DDoS attacks that leverage tens of thousands (or more) of bots to target an online service provider with a flood of seemingly legitimate traffic attempting to overwhelm their capacity. Table 7.3 includes historical examples of malicious packet attacks as well as some general resource exhaustion, or flooding, techniques.

Table 7.2 Types of Malware

Malicious Code	Description
Virus	A virus is malware that does not self propagate: it requires a carrier, such as a human manually moving an infected USB device from one system to another
Macro virus	A macro virus is malware that infects Microsoft Office documents by means of embedding malicious macros within them
Worm	A worm is malware that self-propagates. Some of the most well-known names of malware fall under the worm category: Code Red, Nimda, SQL Slammer, Blaster, MyDoom, and Witty
Trojan Horse	A Trojan Horse is malware that has two functions: one overt (such as a game) and one covert (such as providing an attacker with persistent backdoor access)
Rootkit	A rootkit is malware that violates system integrity and is focused on hiding from system administrators. Typical capabilities include file, folder, process, and network connection hiding

Endnotes

1. Executive Order 12356—National security information. http://www.archives.gov/federalregister/codification/executive-order/12356.html [accessed May 5, 2013].
2. NIST Special Publication 800-61: Computer Security Incident Handling Guide. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf [accessed May 5, 2013].