Lesson Proper for Week 5

THREAT

Threat is a way of creating a problem on the network by taking advantage of its vulnerability.

A threat can be worrisome for any network administrator in terms of protecting critical documents and assets that are of great importance to the organization. A threat can be initiated by a hacker (a criminal hacker) or accidentally (a natural disaster or a malfunction).

1. Threat Consequences

Threat consequence is a scenario where the security parameters might be violated. This generally occurs due to the effect of a threat action. The different types of threat consequence are disclosure, deception, disruption, and usurpation.

2. Disclosure

An unauthorized user trying to access a network device in an illegitimate manner is referred to as disclosure.

3. Threat action – exposure

A threat action where the critical data is directly provided to an unauthorized user.

This includes the following:

- **Deliberate exposure:** Planned way of providing critical data to an unauthorized user
- **Scavenging:** Scanning through leftover data in a system to gain unauthorized access to sensitive data

- **Human error:** This involves human interaction that unintentionally results in a user gaining access to sensitive data

- **Hardware/software error:** An attacker creates the failure of a service or hardware component in the hope of gaining system access

4. Threat action – interception

A threat action where an unauthorized user directly accesses critical data flowing between authorized sources and destinations. This includes the following:

- **Theft:** Obtaining access to data by stealing media, such as HDD, CD/DVD Drives, and USB.

- **Wiretapping:** Monitoring and storing the data flowing between two endpoints in the communication system with the aim of stealing the information.

- **Man-in-the-Middle (MiTM):** Intercepts traffic between the sender and the destination. Sensitive information can be obtained.

5. Threat action – inference

A threat action whereby an unauthorized entity indirectly accesses sensitive information by reasoning characteristics or byproducts of communications. This includes the following:

- **Traffic analysis:** Obtaining information about data by continuously observing the communication characteristics that carry the information

- **Signals analysis:** Monitoring and analyzing the signals emitted from an RF transmitter

6. Threat Action – Intrusion

This is a threat action where there is an attack on the computing system with the harmful intention of causing destruction. This includes the following:

- **Trespass:** Obtaining unauthorized access physically to sensitive information by overtaking the network/system's security

- **Penetration:** Obtaining unauthorized logical access to sensitive information by overtaking the network/system's security

- **Reverse-engineering:** Collecting sensitive information by stripping and analyzing the components of the system/network

- **Cryptanalysis:** The technique or process of deciphering an encrypted message without prior knowledge the secret key

DECEPTION

Deception is the art of falsifying an identity to trick another entity into believing its legitimacy.

1. Threat Action – Masquerade

In a masquerade attack, the attacker uses another identity to gain access to a system or network. This type of deception relies primarily on using a fake identity to be successful.

2. Threat Action – Falsification

A threat action where an attacker uses misleading or false information to trick an authorized system into believing its authenticity:

- **Substitution:** The replacement of valid data with false data to deceive an authorized entity.
- **Insertion:** Introducing false data that serves to deceive an authorized object.

3. Threat Action – Repudiation

This threat action denies the responsibility of an action.

DISRUPTION

A circumstance or an event that disturbs or stops the ongoing operation of system services and functions.

1. Threat action – incapacitation

Incapacitation prevents or interrupts a system's operation by disabling a system component:

- **Malicious logic:** Any hardware, firmware, or software that is brought into the network/system with the intention of destroying its functions and resources
- **Physical destruction:** Intentional harm to a physical system causing the overall performance of the system to be affected
- **Human error:** An action that is caused by a human, whether intentional or unintentional, causing a service interruption
- **Hardware or software error:** A faulty component on a system or a faulty software bug causing an interruption in the system's service

TYPES OF THREAT

There are various different types of threat:

- Physical damage, such as fire, water, and pollution
- Natural events, such as climatic conditions
- Loss of essential services, such as power, AC, and telecommunication
- Compromise of information, such as theft of media including HDD and CD drives
- Failure of technical equipment or software
- Abuse of rights and denial of actions

A threat agent is used to indicate an individual or group that can manifest a threat. It is essential to identify who would want to exploit the assets of a company, and how they might use them against the company.

Threat agents can take one or more of the following actions against an asset:

- **Access:** Simple unauthorized access
- **Misuse:** Unauthorized use of assets
- **Disclose:** The threat agent illicitly discloses sensitive information
- **Modify:** Unauthorized changes to an asset

Deny access: Includes destruction, theft of non-data assets, and so on

◀ Preliminary Activity for Week 5

Jump to...

Analysis, Application, and Exploration for Week 5 ▶

Navigation

Home
Dashboard
Site pages
My courses
121 - CC106
121 - BPM101 / DM103
121 - OAELEC2

the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment

Activities

- Assignments
- Forums
- Quizzes
- Resources