B.Tech, 6th Sem., Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

May 12, 2025

Explain the purpose of mitigation techniques used to secure the enterprise

Dr. Laxmidhar Biswal

1 Chapter 09
- Introduction
- segmentation
- Access Control
- application Allow List
- Application Block List

Introduction/Motivation

Explain the purpose of mitigation techniques used to secure the enterprise

Dr. Laxmidhar Biswal

Chapter 09

Introduction
segmentation
Access Control
application Allow List
Application Block List

Objectives of this chapter

To understand mitigation techniques to secure enterprise environments. And equip learners with knowledge to protect enterprise systems and pass related certification exam questions. In this chapter, the following topics are covered: segmentation, access control, application allow list and application block list.

Explain the purpose of mitigation techniques used to secure the enterprise

Segmentation

- Purpose of Segmentation in Network Security:
    - Limits lateral movement of attackers.
    - Contains breaches to isolated areas.
    - Enhances overall security and control.
- Types of Segmentation:
    - Physical Segmentation: Uses routers, switches, firewalls for network isolation.
    - VLANs: Logically segment networks within switches based on function or department.
    - Subnetting: Divides networks by IP ranges for easier management and security.
    - Micro-segmentation: Applies fine-grained security policies at the workload or device level; ideal for data centers/cloud.

Explain the purpose of mitigation techniques used to secure the enterprise

Segmentation

- Benefits of Segmentation:
  - Improves security and limits malware spread.
  - Enhances access control.
  - Ensures regulatory compliance (e.g., PCI DSS, HIPAA).
    - PCI DSS: Payment Card Industry Data Security Standard (PCI DSS)
    - HIPAA:Health Insurance Portability and Accountability Act.
  - Boosts network performance and efficiency.
  - Isolates critical systems for extra protection.
  - Provides scalability and flexibility for growing networks.

Explain the purpose of mitigation techniques used to secure the enterprise

Dr. Laxmidhar Biswal

Chapter 09

Introduction

segmentation

Access Control

application Allow List

Application Block List

Access Control

- Manages who can access data, applications, networks, or cloud resources based on organizational policies.
- Used in file systems and network devices (firewalls/routers).
- Type:
  - File/Folder ACL: Controls user access to data (e.g., read, write).
  - Network ACL: Controls incoming/outgoing traffic using rules (default: deny all).
- Permissions:
  - Define allowed actions (read, write, execute, delete).
  - Based on user roles and principle of least privilege.
  - Example: Example:
    - Sales Admin (Ben): Read & Write access.
    - Sales Manager (Bill): Read-only access.

Explain the purpose of mitigation techniques used to secure the enterprise

Access Control

- Objective:
  - Prevent unauthorized access.
  - Protect data integrity and confidentiality.

Application Allow List

- Defines a list of explicitly approved applications.
- Blocks all software not on the list, including unauthorized or malicious programs.
- Ensures only sanctioned software runs on the network.
- Example: Prevents users like Bob from installing games or malware from executing (e.g., ransomware).

Explain the purpose of mitigation techniques used to secure the enterprise

Dr. Laxmidhar Biswal

Chapter 09

Introduction

segmentation

Access Control

application Allow List

Application Block List

Application Block List

- Specifies applications that are explicitly forbidden.
- Tools like Microsoft AppLocker help enforce these policies.
- Prevents known malicious or non-compliant applications from running.
- Useful for security, productivity, and compliance enforcement (e.g., blocking games or unsafe apps).

References

Dr. Laxmidhar
Biswal

Chapter 09
Introduction
segmentation
Access Control
application Allow List
Application Block
List

https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question
??

The End