BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – M.Sc.(ANCS)-2023
Course Name – Enterprise Security Architecture and Design
Course Code - MNCS403A
(Semester IV)

Full Marks : 60

Time : 2:30 Hours

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question)

1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Establish the event management in security operations.

a) The process of identifying, monitoring, and analyzing security events in enterprise systems.

b) The process of managing physical events in the enterprise.

c) The process of managing data events in the enterprise.

d) The process of managing network events in the enterprise.

(ii) What is the primary focus of security governance?

a) Implementing security technologies

b) Developing security policies and standards

c) Conducting security audits

d) Managing security operations

(iii) Which security architecture template focuses on the design and development of security services?

a) The Conceptual Framework for Policy-Driven Security

b) The Identity Management Architecture

c) The Other Security Services Template

d) The Border Protection Architecture

(iv) Which of the following is a component of a policy-driven security architecture?

a) The Bill of Materials

b) The Governance Process Overview

c) The Principles Template

d) The Maintenance and Operations Plan

(v) Predict which of the following is a benefit of using a policy template.

a) It eliminates the need for policy customization.

b) It ensures compliance with all applicable laws and regulations.

c) It provides a standard format for policy development.

d) It allows for complete elimination of all security threats.

(vi) Select which of the following is a characteristic of a security technology architecture.

a) It provides guidance for security governance

b) It specifies policies and procedures for security administration

c) It defines security controls and mechanisms for protection   d) It outlines asset management strategies

(vii) Select which of the following is a component of vulnerability management.

a) Incident management

b) Event management

c) Risk assessment

d) Asset management

(viii) Select which of the following is not a factor that affects the system's design.

a) Business goals

b) Threat landscape

c) Regulatory requirements

d) Customer preferences

(ix) What is the purpose of security technology architecture?

a) To develop and enforce corporate security standards

b) To define and implement security policies and procedures

c) To measure and manage security operations

d) To design and develop security technology services

(x) What is the importance of policy framework?

a) To provide guidance on how to implement policies

b) To outline the process for developing policies

c) To identify the objectives and principles that policies should adhere to

d) To establish specific rules and procedures for enforcing policies

(xi) Write the most common form of authentication.

a) A combination of any of these two items

b) Something that you are

c) A magnetic stripe card

d) Password

(xii) What is the purpose of change control?

a) Track changes to system hardware, software, firmware, and documentation.

b) Maintain visibility of changes to the system.

c) Ensure that changes to the system are approved.

d) To track and approve changes to system hardware, software, firmware, and documentation.

(xiii) Assess the main benefit of policy automation.

a) Reduced costs

b) Improved efficiency

c) Increased revenue

d) Better security

(xiv) Show the main goal of the Policy Automation Roadmap.

a) To identify potential policy violations

b) To provide a timeline for implementing policy automation

c) To monitor policy compliance

d) To evaluate the effectiveness of existing policies

(xv) Identify customer-specific products are also known as _____.

a) make-to-order.

b) expected products.

c) make-to-stock.

d) goods.

Group-B
(Short Answer Type Questions)

3 x 5=15

2. Explain security logs to verify potential threats and recommend appropriate actions.   (3)
3. Define the layers of enterprise security architecture.   (3)
4. Decide the role of security analytics in security operations.   (3)
5. Why security governance is important for enterprise security architecture?   (3)
6. Explain the purpose of security governance.   (3)

OR

Analyze the role of Zero Trust Architecture (ZTA) in strengthening enterprise security and compare it with traditional perimeter-based security models.   (3)

Group-C
(Long Answer Type Questions)

5 x 6=30

7. Evaluate the effectiveness of security technology architecture in detecting and mitigating (5)
   advanced persistent threats (APTs).
8. Describe the key components of a policy-driven security architecture. (5)
9. Explain the House Design Model and its relationship to enterprise security architecture. (5)
10. Analyze the importance of conceptual architecture in developing policy-driven security. (5)
11. Explain the significance of incident management in security operations and justify its role. (5)
12. Critically evaluate the impact of emerging technologies on policy-driven security (5)
    architecture.

OR

Critically analyze the benefits and limitations of a policy-driven security architecture in a (5)
cloud computing environment.

****