BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – B.Tech.(CSE)-DS-2021
Course Name – Information Security and Privacy
Course Code - OEC-CSD701C
(Semester VII)

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) Select the primary function of system security tools.
a) Protecting systems from threats b) Optimizing system performance
c) Deleting user data d) Providing software updates

(ii) Select the primary method for preventing web attacks.
a) Input validation b) Ignoring user input
c) Disabling error messages d) Encrypting passwords

(iii) Select the key advantage of regular vulnerability assessments.
a) Proactive threat detection b) Slowing down system performance
c) Increasing power consumption d) Ignoring security risks

(iv) Select the most common security requirement for data protection.
a) Encryption b) Reducing file size
c) Speeding up data transfer d) Limiting user access

(v) Select the most important element in a risk assessment report.
a) Risk probability b) Network performance
c) User satisfaction d) Storage capacity

(vi) Select the best way to ensure third-party compliance with security policies.
a) Regular audits b) Ignoring third-party activities
c) Providing unrestricted access d) Only using manual controls

(vii) Select a method that improves privacy but may lead to information loss.
a) Group-based anonymization b) Data compression
c) Data encryption d) Bandwidth enhancement

(viii) Identify an application of group-based anonymization.

a) Masking identifiable information in large datasets
b) Compressing data for storage
c) Improving network speed
d) Data deletion

(ix) Choose the most effective way to protect sensitive transaction data.

a) Differential privacy
b) Faster data processing
c) Data compression
d) Deleting unnecessary transactions

(x) Select the main benefit of tokenization compared to other anonymization techniques.

a) Reduces data size
b) Protects sensitive data without modifying its structure
c) Increases storage capacity
d) Speeds up analysis

(xi) Select the best definition of tokenization.

a) Replacing sensitive data elements with non-sensitive equivalents
b) Compressing sensitive information for storage
c) Encrypting data for secure access
d) Removing unnecessary information from datasets

(xii) Select the correct definition of l-diversity.

a) Ensuring sensitive attributes have at least l different values within each group
b) Compressing datasets
c) Encrypting sensitive information
d) Deleting unnecessary records

(xiii) Select the primary difference between k-anonymity and l-diversity.

a) l-diversity protects against attribute disclosure by ensuring a variety of sensitive values within groups
b) k-anonymity increases system speed
c) l-diversity reduces data storage
d) k-anonymity compresses data

(xiv) Identify a threat that tokenization mitigates in data protection.

a) Unauthorized access to sensitive data by replacing it with tokens
b) Slower processing speed
c) Increased data storage needs
d) Compression failure

(xv) Choose the benefit of t-closeness over l-diversity in anonymization.

a) t-closeness ensures that the distribution of sensitive attributes is maintained between groups
b) l-diversity improves system processing speed
c) t-closeness reduces data storage
d) l-diversity compresses the dataset

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define Security Policies. (3)
3. Describe the role of Risk Assessment in security. (3)
4. Write the steps of developing and implementing a Security Policies. (3)
5. Identify a method used to protect sensitive data. (3)
6. Construct the concept of Information analytics. (3)

OR

Discuss different types of Hacking in brief. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Define Computer Security and list the objectives of information security (5)
8. Explain the challenges associated with ensuring security in complex systems. (5)
9. Analyze common system vulnerabilities and describe the potential impact they have on organizational security. (5)
10. Evaluate the importance of third-party security management in safeguarding organizational data, and outline two key practices that should be followed. (5)
11. Analyze the steps involved in responding to information security incidents and the process availed by an organization to ensure effective communication during an incident response. (5)
12. Evaluate the importance of Security Policies in organizational security frameworks. (5)

OR

Evaluate the effectiveness of Intrusion Detection Systems (IDS) in identifying security breaches and suggest improvements for modern systems. (5)

****