BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – B.Tech.(CSE)-2019/B.Tech.(CSE)-2020
Course Name – Security and Privacy of Data
Course Code - PEC801A
(Semester VIII)

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 which of the following best describes the stages of the cloud-based Information Life Cycle (ILC)?

a) Creation, Storage, Deletion
b) Ingestion, Processing, Ejection
c) Generation, Archiving, Purging
d) Capture, Manipulation, Retention

(ii) Identify which phase of the cloud-based Information Life Cycle does data typically undergo processing or analysis?

a) Creation
b) Storage
c) Manipulation
d) Purging

(iii) Select which phase of the cloud-based Information Life Cycle focuses on securely removing data that is no longer needed?

a) Generation
b) Storage
c) Archiving
d) Purging

(iv) Cite the concept that involves restricting access to physical locations where data is stored or processed

a) Confidentiality
b) Integrity
c) Availability
d) Physical security

(v) Identify the type of attack that involves flooding a network with traffic in order to overwhelm it:

a) SQL injection
b) DDoS attack
c) Social engineering
d) Phishing

(vi) Cite an example of a vulnerability that can be exploited by an attacker to gain unauthorized access to a system:

a) Weak passwords
b) Firewall
c) Intrusion detection system
d) Access control lists

(vii) Identify the MAIN benefit of using secure isolation strategies for data.

a) Improved data accessibility
b) Reduced risk of unauthorized access

c) Enhanced data processing speed
d) Lower storage requirements

(viii) Recall the strategy that achieves he physical separation of data from a network.

a) Encryption
b) Virtualization
c) Air Gap
d) Multi-Factor Authentication

(ix) State which of these is NOT a common technique for virtual data isolation.

a) Containers
b) Sandboxes
c) Encryption
d) Network Segmentation

(x) Select the most appropriate protocol to monitor for suspicious login attempts:

a) SSH
b) Telnet
c) FTP
d) DNS

(xi) Identify a potential security incident from SIEM data:

a) Successful login
b) Multiple failed login attempts
c) File permission changes
d) New user creation

(xii) Recall the resource you consult for responding to a security incident:

a) SIEM user manual
b) Incident response plan
c) Vulnerability database
d) Penetration testing report

(xiii) Predict the primary purpose of access control enforcement in cloud environments.

a) To restrict access to authorized users only
b) To monitor all user activities within the cloud environment
c) To ensure high availability and performance of cloud services
d) To encrypt all data stored in the cloud to prevent unauthorized access

(xiv) Predict about access control challenge arises from the need to manage access permissions for temporary or transient cloud resources.

a) Compliance requirements
b) Network segmentation
c) Dynamic resource provisioning
d) Interoperability

(xv) Predict about access control challenge that is associated with managing access permissions for cloud resources shared by multiple tenants.

a) Compliance requirements
b) Segregation of duties
c) Multi-tenancy
d) Network segmentation

Group-B

(Short Answer Type Questions) 3 x 5=15

2. State Secure Isolation Strategies for Network Resources (3)
3. Define Cloud-based Information Life Cycle. (3)
4. Describe the inter-tenant network segmentation (3)
5. Explain the principle behind access control in data protection (3)
6. Summarize about honeypots in cloud. (3)

OR

Summarize about host-based IDS in cloud. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Summarize about Intrusion Detection System in cloud. (5)
8. Explain about honeypots in cloud. (5)
9. Explain benefits of data protection for a organization. (5)
10. Explain the key components of a disaster recovery plan for data protection? (5)
11. Describe the Role of Data Classification in Secure Isolation Strategies (5)
12. Evaluate the importance of tamper-proofing audit logs in cybersecurity. (5)

OR

Estimate the impact of poor user management on system security. (5)