BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – B.Tech.(CSE)-DS-2022
Course Name – Information Security Analysis and Audit
Course Code - OEC-CSD601B
(Semester VI)

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) What is the primary purpose of security metrics.
   a) To increase server speed
   b) To measure and improve security performance
   c) To create network diagrams
   d) To develop software applications

(ii) Which methodology tests a system with no prior knowledge of its internal structures.
   a) White-box testing
   b) Black-box testing
   c) Grey-box testing
   d) Penetration testing

(iii) Explain the difference between security metrics and performance metrics.
   a) Security metrics focus on IT infrastructure, while performance metrics focus on sales
   b) Security metrics assess security effectiveness, while performance metrics evaluate general efficiency
   c) Security metrics are used only in finance, while performance metrics apply to IT
   d) There is no difference

(iv) Explain the importance of security logs in performance metrics.
   a) They help analyze security incidents and detect anomalies
   b) They store employee passwords securely
   c) They optimize system speed
   d) They reduce software development time

(v) Choose the best approach for mitigating insider threats in an organization.
   a) Disabling all external network access
   b) Implementing strict access control and monitoring
   c) Allowing unrestricted data sharing
   d) Avoiding background checks on employees

(vi) Choose the right encryption method for securing a database containing sensitive user information.
   a) MD5 hashing
   b) AES-256 encryption
   c) Base64 encoding
   d) Plaintext storage

(vii) Find the correct definition of an external security audit.

a) A review of network security within an organization
b) An audit performed by an external party to assess security risks
c) A process of upgrading outdated security tools
d) A technique for social engineering attacks

(viii) How can social engineering security audits help organizations?
a) By testing employee awareness of security threats
b) By creating stronger encryption algorithms
c) By blocking all social media access
d) By improving internet speed

(ix) Classify the types of security audits based on their scope.
a) Internal, External, Compliance, Risk-based
b) Hardware, Software, Networking
c) Cloud-based, Mobile-based, Web-based
d) All of these

(x) Explain the significance of report retention in information security auditing.
a) Helps in compliance, future reference, and tracking security improvements
b) Allows organizations to delete outdated records
c) Reduces the need for security training
d) Makes audits unnecessary

(xi) Apply the concept of vulnerability analysis to identify a critical security weakness in a web application.
a) SQL injection vulnerability in the login page
b) Increasing the number of user logins per second
c) Installing a faster web server
d) Reducing the number of firewall rules

(xii) Choose the most suitable framework for conducting a cybersecurity audit.
a) NIST Cybersecurity Framework
b) Google Docs
c) Windows Media Player
d) Photoshop

(xiii) What is Vulnerability Management?
a) Identifying security flaws
b) Encrypting sensitive data
c) Blocking unauthorized access
d) Removing malware

(xiv) Classify Social Engineering attacks.
a) External & Internal
b) Hardware & Software
c) Human-based & Computer-based
d) Manual & Automated

(xv) Choose the best tool for Vulnerability Scanning.
a) Notepad
b) Nessus
c) Task Manager
d) Excel

Group-B
(Short Answer Type Questions) 3 x 5=15

2. Choose an appropriate performance metric for evaluating firewall security effectiveness. (3)
3. Classify different types of security audits. (3)
4. Choose an appropriate vulnerability assessment tool for a cloud environment. (3)
5. Select the most effective countermeasure for social media-based social engineering. (3)
6. Compare Information Security Audit Strategies based on compliance and risk-based approaches. (3)

OR

Determine the ethical responsibilities of an Information Security Auditor. (3)

Group-C
(Long Answer Type Questions) 5 x 6=30

7. Classify different approaches to network security audits. (5)
8. Distinguish between qualitative and quantitative security risk assessments. (5)
9. Apply security audit methodologies to assess an organization's firewall and IDS effectiveness. (5)
10. Find the key components of an effective pre-audit checklist. (5)

11. Explain the importance of report retention in security auditing. (5)
12. Discuss the key considerations when choosing a vulnerability assessment tool. (5)

OR

Solutions to mitigate common cybersecurity risks in cloud environments. (5)

****