



BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – B.Sc.(ANCS)-Hons-2023
Course Name – Security Overview
Course Code - VAC00013
(Semester II)

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) Define the illegal activities conducted through computer networks.
- | | |
|------------------|---------------------|
| a) Cybersecurity | b) Cybercrime |
| c) Data storage | d) Network security |
- (ii) Identify the storage directly connected to a computer and not accessible over a network.
- | | |
|----------------------------------|-----------------------------------|
| a) Direct Attached Storage (DAS) | b) Network Attached Storage (NAS) |
| c) Cloud Storage | d) External Hard Drive |
- (iii) Explain the meaning of the CIA triad in cybersecurity.
- | | |
|---|---------------------------------------|
| a) Confidentiality, Integrity, Availability | b) Centralized, Integrated, Automated |
| c) Cybercrime, Internet, Applications | d) Cloud, Identity, Access |
- (iv) Explain the main focus of mobile security.
- | | |
|---|---------------------------------|
| a) Securing mobile devices and applications | b) Protecting data in the cloud |
| c) Monitoring network traffic | d) Application security |
- (v) Identify the SDLC phase that focuses on gathering and analyzing software project requirements.
- | | |
|--|----------------------|
| a) Requirements Gathering and Analysis | b) Feasibility Study |
| c) Design | d) Development |
- (vi) Select the SDLC phase where the actual code is written and the software is developed.
- | | |
|----------------|-------------------|
| a) Development | b) Implementation |
| c) Deployment | d) Maintenance |
- (vii) Explain the significance of using SDLC in software development.
- | | |
|--|---|
| a) Ensures a structured and organized development process. | b) Improves communication and collaboration among stakeholders. |
| c) Reduces development costs and time to market. | d) All of these |
- (viii) Select the option that is NOT an advantage of using SDLC.

- a) Increased flexibility and adaptability to changes.
 - b) Improved software quality and reliability.
 - c) Reduced development costs and risks.
 - d) Increased development time and complexity.
- (ix) State the primary goal when implementing endpoint security measures.
- a) Prevent cyberattacks
 - b) Detect and respond to threats
 - c) Mitigate security risks
 - d) All of these
- (x) Explain the purpose of configuring rules in an endpoint firewall.
- a) Allow/block traffic and control access to applications and websites
 - b) Manage network traffic, monitor user activity, encrypt data
 - c) Neither (a) nor (b)
 - d) Both (a) and (b)
- (xi) State the intended outcomes of a data destruction policy.
- a) Securely erase sensitive data when no longer required
 - b) Prevent unauthorized access to disposed data
 - c) Meet legal and regulatory requirements
 - d) All of these
- (xii) Write the crucial role of compliance with regulations in ensuring cybersecurity.
- a) Enforce data privacy and security best practices
 - b) Protect sensitive information and critical infrastructure
 - c) Manage security risks and vulnerabilities
 - d) All of these
- (xiii) Explain the primary objective of encryption in ensuring data security.
- a) Confidentiality
 - b) Integrity
 - c) Availability
 - d) Non-repudiation
- (xiv) State the primary risk associated with SQL injection attacks.
- a) Unauthorized database access/modification
 - b) System crash
 - c) Data encryption
 - d) Network slowdown
- (xv) Choose the technique that involves injecting malicious SQL code into input fields to manipulate a database.
- a) SQL injection
 - b) Cross-site scripting (XSS) attack
 - c) Password brute-force attack
 - d) Denial-of-service (DoS) attack

Group-B

(Short Answer Type Questions)

3 x 5=15

- 2. Write about the utilization of data encryption in endpoint security. (3)
- 3. Discuss the challenges presented by the heterogeneous endpoint environment. (3)
- 4. Define cloud storage and list its advantages. (3)
- 5. Explain the role of Virtual Private Networks (VPNs) in securing communication. (3)
- 6. Analyze the contribution of firewalls and network segmentation to network security. (3)

OR

- Analyze how Data Loss Prevention (DLP) prevents sensitive data leaks. (3)

Group-C

(Long Answer Type Questions)

5 x 6=30

- 7. Describe some of the best practices for secure network scanning. (5)
- 8. Define Vulnerability Assessment and Penetration Testing (VAPT) and What are the three main goals of VAPT. (5)
- 9. Discuss the role of collaboration between identity management and network security in creating a unified defense strategy. (5)
- 10. Explain how endpoint security safeguards individual devices against cyberattacks. (5)
- 11. Explain the features and advantages of the Advanced Encryption Standard (AES) compared to other encryption algorithms. (5)

12. Explain the methods used for device control in endpoint security and their importance. (5)

OR

Explain why user education is crucial for preventing social engineering attacks in endpoint security. (5)
