BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – BCA-Hons-2023
Course Name – Cyber Security
Course Code - BCA60118
(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) Name the formula used to define risk.
a) Risk = Threat × Vulnerability b) Risk = Impact + Likelihood
c) Risk = Likelihood × Impact d) Risk = Asset − Control

(ii) Identify the ethical hacker category that works with authorization.
a) Black hat b) Grey hat
c) White hat d) Script kiddie

(iii) Explain why data is considered a high-value security target.
a) It occupies large storage b) It is easy to duplicate
c) Its theft or corruption causes direct harm d) It is always encrypted

(iv) Name the type of security that focuses on policies, training, and governance.
a) Technical security b) Network security
c) Organizational security d) Physical security

(v) Explain why organizational security alone cannot prevent social engineering attacks.
a) It lacks encryption b) It does not include firewalls
c) It depends on human behavior d) It is optional

(vi) Explain why interoperability agreements are necessary in modern organizations.
a) Organizations operate in isolation b) Data sharing introduces security risks
c) They replace policies d) They reduce documentation

(vii) Name the output produced after encrypting plaintext.
a) Hash b) Ciphertext
c) Signature d) Key

(viii) Identify the substitution cipher attributed to Julius Caesar.
a) Vigenère Cipher b) Caesar Cipher
c) Playfair Cipher d) DES

(ix) Explain why DES is considered insecure today.

a) Large block size
b) Weak algorithm design
c) Short key length
d) High latency

(x) Define Role-Based Access Control (RBAC).

a) Access based on user location
b) Access based on job roles
c) Access based on time
d) Access based on device type

(xi) Explain why account lockout policies are implemented.

a) To prevent phishing
b) To stop brute-force attacks
c) To improve usability
d) To increase password reuse

(xii) Explain how improper permissions can lead to attacks.

a) Malware infection
b) Privilege escalation
c) Data compression
d) Network delay

(xiii) Name the type of IDS that monitors activities on individual systems.

a) NIDS
b) HIDS
c) IPS
d) WIPS

(xiv) Identify the main function of a Network-Based IDS (NIDS).

a) Monitor file integrity
b) Analyze system calls
c) Monitor network traffic
d) Encrypt packets

(xv) Compare NIDS and HIDS in terms of encrypted traffic analysis.

a) NIDS is more effective
b) HIDS is more effective
c) Both are ineffective
d) Both are identical

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define a cryptographic hash function and state its purpose. (3)
3. Apply secure remote access practices for work-from-home scenarios. (3)
4. Classify the different types of malware attacks. (3)
5. Name the different phases of a security policy lifecycle. (3)
6. Write the differences between signature-based and anomaly-based intrusion detection techniques. (3)

OR

Devise a basic IDS deployment strategy suitable for a small organization. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Justify why people are considered both a security problem and a security asset in organizations. (5)
8. Illustrate the basic working principle of symmetric key cryptography with suitable examples. (5)
9. Describe how poor user account lifecycle management can lead to serious security breaches in organizations. (5)
10. Define computer security and explain its importance in modern interconnected computing environments. (5)
11. Evaluate the need for interoperability agreements when organizations share data and systems. (5)
12. Analyze the advantages and limitations of Network-Based Intrusion Detection Systems in enterprise networks. (5)

OR

Compare Host-Based Intrusion Detection Systems and Network-Based Intrusion Detection Systems with suitable examples. (5)

****