BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Tech.(RA)-2023
Course Name – Cyber Threat Intelligence
Course Code - OEC-ECR601B
(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) Define information security as protection of
 a) Data from unauthorized access b) Network speed
 c) System performance d) Software usability

(ii) List the element that ensures authorized access
 a) Availability b) Confidentiality
 c) Integrity d) Authentication

(iii) Identify the security issue related to unauthorized disclosure
 a) Integrity violation b) Confidentiality breach
 c) Availability loss d) Authentication failure

(iv) Explain security mechanisms as
 a) Policies only b) Implementation tools
 c) Threat sources d) Attack vectors

(v) Recognize decryption as the process of
 a) Ciphertext creation b) Hash generation
 c) Plaintext recovery d) Key exchange

(vi) Identify cryptographic hash as a function producing
 a) Variable-length output b) Fixed-length output
 c) Encrypted text d) Public key

(vii) Describe cryptographic systems as tools for
 a) Data compression b) Secure communication
 c) Traffic routing d) Error control

(viii) Explain cryptanalysis as a threat to
 a) Network speed b) Cryptographic strength
 c) Data availability d) Hardware reliability

(ix) Explain encryption role in network security

a) Traffic monitoring
b) Data confidentiality
c) Bandwidth control
d) Error correction

(x) Identify denial-of-service attack as causing

a) Data modification
b) Confidentiality breach
c) Authentication failure
d) Service unavailability

(xi) Recognize distributed denial-of-service as an attack using

a) Insider access
b) Physical damage
c) Multiple compromised sources
d) Single device

(xii) Identify OS security objective as ensuring

a) Faster execution
b) Visual appeal
c) User convenience
d) Controlled resource access

(xiii) Recognize IDS alert outcome as

a) Data encryption
b) Attack notification
c) Automatic blocking
d) User logout

(xiv) Identify IPS action as

a) Key exchange
b) Blocking malicious packets
c) Logging only
d) Data mining

(xv) Identify database disclosure cause as

a) Weak access control
b) Fast indexing
c) Data redundancy
d) Backup process

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Describe the core objectives of information security in organizational systems. (3)
3. Explain the purpose of steganography in secure communication. (3)
4. Differentiate symmetric key and asymmetric key cryptography. (3)
5. Explain the purpose of firewalls in network protection. (3)
6. Analyze the impact of rootkits on operating system integrity. (3)

OR

Analyze threats affecting network communication reliability. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain the scope and significance of information security in digital environments. (5)
8. Analyze different attack types targeting confidentiality, integrity, and availability. (5)
9. Explain asymmetric key cryptographic techniques. (5)
10. Explain rootkit detection challenges in operating systems. (5)
11. Describe firewall mechanisms supporting network security enforcement. (5)
12. Analyze cryptanalysis techniques targeting encryption algorithms. (5)

OR

Analyze security implications of poor key management practices. (5)

****