# BRAINWARE UNIVERSITY

## Term End Examination 2025-2026
## Programme – B.Sc.(ANCS)-Hons-2024
## Course Name – Threat Modelling
## Course Code - BNC40109
## ( Semester IV )

**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 does the letter "S" stand for in STRIDE Model?
a) Security b) Spoofing
c) Scanning d) Sniffing

(ii) Select which security control implimented due to repudiation threats.
a) Encryption b) Logging and auditing
c) Input validation d) Access control

(iii) Select which CIA triad component affects Denial of Service (DoS) attacks.
a) Confidentiality b) Integrity
c) Availability d) Authentication

(iv) Identify DREAD is mainly used for.
a) Threat identification b) Vulnerability scanning
c) Risk ranking d) Exploit development

(v) Select how Threat Modeling helps organizations.
a) Replacing penetration testing b) Reducing security costs
c) Preventing vulnerabilities early d) Eliminating all attacks

(vi) Select the traffic analysis
a) Altering encrypted messages b) Studying communication patterns without decrypting data
c) Cracking encryption keys d) Replacing encryption algorithms

(vii) Identify the threat involves impersonating a legitimate user
a) Replay attack b) Masquerade attack
c) Side-channel attack d) Cryptanalytic attack

(viii) Indicate symmetric encryption vulnerable if the key is exposed
a) Algorithm complexity b) Single shared secret

c) Key exchange overhead
d) Public availability

(ix) Select threat results from using outdated cryptographic algorithms

a) Strong authentication
b) Backward compatibility
c) Increased vulnerability to known attacks
d) Improved performance

(x) Predict the primary objective of ERM

a) Remove uncertainty completely
b) Identify, assess, and manage risks within risk appetite
c) Focus only on compliance risks
d) Increase organizational complexity

(xi) Determine the PRIMARY objective of managing threats in threat modelling.

a) Identify, track, and address security threats
b) Replace penetration testing
c) Increase system performance
d) Eliminate all attacks

(xii) Identify the activity that marks the formal beginning of a threat modelling project.

a) Applying encryption
b) Writing secure code
c) Drawing a system or data flow diagram
d) Running vulnerability scanners

(xiii) Choose why threat tables and lists are used in threat modelling.

a) To track and manage identified threats systematically
b) To replace documentation
c) To improve coding speed
d) To automate mitigation

(xiv) Select what incidents like the JP Morgan and Lehman breaches demonstrate.

a) Poor UI design
b) The need for integrated cyber risk management
c) Only technical weaknesses
d) Failure of encryption

(xv) Choose the measure that BEST reduces organizational cyber risk exposure.

a) Manual monitoring only
b) Single security control
c) Regular risk assessment and collaboration
d) Ignoring low-risk assets

## Group-B

(Short Answer Type Questions) 3 x 5=15

2. Describe what a "Trust Boundary" represents. (3)
3. Distinguish between Authentication and Authorization. (3)
4. Evaluate the use of "Obscurity" Under what condition does it provide actual value? (3)
5. A startup "rolls their own" hash function by XORing segments of a message to save costs for an IoT device. Appraise this decision from the perspective of an "Organized Crime" actor looking to launch a collision attack. Predict a more secure, standard-based lightweight alternative. (3)
6. Analyze the technical shift popularized by "Mafiaboy" and its impact on how Fortune 500 companies perceive digital risk. (3)

**OR**

Analyze the role of ISACs as a "force multiplier" for industry-specific security postures. (3)

## Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain the primary objective of each of the seven stages in the PASTA methodology and how they build upon one another. (5)
8. Summarize a plan for making threat modeling an "iterative process" within a DevOps pipeline, explaining how it stays relevant during fast-paced releases. (5)
9. Write the step-by-step experimental hypothesis and testing procedure to determine if a session cookie is vulnerable to a Replay Attack. (5)
10. Explain the strategic framework to resolve the "Innovator's Dilemma" by balancing disruptive innovation with architectural stability. (5)

11. Explain a "Strategic Advisor" role for the 2026 Risk Manager, detailing how they should present "Risk-Adjusted Return" to a Board. (5)
12. Summarize the "Three Lines of Defense" oversight model that eliminates "Single Points of Failure" in corporate governance. (5)

**OR**

Evaluate NIST 2.0 compliant Incident Response Plan (IRP) that automates the transition from "Detection" to "Recovery." (5)

**********