BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – MCA-2024
Course Name – Cyber Security
Course Code - MCA20301B
(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) Connect "C" in the CIA triad.

a) Confidentiality b) Configuration
c) Communication d) Cybersecurity

(ii) Establish the formula for risk.

a) Vulnerability × Exploit × Data b) Confidentiality × Integrity × Availability
c) Threat × Vulnerability × Impact d) None of these

(iii) Assess the primary purpose of network scanning and enumeration in cybersecurity.

a) To identify vulnerabilities and gather information about a network b) To encrypt sensitive data
c) To block unauthorized access to a system d) To perform penetration testing on a server

(iv) Differentiate HTTP and HTTPS in terms of security.

a) It loads web pages faster b) It encrypts data transmitted over the internet
c) It blocks pop-ups d) It prevents all cyber threats

(v) Select an effective countermeasure against reconnaissance.

a) Using weak passwords b) Implementing intrusion detection systems (IDS)
c) Ignoring security updates d) Making sensitive data public

(vi) Select the scanning technique that is used to determine the operating system of a target in Nmap.

a) -O b) A

c) B   d) EE

(vii) List three common types of cyber threats.

    a) Firewalls, VPNs, Encryption   b) Malware, Phishing, Denial of Service
    c) HTTPS, AES, RSA   d) TCP, IP, HTTP

(viii) Recognize an example of malware from the options below.

    a) VPN   b) Antivirus
    c) Trojan Horse   d) Firewall

(ix) Recall the primary function of a firewall.

    a) Blocking unauthorized access to a network   b) Encrypting email messages
    c) Destroying physical hardware   d) Managing cloud storage

(x) State the purpose of two-factor authentication.

    a) To create longer passwords   b) To require multiple verification steps before granting access
    c) To eliminate the need for passwords   d) To remove encryption from systems

(xi) Name the cryptographic hashing algorithm commonly used for password security.

    a) AES   b) SHA-256
    c) HTTPS   d) HTML

(xii) Classify AES under its correct cryptographic category.

    a) Hashing algorithm   b) Symmetric encryption algorithm
    c) Asymmetric encryption algorithm   d) Key exchange protocol

(xiii) Recall the final phase in the hacking process.

    a) Gaining access   b) Covering tracks
    c) maintaining access   d) scanning

(xiv) Recognize a common sign of a ransomware attack.

    a) A sudden increase in system speed   b) A demand for payment to unlock encrypted files
    c) An unexpected firewall warning   d) An increase in CPU temperature

(xv) State one common method used to prevent brute-force attacks.

    a) Using complex and long passwords   b) Avoiding antivirus software
    c) Disabling firewalls   d) Sharing credentials

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

2. Explain the importance of the CIA triad in information security.   (3)
3. Differentiate between authentication and authorization in security.   (3)
4. Classify different types of hackers based on intent and ethics.   (3)
5. Distinguish between virus and worm.   (3)
6. Distinguish between DDoS attack and Botnet attack.   (3)

OR

Justify the concept of SQL Injection (SQLi) in web applications.   (3)

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

7. List the elements of the CIA triad and explain their importance.   (5)
8. Define vulnerability and exploit.   (5)

9. Explain the impact of zero-day vulnerabilities. (5)
10. Explain types of network scanning techniques. (5)
11. Summerize SQL injection and its countermeasures. (5)
12. Analyze the role of digital forensics in cybersecurity and its importance in investigating (5)
    cybercrimes.

OR

Analyze the impact of cloud computing on cybersecurity. (5)

****