45364

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – MCA-2025
Course Name – Cyber Security
Course Code - MCA20408B
(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) Select the phase of hacking that involves hiding evidence of an attack.
a) Reconnaissance b) Covering tracks
c) Gaining access d) Maintaining access

(iii) Write the formula for risk.
a) Vulnerability × Exploit × Data b) Confidentiality × Integrity × Availability
c) Threat × Vulnerability × Impact d) None of these

(iv) Choose the full form of NMAP.
a) Network mapper b) Network monitor
c) Network probe d) Network protocol

(v) Select the type of reconnaissance that involves interacting directly with a target system.
a) Active reconnaissance b) Passive reconnaissance
c) Social engineering d) DDoS

(vi) Select an example of a passive attack.
a) Denial of Service (DoS) b) Man-in-the-Middle
c) Phishing d) Eavesdropping

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

(ix) Identify the correct cryptographic category of AES.

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

(x) Summarize the purpose of reconnaissance in penetration testing.

a) Exploit vulnerabilities
b) Gather information about the target
c) Delete system logs
d) Encrypt company data

(xi) Identify a commonly used network scanning tool in penetration testing.

a) Nmap
b) Burp Suite
c) Metasploit
d) Nessus

(xii) Identify a countermeasure for preventing XSS attacks.

a) Using input validation
b) Disabling firewalls
c) Encrypting IP addresses
d) Allowing all content

(xiii) Select a tool used for detecting SQL injection vulnerabilities.

a) SQLmap
b) Wireshark
c) Shodan
d) Metasploit

(xiv) Choose what make biometric authentication secure.

a) Based on unique human characteristics
b) Allows sharing
c) No encryption
d) Prevents all attacks

(xv) Compare brute-force attacks and dictionary attacks.

a) Dictionary tries all combos
b) Brute uses wordlist
c) Dictionary uses wordlist; brute tries all combinations
d) Same method

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Analyze the impact of social engineering attacks on security. (3)
3. Describe the steps followed in a penetration testing process. (3)
4. Describe the difference between active and passive scanning. (3)
5. Explain how packet sniffing can be used for attacks. (3)
6. Distinguish between covering tracks and maintaining access in hacking. (3)

OR

Distinguish between static and dynamic Trojan analysis. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Recall the difference between black-box, white-box, and gray-box testing. (5)
8. Explain social engineering and its common types. (5)
9. Explain the importance of multi-factor authentication (MFA). (5)
10. Evaluate IDS and IPS in cybersecurity. (5)
11. Analyze the impact of insider threats on cybersecurity and suggest mitigation techniques. (5)
12. Assess ransomware and how it spreads. (5)

OR

Examine how session hijacking attacks work and their impact. (5)

****