2/21

2111N780

Candidate's Seat No :_____

IMBA (CSM) (NEP) Sem.-3 Examination
DSC-C-ICSM-231T
Cyber Security Fundamentals-I
November-2025

Time : 2-00 Hours] **[Max. Marks : 50**

Question 1: Answer the following questions:

i. Explain sessions, cookies (including their key attributes), and tokens. 5Marks

ii. Describe threat, vulnerability, exploit, risk, and impact. Illustrate their relationship with a simple scenario. 5Marks

OR

i. Compare encoding, encryption, and hashing. Provide examples and explain when each should be used. 5Marks

ii. Describe various identity theft techniques and propose a layered defence plan suitable for students. 5Marks

Question 2: Answer the following questions:

i. Explain the different types of cybercrimes with suitable examples. 5Marks

ii. Detail the Identity and Access Management lifecycle stages step-by-step. 5Marks

OR

i. Describe a brute-force attack and explain its various types. 5Marks

ii. Describe the major phases of penetration testing and list one tool used in each phase. 5Marks

Question 3: Answer the following questions:

i. Describe Vulnerability Assessment (VA) and Penetration Testing (PT). Explain when each is preferred, including outputs and tool examples. 5Marks

ii. Describe how Role-Based Access Control (RBAC) helps in regulating access to resources. Include its benefits and limitations. 5Marks

OR

i. Explain Nmap and describe any five commonly used Nmap commands with examples. 5Marks

ii. Describe at least five current cyber threats. 5Marks

P.T.O

N780-2

Question 4: Answer the following questions:

i. Explain the difference between CVE and CWE, and describe how CVSS and CWSS help prioritize remediation. 5Marks

ii. What is cyberbullying? Explain its types with suitable examples. 5Marks

OR

i. What are the primary security challenges in Android application architecture? How can developers mitigate these risks? 5Marks

ii. What is a DMZ (Demilitarized Zone) in network security? Explain its role in protecting internal systems from external threats. 5Marks

Question 5: Attempt any ten out of twelve. 10 Marks

1. Which pillar of the CIA triad ensures data is accurate and unchanged?
2. A weakness that can be exploited by a threat actor is called: _____.
3. Which penetration testing approach assumes no prior knowledge of the target system?
   a) White-box testing b) Gray-box testing
   c) Black-box testing d) Open-box testing
4. What is the key difference between ethics and laws in the context of cybersecurity?
5. A law protecting children's online privacy in the US is: _____.
6. Which phishing variant targets high-profile executives?
7. Public Key Infrastructure's trust anchor that issues certificates is called: _____.
8. Define cryptography in one sentence.
9. What is chip technology used for in cybersecurity?
10. In Identity Theft, which technique involves fake emails or sites to trick users_____.
11. What does IDS/IPS stand for in cybersecurity?
12. The primary goal of encryption in the CIA triad maps to: _____.

.....X.....X.....