२ /131

2111N796

Candidate's Seat No :_____

IMSc (CSF) (NEP) Sem.-3 Examination
DSC-C-ICSF-231T
Cyber Security Fundamentals-I
November-2025

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

Question 1: Answer the following questions:

i. What are the components of the CIA Triad? Explain each with an example. 5 Marks

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

OR

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

ii. Explain the different types of web application attacks. 5 Marks

Question 2: Answer the following questions:

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

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

OR

i. Differentiate between DAC, RBAC, ABAC, MAC, and JIT access control models. 5 Marks

ii. Describe the phases of penetration testing. 5 Marks

Question 3: Answer the following questions:

i. Explain the difference between authentication and authorization with an example. 5 Marks

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

OR

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

ii. Describe cyber threats, Phishing, Ransomware, APTs, Insider Threats, and Social Engineering. 5 Marks

Question 4: Answer the following questions:

i. Explain major data protection and compliance laws DPDP 2023, GDPR, PCI DSS, and HIPAA. 5 Marks

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

OR

N 796-2

i. What is Chip Technology? Explain its types. 5 Marks

ii. What is Firewall? Explain its types? 5 Marks

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

1. In a DMZ, services are placed:
   a) On internal network only
   b) In an isolated network zone exposed to internet
   c) On client devices
   d) D. In the same VLAN as endpoints
2. During the "gaining access" phase, ethical hackers:
   a) Identify vulnerabilities b) Exploit the system to enter
   c) Install patches d) Delete logs
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 access model grants permissions based on user attributes like time and location?
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. Mention one common method used in automobile hacking.
11. What does IDS/IPS stand for in cybersecurity?
12. An attack that overwhelms a service with traffic is:_____.

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