1312N971 Candidate's Seat No :_____

IMSc in CSF (NEP) Sem-3 Examination
ICSF-202
Cyber Security Fundamental-I

Time : 2-30 Hours] December-2024 [Max. Marks : 70

Question 1 Answer the following questions:

i.	What Cyber Security? Explain different types of Cyber Security.	7Marks
ii.	Differentiate between Security Auditing and Security Governance.	7Marks

OR

i.	List and explain the phases of ethical hacking.	7Marks
ii.	Differentiate between white-hat, black-hat, and grey-hat hackers.	7Marks

Question 2 Answer the following questions:

i.	Describe five warning signs that may indicate someone is a victim of cyberbullying.	7Marks
ii.	Explain the difference between a cyber threat and a vulnerability with examples.	7Marks

OR

i.	Identify and explain five key characteristics of vulnerabilities in cybersecurity systems.	7Marks
ii.	Define malware and explain five techniques to protect systems against it.	7Marks

Question 3 Answer the following questions:

i.	Explain the difference between authentication and authorization with an example.	7Marks
ii.	What is Data Recovery? Explain any five data recovery tools.	7Marks

OR

i.	Explain steps involved in Analysing the Type of Cyber Threat	7Marks
ii.	Describe how Role-Based Access Control (RBAC) helps in regulating access to resources. Include its benefits and limitations.	7Marks

Questions 4 Answer the following questions:

i.	Explain the key components of a secure web application architecture and their role in preventing cyberattacks.	7Marks
ii.	What is a DMZ (Demilitarized Zone) in network security? Explain its role in protecting internal systems from external threats.	7Marks

OR

i.	What are the primary security challenges in Android application architecture? How can developers mitigate these risks?	7Marks
ii.	How does Multi-Factor Authentication (MFA) contribute to the regulation of access in an IdAM system? Provide examples of MFA methods.	7Marks

P.T.O

Questions 7: Attempt any Seven out of Twelve.   14 Marks

1. The first phase of ethical hacking is: _____

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. Name one law that relates to cybersecurity.

6. What is the primary goal of Password Protection in IdAM?
   a) To limit user roles   b) To strengthen user authentication methods
   c) To regulate access control   d) To monitor system logs

7. Which principle is foundational to IdAM to ensure least privilege access?
   a) Multi-factor authentication   b) Role-based access control (RBAC)
   c) Password rotation policies   d) Identity federation

8. Define Hashing 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 Define cryptography in one sentence.

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