Question Paper

Exam Date & Time: 11-Jan-2024 (02:30 PM - 05:30 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

FIFTH SEMESTER B.TECH. DEGREE EXAMINATIONS -JANUARY 2024
SUBJECT: ICT 3156- CYBER SECURITY

Marks: 50 **Duration: 180 mins.**

Answer all the questions.

Any data not provided may be suitably assumed.

1A)	Identify and explain the different types of attackers in cybersecurity. Discuss how these attackers differ in their motivations and capabilities, and how they can exploit the different types of security vulnerabilities that exist in information systems	(5)
1B)	Consider the C-I-A triad and the four acts of harm are two fundamental concepts in information security. Analyse how these concepts are interrelated, and explain how the four acts can cause harm to the confidentiality, integrity, and availability of assets in a complex and interconnected system	(3)
1C)	In the context of online services, explain how the concept of "identities are typically public or well-known, authentication should be private" can be applied to improve security.	(2)
2A)	Biometric authentication systems are increasingly being used to verify identity and access control. However, these systems are not without their problems. Discuss the problems with biometric authentication systems and analyse their implications for security and privacy.	(5)
2B)	A large and complex organization has a decentralized access control system. Each department has its own access control policies and procedures, and there is no central authority responsible for coordinating access control across the organization. Analyse the specific challenges that this organization would face in implementing a robust access control system? How would you recommend that this organization address these challenges?	(3)
2C)	Explain the key critical distinctions between AES and DES?	(2)
3A)	Demonstrate the following Programming Oversights in detail: 1) Undocumented access points (backdoors) 2) Off-by-one errors 3) Integer overflows 4) Unterminated null-terminated string 5) Parameter length, type, or number errors	(5)
3B)	How do hardware components like fence registers and Memory Management Units (MMU)s collaboratively enable dynamic program relocation while ensuring memory isolation and security in a multi-programming environment?	(3)
3C)	What is tiger team analysis for security? How does it differ from vulnerability?	(2)
4A)	Evaluate the role and significance of the Trusted Computing Base (TCB) in trusted systems, including the functions it encompasses, the design principles for a secure TCB, the implications of a trusted path, challenges and strategies related to object reuse and data security, and the role and importance of audit logs.	(5)

4B)	Examine the roles of users and operating systems in safeguarding against malicious web pages and analyze the challenges associated with enforcing good and secure code on web pages.	(3)
4C)	How do base/bounds registers represent an advancement over the use of fences in terms of memory protection, and what specific benefits do they offer in the context of ensuring secure memory operations?	(2)
5A)	Why is Onion Routing used? Consider a situation where Alice wants to send an encrypted communication to Bob using Onion Routing technique. She chooses two forwarding hosts (X and Y) for this purpose. With the help of a proper diagram, show the structure of the communication package (at each node) as it travels from Alice to Bob.	(5)
5B)	Categorize computer crimes based on the role that plays in the criminal activity	(3)
5C)	What are the contents of security plan? How incidents are handled?	(2)

-----End-----