Question Paper

Exam Date & Time: 03-Jun-2023 (02:30 PM - 05:30 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

VIth SEMESTER B.TECH END SEMESTER EXAMINATIONS,MAY - JUNE 2023

CYBER SECURITY [ICT 4306]

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

A

Answer all the questions.

Instructions to Candidates:
Answer ALL questions
Missing data may be suitably assumed

1) Examine how single sign-on (SSO) incorporates different authentication protocols and technologies, such as SAML and Kerberos. (5)

A)

B) Evaluate with suitable justification the effectiveness of the same origin policy in preventing cross-site scripting attacks. (3)

C) Assess the scope and applicability of various forms of intellectual property protection employed in modern times, highlighting the differences between them (2)

2) List and explain commonly used techniques for preventing SQL injection vulnerabilities. Additionally, evaluate the testing methods employed by developers and security professionals to ensure their applications are not susceptible to SQL injection attacks. (5)

A)

B) Explain how fuzz testing is utilized in software testing and the process for selecting appropriate input data for it. (3)

C) Evaluate the potential advantages and disadvantages of relaxing the Same Origin Policy, and analyze its potential impact on web security. (2)

3) Explain the difference between passive and active threats in the context of cybersecurity. Provide examples of each and describe the potential impact of each type of threat on an organization's security posture. (5)

A)

B) Analyze how the utilization of cookies in web applications jeopardizes user privacy. Furthermore, evaluate common techniques utilized by attackers to exploit this vulnerability. (3)

C) Comment on the emerging trends in cybercrime, such as the use of artificial intelligence in breach of privacy and data diddling. (2)

4) Compare and contrast various types of firewalls, highlighting the differences in their functionalities. (5)

A)

B) Examine the methods used by attackers to exploit social engineering techniques to deceive users into downloading and installing malicious software. Evaluate the role of antivirus and anti-malware software in mitigating the risks of virus and malware infections, and describe their underlying (3) mechanisms.

C) Justify the assertion that biometrics is the most reliable form of evidence in digital forensics. (2)

5) A) Compare and contrast steganography and cryptography. How do these techniques differ in terms of their goals, methods, and effectiveness? Can these techniques be used in combination to enhance security, and if so, what are some examples? (5)

B) With some common well-known incidents of hacking exemplify how hacking attacks impact individuals, organizations, and society as a whole, in terms of financial losses, data breaches, reputational damage, or national security threats. (3)

C) Identify the type of laws in the Indian Judiciary system (Civil, Criminal, Constitutional, or any combination) with suitable justification for the following scenarios: (2)

a. Seeking compensation from a company for a faulty product

b. Cyberstalking and posting defamatory photos

c. Government violates the right to privacy.

d. Infringement of Copyright.

-----End-----