Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 50423

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2024.

Fifth/Sixth Semester

Computer Science and Design

CCS 340 – CYBER SECURITY

(Common to: Computer Science and Engineering/Computer Science and Engineering (Artificial Intelligence and Machine Learning)/Computer Science and Engineering (Cyber Security)/Computer and Communication Engineering/Artificial Intelligence and Data Science/Computer Science and Business Systems/Information Technology)

(Regulations 2021)

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Brief about the CIA Triad in cybersecurity.

2. Outline the significance of the Indian IT Act in addressing cybercrime.

3. Define OWASP and its significance in cybersecurity.

4. Name two common types of malicious software.

5. Express the term "harvester" in the context of cyber reconnaissance.

6. State the purpose of port scanning in cybersecurity.

7. Distinguish between host-based and network-based intrusion detection systems.

8. Recall the concept of a honeypot and its role in intrusion detection.

9. Discuss the need for firewalls in cybersecurity.

10. List the characteristics of Intrusion Prevention Systems (IPS).

PART B — (5 × 13 = 65 marks)

11. (a) Analyze a case study where the lack of cyber security measures resulted in a significant cyber-attack. Assess the impact of the attack and propose preventive measures based on the CIA Triad.

Or

(b) Apply the principles of cyber laws discussed in the Indian IT Act to a real-world scenario involving cybercrime prosecution. Deliberate the legal implications and challenges faced in the process.

12. (a) Investigate a recent cyber-attack involving social engineering tactics. Analyze the attack vectors and countermeasures implemented to mitigate the risks.

Or

(b) Illustrate a comprehensive security strategy for a web application vulnerable to common attack vectors. Discuss the effectiveness of each countermeasure in protecting against potential threats.

13. (a) Examine and analyze a case study involving reconnaissance techniques used in a cyber espionage operation. Assess the effectiveness of the reconnaissance methods employed and propose countermeasures to prevent similar attacks.

Or

(b) Apply the principles of network scanning and vulnerability scanning to assess the security posture of a corporate network. Develop a report outlining the identified vulnerabilities and recommendations for remediation.

14. (a) Examine a real-world intrusion detection scenario where a hybrid intrusion detection system detected and responded to a cyber-attack. Elaborate the system's effectiveness in mitigating the attack and preventing data loss.

Or

(b) Design an intrusion detection system architecture for a large enterprise network. Evaluate the advantages and disadvantages of host-based, network-based, and hybrid intrusion detection approaches in this context.

15. (a) Analyze a case study where a firewall misconfiguration led to a security breach in a corporate network. Investigate the impact of the breach and propose measures to prevent similar incidents in the future.

Or

(b) Develop a comprehensive intrusion prevention strategy for a financial institution aiming to safeguard its online banking services. Analyze the potential risks and propose preventive measures using a combination of firewalls and intrusion prevention systems.

PART C — (1 × 15 = 15 marks)

16. (a) Design an intrusion detection and response framework for a cloud computing environment. Consider the unique challenges posed by cloud infrastructure, such as dynamic resource allocation and multi-tenant environments. Evaluate different approaches for deploying intrusion detection sensors within the cloud and integrating them with centralized monitoring and response systems. Analyze the trade-offs between scalability, performance and security in designing the framework and propose best practices for effective threat detection and mitigation in cloud environments.

Or

(b) Explore a scenario where a distributed intrusion detection system (DIDS) was deployed across multiple organizations to detect coordinated cyber-attacks. Analyze the effectiveness of DIDS in detecting and mitigating the attack, considering factors such as data sharing, collaboration among organizations and scalability of the system. Evaluate the lessons learned and propose recommendations for enhancing the resilience of DIDS in future deployments.

———————