**Birla Institute of Technology & Science, Pilani**

**Work Integrated Learning Programmes Division**

**First Semester 2024-2025**

**Comprehensive Examination**

**(EC-3 REGULAR)**

Course No. : SS ZG681

Course Title : Cyber Security

Nature of Exam : Open Book

Weightage : 40%

No. of Pages = 3

# No. of Questions = 5

Duration : 2 ½ Hours

Date of Exam : 01/12/2024 (EN)

Note to Students:

1. Each question carries 5 marks
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q.1. [10]

You are a security analyst at a healthcare technology company that manages sensitive patient data. The company’s primary objectives are to ensure data integrity, prevent unauthorized data manipulation, and maintain high availability for its healthcare applications, which doctors rely on for critical patient care. Given the nature of the data, the company has asked you to recommend security models that will help enforce strict data integrity and availability policies.

The company is concerned about possible data integrity breaches, such as accidental or malicious data changes, and the impact of potential system deadlocks on data availability. They have asked you to evaluate the Biba Integrity Model for integrity control and propose policies for availability that would help prevent deadlocks and ensure continuous access to critical data.

*Question: Explain the goals of integrity policies. Discuss how the Biba Model enforces data integrity and its relevance to preventing unauthorized modifications in data.*

*Define the goals of availability policies and discuss their importance in a healthcare environment where timely access to information is crucial.*

*Explain the concept of deadlock and why it is a concern for system availability. Describe a deadlock prevention or recovery method the company could implement to maintain high availability and minimize the risk of service interruptions.*

Q.2. [10]

You are an IT consultant hired by a tech startup, Brighten, that specializes in developing a cloud-based application for businesses to manage and analyze customer data. Although BrightNet’s team has basic technical skills, they lack an in-depth understanding of networking principles essential for the smooth functioning, scalability, and security of their application.

The founders have asked for a comprehensive report that covers fundamental networking concepts, a deep dive into how data flows across the internet, and a guide to using the OSI model for diagnosing network related issues. They are also curious about the historical milestones that have shaped today’s internet and want to understand the importance of network protocols for efficient and secure communication in their application.

*Question:*

*1.Explain Network Basics and Internet Functionality 2. OSI Model and Its Application in Troubleshooting, 3.Historical Development of the Internet 4.Importance of Network Protocols in Cloud Based Applications*

Q.3. [10]

You are the Chief Information Security Officer (CISO) at a large retail company with both an online ecommerce platform and several physical store locations. Recently, there was an attempted cyberattack targeting your company’s customer database, but luckily, it was stopped before any data was stolen.

During the incident analysis, you noticed that the attackers tried multiple tactics, from phishing emails sent to employees, to brute forcing network credentials, and even attempting to exploit vulnerabilities in the company’s website. This incident highlights the growing complexity of threats and the need to implement a more robust, layered security model.

The executive team has asked you to explain the brute forcing approach and how a layered security model can help safeguard the organization from future attacks. They want a clear strategy on the different security layers you would implement to protect various areas, from network and endpoint security to user education and physical security.

*Describe the brute forcing approach and outline the specific layers you would implement in a layered security model for your company to protect against diverse cyber threats. Explain how each layer would contribute to the overall security posture and reduce the likelihood of successful cyberattacks.*

Q.4. [5]

You are the cybersecurity manager at TechWave Inc., a financial services company that offers online banking solutions. Recently, your organization experienced reports from several customers about unauthorized transactions in their accounts. Upon investigation, you suspect that attackers may be using session hijacking and man-in-the-middle (MitM) attacks to gain access to user sessions and perform unauthorized actions.

What are the mechanisms of session hijacking and man-in-the-middle attacks, and what specific measures can TechWave Inc. implement to protect its online banking platform from these types of attacks? Include examples of how each attack works and the security practices to mitigate them.

Q.5. [5]

You are an IT security analyst at a mid-sized financial company. Your company has recently been targeted by a cyberattack where a hacker attempted to steal customer data by intercepting network traffic. In a meeting with your team, your manager asks you to evaluate the incident in terms of the CIA Triad (Confidentiality, Integrity, and Availability) and identify which aspects of the company’s security fundamentals were compromised.

Based on the CIA Triad, which security aspects were compromised during the cyberattack, and what actions can you take to mitigate future risks?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_