VIT Vellore Institute of Technology

Reg. No. : 21BCE1808

Final Assessment Test (FAT) - July/August 2023

Programme	**B.Tech.**	Semester	**Fall Inter Semester 22-23**
Course Title	**INFORMATION SECURITY ANALYSIS AND AUDIT**	Course Code	**BCSE353E**
Faculty Name	**Prof. GANESH N**	Slot	**TB1**
		Class Nbr	**CH2022232501112**
Time	**3 Hours**	Max. Marks	**100**

PART-A (10 X 10 Marks)
Answer All questions

01. Ramnath and Samuel - the Directors of the same organization working in two different countries would like to share their organization's documents which are very sensitive information over a communication channel. They are concerned that their documents might be intercepted and read by an unauthorized third party over the internet. As a security specialist of the organization suggest them a technique which helps to achieve **[10]**
    a. Confidentiality of the documents (5 marks)
    b. Authentication and Integrity. (5 marks)

02. An employee in your organization is using a laptop to access the data and connecting to internet for web surfing. At this time the employee notices that the laptop is acting abnormally as the following, **[10]**
    (i) It takes longer than usual to access a file and the files are replicating
    (ii) Sometimes the camera is enabled with its light blinking,
    (iii) The employee often experiences unexpected pop-up advertisements.
    (iv) Additionally, the employee suspects that someone may be remotely monitoring the activities through the backdoor of the system without the employee's consent.
    a. Identify the above types of unusual behaviors. (5 marks)
    b. Differentiate the identified unusual behaviors with a detailed description. (5 marks)

03. Imagine, you are a cybersecurity consultant hired by a software development company to assess the security of their web application. During your assessment, you discover several vulnerabilities that align with the OWASP Top 10 security issues. You need to explain these issues to the development team, highlighting the potential risks and providing recommendations to mitigate these issues. Explain them with complete information on all the 10 security issues and create awareness to the development team. **[10]**

04. You are a cybersecurity expert working with a small e-commerce startup. The company has recently launched its online platform, and they want to ensure the security of their website and customer data. As part of your consultation, you are asked to explain in detail about the various Web Security Threats and their types to all the employee of the company, so that they can proactively address potential vulnerabilities with knowledge and confidence. **[10]**

05. Imagine, you are the newly appointed Certified Information System Security Professional for a large-sized company. Recently, there was an incident where critical data was accidentally deleted, causing significant disruption to the business operations. As a result, the senior **[10]**

management wants you to explain the importance of backups and its different types to all the employees of the company. Following the scenario-based training methodology, the management provides you the scenario to train the employee on

a. How to take backup from Monday to Friday in a week with different types of backups. (5 marks)

b. Which kind of back up can be adopted in your company to achieve the highest level of information security with the reason. (5 marks)

06. Mahindra & Mahindra is a leading Car manufacturing company which has planned to bring some IoT devices in all the cars manufactured by the company. Assume you are the Certified security specialist for the company and you are asked to manage Risks involved with the IoT devices. Explain the company about the procedures involved in managing the Risks involved in utilizing the IoT devices with the components of Risk Management. **[10]**

07. Assume you are a Certified Security Professional running a small-sized company and providing security services to Apollo healthcare organization in Chennai. You are protecting the complete medical records of the patients over several connected devices in different locations. Today a security breach has occurred and all the patient information have been hacked which are treated as asset of the organization. Now the management is asking you to give a complete report of the Incident. As the responsible person explain the management about the incident and your response to the incident by following the lifecycle in order to mitigate the security breach. **[10]**

08. You are working as an Information Security Auditor for a large multinational corporation. The company has recently expanded its operations with new application hosting and content management system. Your task is to, **[10]**

a. Conduct an information security audit by following the Audit process to focus on the Risks involved in the application hosting and content management system, ensuring the confidentiality, integrity, and availability of critical corporate data. (5 marks)

b. Discuss about the sequential Phases of Information Security Audit you follow for the audit. (5 marks)

09. a. "Penetration test is intended to assess the prevention, detection, and correction controls of a network by attempting to exploit vulnerabilities and gain control of systems and services" Based on this statement, elucidate the penetration testing types in detail. (5 marks) **[10]**

b. Assume that you work in a firm as a security specialist and now you wish to become an security auditor. As an experienced security specialist, elaborate about the ethics to be followed by the security auditor and what sort of roles and responsibilities that an auditor should possess. (5 Marks)

10. Your organization is a financial servicing company that handles highly sensitive customer financial data. Recently, an employee inadvertently sent an email containing confidential customer information to a recipient outside the organization. This incident has raised concerns about the correct handling of confidential information within the organization. As an information security analyst, insist your employees about **[10]**

a. The importance of maintaining data confidentiality and the type of information to be protected very carefully. (5 marks)

b. The policies and procedures to be followed to achieve data confidentiality. (5 marks)