F/L/TX

Reg. No: 21MIS0395

VIT
Vellore Institute of Technology

Final Assessment Test – November 2024

Course: CSE3501 - Information Security Analysis and Audit
Slot: E2
Class NBR(s): 3011/3028/3047/3053
Max. Marks: 100
Time: Three Hours

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

Answer ALL Questions
(10 X 10 = 100 Marks)

1. Assume you are a HR manager at a large corporation. One afternoon, you receive an email from a colleague in the IT department. The email explains that the company is performing an urgent security update, and all employees must confirm their login credentials to avoid being locked out of the system. The email includes a link to a page where you are asked to enter your username and password. The message is marked as "high priority" and claims that failing to act immediately could result in your account being deactivated. Address the following inquiries pertaining to this scenario.
   i) What should you do before clicking on the link and providing your credentials?
   ii) Justify the scenario that indicate this could be a social engineering attack?
   iii) What are some preventive measures that could protect against this type of social engineering attack?

2. A smart home network uses various Internet of Things (IoT) devices, including smart thermostats, cameras, lights, and door locks. The home owner is concerned about privacy and security vulnerabilities in these devices. What security measures would you recommend for securing IoT devices and how would you manage network segmentation to protect sensitive devices?

3. A financial firm is concerned about the increasing number of phishing attacks targeting employees through email. To safeguard sensitive client information and ensure compliance with regulatory standards, the firm decides to implement a formal email security policy. You have been tasked with creating an email security policy template for the financial firm. What key components would you include in the policy to address phishing threats, prevent data leakage, and ensure compliance with industry standards?

4. An e-commerce company experiences a significant data breach, where unauthorized access to customer payment information is detected. The incident response team is activated to manage the situation and mitigate potential damage. What key roles are essential in the security incident management process for effectively handling the data breach, and what responsibilities does each role entail?

5. A reputed hospital has recently launched a new web portal for patients to view their medical records, schedule appointments, and communicate with doctors. During a routine vulnerability assessment, several security issues were discovered, including weak password policies, insecure API endpoints and out-dated server software. How would you approach the entire vulnerability assessment process for the healthcare web portal to ensure patient data is protected?

6. Imagine a large retail company that processes thousands of transactions daily. The internal audit team sets up a real-time auditing system to monitor these transactions. As transactions occur, the system continuously analyzes the data. One day, the system alerts a series of high-value transactions processed late at night. The audit team receives an alert and investigates immediately, discovering that an employee's credentials were compromised. Describe the various functions in an audit to quickly take action to prevent further unauthorized transactions and to recommend additional security measures to prevent future incidents.

7. A multinational company receives feedback from customers about slow page load times and difficulties navigating the site on mobile devices. The internal audit team is tasked with conducting a website performance and user experience audit. During the audit, the team discovers that the home page takes over 10 seconds to load, images are not optimized and the mobile version of the site has touch elements that are too small. Prepare the audit check list for the given scenario.

8. An internal audit team at a healthcare organization is tasked with conducting a compliance audit focusing on HIPAA regulations. Discuss the steps for work planning and creating a favourable environment for an IT Security Audit to ensure a thorough and efficient audit.

9.a) Explore the identity and access management for an employee at a large corporation using a single set of login credentials to access multiple applications, such as email, HR systems, and project management tools. How will you add an extra layer of security, making it harder for unauthorized users to gain access? Ensure that an employee leaving the company should lose all access to all systems and data, to prevent any unwanted access.

OR

9.b) A manufacturing company is looking to implement a comprehensive risk management framework to address various risks, including operational, financial, regulatory, and cyber security risks. The management is aware that a strong risk management approach is essential for the company's long-term sustainability and success. What key components should be included in the risk management framework for the manufacturing company to effectively identify, assess, mitigate, and monitor risks across its operations?

10.a) The major financial organization handles sensitive customer data, including personal information, account details, and transaction histories. They rely heavily on their online banking platform to serve millions of customers. The online banking platform has an unpatched vulnerability in its web application firewall, which allows for a ransomware attack. A cybercriminal discovers the vulnerability and exploits it to gain unauthorized access to the bank's database and extracts the sensitive customer data. Discuss the consequences of the cyber-attack on this financial organization in detail.

OR

10.b) Illustrate how White-box, Black-box and Grey-box penetration testing methodologies help organizations to identify and mitigate security risks from different perspectives, ensuring a robust security posture.

⇔⇔⇔F/L/TX⇔⇔⇔