Y/K/TX

Reg. No: 21BIT0174

VIT
Vellore Institute of Technology

Final Assessment Test – November 2024

Course: **BITE413L - Cyber Security**

Class NBR(s): **3546 / 3550**

Slot: **A1+TA1**

Time: **Three Hours**

Max. Marks: **100**

- **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. Illustrate a detailed explanation of the concept of social engineering attack. Discuss in detail with suitable example about any 4 human based social engineering attacks that made against a reputed organization for resulting in significant financial loss.

2. The cyber-criminal emailing you while pretending to be your relative. In the email, they may try to get you to reveal personal information such as your address, birthday, login credentials, or more. Identify the attack with your answer in detail for given scenario.

3. You make an online purchase using your credit card while connected to a public Wi-Fi network, and later find unauthorized transactions on your account. Illustrate the risks of using public Wi-Fi for financial transactions, and how can you protect your credit card information in such situations.

4. a) Distinguish Viruses, Worms and Trojan Horses. Also, discuss each in detail. **[5]**

   b) Imagine you are a security analyst tasked with implementing multi-factor authentication for a corporate email system. Outline the steps would you take to ensure that the multi-factor authentication implementation is both secure and user-friendly. **[5]**

5. During a routine security assessment, you discover that a specific input causes an application to crash. Further investigation reveals that the crash is due to a buffer overflow vulnerability. Explain how you would exploit this vulnerability to demonstrate its impact. Outline the steps should be taken to spot the vulnerability and prevent future occurrences.

6. Illustrate the serious offenses and with Cyber Crime, Punishment and Penalty under the Section of 477.1, Section 477.2, and Section 477.3 of Division 477 in the Australian Cyber Crime Act 2001. Explain the serious offenses under Section 478.1, Section 478.2, Section 478.3, and Section 478.4 of Division 478 in the same Act with Cyber Crime, Punishment and Penalty.

7. A social media user is arrested for posting an allegedly offensive message online. How does the amendment to Section 66A of the IT Act 2000 impact this case? Discuss in detail about legal arguments can be made regarding the constitutionality of this section.

8. Explain the Digital Forensics Lifecycle in detail. Discuss each phase with its significance and the key activities involved. Illustrate the practical application of these phases with real-time examples.

9.a) An employee's smartphone, containing sensitive company data, is lost or stolen. How would you conduct a forensic investigation to determine if any data was accessed or compromised? Explain the steps should be taken to secure the data and prevent unauthorized access.

OR

9.b) A mobile device used in a criminal investigation has been intentionally damaged to destroy evidence. Explain how you would approach the forensic recovery of data from this damaged device. What challenges might you face, and how would you overcome them?

10.a) Your Company stores sensitive customer data in a cloud service and you notice that unauthorized parties have accessed this data. Illustrate how would you investigate the breach and outline the steps would you take to mitigate the damage and prevent future incidents.

OR

10.b) The organization needs to develop a comprehensive cyber security policy. Discuss the key elements that should be included in this policy. Illustrate how the organization ensure that all employees understand and adhere to the new security policy.

⇔⇔⇔ V/K/TX ⇔⇔⇔