ourdiu.com | Shared by Md. Ferdous Foysal Hridoy

Daffodil International University

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Final Examination, Fall'2023

Course Code: CSE423, Course Title: Information Security

Level: 4, Term: 1 **Batch: 56**

Time: 2 Hour **Marks: 40**

Answer ALL Questions

[The figures in the right margin indicate the full marks and corresponding course outcomes. All portions of each question must be answered sequentially.]

1.	*a)*	Suhita is a cyber security enthusiast. Her interest is in learning new tools and techniques of system hacking. As a mean of assessing her efficiency she decided to hack one the leading online book store. Now **construct** the hacking steps she has to follow in order to hack the system mentioning methods/tools she can use in each step.	10	CO1
	b)	**Explain** your understanding on VAPT report and why do organizations need to develop it?	5	
2.	*a)*	Imagine you are the IT security manager for a medium-sized company that handles sensitive customer infonnation. Recently, there has been a surge in cyber security threats, and the company is concerned about the security of its network and data. **Develop** a comprehensive scenario-based plan outlining the key components and strategies you would implement to ensure the robust security of both the network infrastructure and the sensitive transmitted data, taking into account potential external attacks, network threats and the need for continuous monitoring and adaptation to emerging threats.	10	CO2
	b)	A financial institution stores critical transactional data that must remain tamper-proof for regulatory compliance. **Explain** how would you utilize hash encryption to ensure the *integrity* of this sensitive data during transmission and delivery?	5	
3.	*a)*	A skilled hacker gains unauthorized access to the computer network of a prominent bank in Bangladesh. Using advanced techniques, the hacker breaches the bank's security systems and successfully extracts confidential customer data, including account details, credit card information, and transaction history. The perpetrator, aware of the sensitive nature of the stolen data, attempts to exploit it for personal gain, intending to sell the information on the dark web. The bank, upon discovering the breach, promptly reports the incident to the law enforcement agencies. **Analyze** what potential legal consequences could he/she face publish under Digital Security Act-2018?	7	CO3
	b)	**Illustrate** how *Trademarks* can be used to safeguard intellectual properties?	3	