Daffodil International University

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Midterm Examination, Spring 2023
Course Code:CSE423, Course Title:Information Security
Level:4 Term:1 + 2 Batch: 54 + 55

Time: 1 Hour and 30 Minutes **Marks: 25**

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.		You may be used to seeing stories like robbing money from the vault in movies or TV Series like The Money Heist. The "Central Bank of Bangladesh (CBB) Cyber Heist" was one such incident. Like other government banks, CBB too has a branch located at USA for money transaction. A malicious e-mail started the whole story. In January 2015, an anonymous person sent a job-seeking application via email to the employees of CBB, where a CV was attached in the mail. But, it was not a regular job application; a malware was linked with the file which later helped them to enter into the central bank's computer system after some employee clicked on the link. The malware started installing on the computer system of the CBB. Although hackers were able to enter the computer system, they did nothing but gained access to the system and collected all the important data throughout the year. A printer that was located at the Bangladesh, main branch of CBB Bank played a pivotal role here. Any transaction made by any branches printed automatically on it. On February 4, 2016, the attackers started executing the attack by making transaction requests from the USA branch of CBB Bank to some fake accounts. Suddenly(!) the printer started showing some technical problem hence any transaction information from abroad didn't reach to Bangladeshi branch of the bank. The hackers intentionally deleted all those confirmation messages from the database used by the USA branch, crashing the entire program on the automatic printer. By the time the employees noticed the problem, hackers managed to transfer 81$ million dollars to their fake accounts.		**CO2**
	a)	Can you **analyze** and describe the types of attacks mentioned in the above scenario? Also, **classify** the hacker team.	**5**	
	b)	Now, **identify** at least 3 threat sources and risks to **analyze** the overall risk calculation and show the result and conclusion according to the Overall Risk Rating Matrix and Calculation.	**4**	
	c)	**Explain** which of the CIA traits have been violated here and how? **Suggest** some features to implement those traits.	**4**	
2.	***a)***	ChatGPT is a chatbot developed by OpenAI and launched in November 2022. It uses both supervised and reinforcement learning techniques for its training purposes. Although the core function of a chatbot is to mimic a human conversationalist, ChatGPT is unique. For example, it can write and debug computer programs; compose music, teleplays, fairy tales, and essays; answer test questions (sometimes, depending on the test, at a level above the average human test-taker); and write poetry and song lyrics. ChatGPT's training data includes information about Internet phenomena and programming languages, such as bulletin board systems and the Python programming language. **Discover** the risk scenarios that can be triggered using ChatGPT based on the information provided above.	**4**	**CO2**
3.	***a)***	DIU Finance Ltd. has experienced a security incident that has compromised the personal data of its customers. The incident highlights the importance of effective incident management in responding to security breaches. Can you **define** the key components of incident management in the context of this security breach?	**3**	**CO1**
	b)	Suppose Session hijacking has occurred on your university's web server. By knowing your sessionID, the hacker can access your student account and disrupt the communication. Now **solve** the problem using some techniques of AI and ML.	**3**	
	c)	A malware attack has compromised a computer system. The malware is using multiple components to achieve its goals. **Name** them and determine **which** component of the malware is the most critical and explain why?	**2**	