Daffodil International University

Faculty of Science & Information Technology

Final Examination, Fall 2022

Course Code: CSE423 Course Title: Information Security

Sections & Teachers: All Sections (Batch- 53).

Time: 2:00 hours **Marks: 40**

[Read the given scenario below and answer all the questions. The cells in the right margin indicate the full marks and corresponding course outcomes. All portions of each question must be answered sequentially.]

Year 2021 was not easy for E-corporation as they were the victim of a significant number of cyber-attacks which caused a great financial, social and reputational damage. Most of the unhandled risks and ignored threats came to a reality and exposed the information system to several cyber-attacks by different local and international parties. Through incident management report it is found that attackers compromised the organization's private network and its information system by exploiting both previously known and unknown vulnerabilities.

Today, Mr. Elliot; a new security expert; specially hired by the CTO suggested to redefine the firewall rules and incorporate IPS with the existing firewall. He also asked Mr. Khan, senior stuff to ensure that all employees' personal devices and antiviruses remain up to date including security patches whenever available.

1.	*a)*	How IDS detect Intrusion? Differentiate between Antivirus and Firewall.	3	CO2
	b)	Analyze the roles and objectives of Honeypot and identify the suitable placement in the system of E-corporation with the help of diagram.	3	
2.	*a)*	Why do you think Vulnerability Assessment is necessary for any organization like E-corporation? Evaluate its significance and highlight the components of the vulnerability assessment report.	3	CO2
	b)	Relating to the **unknown vulnerabilities** explain zero-day exploit and zero-day attack.	3	
3.	*a)*	Footprinting is the technique used for gathering information about computer systems and the entities they belong to. What is active Footprinting? Highlight useful active Footprinting techniques.	4	CO1
	b)	If you play the role of a hacker then what are the standard steps you would follow for a successful hacking event. Give proper explanation for each of the steps.	6	
4.	*a)*	Demonstrate your understanding about Hashing in the field of Cryptography and point out why and in which case you are required to use Hashing mechanism.	3	CO2
	b)	Why would you choose to use Asymmetric Encryption keeping aside another easiest encryption technique? List and Explain your point for making such choice.	3	
	c)	Cybersecurity experts use cryptography to design algorithms, ciphers, and other security measures that codify and protect company and customer data. What do you understand by Public Key Cryptography? Provide a comparative analysis of the characteristics of DES and AES Algorithm.	5	
5.	*a)*	Shanto, a 26-year-old successful software engineer was arrested for a list of serious accusation made by the lawyer of the company he was working for the last 4 years. The lawyer stated "This employee deleted one of the directories from the company's cloud based private storage which was used to store source code of deliverable software projects and it is causing us to face a loss of at least 3million Taka.". Moreover, the next day one of his female colleagues filled another case saying the accused person broke her phone while she was trying to convince him for not sending any adultery contents link via messenger. What kind of offences he has made in the light of Bangladesh Digital Security Act-2018? **Apply** your knowledge to **create** a list of the offences and mention the laws, sections and corresponding punishment for the each of them.	7	CO3