Daffodil International University

Faculty of Science & Information Technology

Department of Computer Science & Engineering

Final Examination, Fall 2025

Course Code: CSE423, Course Title: Information Security

Level: 4 Term: 3, Batch: 61

Time: 2 Hrs **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 global bank notices unusual outgoing traffic from some of its internal servers, which may mean a data breach has happened. The incident response team quickly isolates the affected servers, blocks suspicious IP addresses, and temporarily disables the accounts that may have been hacked. They remove malware and unauthorized access, fix security weaknesses, and reset passwords. Important evidence, like system logs, disk copies, and malware samples, is collected and analyzed to find out how the attack happened, how much damage was done, and the main cause. Finally, security rules are updated, employees are trained to prevent future attacks, affected customers are informed, and a detailed incident report is written.			
	a)	**Compare** security risk management and incident management, providing proper examples. Also, **explain** the purpose of risk management in the context of these challenges.	[2+2]	CO1
	b)	In the scenario, attackers attempt to use various anti-forensic techniques to hide their activities and mislead investigators during the breach. Now, **apply** your knowledge to describe the different types of anti-forensic techniques used by attackers to hide, destroy, manipulate, or mislead digital evidence.	[5]	
	b)	**Relate** each action described in the scenario to its corresponding stage in the Incident Handling and Response (IH&R) process.	[6]	
2.	A large e-commerce company in Bangladesh relies on four key systems: an Order Processing System with moderately likely failure but high financial impact, a Customer Login & Authentication Service with low likelihood but high impact, a Warehouse Management Dashboard with medium impact and medium likelihood, and an outdated Employee Communication Portal with low impact but a higher chance of failing. One morning, the SOC team notices abnormal CPU spikes and unauthorized PHP files on the main web server, and sees it trying to connect to unknown foreign IP addresses. Firewall logs show multiple outbound attempts, some blocked but some allowed. The installed antivirus repeatedly warns about a suspicious program acting like a "fake antivirus," yet fails to quarantine or delete it. Suspecting a breach, IT isolates the server from the network but keeps it powered on to preserve evidence. During forensic analysis, investigators capture memory and find suspicious processes encrypting outgoing data continuously, while fragments of encrypted files on disk are stored in fixed-size chunks.			**CO2**

	a)	**Calculate** the overall risk rating from the scenario along with prioritized assets.	[5]	
	b)	Based on the scenario, **analyze** the failure of the antivirus in detecting the fake-antivirus malware and **discover** how firewall logs can be used to trace and block the attacker's outbound connections.	[5]	
	c)	**Analyze** the given scenario to identify the data acquisition techniques employed by the forensic team. Considering the encrypted data discovered during the investigation, **categorize** the types of symmetric encryption (block ciphers vs. stream ciphers) that could have been used in the attack.	[3+2]	
3.	a)	A Bangladeshi digital health and payment platform collects personal data from local users, provides telemedicine services to EU citizens living in Bangladesh, exchanges medical reports with a partnered hospital in the United States for expert review, and stores customer card information for online payments. The organization is unsure when GDPR, HIPAA, and PCI DSS apply within Bangladesh. **Analyze** the scenario and **categorize** the situations in which GDPR, HIPAA, and PCI DSS become applicable to organizations in Bangladesh, and **distinguish** the different user groups and data types that fall under each law.	[5]	**CO3**
	b)	A junior programmer at a Bangladeshi IT firm secretly modifies the source code of a government web application to insert a hidden backdoor, claiming it is to "test" the system. Later, he leaks access credentials to an online group, which uses the backdoor to steal protected data and threatens to target a foreign embassy's system. The incident disrupts operations and raises cross-border security concerns. Based on this scenario, **inspect** how the actions violate Section 20 and Section 27 by describing both the offenses and the punishments for breaking these laws.	[5]	