Daffodil International University

Faculty of Science & Information Technology

Department of Computer Science and Engineering

Midterm Examination, Spring 2025

Course Code: CSE423, Course Title: Information Security

Level: 3 Term: 2 Batch: 62

Time: 01:30 Hrs **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.	*a)*	Equifax, one of the largest credit reporting agencies in the U.S., suffered a massive data breach in 2017 that exposed sensitive personal information of 147 million people, including names, Social Security numbers, birth dates, and addresses. Hackers exploited a vulnerability in the company's web application that had not been patched, allowing unauthorized access to sensitive data and were able to manipulate Equifax's database. After the breach, Equifax had to take parts of its system offline for investigation and recovery, which hampered the regular customer services. **i) Explain** how each component of the CIA triad is compromised in this scenario. **ii) Outline** some security measures to mitigate these risks.	[3+2]	**CO1**
	b)	**i) Define** Vulnerability Assessment and Penetration Testing, and explain how they help the company improve its security. **ii) How** the Color Wheel of Information Security works? **List** the activities of Red & Blue teams.	[3+2]	
2.	*a)*	*"Shopify,"* initially an f-commerce company, recently expanded its online services, attracting increased attention from external entities. Without the company's knowledge, an unauthorized individual intercepted and analyzed their network communications. Over time, it gathered substantial information about the site's internal mechanisms without modifying or damaging any data. Armed with the collected intelligence, the individual identified a flaw in the site's input validation mechanisms. Exploiting this vulnerability, they submitted manipulated inputs to the login form, gaining unauthorized access to sensitive areas of the platform. Once access was established, the individual deployed a malicious script within the company's network. Shortly afterward, employees lost access to their critical files. The system displayed a message demanding specific actions to restore access. **Classify** and **explain** the distinct cyberattacks that occurred in each phase of this scenario.	[5]	**CO2**
	b)	During a recent incident, an organization's IT department discovered an unfamiliar executable on several endpoints. Upon further investigation, the file was found to perform multiple functions: *1.* Immediately after execution, it began altering files and exfiltrating sensitive data, causing noticeable disruptions in normal operations. *2.* The executable also modified system configurations, including startup settings and scheduled tasks, ensuring that it reactivated automatically upon system reboot. *3.* Additionally, periodic outbound connections to an external server were detected, suggesting that the executable was receiving further instructions or updates from a remote source. Based on the scenario, **analyze** the three distinct functionalities exhibited by the executable. For each functionality, **explain** its role in the overall malicious operation.	[5]	
	c)	A hacker targeted TechSolutions, a software development company. The hacker began by researching the company through public websites and social media, gathering information about its employees, network structure, and business operations. After accumulating enough details, the hacker used this information to scan the company's	[5]	

		website for potential vulnerabilities. Upon discovering an outdated content management system (CMS) on one of the company's public-facing servers, the hacker took advantage of this weakness to gain unauthorized access. Once inside, they planted malicious code to remain in the system without getting caught, ensuring they could return later without detection. Finally, the hacker wiped out any logs or traces of their activity, preventing the company from noticing the breach during their routine security checks. **Analyze** the steps the hacker followed in this attack, breaking down each phase of the hacking process.		