ourdiu.com | Shared by Abdullah Tawsif (CSE-232)

Daffodil International University

Faculty of Science & Information Technology
Department of Computer Science & Engineering
Midterm Examination, Fall 2025
Course Code: CSE423, Course Title: Information Security
Level: 4, Term: 3, Batch: 61

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.	The National e-Archive has digitized millions of historical documents and uses strict security measures to protect them. Researchers can only view documents related to their projects under strict Access Control Policies (ACP) and are restricted from downloading or changing any files. The system regularly checks that each document remains unchanged by making a fixed-size hash value and securely verifies the identity of each researcher during access, keeping a permanent record of every action performed using a digital signature. The organization also performs Vulnerability Assessment and Penetration Testing (VAPT) to identify weaknesses, and reports them using Common Vulnerabilities and Exposures (CVE) IDs.			**CO1**
	a)	**Explain** which elements of the CIA Triad are protected in the National e-Archive example, and **describe** how Access Control Policies (ACP) and Hashing are used to achieve these security protections.	**[4]**	
	b)	**Interpret** which security principle is ensured through the use of a digital signature, and **illustrate** the mechanism of how a digital signature works to support that principle	**[3]**	
	c)	**Define** the terms Vulnerability Assessment and Penetration Testing (VAPT) and Common Vulnerabilities and Exposures (CVE), and **state** their purpose in system security.	**[3]**	
2.	A university's student portal was compromised after staff downloaded what looked like a legitimate system update. The program secretly gave hackers remote access to university systems and hid deep within the operating system, avoiding detection. While inside the network, attackers captured usernames and other credentials from infected machines. Using these, they launched a password-guessing attack with common and leaked passwords, gaining access to several key accounts, including some administrative ones. As more systems were compromised, infected computers began sending heavy traffic to the university's servers, causing the student portal to shut down for nearly two days. Finally, using stolen accounts, the attackers posted false messages on social media about a student data leak, spreading panic and damaging the university's reputation.			
	a)	**Analyze** the scenario to identify the types of malware involved and **inspect** the role each played in the overall incident.	**[4]**	**CO2**

ourdiu.com | Shared by Abdullah Tawsif (CSE-232)

	b)	**Apply** your knowledge of password attacks to identify which type of attack was used in the scenario and justify your answer	[3]	
	c)	**Analyze** the offensive and defensive elements of Information Warfare demonstrated in the university cyberattack. **Categorize** the attackers' motives and **distinguish** how their actions align with established information warfare strategies.	[3]	
3.	a)	**Compare** between footprinting and reconnaissance in the context of information security.	[2]	CO2
	b)	A hacker is trying to access a database server within an industry's private network. He was able to find the address of the server itself, but needs to identify the port at which the service is running. **Identify** with proper explanation which port scanning method the hacker in the scenario can use to identify open, closed and protected ports while looking for the database server.	[3]	