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

Daffodil International University

Faculty of Science & Information Technology
Department of Computer Science & Engineering
Final Examination, Summer 2026
Course Code: CSE454, Course Title: Cyber Security and Forensic
Level: 4 Term: 1 Batch: 64

Time: 02:00 Hrs **Marks: 40**

Answer ALL Question

[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 private hospital uses a centralized information system to store patients' medical records, laboratory reports, billing information, and staff login credentials. The system is protected by firewall and antivirus software, but an important security update has not been installed. An attacker sends a specially crafted request to the hospital's web application and exploits the unpatched weakness. The attacker gains access to a staff account, copies confidential patient records, modifies several laboratory reports, and installs malicious software that slows down the hospital's network. During the incident, doctors could not access patient records for nearly three hours.			CO1
	a)	Explain the difference between cybersecurity and information security using two examples from the scenario.	[2]	
	b)	Identify how confidentiality, integrity, and availability were affected. Give one relevant example for each element of the CIA triad.	[3]	
	c)	In the context of this scenario, distinguish between vulnerability, exploit, threat, and impact. Then recommend two technical security controls that could have prevented or reduced the attack.	[5]	
2.	A financial organization receives an email that appears to come from its software vendor. The email claims that an urgent security update must be installed and includes a link to download a file named Security_Update.exe. An accounts officer downloads and runs the program using an administrator account. The program displays a normal installation window, but it secretly installs Malware. The Malware creates a hidden connection to an external command-and-control server whenever the computer connects to the internet. It also disables some security tools, records keystrokes, captures screenshots, steals saved browser credentials, and allows the attacker to browse and download files remotely. Using the stolen credentials, the attacker accesses the organization's internal file server and copies financial reports and customer information. The attacker then creates another user account and installs the RAT on two additional computers to maintain access. The activity continues unnoticed for several weeks, suggesting that the attacker is interested in long-term surveillance and data theft rather than immediate damage.			CO2
	a	Identify the main type of malware used in the incident and mention two characteristics that support your answer.	[2]	
	b)	Explain three malicious activities performed by the RAT after installation.	[3]	

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

	c)	Analyze how the attacker gained initial access, maintained persistence, and moved to other systems. Also discuss whether this incident may be considered part of an APT and recommend two security controls.	[5]	

3.	A university uses an online portal where students can view their own assignment submissions, marks, and instructor feedback. After logging in, a student opens the following request in the browser:
	
	GET /api/v1/submissions/5842
	
	The server returns the student's submission details. The student changes the number from 5842 to 5843 and receives another student's name, student ID, uploaded file, marks, and instructor comments. The student then notices that the portal sends the following request when an instructor updates a result:
	
	PATCH /api/v1/submissions/5843
	
	{
	"marks": 95,
	"status": "graded"
	}
	
	The student sends the same request using their own valid login session. The server accepts it and updates the other student's result. The application verifies that the requester is logged in, but it does not properly verify whether the requester owns the requested record or has permission to modify academic results. The student writes a script that sends requests using sequential submission numbers and successfully retrieves many student records. The same script can also modify selected marks.
			CO3

	a)	Identify the vulnerability demonstrated by the GET request and justify your answer.	[2]	
	b)	Identify three authorization weaknesses demonstrated by the PATCH request.	[3]	
	c)	Analyze how the weakness could be exploited at scale, describe its impact on confidentiality and integrity, and recommend three technical controls.	[5]	
4.	A security researcher analyzes WordPress source code and identifies two weaknesses that may be chained together. The researcher uses an advanced OpenAI model to review the code, test different attack paths, and help develop a working proof of concept named wp2shell. The combined weaknesses allow an unauthenticated attacker to send specially crafted API requests and execute commands on a vulnerable WordPress server. This could allow the attacker to install a web shell, steal data, modify website content, or take control of the server. The case demonstrates how AI can accelerate vulnerability analysis, exploit validation, and defensive security research.			**CO3**
	a)	Identify two cybersecurity tasks in which AI assisted the researcher.	[2]	
	b)	Explain three security consequences if the weakness is exploited against a vulnerable website.	[3]	
	c)	Analyze the benefits and risks of using advanced AI for vulnerability research. Recommend three controls for ensuring that such AI-assisted research is performed safely and ethically.	[5]	