ourdiu.com | Shared by Md Alif Rabbi

Daffodil International University

Faculty of Science & Information Technology

Department of Computer Science & Engineering

Midterm Examination, Fall 2026

Course Code: CSE454 , Course Title: Cyber Security and Forensics

Level: 4 Term: 2 Batch: 65

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.		You are the Chief Information Security Officer (CISO) for "MedData Hub," a healthcare analytics company. Your primary infrastructure includes a centralized cloud database that stores the highly sensitive Electronic Health Records (EHR) of over two million patients, including medical histories and social security numbers. Following a recent internal audit, your team discovers that a legacy external web portal, still connected to this database, is running on outdated software with a known vulnerability. This vulnerability could theoretically allow a remote attacker to bypass authentication protocols.		CO1
	a)	Define the terms Confidentiality, Integrity and Availability, including some technologies that are used to implement them.	[2]	
	b)	Explain how the vulnerability from the scenario above can lead to a breach of each of the CIA triad principles.	[3]	
	c)	Identify the asset, the risk, and the impact from the scenario, while defining each of these terms with respect to Cyber Security.	[5]	
2.	*a)*	Explain what you mean by the Cyber Threat Landscape. From your knowledge, mention some of the prevailing threats identified in the Global Cyber Threat Landscape.	[2]	CO1
	b)	While one security unit actively breached the company's network using simulated malware, a second unit simultaneously worked to detect, contain, and block the ongoing intrusion using their monitoring tools. Following the exercise, a third unit coordinated a joint debriefing session to directly integrate the attackers' successful tactics into the defenders' permanent security protocols. Apply your knowledge about the Color Wheel of Information Security and identify the Red, Blue and Purple Teams from the above scenario.	[3]	
3.	*a)*	The Transmission Control Protocol (TCP) is a connection-oriented standard that guarantees reliable, ordered data delivery by utilizing a three-way handshake, sequence numbers, acknowledgements, retransmissions, and flow control mechanisms. Analyze the protocol to explain two attacks targeting this protocol.	[4]	CO3

Syn Ack replis
Ack

ourdiu.com | Shared by Md Alif Rabbi

	b)	The Transport Layer Security (TLS) protocol is a cryptographic standard that ensures secure end-to-end network communication by utilizing a handshake process, cipher suite negotiation, asymmetric key exchange, digital certificates for authentication, symmetric encryption for data privacy, and message authentication codes for integrity. Demonstrate the server authentication process of TLS through digital certificates, with the help of proper diagrams and appropriate description. Also use this process to explain safety of the HTTPS protocol and how the users are informed about this safety.	[6]	