


Name: Enrolment No:			
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES Supplementary Examination, December 2023			
Course: Information Security Fundamentals Program: B. TECH (CSE) + CSF Course Code: CSSF 2001		Semester: 3rd Time: 03 hrs. Max. Marks: 100	
Instructions: (i) Exam is Close Book, (ii) Exchange of mobile phone, calculator or any other item is not allowed, (iii) Start answers to a new question on fresh page, (iv) All parts of a question should be answered together and (v) Scattered part answers will not be evaluated.			
SECTION A (5Qx4M=20Marks)			
S. No.		Marks	CO
Q 1	Compare and contrast the distinctive features of symmetric key cryptography and asymmetric key cryptography. Highlight their respective strengths, weaknesses, and common use cases in the field of cybersecurity.	4	CO1
Q 2	Define data leakage and elaborate on the methods used to detect and prevent it in a cybersecurity context. Discuss the role of encryption, access controls, and monitoring in mitigating the risks associated with data leakage.	4	CO2
Q 3	Examine the major differences between static and dynamic malware analysis. Provide an example of malware analysis for each approach and discuss the advantages and limitations of static and dynamic analysis in identifying and mitigating cyber threats.	4	CO5
Q 4	Explain the significance of continuous log disposal in the cybersecurity domain. Discuss the potential risks and security implications associated with neglecting log disposal practices.	4	CO3
Q 5	Explain the role of a firewall in network security. Compare and contrast stateful and stateless firewalls, outlining their functionalities, advantages, and potential limitations in protecting against cyber threats.	4	CO4
SECTION B (4Qx10M= 40 Marks)			
Q 6	Explain the role of multi-factor authentication (MFA) in strengthening user authentication processes. Compare different methods of implementing MFA, and discuss the advantages and challenges associated with each approach in enhancing overall cybersecurity.	10	CO2
Q 7	Explore the characteristics and motivations behind Advanced Persistent Threats (APTs). How do APTs differ from traditional malware attacks, and what strategies can organizations employ to detect and mitigate APTs?	10	CO1

Q 8	List and discuss common vectors for malware distribution. How can users protect themselves against malware infections through these vectors?	10	CO3 & CO4
Q 9	<p>Explain the importance of regular software updates in mitigating malware threats. Highlight the specific vulnerabilities that can be addressed through timely updates and patches.</p> <p style="text-align: center;">OR</p> <p>Consider a scenario where a web application is vulnerable to SQL injection attacks. Explain the potential risks associated with SQL injection and how an attacker might exploit this vulnerability.</p>	10	CO4 & CO5
SECTION-C (2Qx20M=40 Marks)			
Q 10	<p>a. Define phishing and discuss its role as a common method for malware delivery. Identify the indicators of phishing attempts and describe countermeasures to prevent falling victim to phishing attacks.</p> <p>b. Explain the concept of endpoint security in the context of malware prevention. Discuss different strategies and technologies used to secure endpoints from malware threats, and highlight their importance in overall cybersecurity.</p> <p>c. Define intrusion detection systems (IDS) and intrusion prevention systems (IPS) in the context of cybersecurity. Compare their functionalities and discuss how they contribute to the detection and prevention of various cyber threats, including malware.</p> <p>d. Discuss the significance of user education and awareness in the fight against malware. Outline key principles and best practices for educating users about cybersecurity, and explain how this contributes to a more resilient security posture.</p>	20	CO5
Q 11	<p>Explain the concept of a Feistel Network in the context of block cipher encryption. Design a simplified 4-round Feistel network, illustrating the data transformation process at each round. Additionally, discuss how the Feistel structure is employed in the Data Encryption Standard (DES) and provide a diagram to illustrate its application in DES encryption.</p> <p style="text-align: center;">OR</p> <p>Describe the concept of a zero-day vulnerability. Provide an example of a recent zero-day exploit, discuss the potential risks associated with such vulnerabilities, and outline strategies that organizations can employ to mitigate the impact of zero-day attacks.</p> <p>i. Identify and discuss the security implications of a zero-day vulnerability.</p> <p>ii. Explain the measures and best practices that developers can implement to prevent zero-day vulnerability and attacks in web applications.</p>	20	CO1, CO2 & CO4