1311E1121

Candidate's Seat No :_____

M.Sc. Sem.-3 Examination
501
Cyber Security & Forensics
November-2025

Time : 2-30 Hours] **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Explain the concept of Security Operations. Discuss its role in maintaining the overall cybersecurity posture of an organization. 7Marks

ii. Define Security and Control. How do control mechanisms contribute to strengthening an organization's security framework? 7Marks

OR

i. Discuss the trade-off between Reliability and Security. Provide real-world examples where improving one may impact the other. 7Marks

ii. Describe the basic components of a Security Operations Center (SOC). Explain how these components work together to detect and respond to incidents. 7Marks

Question 2 Answer the following questions:

i. Define Log Management. Explain its importance in maintaining computer and network security. 7Marks

ii. Explain the role of a Centralized Log Server in a log management system. What advantages does centralization offer over distributed logging? 7Marks

OR

i. What are the main objectives of Log Management Operations? Describe how logs are collected, normalized, and archived in a typical environment. 7Marks

ii. Explain the challenges of Log Management in large-scale enterprise environments. How can automation and SIEM tools help address these issues? 7Marks

Question 3 Answer the following questions:

i. Define SIEM (Security Information and Event Management). Explain its role in modern cybersecurity operations. 7Marks

ii. Differentiate between Logs and Events. How does a SIEM use both to detect and respond to security incidents? 7Marks

OR

i. List and describe various Log Formats. Discuss their advantages and common use cases. 7Marks

P.T.O

E 1121-2

ii. Discuss Aggregation and Normalization in SIEM systems. Why are these processes essential before analysis or correlation? 7Marks

Questions 4 Answer the following questions:

i. Explain the Purpose of an Incident Response Plan (IRP). Why is it critical for maintaining organizational security and business continuity? 7Marks

ii. Describe the Preparation phase of Incident Response. What proactive steps should an organization take before an incident occurs? 7Marks

OR

i. Discuss the importance of Communicating the Incident. Who should be notified, and what communication protocols should be followed? 7Marks

ii. Describe the process of Incident Classification and Investigation. What criteria are used to determine the severity and scope of an incident? 7Marks

Questions 5: Attempt any Seven out of Twelve. 14 Marks

1. What is the primary objective of a Security Operations Center?
2. Explain the term "sweet spot" in the context of security monitoring.
3. Define proactive monitoring in security operations.
4. What is the purpose of monitoring logs?
5. Name a technique for baseline establishment.
6. What is the purpose of feedback loop in monitoring?
7. Give one reason for documentation in SOC.
8. What does SOC infrastructure refer to?
9. Give one example of cloud security monitoring challenge.
10. What is system reliability?
11. What is on-premise infrastructure?
12. What is root cause analysis?

.....X.....X.....