6/71

1711E1311

Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

504

Cyber Security & Forensics (EA)

November-2025

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

Question 1 Answer the following questions:

i. Explain the definition, purpose, and overall importance of a Security Operations Centre in modern organizations. 7Marks

ii. Illustrate typical SOC architecture, outlining its main components and layout. 7Marks

OR

i. Compare the responsibilities of all SOC Tier analysts, giving relevant examples. 7Marks

ii. Describe the typical workflow for incident escalation in a SOC. 7Marks

Question 2 Answer the following questions:

i. Explain the role of SIEM tools in SOC operations; include their main features and advantages. 7Marks

ii. Elaborate on the basics of threat intelligence and how it supports proactive detection in the SOC. 7Marks

OR

i. Compare different types of log sources and their relevance in detecting security incidents. 7Marks

ii. Describe the process of log correlation and its significance in threat detection. 7Marks

Question 3 Answer the following questions:

i. Evaluate common challenges in implementing SOAR and automation in large SOCs. 7Marks

ii. Analyze the integration process of threat intelligence with SIEM, providing examples of use cases. 7Marks

OR

i. Explain threat actor profiling and discuss its significance in threat mitigation. 7Marks

ii. Discuss the importance of threat feed quality and timeliness for successful SOC monitoring. 7Marks

Questions 4 Answer the following questions:

i. Compare and contrast indicator-based (IOC) and behavioural-based (IOA) detection techniques in SOC. 7Marks

ii. Describe the structure and application of the MITRE ATT&CK framework in a 7Marks

P.T.O

SOC environment.

OR

i. Illustrate how SOC metrics can be used for continuous improvement of security operations. 7Marks

ii. Assess the role of reporting and documentation in achieving and maintaining SOCcompliance. 7Marks

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

1. Define a Security Operations Centre (SOC).
2. State any two primary objectives of a SOC.
3. List any two roles within a SOC.
4. Give an example of a log source in a SOC environment.
5. What is the purpose of integrating threat intelligence into SOC operations?
6. Define "correlation" in the context of SIEM.
7. What is SOAR in SOC operations?
8. What is a security playbook?
9. Provide example use case for automation in SOC.
10 Why are SOC metrics important?
11 What is meant by "reporting" in SOC operations?
12 List any two benefits of compliance for organizations.

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

1711E1311 –3 Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

504

Cyber Security & Forensics (EB)

November-2025

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

Question 1 Answer the following questions:

i. Explain the term Digital Forensics. Discuss its importance in modern criminal and cyber investigations. 7Marks

ii. Explain the different types of digital forensics with suitable examples. 7Marks

OR

i. Differentiate between volatile and non-volatile data with examples of each. 7Marks

ii. What is forensic imaging? Describe its types and purpose in an investigation. 7Marks

Question 2 Answer the following questions:

i. Describe the main file system structuresFAT, NTFS, EXT4, and HFS+highlighting one key forensic feature of each. 7Marks

ii. Write short notes on any four tools used for file carving in digital forensics. 7Marks

OR

i. Explain network forensics and discuss its core approachesreal-time monitoring, log analysis, and anomaly detection. 7Marks

ii. Define malware forensics. Explain the types of malwares based on their nature and behaviour. 7Marks

Question 3 Answer the following questions:

i. Explain Cloud Forensics. Discuss its importance and key challenges such as jurisdiction, multi-tenancy, and data volatility. 7Marks

ii. Explain the role of metadata and log correlation in the analysis of cloud forensic evidence. 7Marks

OR

i. Discuss the methods of IoT data acquisition — differentiate between non-intrusive (logical) and intrusive (physical) techniques. 7Marks

ii. Explain the phases of the APT attack lifecycle and the corresponding forensic focus at each stage. 7Marks

Questions 4 Answer the following questions:

i. Explain the best practices for evidence documentation during a digital forensicinvestigation. 7Marks

P.T.O

ii. Write short notes on any three famous digital forensic cases and the lessons learned from each. 7Marks

OR

i. What is the role of an expert witness in court? Describe how a forensic examiner presents digital evidence during testimony. 7Marks

ii. Explain the importance of documentation and the chain of custody in a digital forensic investigation. Why are these steps essential for court admissibility? 7Marks

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

1. What is Chain of Custody?
2. What is the main difference between live acquisition and dead acquisition?
3. What is meant by volatile data? Give one example.
4. What is file system forensics?
5. Define file carving in digital forensics.
6. Write the full form of FAT and NTFS.
7. What is the main purpose of network forensics?
8. What is Cloud Forensics?
9. Name any two challenges faced in cloud forensics.
10 What is meant by multi-tenancy in cloud environments?
11 What is a case study in digital forensics?
12 Name any two famous digital forensic cases.

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

1711E1311 –S Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

504 EC

Cyber Security & Forensics

Time : 2-30 Hours] November-2025 [Max. Marks : 70

Question 1 Answer the following questions:

i. Discuss various deployment models in cloud computing and compare their features. 7Marks

ii. Compare and contrast the security features offered by AWS, Azure, and Google Cloud. 7Marks

OR

i. Describe common cloud security threats and mitigation strategies. 7Marks

ii. Describe the importance and usage of API security in cloud services. 7Marks

Question 2 Answer the following questions:

i. Explain the fundamentals and importance of IAM in securing cloud environments. 7Marks

ii. Compare IAM tools and features across AWS, Azure, and Google Cloud. 7Marks

OR

i. Discuss how role-based access control (RBAC) improves access management in cloudcomputing. 7Marks

ii. Describe how OAuth and OpenID Connect are used for secure cloud access. 7Marks

Question 3 Answer the following questions:

i. Explain cloud security posture management (CSPM) and discuss its importance in moderncloud environments. 7Marks

ii. Compare AWS Config, Azure Security Center, and Prisma Cloud in terms of CSPM featuresand use cases. 7Marks

OR

i. Discuss the architecture and workflow of a cloud policy automation pipeline using tools likeOpen Policy Agent. 7Marks

ii. Discuss the challenges of policy and compliance drift in cloud platforms. 7Marks

Questions 4 Answer the following questions:

i. Explain the significance of cloud-specific compliance frameworks such as ISO 27017 and NISTSP 800-53. 7Marks

P.T.O

E1311-6

ii. Compare and contrast PCI DSS with other major cloud compliance standards. 7Marks

OR

i. Illustrate how security metrics and KPIs inform compliance management in cloudorganizations. 7Marks

ii. Assess the readiness of an enterprise for cloud compliance audits, suggesting improvementstrategies. 7Marks

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

1. Name one SLA metric commonly tracked in cloud agreements.
2. What is the difference between audit log and event log in the cloud?
3. What is meant by "cloud risk management"?
4. What is Azure Security Center used for?
5. Give one use of a Hardware Security Module (HSM).
6. Name a policy-as-code tool.
7. What is a group in IAM?
8. List any one best practice for IAM management.
9. Name a key difference between authentication and authorization.
10. Name any one Google Cloud security tool.
11. What is the main benefit of PaaS?
12. What is the difference between public and private cloud?

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