6/51

2811E835 Candidate's Seat No :________

M.Sc Sem-3 Examination

504

Cyber Security & Forensic (EA)

Time : 2-30 Hours] **November-2024** **[Max. Marks : 70**

Question 1 Answer the following questions:

i.	Explain the primary functions and objectives of a Security Operations Center (SOC) and its role in modern organizations.	7Marks
ii.	Explain how a SOC contributes to proactive cybersecurity measures and why it is critical for incident detection and response.	7Marks
	OR	
i.	Describe the architecture of a SOC, outlining the main components and their functions.	7Marks
ii.	Explain how SOCs align with an organization's broader cybersecurity strategy and business goals.	7Marks

Question 2 Answer the following questions:

i.	Explain how correlation rules and alerts are used in SIEM tools to detect suspicious activity and generate security alerts.	7Marks
ii.	Describe the process of configuring a SIEM tool in a SOC environment and the key steps involved in ingesting log data.	7Marks
	OR	
i.	Discuss the importance of log management in SOC operations, including the types of logs collected and how they are analyzed.	7Marks
ii.	Explain how SOC teams analyze logs from different sources to detect security incidents.	7Marks

Question 3 Answer the following questions:

i.	Describe the role of forensics in incident response and how it helps in investigating and mitigating security breaches.	7Marks
ii.	Explain the role of post-incident analysis in improving an organization's cybersecurity posture and reducing future risks	7Marks
	OR	
i.	Explain how SOCs handle multi-stage attacks (such as advanced persistent threats) and the importance of timely detection and response.	7Marks
ii.	Discuss how SOCs simulate and practice incident response procedures to ensure readiness in case of real security incidents.	7Marks

Questions 4 Answer the following questions:

i.	Explain the compliance requirements (e.g., GDPR, HIPAA) that SOCs must adhere to and their impact on SOC operations.	7Marks
ii.	Discuss the legal and regulatory issues SOCs need to consider when handling security incidents and responding to breaches.	7Marks

(P.T.O)

E835-2

OR

i. Discuss the key performance indicators (KPIs) and metrics that SOCs use to measure their performance and operational efficiency. 7Marks

ii. Describe the importance of regular SOC audits and assessments in maintaining compliance and operational effectiveness. 7Marks

Questions 5 Attempt any Seven out of Twelve.

14Marks

1. List any two key roles within a SOC.
2. What is the primary purpose of a SOC?
3. Automation in SOCs helps in:
   A. Minimizing human errors
   B. Conducting manual incident investigations
   C. Reporting data breaches to external authorities
   D. Auditing user access privileges
4. What are SOC metrics?
5. Incident analysis primarily focuses on:
   A. Documenting security policies
   B. Identifying the scope of the security breach
   C. Enhancing firewalls
   D. Updating antivirus software
6. What is incident mitigation in SOC?
7. Which phase involves removing the threat from the environment?
   A. Identification
   B. Containment
   C. Eradication
   D. Recovery
8. What does SIEM stand for in cybersecurity?
9. Which type of log is typically collected from firewalls?
   A. Network traffic logs
   B. Error logs
   C. Application logs
   D. Security event logs
10. What is a SIEM tool?
11. Which of the following is NOT a key role in a SOC?
    A. SOC Analyst
    B. SOC Manager
    C. Data Scientist
    D. Incident Responder
12. List any two types of logs that are important for SOC monitoring.

....X...X..

2811E835-3 Candidate's Seat No :________

M.Sc Sem-3 Examination

504

Cyber Security & Forensic (EB)

Time : 2-30 Hours] **November-2024** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Define digital forensics and provide a detailed explanation of its significance in modern cybercrime investigations. 7Marks

ii. Explain the various sub-disciplines of digital forensics and discuss their significance in modern criminal investigations. 7Marks

OR

i. How can the Indian legal frameworks, such as the Information Technology Act, 2000, and the Indian Evidence Act, 1872, be applied to justify the collection, preservation, and admissibility of digital evidence in court? Support your response examples. 7Marks

ii. Imagine you are a digital forensic investigator working on cybercrime case where crucial digital evidence needs to be presented in court. The defense challenges the admissibility of the evidence, arguing that it was not collected or preserved properly. 7Marks

Question 2 Answer the following questions:

i. Explain the role and importance of file systems in managing data on storage devices. Discuss how file systems control data storage and retrieval. 7Marks

ii. Explain the key techniques used in network traffic analysis, such as packet capture, flow data collection, and log analysis. How do these techniques contribute to understanding and improving network performance and security? 7Marks

OR

i. Explain the concept of memory forensics and its significance in digital investigations. 7Marks

ii. How does malware forensics contribute to understanding the attack vectors and impact of a cyberattack? 7Marks

Question 3 Answer the following questions:

i. Discuss the challenges forensic investigators face when dealing with the Internet of Things (IoT) device ecosystem. How do factors such as device heterogeneity, data volatility, and encryption impact the process of evidence collection and analysis? 7Marks

ii. Describe the key challenges faced in mobile forensics due to the variety of devices, operating systems, and security features. 7Marks

OR

i. Define cloud forensics and discuss its importance in digital investigations involving cloud environments. 7Marks

ii. Explain the process of data acquisition in mobile forensics and the difference between logical, file system, and physical acquisition. 7Marks

Questions 4 Answer the following questions:

i. **Scenario:** A company's internal network has been breached, and sensitive data has been exfiltrated to an unknown external IP address. 7Marks
Question: As a network forensic investigator, what steps would you take to identify the source of the breach and track the data exfiltration? What tools and techniques would be most effective in this investigation?

ii. **Scenario:** A mobile device was used to take photos at the robbery scene. The suspect claims the device wasn't in their possession at the time. 7Marks
Question: How would you use mobile forensics to determine when and where the photos were taken, and whether the suspect was using the device during the time of the crime?

(P.T.O)

E835-4

OR

i. **Scenario:** A company's mobile app development team discovers that one of their apps was compromised and distributed with malware embedded in the code, affecting thousands of users. 7Marks

Question: How would you approach the forensic analysis of the compromised mobile app? What methods would you use to identify the source of the malware injection, and how would you trace the impact on affected users?

ii. **Scenario:** A smart home system, including IoT-enabled security cameras and smart locks, is hacked, allowing an intruder to enter the home without authorization. 7Marks

Question: How would you conduct a forensic investigation to determine how the IoT devices were compromised? What specific data from the IoT devices would you examine to identify the method of entry and the attacker's activities?

Questions 5 Attempt any Seven out of Twelve. 14Marks

1. What is the first step in digital forensic investigations? Explain.
2. What was a significant development in digital forensics afterp the emergence of IoT devices?
   A. Development of live forensics techniques
   B. Creation of specialized forensic tools for IoT device analysis
   C. Use of artificial intelligence in forensic investigations
   D. Introduction of cloud-based forensic tools
3. What is metadata in the context of digital forensics?
4. What is the primary challenge of cloud forensics compared to traditional digital forensics?
   A. Access to the physical hardware
   B. Lack of network logs
   C. Availability of forensic tools
   D. Speed of analysis
5. What is file carving in digital forensics?
6. What is the key difference between static and dynamic malware analysis?
   A. Static analysis involves examining the malware code without execution, while dynamic analysis involves running the malware to observe its behavior.
   B. Static analysis focuses on network traffic, while dynamic analysis looks at file system changes.
   C. Static analysis is conducted in real-time, while dynamic analysis is delayed.
   D. Static analysis requires internet access, while dynamic analysis does not.
7. What kind of information would you expect to gather from volatile data during a forensic investigation?
8. Why is volatile data often a priority in live forensics investigations?
   A. It can be lost when the system is powered off or rebooted.
   B. It contains the most reliable evidence for long-term storage.
   C. It is always encrypted and needs immediate decryption.
   D. It is easier to collect than non-volatile data.
9. What is the primary goal of mobile application analysis in digital forensics?
10. Which of the following is a primary challenge in analyzing data from IoT devices in a forensic investigation?
    A. Encryption and proprietary data formats used by different devices
    B. The large storage capacities of IoT devices
    C. The inability to collect data without powering off the device
    D. The complexity of programming languages used in IoT
11. Which of the following techniques is commonly used to recover deleted data from mobile applications?
    A. Logical extraction
    B. Cloud-based acquisition
    C. Physical extraction
    D. Manual file searching
12. Which method is typically used for acquiring data from cloud services?

2811E835-5 Candidate's Seat No :________

M.Sc Sem-3 Examination

504

Cyber Security & Forensic (EC)

Time : 2-30 Hours] **November-2024** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Explain the public, private, and hybrid cloud deployment models, and discuss the advantages and challenges associated with each. 7Marks

ii. What are the major cloud security certifications and their importance for organizations using cloud services. 7Marks

OR

i. Describe the shared responsibility model in cloud computing, and explain the roles of cloud service providers and customers in ensuring security. 7Marks

ii. Explain the security features of AWS Cloud. How do these providers ensure data protection and compliance? 7Marks

Question 2 Answer the following questions:

i. Describe the concept of federated identity management in cloud environments and explain how it enables secure access to multiple systems with a single identity. 7Marks

ii. What IAM tools does AWS Cloud offer, and how do they compare in terms of functionality and security? Highlight their similarities and differences. 7Marks

OR

i. What are the key principles of Identity and Access Management (IAM) and its importance in securing cloud environments. 7Marks

ii. What is the concept of least privilege access in cloud IAM and why it is critical to cloud security 7Marks

Question 3 Answer the following questions:

i. Explain the importance of network segmentation in the cloud and how it can help mitigate security risks. 7Marks

ii. Describe the different types of data encryption used in the cloud and their role in data protection. 7Marks

OR

i. What are the challenges of securing cloud networks compared to on-premise networks, and what strategies can be used to ensure cloud infrastructure security? Describe key approaches for effective cloud security management. 7Marks

ii. Explain the importance of network security in the cloud and discuss the use of firewalls, VPNs, and security groups in securing cloud infrastructure. 7Marks

Questions 4 Answer the following questions:

i. Discuss the key compliance requirements that cloud providers and users must adhere to and explain how non-compliance can impact an organization. 7Marks

(P.T.O)

E835-6

ii. What strategies do cloud service providers use to manage and mitigate the effects of DDoS attacks? Describe key approaches and their effectiveness in protecting cloud infrastructure. 7Marks

OR

i. What are the challenges of responding to security incidents in the cloud, and explain how incident response differs in cloud and on-premises environments. 7Marks

ii. Explain the steps involved in a cloud incident response plan and the importance of each phase. 7Marks

Questions 5 Attempt any Seven out of Twelve. 14Marks

1. What is cloud security, and why is it essential for businesses?
2. AWS, Azure, and Google Cloud are examples of which type of cloud service provider?
   A. PaaS C. IaaS
   B. SaaS D. All of the above
3. Define the principle of least privilege in IAM and explain its importance in securing cloud resources.
4. What is the concept of a public cloud model?
5. Multi-Factor Authentication enhances security by:

   A. Requiring only a username and password
   B. Using two or more verification methods
   C. Limiting access to certain geographic locations
   D. Encrypting passwords
6. What is the concept of network access control lists in cloud security?
7. Describe the process of federated identity management in cloud environments and its benefits for secure access.
8. A Denial of Service (DoS) attack aims to:
   A. Secure cloud resources
   B. Increase application performance
   C. Overwhelm resources, making services unavailable
   D. Encrypt data in transit
9. Which compliance standard applies to protecting personal data in the European Union?
   A. HIPAA C. GDPR
   B. SOX D. PCI DSS
10. DDoS attacks on cloud infrastructure aim to:
    A. Encrypt cloud data
    B. Reduce latency
    C. Overwhelm cloud services
    D. Improve network speed
11. Define the role of a firewall in cloud security
12. What is the first step in an incident response plan?
    A. Containment
    B. Recovery
    C. Preparation
    D. Eradication