**LMS Questions for [DLBCSEEISC01\_D]**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 1/1 | 1 | What does CVE stand for? | Common Vulnerabilities and Exposures | Common Vulnerabilities and Exploits | Common Vulnerabilities and Events | Certified Vulnerabilities and Events |
| 1/2 | 2 | Which among the following layers deals with the data in the form of 0s and 1s? | Physical layer | Application layer | Session layer | Transport layer |
| 1/3 | 3 | Which among the following is correct for static detection? | Detection is possible even when the code is not executable | Identifies the vulnerability by executing the code | Expensive | Complex |
| 1/4 | 4 | Select the correct syntax for scanning vulnerabilities using nmap. | nmap -Pn --script vuln <IP address> | nmap -Pn --script vuln <MAC address> | nmap -Pn --script vu <Port address> | nmap -Pn --script vu <MAC address> |
| 1/5 | 4 | Which among the following is the GUI used for network mapper vulnerability scanning tool? | Zenmap | Netmap | Nessmap | Zuimap |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 2/1 | 1 | Which among the following is correct regarding Security Reference Architecture? | SRA has various abstraction levels and functionalities. | SRA do not represent logical security-relevant views of system architecture | Risk management strategy is not a matter of concern for SRA. | It is a standard that has rules on the product security. |
| 2/2 | 2 | Select the equation for quantifying residual risk. | Residual risk = Inherent Risks - Impact of Risk Controls | Residual risk = Inherent Risks \* Impact of Risk Controls | Residual risk = Inherent Risks + Impact of Risk Controls | Residual risk = Inherent Risks / Impact of Risk Controls |
| 2/3 | 3 | Which among the following is a security assurance requirement? | Configuration management | User Data Protection | Security Audit | Cryptographic Support |
| 2/4 | 4 | Evaluation Assurance Level is related to the standard … | Common Criteria | Federal Information Processing Standards | Trusted Computer System Evaluation Criteria | **Information Technology Security Evaluation Criteria** |
| 2/5 | 5 | Security is ensured in Information systems, through a two-step process known as… | Security Certification and Security Accreditation. | Security Components and Security Assurance. | Security Clearance and Security Allocation. | Security Confirmation and Security Alliance. |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 3/1 | 1 | Which of the following Intrusion Detection System is not a category based on the data source? | Anomaly-based IDS | Network-based IDS | Host-based IDS | Hybrid IDS |
| 3/2 | 2 | Signature-based detection methods are … | Using rules for identifying the intrusion. | Capable of detecting unknown attacks. | Capturing behavior through profiling. | Appropriate for large network. |
| 3/3 | 2 | Which among the following is not an Intrusion detection tool? | Wireshark | Zeek | Snort | Suricata |
| 3/4 | 3 | SIEM stands for… | Security Information and Event Management. | Security Issues and Event Monitoring. | Security Identification and Event Monitoring. | Security Invigilation and Event Measuring. |
| 3/5 | 3 | Most used ratio for training data and test data in machine learning-based IDS. | 80:20 | 50:50 | 90:10 | 60:40 |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 4/1 | 1 | Select the feature of Advanced Threat Protection that assesses and monitors the internal and external assets for identifying the vulnerabilities which cause a threat to the organization. | Attack Surface Management | File Analytics | Rich Threat Intelligence | Combination of detection and prevention |
| 4/2 | 1 | The main advantage of the static analysis is that… | it identifies the malicious presence by navigating through the file content like instructions, structure etc. | it executes the code and identifies the presence of malicious structures in it. | It consumes more time with a high cost irrespective of any other factors. | It runs in sandboxes for analyzing the hidden behaviour. |
| 4/3 | 2 | Which statement is wrong? | Sybil attacks use a single sensor node in the network to simultaneously act as multiple sensor networks. | Once the sybil identity gains most of the access to the system, it makes the network believe that redundancy is achieved. | A node replication attack involves the replication of a sensor node by copying the ID or key of an existing sensor node. | Active attack focus on the modification of packets within the wireless sensor networks. |
| 4/4 | 1 | Which among the following is correct for ATP? | Static analysis is a part of ATP. | ATP does not perform dynamic analysis. | File Analytics does not have any role in ATP. | False positive rate in ATP is high. |
| 4/5 | 3 | Indicators are … | technical artefacts that make the organizations aware about threats. | notifications received from bodies such as Product Security Incident Response Teams. | Used for sharing threat information across organizations | human-readable notifications that give information on vulnerabilities, exploits etc. |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 5/1 | 1 | Which one among the following is not a characteristic of Operational Data Store | Handles less data | More comprehensive reporting | Fault-tolerant | Less space consumption |
| 5/2 | 1 | ODS work similar to the ETL except the fact that… | extracted data is transformed and loaded to the final destination in ETL. | extracted data is directly loaded to the destination in ETL. | extracted data is transformed and loaded to the recipient in ODS. | extracted data is transformed slower than ODS in ETL. |
| 5/3 | 3 | NBA provides various capabilities to network administrators except… | Network intelligence | Network behaviour detection | Network troubleshooting | Network visibility |
| 5/4 | 6 | Which among the following is not a phase of NIST Incident Response Framework | Lessons Learned | Preparation | Containment | Eradication |
| 5/5 | 6 | The IRP framework SANS stands for ... | SysAdmin, Audit, Network, and Security | SysAdmin, Accredit, Netmask, and Security | SysAdmin, Accredit, Network, and Services | SysAdmin, Audit, Network, and Services |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 6/1 | 1 | As data is almost non-existent, its collection difficulty is very high in… | Level 1 | Level 2 | Level 3 | Level 4 |
| 6/2 | 1 | What is the metric type of Level 3 in security metric levels? | Implementation | Objectives-identified | Goal-oriented | Impact |
| 6/3 | 1 | Which among the following is a secondary stakeholder? | Inspectors General | Chief Information Officer | System Security Officer | Program Manager |
| 6/4 | 2 | Penetration test toolkit comprises of three assessments. Which one of the following is not part of it? | Green box testing | white box testing | grey box testing | black box testing |
| 6/5 | 2 | Which is the product line of Beyond Security that perform Black Box Fuzzing? | beSTORM | beSECURE | beSOURCE | beSTATIC |