ACCESS CONTROL AND RECOVERY INTERVIEW QUESTIONS

1.What are the main types of access control models?

Answer: The main types of access control models are discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC).

2.How does role-based access control (RBAC) work?

Answer: RBAC assigns permissions to roles rather than individual users. Users are then assigned to roles based on their job responsibilities, simplifying the management of permissions.

3.What is the principle of least privilege?

Answer: The principle of least privilege states that users should be granted the minimum level of access necessary to perform their job functions, reducing the risk of unauthorized access and data breaches.

4.What are security policies, and why are they important?

Answer: Security policies are formalized documents that outline an organization's security requirements, procedures, and guidelines. They are important because they provide a clear framework for maintaining security and ensuring compliance with regulations.

5.What is an access control list (ACL)?

Answer: An ACL is a list of permissions attached to an object (e.g., a file or directory) that specifies which users or system processes can access the object and what operations they can perform.

6.What is the purpose of a security audit?

Answer: A security audit is a comprehensive evaluation of an organization's information systems and processes to ensure they comply with security policies and regulatory requirements. It identifies vulnerabilities and suggests improvements.

7.What tools are commonly used for system security analysis?

Answer: Common tools include vulnerability scanners (e.g., Nessus, OpenVAS), penetration testing tools (e.g., Metasploit, Kali Linux), and log analysis tools (e.g., Splunk, ELK Stack).

8.What is the difference between vulnerability assessment and penetration testing?

Answer: A vulnerability assessment identifies and quantifies security vulnerabilities in a system, while penetration testing involves actively exploiting these vulnerabilities to evaluate the security posture of the system.

9.What is a threat model?

Answer: A threat model is a structured representation of potential threats to a system. It helps identify, prioritize, and mitigate security risks by understanding how an attacker could exploit vulnerabilities.

10.What is the purpose of log management in security analysis?

Answer: Log management involves collecting, analyzing, and storing logs from various systems and applications to detect security incidents, monitor system activity, and support forensic investigations.

11.What is system recovery?

Answer: System recovery involves restoring a system to a previous, functioning state after a failure or compromise. This process can include data restoration, reconfiguration, and software reinstallation.

12.What are the key components of a system recovery plan?

Answer: Key components include backup procedures, recovery point objectives (RPO), recovery time objectives (RTO), and detailed step-by-step recovery procedures.

13.How often should backups be performed for critical systems?

Answer: The frequency of backups depends on the organization's needs and RPO. Critical systems often require daily backups, or even more frequent backups, to minimize data loss.

14.What is the difference between full, incremental, and differential backups?

Answer: A full backup copies all data. An incremental backup copies only data that has changed since the last backup (full or incremental). A differential backup copies all data changed since the last full backup.

15.What are common methods for testing system recovery procedures?

Answer: Common methods include tabletop exercises, simulation exercises, and full-scale recovery drills. Regular testing ensures that recovery procedures are effective and that staff are familiar with them.

16.What is physical recovery in the context of IT security?

Answer: Physical recovery involves restoring the physical infrastructure and environment after a disaster or physical breach. This includes repairing hardware, restoring power, and ensuring the physical security of facilities.

17.What measures can be taken to protect physical IT assets?

Answer: Measures include securing data centers with controlled access, using surveillance cameras, implementing environmental controls (e.g., fire suppression, climate control), and ensuring robust physical barriers.

18.How does physical security complement cybersecurity measures?

Answer: Physical security prevents unauthorized physical access to hardware and facilities, which can protect against data theft, sabotage, and other forms of physical tampering that could compromise cybersecurity measures.

19.What is a disaster recovery plan (DRP)?

Answer: A DRP is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. It includes strategies for data recovery, system restoration, and continuity of operations.

20.What is fault tolerance in IT systems?

Answer: Fault tolerance refers to the ability of a system to continue operating properly in the event of a failure of some of its components. It often involves redundancy and failover mechanisms.