CLOUD COMPUTING INTERVIEW QUESTIONS

1.What is cloud computing?

Answer: Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

2.What are the different types of cloud computing deployment models?

Answer: The main deployment models are Public Cloud, Private Cloud, Hybrid Cloud, and Multi-Cloud.

3.What are the three primary service models of cloud computing?

Answer: The three primary service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

4.What is Infrastructure as a Service (IaaS)?

Answer: IaaS provides virtualized computing resources over the internet, allowing users to rent servers, storage, and networking infrastructure on a pay-as-you-go basis.

5.What is Platform as a Service (PaaS)?

Answer: PaaS provides a platform allowing customers to develop, run, and manage applications without dealing with the underlying infrastructure, which simplifies the development process.

6.What is Software as a Service (SaaS)?

Answer: SaaS delivers software applications over the internet, on a subscription basis, allowing users to access applications via a web browser without installing them locally.

7.What are container technologies?

Answer: Container technologies, like Docker, allow developers to package applications and their dependencies into a standardized unit for software development, ensuring consistency across multiple environments.

8.What is Kubernetes?

Answer: Kubernetes is an open-source platform designed to automate deploying, scaling, and operating application containers across clusters of hosts, providing container orchestration.

9.What is serverless computing?

Answer: Serverless computing allows developers to build and run applications without managing infrastructure. The cloud provider automatically provisions, scales, and manages the infrastructure required to run the code.

10.What are the advantages of serverless computing?

Answer: Advantages include reduced operational overhead, automatic scaling, cost efficiency (pay-per-use), and quicker time to market.

11.What are some common threats to cloud computing?

Answer: Common threats include data breaches, account hijacking, insecure APIs, Denial of Service (DoS) attacks, and data loss.

12.What is a Denial of Service (DoS) attack in cloud computing?

Answer: A DoS attack in cloud computing aims to overwhelm cloud services with excessive traffic, causing disruptions or making the service unavailable to legitimate users.

13.What is account hijacking in the context of cloud computing?

Answer: Account hijacking involves unauthorized access to cloud accounts, allowing attackers to steal sensitive information, manipulate data, or misuse cloud resources.

14.What is the typical methodology for hacking cloud environments?

Answer: The typical hacking methodology includes reconnaissance, gaining access, maintaining access, and covering tracks. In cloud environments, it also involves exploiting cloud-specific vulnerabilities like misconfigured cloud storage and insecure API endpoints.

15.How can attackers exploit insecure APIs in cloud environments?

Answer: Attackers can exploit insecure APIs by sending crafted requests to gain unauthorized access to cloud resources, extract data, or execute arbitrary commands.

16.What are some key cloud security techniques?

Answer: Key techniques include encryption, identity and access management (IAM), multi-factor authentication (MFA), regular security assessments, and implementing security policies and best practices.

17.Why is encryption important in cloud computing?

Answer: Encryption protects data by converting it into an unreadable format, ensuring that even if data is intercepted or accessed without authorization, it remains secure.

18.What is Identity and Access Management (IAM)?

Answer: IAM is a framework of policies and technologies for ensuring that the right individuals access the right resources at the right times for the right reasons, enhancing security and compliance.

19.What are some popular cloud security tools?

Answer: Popular tools include AWS Identity and Access Management (IAM), Microsoft Azure Security Center, Google Cloud Security Command Center, Cloudflare, and Palo Alto Networks Prisma Cloud.

20.How does multi-factor authentication (MFA) enhance cloud security?

Answer: MFA enhances security by requiring multiple forms of verification (e.g., password and a one-time code sent to a mobile device) before granting access, reducing the risk of unauthorized access.