**Cyber Security - Virtualization And Cloud Basics**

**1. What is virtualization and virtualization type?**

Virtualization is the process of creating a virtual version of physical hardware resources such as servers, storage, and networks.  
Types of virtualization:

* Server virtualization
* Storage virtualization
* Network virtualization
* Desktop virtualization
* Application virtualization

**2. Type of hypervisor and how to manage it?**

Hypervisors allow multiple virtual machines (VMs) to run on a single physical machine.  
Types:

* Type 1 (Bare-metal): Installed directly on hardware (e.g., VMware ESXi, Microsoft Hyper-V).
* Type 2 (Hosted): Runs on a host OS (e.g., Oracle VirtualBox, VMware Workstation).

Management:

* Use vSphere for VMware
* SCVMM for Hyper-V
* CLI tools or cloud platforms for others

**3. Roles of virtualization in cloud computing?**

* Efficient resource utilization
* Supports multi-tenancy
* Enables scalability and flexibility
* Facilitates disaster recovery
* Helps in cost reduction

**4. What is a container?**

A container is a lightweight, standalone, and executable software package that includes the application and all its dependencies. Containers share the host OS kernel but are isolated from each other (e.g., Docker).

5. What is high availability and live migration in virtualization?

* High Availability (HA): Ensures continuous availability of services by minimizing downtime using clustering and failover techniques.
* Live Migration: Moving a running VM from one host to another without downtime, useful for maintenance and load balancing.

6. Storage configuration – Describe block, file, and object storage. Also, DAS, NAS, and SAN

* Block Storage: Data is stored in fixed-sized blocks (e.g., HDD/SSD); used in databases and VMs.
* File Storage: Data is stored and accessed as files in folders (e.g., NFS, SMB).
* Object Storage: Data stored as objects with metadata and ID; ideal for unstructured data like images/videos (e.g., Amazon S3).

DAS, NAS, SAN:

* DAS (Direct Attached Storage): Storage directly connected to the server (e.g., internal HDD).
* NAS (Network Attached Storage): File-level storage shared over a network.
* SAN (Storage Area Network): High-speed block-level storage used in enterprise environments.

**7. Describe storage allocation and provisioning**

* Storage Allocation: Assigning specific amounts of storage to VMs or applications.
* Provisioning Types:
  + Thick provisioning: Full storage allocated in advance.
  + Thin provisioning: Allocates storage on-demand, conserving space.

CLOUD BASICS :

**1. Different types of cloud storage**

* **Public Cloud Storage** (e.g., Google Drive, AWS S3)
* **Private Cloud Storage** (in-house data centers)
* **Hybrid Cloud Storage** (combination of public and private)
* **Community Cloud Storage** (shared among organizations with common concerns)

**2. What is Role-Based Access Control (RBAC), Identity and Access Management (IAM), and MFA?**

* **RBAC:** Access rights based on roles assigned to users (e.g., admin, viewer).
* **IAM:** Framework for managing digital identities and permissions securely.
* **MFA (Multi-Factor Authentication):** Requires two or more verification methods (e.g., password + OTP).

**3. What is physical and virtual host allocation?**

* **Physical Host:** A real server providing compute resources.
* **Virtual Host:** A logical server running on a physical host using a hypervisor.  
  **Allocation:** Resources are distributed to VMs or containers based on workload.

**4. How to access resources of cloud computing?**

* Through **Web interfaces (console)**
* **APIs and SDKs**
* **Command Line Interface (CLI)**
* **Remote Desktop or SSH**

**5. Types of backup in cloud**

* **Full Backup:** Complete data backup.
* **Incremental Backup:** Backs up only the changed data since the last backup.
* **Differential Backup:** Backs up changes since the last **full** backup.
* **Snapshot Backup:** Image of the system at a specific time.

**6. What is disaster recovery?**

**Disaster Recovery (DR)** is a strategy for restoring IT systems, data, and operations after a disaster (natural or cyber attack), ensuring business continuity. It includes **backups**, **replication**, and **failover plans**.