Cyber Security – Virtualization and Cloud Basics

1. What is Virtualization?

Virtualization is the technology that allows multiple virtual machines (VMs) to run on a single physical machine. It helps in better resource utilization, cost reduction, and isolation between systems.

2. Types of Virtualization

• Server Virtualization – Multiple servers on one physical machine.
• Desktop Virtualization – Virtual desktops for users.
• Network Virtualization – Virtual networks using software.
• Storage Virtualization – Pooling physical storage resources.

3. What is a Hypervisor? Explain its Types

A hypervisor is software that creates and manages virtual machines.

• Type 1 (Bare Metal): Runs directly on hardware (e.g., VMware ESXi).
• Type 2 (Hosted): Runs on an operating system (e.g., VirtualBox).

4. Advantages of Virtualization in Cyber Security

• Safe testing environment
• Malware analysis using isolated VMs
• Snapshot and rollback capability
• Reduced hardware cost

5. What is Cloud Computing?

Cloud computing provides on-demand access to computing resources like servers, storage, and applications over the internet without direct hardware management.

6. Types of Cloud Deployment Models

• Public Cloud – Services offered over the internet (AWS, Azure).
• Private Cloud – Dedicated to one organization.
• Hybrid Cloud – Combination of public and private cloud.
• Community Cloud – Shared by organizations with common goals.

7. Cloud Service Models

• IaaS (Infrastructure as a Service)
• PaaS (Platform as a Service)
• SaaS (Software as a Service)

8. Role of Cloud in Cyber Security

Cloud platforms provide built-in security features such as encryption, IAM, monitoring, and DDoS protection. They help organizations scale security effectively.

9. Security Challenges in Virtualization and Cloud

- VM escape attacks
- Data breaches
- Misconfiguration
- Insider threats
- Compliance issues

10. Best Security Practices for Cloud and Virtualization

- Strong access control and IAM
- Regular patching and updates
- Encryption of data
- Network segmentation
- Continuous monitoring