Module -4

1-Resource Monitoring Techniques

- Performance Metrics Collection: Monitoring tools collect data on resource utilization, such as CPU load, memory usage, disk I/O, and network traffic.
- Alerts and Thresholds: Setting thresholds for resource consumption (e.g., CPU > 85% usage). Alerts can be triggered when these thresholds are crossed.
- Log Monitoring: Regularly reviewing logs for resource usage patterns. Tools like Splunk or ELK Stack (Elasticsearch, Logstash, Kibana) can assist with log aggregation and analysis.
- Real-Time Monitoring: Tools like Nagios, or Prometheus allow for real-time monitoring and visualization of system resources.
- Cloud Monitoring Tools: For cloud environments, services such as AWS CloudWatch, Azure Monitor, or Google Cloud Operations Suite track resource utilization on the cloud infrastructure.
- Capacity Planning and Forecasting: Predicting future resource needs based on historical data to avoid over-provisioning or resource starvation.
- Distributed Monitoring: In larger systems, distributed monitoring tools such as Datadog or New Relic help keep track of performance across multiple nodes or services.

2-How to access compute (windows and Linux) from internet? describe tools and its security

Accessing Windows Systems:

- Remote Desktop Protocol (RDP): Commonly used for Windows systems.
    - Security Measures:
        - Use Strong Passwords: Enforce password complexity.
        - Enable Network Level Authentication (NLA): Requires authentication before a full connection.
        - Use VPNs: To secure remote connections.
        - Two-Factor Authentication (2FA): Adds an extra layer of security.
        - Firewall Rules: Only allow RDP from specific IPs.

- PowerShell Remoting: For managing Windows systems remotely.
    - Security Measures:
        - SSL/TLS Encryption: For secure data transmission.
        - Limit Access with Role-Based Access Control (RBAC): Restrict actions based on the user's role.

Accessing Linux Systems:

- SSH (Secure Shell): Most commonly used for remote Linux access.
    - Security Measures:
        - Use SSH Key Authentication: Avoid password-based logins.
        - Disable Root Login: Prevent direct root access.
        - Enable Fail2Ban: Protect against brute-force attacks by blocking IP addresses after multiple failed login attempts.
        - Use Strong Passphrases for SSH Keys: Enhance SSH key security.
        - Firewall Rules: Limit access to specific IP addresses.
- Virtual Network Computing (VNC): An alternative to RDP for Linux systems (can be used with a GUI interface).
    - Security Measures:
        - Use SSH Tunneling: To secure the VNC traffic.
        - Password Protection: For accessing VNC servers.

3-Encryption Technologies and Methods

Types of Encryption:

- Symmetric Encryption: The same key is used for both encryption and decryption.
    - AES (Advanced Encryption Standard): One of the most widely used symmetric encryption algorithms.
    - 3DES (Triple DES): Uses three passes of DES encryption, but less secure than AES.
- Asymmetric Encryption: Uses a pair of public and private keys.
    - RSA (Rivest-Shamir-Adleman): A widely used asymmetric encryption algorithm.

    - ECC (Elliptic Curve Cryptography): Provides high security with smaller key sizes than RSA.
    - DSA (Digital Signature Algorithm): Used for digital signatures.
- Hashing: Converts data into a fixed-length value.
    - SHA-256: A secure hashing algorithm that is widely used in blockchain and certificate generation.
    - MD5: An older, now insecure, hash function.

Methods of Encryption:

- TLS/SSL (Transport Layer Security/Secure Sockets Layer): Used to encrypt data transmitted over networks, including HTTPS for web traffic.
- End-to-End Encryption: Ensures that data is encrypted on the sender's side and decrypted only on the recipient's side (e.g., in messaging apps like Signal).
- Full Disk Encryption (FDE): Encrypts all data on a storage device, protecting data even if the device is lost or stolen (e.g., BitLocker for Windows, FileVault for macOS).
- Database Encryption: Encrypting data within databases to protect it while stored. Methods like Transparent Data Encryption (TDE) are used in systems like SQL Server or Oracle.
- File-Level Encryption: Encrypts specific files or folders (e.g., using tools like VeraCrypt).

4-Describe network security in cloud, compute security and storage security

- Network Security in Cloud:

Cloud network security involves securing data in transit and managing access to cloud-based resources.

- Firewalls: Cloud providers like AWS, Azure, and Google Cloud provide Virtual Firewalls to control traffic flow between resources.
- Security Groups: Define which traffic is allowed to reach virtual machines, similar to firewalls.

- VPN and Direct Connect: Secure private network connections between on-premises networks and cloud environments.
- DDoS Protection: Tools like AWS Shield or Azure DDoS Protection mitigate distributed denial-of-service attacks.
- Identity and Access Management (IAM): Ensure that users and services have the least privilege required to access cloud resources.

Compute Security:

Compute security ensures the protection of virtual machines, containers, and other computing resources.

- VM Security: Virtual machine protection includes securing hypervisors, patching vulnerabilities, and configuring secure access controls.
- Container Security: Securing containers includes practices like scanning container images for vulnerabilities and running containers with limited privileges (e.g., Kubernetes RBAC).
- Endpoint Protection: Anti-malware software, firewalls, and intrusion detection systems protect cloud compute resources.
- Patching: Ensure that operating systems and software are regularly patched to fix vulnerabilities.
- Intrusion Detection and Prevention Systems (IDPS): Detect and prevent unauthorized access to compute systems.

Storage Security:

Storage security ensures that data stored in cloud environments is protected from unauthorized access, corruption, or loss.

- Encryption: As mentioned above, encryption (both at rest and in transit) is key to securing cloud storage.
- Access Control: Using role-based access control (RBAC) and identity-based authentication mechanisms to restrict access to data.
- Data Redundancy: Cloud providers typically offer automated backups and replication across multiple regions or availability zones.

- Data Integrity: Techniques like checksums, digital signatures, and hash functions ensure the integrity of stored data.
- Backup and Disaster Recovery: Cloud providers offer backup services (e.g., AWS S3 and Google Cloud Storage) with versioning, to prevent data loss.