**Day 20**





**“CLOUD SECURITY”**

**Best practices for managing IAM roles and users in AWS:**

1. Apply the Principle of Least Privilege

* Grant only the permissions needed for a user or role to perform their tasks.
* Avoid assigning broad permissions like AdministratorAccess unless absolutely necessary.

2. Use Roles Instead of Long-Term Access Keys

* For EC2 instances, Lambda functions, or other AWS services, use IAM roles instead of embedding credentials in code.

3. Enable MFA (Multi-Factor Authentication)

* Require MFA for all IAM users, especially those with console or administrative access.

4. Avoid Using the Root Account for Daily Tasks

* Use the root account only for initial setup and critical account-wide tasks.
* Create admin IAM users instead.

5. Rotate Access Keys Regularly

* Periodically change access keys and remove unused ones.
* Monitor for stale credentials in IAM.

6. Use IAM Groups to Manage Permissions

* Assign policies to groups, not directly to individual users, to simplify management.

7. Use Service Control Policies (SCPs) with AWS Organizations

* Restrict what accounts in your organization can do, even if users have high-level permissions.

8. Monitor and Audit IAM Activity

* Enable AWS CloudTrail to track IAM changes and log activity.
* Use AWS IAM Access Analyzer to detect overly broad access.

9. Tag IAM Resources for Management

* Use tags to identify owners, purpose, or environment for roles and users.

10. Regularly Review IAM Policies and Access

* Audit user access quarterly and remove unnecessary permissions or accounts**.**

**--**The End--