NAME: AMUDA RANTI

ROLE: CLOUD SECURITY ENGINEER

TASK: IAM Security Management in AWS

As a Cloud Security Professional, I designed and implemented a secure Identity and Access Management (IAM) system in AWS, demonstrating best practices in access control, least privilege enforcement, and Multi-Factor Authentication (MFA). This project showcases my ability to manage IAM effectively, ensuring security and compliance in cloud environments.

Key Responsibilities & Implementation

1. IAM Users & Groups Management

Created IAM users with role-based access control to minimize exposure to sensitive resources.

Organized users into groups (e.g., Admins, Developers, Auditors) to streamline permission management.

Assigned AWS Managed Policies where applicable and enforced the Principle of Least Privilege (PoLP).

2. Applying Least Privilege Access

Designed and implemented custom IAM policies to restrict unnecessary access.

Example: A policy allowing users to list S3 buckets but preventing deletion:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": "arn:aws:s3:::example-bucket"
        },
        {
            "Effect": "Deny",
            "Action": "s3:DeleteBucket",
            "Resource": "arn:aws:s3:::example-bucket"
        }
    ]
}
```

Ensured that only authorized personnel could access specific AWS resources.

3. Secure Role Management

Created IAM roles with well-defined permissions to grant temporary access to AWS services.

Example: An EC2 role with read-only S3 access.

Implemented cross-account access with IAM roles to enhance security and scalability.

4. Enforcing Multi-Factor Authentication (MFA)

Enabled MFA for all users accessing AWS Management Console.

Configured IAM policies to require MFA for high-privilege actions.

Enforced account-wide MFA compliance using AWS Security Hub and IAM Conditions.

5. Monitoring & Auditing IAM Activities

Activated AWS CloudTrail to log and track IAM actions.

Configured AWS Config rules to monitor IAM policy changes and flag violations.

Set up CloudWatch alarms to detect unauthorized access attempts and policy misconfigurations.

Key Takeaways & Impact

- Strengthened AWS security posture by implementing robust IAM best practices.
- Reduced risk by enforcing least privilege and MFA for all users.
- Ensured compliance with security standards through continuous monitoring and auditing.
- Demonstrated ability to design, implement, and manage IAM security effectively in AWS

This experience serves as a tangible proof of my expertise in AWS IAM security and showcases my ability to implement security best practices in a cloud environment.