Cloud Computing – Assignment 3

Muneel Haider 21i-0640
Abbas Ahsan 21i-2545

Recommendation #1: MFA on Root Account

What is the status?

The status is that MFA (Multi Factor Authentication) is not enabled on the AWS root account, which means the root account's only security is its username and password. This is a security risk.

What is the problem?

The problem is that without Multi Factor Authentication, the root accounts security is weak and is vulnerable to unauthorized access. This account has full rights and privileges, and the case of it being compromised, the entire AWS setup is breached.

What specific environment details are you given?

The environment detail provided is that the alert is triggered due to MFA not enabled on the AWS root account. This is a baseline check that applies to all AWS setups and environments where MFA is not enabled by the root user.

What is the best practice?

The best practice is to always enable MFA immediately after account creation. AWS also recommends to add additional security measures such that virtual or hardware MFA device for an extra layer of security.

What is the recommended action?

The recommended action to enable MFA as soon as you log in to the AWS root account.

Muneel Haider i21-0640
Abbas Ahsan i21-2545

Recommendation #2:
IAM Password Policy

What is the status?

The password policy for IAM users exists but lacks one or more key content requirements. This partial setup weakens the effectiveness of the policy and does not fully enforce strong password hygiene.

What is the problem?

When a password policy does not enforce all rules, such as requiring uppercase letters, numbers, or symbols, it becomes easier for attackers to guess or brute-force user passwords. This reduces the overall security of IAM-based authentication.

What specific environment details are you given?

The alert indicates that while a password policy is active, it fails to include at least one recommended setting. The system does not specify which requirement is missing, only that the policy is incomplete.

What is the best practice?

Best practice suggests implementing a comprehensive password policy that includes minimum length, use of uppercase, numbers, symbols, and expiration rules. This ensures IAM users are using strong and regularly updated credentials.

What is the recommended action?

You should review the existing IAM password policy and enable all recommended settings. If no policy is currently defined, create a new one that enforces strong password standards across all IAM users.

Muneel Haider i21-0640
Abbas Ahsan i21-2545

Recommendation #3:
Security Groups – Unrestricted Access

What is the status?

Security groups in two regions are allowing unrestricted access from any IP address on specific ports. This is a critical issue and marked with a high-risk indicator.

What is the problem?

Allowing unrestricted public access to sensitive ports, such as SSH (port 22) and web service ports (like 8080), exposes the infrastructure to unauthorized access attempts. This increases the likelihood of brute-force attacks or exploitation of unpatched services.

What specific environment details are you given?

In us-east-1, the WebServerSG security group allows inbound traffic on port 22 from all IP addresses. Similarly, in us-west-2, the DatabaseServerSG permits access to port 8080 from the public internet. These configurations use 0.0.0.0/0, which grants access from anywhere around the world.

What is the best practice?

It is strongly recommended to limit access to critical ports to trusted IP addresses only. Using specific IP ranges (e.g., /32 for a single IP) minimizes exposure and prevents unauthorized scanning or connection attempts.

What is the recommended action?

Update the security group rules to restrict access to only necessary and trusted IP addresses. Remove or modify rules that use 0.0.0.0/0 for ports like 22 and 8080, replacing them with targeted, secure ranges.

Muneel Haider i21-0640
Abbas Ahsan i21-2545

Recommendation #4: Amazon EBS Snapshots

What is the status?

An EBS volume currently in use does not have any associated snapshots. This lack of backup is marked with a critical warning.

What is the problem?

Without snapshots, there is no recovery point in case of data loss, corruption, or accidental deletion. This makes the system vulnerable to permanent data loss in the event of unexpected failures.

What specific environment details are you given?

The affected volume is located in the us-east-1 region, named “My-EBS-Volume.” It is currently attached to a resource, but there are no snapshot records—neither snapshot ID nor name is present.

What is the best practice?

The recommended approach is to take regular snapshots of EBS volumes, especially those used in production. Weekly or monthly snapshots provide a safety net for restoring data when issues arise.

What is the recommended action?

You should configure automatic snapshots for the volume through backup plans or lifecycle policies. At the very least, have a manual snapshot immediately to establish a recovery point.

Muneel Haider i21-0640
Abbas Ahsan i21-2545

Recommendation #5:
Amazon S3 Bucket Logging

What is the status?

Logging is not enabled for the S3 bucket in question, and necessary settings such as a logging target and appropriate write permissions are missing.

What is the problem?

Without logging, there is no visibility into access patterns or events for the bucket. This makes it difficult to audit user actions, investigate suspicious activity, or comply with security and compliance requirements.

What specific environment details are you given?

The bucket is located in the us-east-2 region and named “my-hello-world-bucket.” The logging target does not exist or is misconfigured, and the bucket lacks the proper ownership and permissions to enable logging.

What is the best practice?

It is a best practice to enable server access logging for S3 buckets, especially those storing important data. Logging should be directed to a target bucket within the same account that has proper write permissions.

What is the recommended action?

Set up a designated logging bucket with the correct permissions, and enable access logging on the original bucket. This allows AWS to track access requests and generate logs that can be used for monitoring and auditing.