

Cloud Pentesting Report

Client : [REDACTED] (Fictional Fintech Startup)

Assessment Dates Feb 10, 2025 Feb 24, 2025

Prepared by: Shoumik Chandra – Cybersecurity Consultant

Table of Content

1. Assessment Overview
2. Cloud Environment Summary
3. Scope of Engagement
4. Testing Methodology
5. Security Posture Overview
6. Key Security Strengths
7. Key Security Weaknesses
8. Vulnerability Summary
9. Technical Findings
10. Conclusion and Recommendations

Assessment Overview

This assessment was performed to evaluate the cloud security posture of [REDACTED] [REDACTED] AWS environment, focusing on identity management, storage security, networking configuration, and service-level hardening

Cloud Environment Summary

- **AWS Services in Use:** EC2, S3, IAM, RDS, Lambda, CloudTrail
- **Architecture:** Single VPC across 2 availability zones
- **Authentication:** IAM Users and Roles, SSO configured partially

Scope of Engagement

- EC2 instances and public interfaces
- S3 buckets
- IAM policies and roles
- CloudTrail logging
- Security Groups and Network ACLs
- RDS database security
- Lambda functions

Testing Methodology

- **External Attack Surface Mapping**
- **Configuration Review**
- **Privilege Escalation Testing**
- **Resource Misconfiguration Testing**
- **Identity & Access Management Review**
- **Public Exposure Analysis**

Tools used included: **ScoutSuite**, **Prowler**, **CloudSploit**, **AWS CLI**, manual inspection via AWS Console.

Cloud Security Posture Overview

Overall Risk Level: Moderate

Key Security Strengths

- CloudTrail is enabled across all regions
- Multi-Factor Authentication (MFA) enforced on root account
- Security Groups mostly follow least privilege
- S3 bucket versioning enabled

Key Security Weaknesses

- Unrestricted SSH access (0.0.0.0/0) on EC2 instances
- Publicly accessible S3 bucket without encryption
- Over-permissive IAM policies (":" actions allowed)
- RDS database not encrypted at rest
- Lambda functions with excessive permissions

Vulnerability Summary

Category	Critical	High	Medium	Low	Informational
Identity Management	0	1	0	0	0
Storage (S3/RDS)	0	1	0	0	0
Compute (EC2)	1	0	0	0	0

Technical Findings

11.1 Identity Management Findings

Finding 1: Over-Permissive IAM Policies (High)

- **Description:** Multiple IAM roles allowed `iam:*` actions across all resources.
- **Affected Resources:** 3 IAM Roles
- **Risk:** High — Privilege Escalation possible.
- **Tools Used:** ScoutSuite, AWS Console
- Evidence :



Policy snippet:

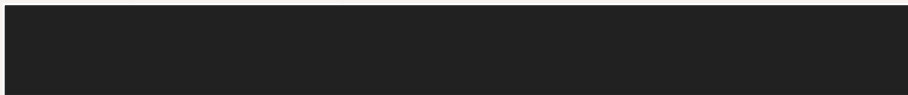
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Remediation: Replace wild-card permissions with specific allowed actions and define least-privileged roles.

11.2 Storage Findings

Finding 2: Public S3 Bucket without Encryption (High)

- **Description:** One S3 bucket (bucket-name: `customer-data-bucket`) is publicly accessible and has no encryption.
- **Affected Resources:** S3 Bucket
- **Risk:** High — Potential sensitive data exposure.
- **Tools Used:** AWS CLI, CloudSploit
- **Evidence:**



Bucket policy:

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::customer-records/*"
}
```

Bucket policy:

An error occurred (ServerSideEncryptionConfigurationNotFoundError)

Remediation:

- Remove public access via bucket policies or block public access settings.
- Enforce server-side encryption using AES-256 or KMS.

11.3 Compute Findings

Finding 3: EC2 Security Group Allows Open SSH (Critical)

- **Description:** Security Group `sg-12345` allows inbound SSH (port 22) from `0.0.0.0/0`.
- **Affected Resources:** EC2 Security Group
- **Risk:** Critical — Brute-force attack surface.
- **Tools Used:** AWS CLI, Prowler
- **Evidence:**



Output Snippet:



Remediation:

- Restrict SSH access to known IP addresses only.
- Consider using AWS Systems Manager Session Manager as a more secure alternative to direct SSH.

Conclusion and Recommendations

The AWS environment has a solid foundation but critical issues, mainly related to IAM over-privilege and public S3 buckets, must be addressed immediately. A regular cloud security assessment, tighter IAM role management, and encryption enforcement policies are recommended.