Pacu AWS Security Assessment Report

Date: 2025-04-17 11:39:11

Tool: Pacu (AWS exploitation framework)

Target: AWS Account used in assessment

# 1. IAM and Identity Enumeration

Modules run:  
- aws\_\_enum\_account  
- iam\_\_enum\_users\_roles\_policies\_groups  
- iam\_\_enum\_permissions  
- iam\_\_enum\_action\_query  
  
Findings:  
- Two IAM users and roles were found.  
- One customer-managed policy is in use.  
- No IAM groups detected.  
- Permission enumeration successfully collected user-level permissions.  
  
Recommendations:  
- Review IAM users and attached policies.  
- Follow the principle of least privilege.  
- Enable MFA for all users.

# 2. EC2 and Storage Reconnaissance

Modules run:  
- ec2\_\_enum  
- ebs\_\_enum\_volumes\_snapshots  
- rds\_\_enum  
- rds\_\_enum\_snapshots  
  
Findings:  
- EC2 instances and their attached volumes were enumerated.  
- Snapshot details retrieved.  
- Encryption status of snapshots reviewed.  
  
Recommendations:  
- Ensure all EBS volumes and snapshots are encrypted.  
- Audit RDS settings for public access.

# 3. Secrets and Sensitive Data

Modules run:  
- secrets\_\_enum  
- elasticbeanstalk\_\_enum  
- codebuild\_\_enum  
  
Findings:  
- Secrets Manager secrets were enumerated.  
- Elastic Beanstalk configurations retrieved.  
- CodeBuild projects checked for embedded secrets.  
  
Recommendations:  
- Rotate sensitive keys stored in secrets regularly.  
- Use environment variables in Beanstalk and CodeBuild.

# 4. Other Key AWS Services

Modules run:  
- s3\_\_enum  
- lambda\_\_enum  
- dynamodb\_\_enum  
- glue\_\_enum  
- apigateway\_\_enum  
  
Findings:  
- Buckets were discovered but may lack granular permission details.  
- Lambda functions retrieved.  
- No overly permissive API Gateway configuration found.  
  
Recommendations:  
- Harden S3 bucket policies (public read/write should be avoided).  
- Monitor Lambda access logs for abuse.  
- Validate DynamoDB access levels.

# 5. DNS, Logging, and Organization Setup

Modules run:  
- route53\_\_enum  
- elb\_\_enum\_logging  
- detection\_\_enum\_services  
- organizations\_\_enum  
  
Findings:  
- Route53 and ELB log configurations were reviewed.  
- Organization data was unavailable.  
- DNS and logging settings require configuration in some services.  
  
Recommendations:  
- Enable Route53 and ELB access logging.  
- Review and implement GuardDuty or similar tools.