Pacu Assessment Report

Generated on: 2025-04-17 11:36:45

Assessment Tool: Pacu

Assessment Focus: AWS IAM, EC2, RDS, Secrets, Network, and Logging Enumeration

# 1. Session Overview

- Session: finaltest  
- Users Enumerated: 2 (scoutsuite-user, cloudsploit-user)  
- IAM Roles: 2  
- Policies: 1 (Inline or Managed)  
- No IAM groups found.

# 2. Identity and Access Management

- The account has 2 users with distinct AWS keys used during enumeration.  
- IAM permission enumeration was successful, highlighting permissions tied to each user and roles.  
- Some users may have elevated privileges. Further manual privilege escalation checks are recommended.

# 3. Resource Enumeration

- EC2 and EBS volume information was gathered.  
- RDS instances and snapshots were analyzed.  
- Lambda, S3, Glue, and DynamoDB resources were queried.  
- Secret Manager and parameter store secrets enumeration completed.

# 4. Logging and Monitoring

- CloudTrail logging setup was assessed.  
- Route53 DNS zone enumeration executed.  
- GuardDuty configurations and ELB logging states reviewed.

# 5. Recommendations

- Review IAM policies for least-privilege enforcement.  
- Enable logging (CloudTrail, ELB access logs, Route53 query logs) across regions.  
- Encrypt all RDS and EBS snapshots.  
- Rotate AWS IAM credentials and consider MFA.  
- Regularly audit secrets and remove unused keys or credentials.