# PRACTICAL – 2

## Cloud Attack Lab – AWS Recon, Escalation & Exfiltration

### Objective

Identify misconfigured cloud services, escalate IAM permissions, and exfiltrate data covertly.

### Tools Used

AWS CLI, Pacu (Red Team Tool), CloudGoat (Scenario)

### Procedure

1. Listed all cloud S3 buckets
2. Found **public-read enabled bucket**
3. Downloaded confidential file
4. Enumerated IAM privileges
5. Escalated to **Administrator Role** using Assum eRole
6. Performed data exfiltration for proof-of-compromise

### Commands Executed

*aws s3 ls*
*aws s3api get-bucket-acl --bucket target-bucket*
*aws s3 cp s3://target-bucket/secret.txt ./loot/*
*pacu*
*run iam__enum_users*
*assume-role exploitAdmin*

### Recon Log

| Asset ID | Service | Misconfiguration | Risk Level | Notes |
|---|---|---|---|---|
| CLOUD-A01 | S3 Bucket | Public Read | High | Sensitive data exposed |

### Summary (50 Words)

Using AWS CLI and Pacu, I abused cloud misconfigurations to escalate privileges to an admin role and extract data. This shows how insecure IAM policies allow full compromise of cloud environments.