AWS IAM Privilege Escalation: Pacu for Security Assessment

By: Ritvik Indupuri

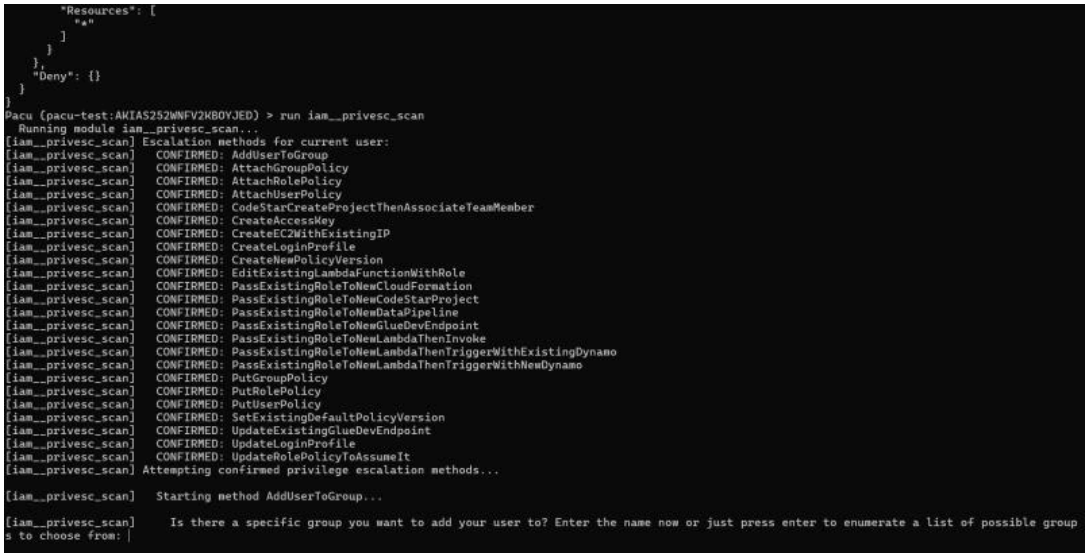
1. Executive Summary

This document provides a comprehensive overview of a security assessment conducted on an AWS Identity and Access Management (IAM) environment. The assessment, utilizing the open-source exploitation framework **Pacu**, aimed to identify and map potential privilege escalation paths. Our analysis successfully identified critical escalation vectors, uncovered high-risk IAM policies, and demonstrated real-world post-exploitation techniques. The findings highlight significant security vulnerabilities and underscore the importance of robust identity and access governance within cloud-native environments.

2. Methodology

The assessment was performed using **Pacu**, an open-source exploitation framework designed for AWS. The `iam__privesc_scan` module was the primary tool used to automatically identify potential privilege escalation paths from a compromised IAM user. This module systematically tested various methods, such as adding policies, creating access keys, and assuming roles, to confirm which vectors were viable for privilege escalation.

Figure 1: Pacu IAM Privilege Escalation Scan Output

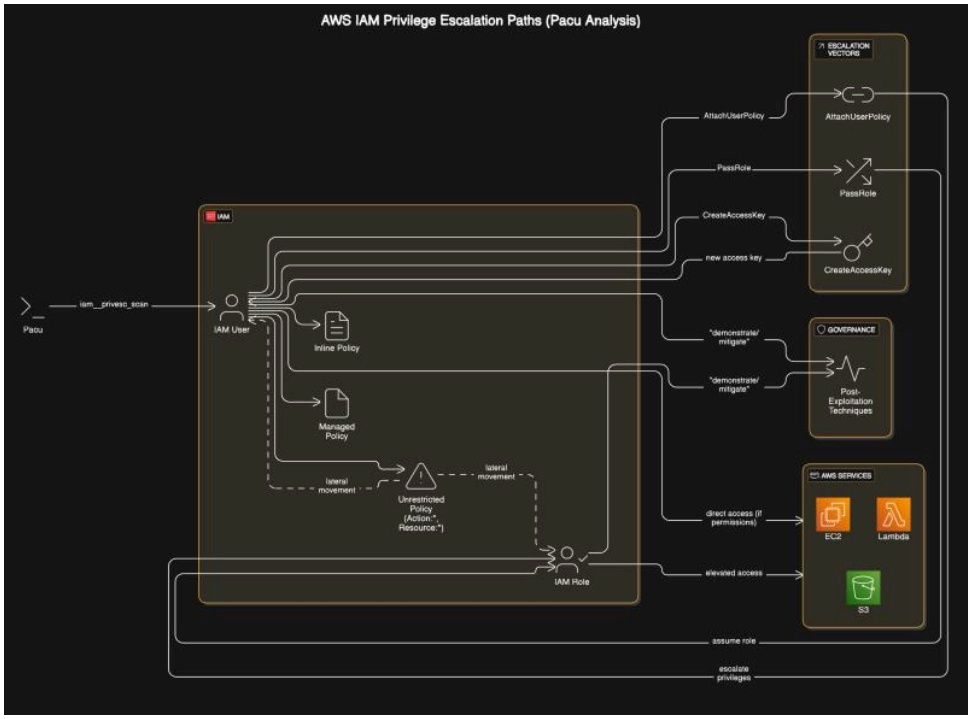


3. Identified Privilege Escalation Paths

Our analysis confirmed several critical privilege escalation paths, which were then mapped to provide a clear visualization of potential attack vectors. The primary vectors identified were:

- **AttachUserPolicy:** The ability to attach a new IAM policy to the compromised user, granting them additional permissions. This is a direct method of privilege escalation.
- **CreateAccessKey:** The ability to create new access keys for the current IAM user. This allows an attacker to generate new credentials, effectively creating a backdoor for persistent access to the account.
- **PassRole:** The ability to pass an IAM role to an AWS service (e.g., EC2 or Lambda). This allows the compromised user to leverage the permissions of the passed role, potentially escalating their privileges far beyond their initial scope.

Figure 2: AWS IAM Privilege Escalation Paths Architecture Diagram

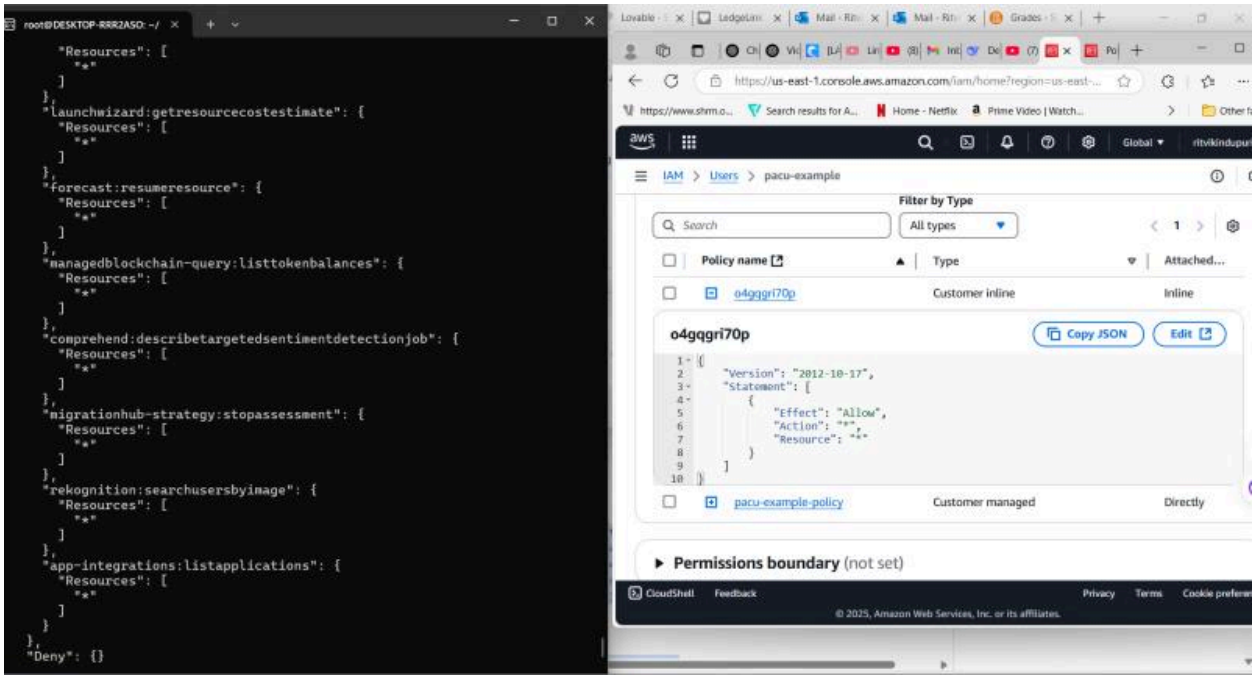


4. Analysis of High-Risk IAM Policies

During the assessment, a key finding was the presence of an inline IAM policy that granted unrestricted permissions. This policy, configured with `"Action": "*"` and `"Resource": "*"`, is an extremely high-risk configuration.

- **Unrestricted Access:** A policy with `"Action": "*"` and `"Resource": "*"` effectively grants a user or role administrative control over all resources within the account. This configuration is a significant security risk, as it provides a clear and direct path for an attacker to escalate privileges and perform lateral movement across the entire AWS environment.
- **Lateral Movement & Account Takeover:** An attacker who gains access to a user with such a policy can pivot to other services, compromise additional resources, and ultimately achieve a full account takeover. The policy acts as a "skeleton key," unlocking all doors within the AWS infrastructure.

Figure 3: AWS Management Console showing an Inline IAM Policy with unrestricted permissions



---

5. Post-Exploitation Techniques & Governance

The Privilege Escalation project not only showcased practical post-exploitation techniques, demonstrating the real-world impact of these vulnerabilities, but it also highlighted how attackers can create new access keys and attach new policies to escalate privileges and maintain persistent account control. This underscores the critical importance of robust identity and access governance.

- **Monitoring and Auditing:** It is crucial to implement continuous monitoring of IAM activity, specifically for actions like `CreateAccessKey`, `AttachUserPolicy`, and `PassRole`. Regular audits of IAM policies are also essential to identify and remediate overly permissive policies.
- **Principle of Least Privilege (PoLP):** The most effective mitigation strategy is to enforce the **Principle of Least Privilege**. Users and roles should only be granted the minimum permissions necessary to perform their specific tasks. This minimizes the blast radius of a compromised credential and makes privilege escalation significantly more difficult.
- **Permissions Boundaries:** Using IAM Permissions Boundaries can help enforce the maximum permissions an IAM entity can have, acting as a safeguard against malicious or accidental over-permissioning.

---

6. Conclusion

This project successfully leveraged the Pacu framework to identify and map critical privilege escalation paths within an AWS IAM environment. The findings underscore that misconfigurations, particularly overly permissive IAM policies, are a major source of security risk. To secure cloud-native environments, organizations must move beyond a perimeter-based security model and focus on strengthening identity and access governance. By enforcing the **Principle of Least Privilege** and implementing proactive monitoring and auditing, organizations can significantly reduce their exposure to privilege escalation attacks.
