IAM Enumeration with PACU (RhinoSecurityLabs)

Mastering AWS Identity and Access Management reconnaissance through systematic enumeration techniques

Overview

IAM enumeration forms the backbone of AWS security assessments, revealing the identity landscape that governs cloud resources. This walkthrough demonstrates how **PACU** (Principal Attack Collection Utility) transforms the complex task of IAM reconnaissance into a methodical, comprehensive process that uncovers critical security insights.

Understanding IAM permissions isn't just about collecting data, it's about mapping the pathways that define what's possible within an AWS environment. Every enumerated permission tells a story of access, privilege, and potential attack vectors that can make or break a security assessment.

Setting Up the Foundation

Configuring AWS CLI Profile

Before diving into PACU's capabilities, establishing proper AWS credentials creates the foundation for our enumeration journey. The AWS CLI profile acts as our gateway into the target environment.

```
┌──(kali㉿kali)-[~]
└─$ aws configure --profile cybr
AWS Access Key ID [****************NIHN]: AKIAQGYBPW3ZEI2GYNYP
AWS Secret Access Key [****************hCsa]: r96VeQ3yXU3AcyTTxGAP6
AN5mW64k8ruD/dmwu49
Default region name [us-east-1]: us-east-1
Default output format [json]: json
```

Key Insight: Notice how we're using a dedicated profile (`cybr`) rather than the default profile. This isolation prevents credential contamination and maintains clean separation between different assessment targets, a best practice that saves countless headaches during complex engagements.

Initializing PACU Session

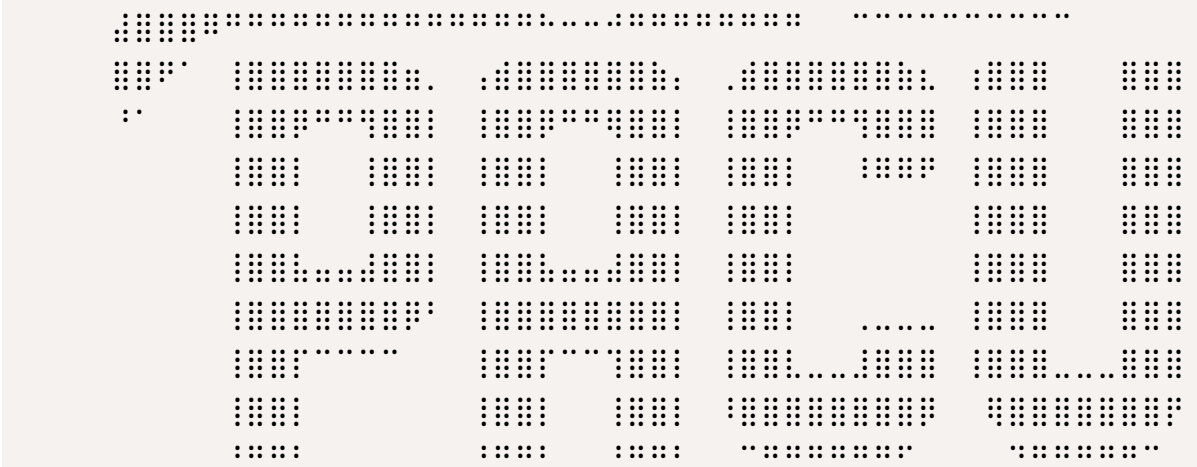
PACU's session management system ensures that enumeration data persists across multiple assessment phases, creating a comprehensive knowledge base that builds upon itself.

```
┌──(kali㉿kali)-[~]
└─$ pacu --new-session cybr
Session cybr created.
```

Launching PACU and Credential Import

Starting PACU Environment

```
┌──(kali㉿kali)-[~]
└─$ pacu
```



```
Version: unknown
Found existing sessions:
  [0] New session
  [1] cloudgoat
  [2] cybr
Choose an option: 2
```

Importing AWS Credentials

The credential import process seamlessly bridges AWS CLI profiles with PACU's enumeration capabilities, establishing the authentication context for our reconnaissance activities.

```
Pacu (cybr:No Keys Set) > import_keys cybr
  Imported keys as "imported-cybr"
Pacu (cybr:imported-cybr) > whoami
{
  "UserName": null,
  "RoleName": null,
  "Arn": null,
  "AccountId": null,
  "UserId": null,
  "Roles": null,
  "Groups": null,
  "Policies": null,
  "AccessKeyId": "AKIAQGYBPW3ZEI2GYNYP",
```

```
  "SecretAccessKey": "r96VeQ3yXU3AcyTTxGAP********************",
  "SessionToken": null,
  "KeyAlias": "imported-cybr",
  "PermissionsConfirmed": null,
  "Permissions": {
    "Allow": {},
    "Deny": {}
  }
}
```

Critical Observation: At this initial stage, PACU shows us the raw credential information without any context about the associated identity. The empty `UserName`, `RoleName`, and `Permissions` fields represent our starting point, a blank canvas that enumeration will progressively fill with valuable intelligence.

Permission Discovery Phase

Running IAM Permission Enumeration

The `iam__enum_permissions` module represents PACU's methodical approach to discovering what actions our credentials can perform within the AWS environment.

```
Pacu (cybr:imported-cybr) > run iam__enum_permissions
  Running module iam__enum_permissions...
[iam__enum_permissions] Confirming permissions for users:
[iam__enum_permissions]   introduction-to-aws-iam-enumeration-1760181664
157-Joel...
[iam__enum_permissions]     Confirmed Permissions for introduction-to-aws-i
am-enumeration-1760181664157-Joel
[iam__enum_permissions] iam__enum_permissions completed.

[iam__enum_permissions] MODULE SUMMARY:

  20 Confirmed permissions for user: introduction-to-aws-iam-enumeration-17
60181664157-Joel.
   0 Confirmed permissions for 0 role(s).
```

```
  0 Unconfirmed permissions for 0 user(s).
  0 Unconfirmed permissions for 0 role(s).
Type 'whoami' to see detailed list of permissions.
```

Strategic Insight: The enumeration discovered **20 confirmed permissions,** a substantial permission set that immediately signals this isn't a minimal-privilege account. This volume of permissions suggests either elevated access or a service account with broad IAM visibility, both scenarios worthy of deeper investigation.

Detailed Identity and Permission Analysis


```
Pacu (cybr:imported-cybr) > whoami
{
  "UserName": "introduction-to-aws-iam-enumeration-1760181664157-Joel",
  "RoleName": null,
  "Arn": "arn:aws:iam::014498641650:user/introduction-to-aws-iam-enumerati
on-1760181664157-Joel",
  "AccountId": "014498641650",
  "UserId": "AIDAQGYBPW3ZG3YO2STKD",
  "Roles": null,
  "Groups": [
    {
      "Path": "/",
      "GroupName": "introduction-to-aws-iam-enumeration-1760181664157-De
velopers",
      "GroupId": "AGPAQGYBPW3ZBWQ6SHJN4",
      "Arn": "arn:aws:iam::014498641650:group/introduction-to-aws-iam-enum
eration-1760181664157-Developers",
      "CreateDate": "Sat, 11 Oct 2025 11:21:08",
      "Policies": [
        {
          "PolicyName": "introduction-to-aws-iam-enumeration-1760181664157-d
evs-policy"
        }
      ]
    }
```

```
  ],
  "Policies": [
   {
    "PolicyName": "AllowEnumerateRoles"
   }
  ],
  "AccessKeyId": "AKIAQGYBPW3ZEI2GYNYP",
  "SecretAccessKey": "r96VeQ3yXU3AcyTTxGAP********************",
  "SessionToken": null,
  "KeyAlias": "imported-cybr",
  "PermissionsConfirmed": true,
  "Permissions": {
   "Allow": {
    "iam:listaccesskeys": {
     "Resources": [
      "arn:aws:iam::014498641650:user/introduction-to-aws-iam-enumeratio
n-1760181664157-Joel",
      "arn:aws:iam::014498641650:user/introduction-to-aws-iam-enumeratio
n-1760181664157-Mike"
     ]
    },
    "iam:getpolicy": {
     "Resources": ["*"]
    },
    "iam:listattacheduserpolicies": {
     "Resources": ["*"]
    },
    "iam:getpolicyversion": {
     "Resources": ["*"]
    },
    "iam:listgroupsforuser": {
     "Resources": ["*"]
    },
    "iam:listgrouppolicies": {
     "Resources": ["*"]
    },
```

```
    "iam:getuserpolicy": {
      "Resources": ["*"]
    },
    "iam:getgroup": {
      "Resources": ["*"]
    },
    "iam:listuserpolicies": {
      "Resources": ["*"]
    },
    "iam:listpolicyversions": {
      "Resources": ["*"]
    },
    "iam:listattachedgrouppolicies": {
      "Resources": ["*"]
    },
    "iam:listgroups": {
      "Resources": ["*"]
    },
    "iam:listattachedpolicies": {
      "Resources": ["*"]
    },
    "iam:getuser": {
      "Resources": ["*"]
    },
    "iam:listusers": {
      "Resources": ["*"]
    },
    "iam:getgrouppolicy": {
      "Resources": ["*"]
    },
    "iam:listrolepolicies": {
      "Resources": ["*"]
    },
    "iam:getrole": {
      "Resources": ["*"]
    },
```

```
      "iam:getrolepolicy": {
        "Resources": ["*"]
      },
      "iam:listroles": {
        "Resources": ["*"]
      }
    },
    "Deny": {}
  }
}
```

Deep Analysis Highlights:

1. **Identity Context:** We're operating as user `Joel` within account `014498641650`, with membership in the `Developers` group
2. **Permission Scope:** The wildcard (*) resources for most IAM actions indicate broad read access across the entire AWS account
3. **Security Implication:** These permissions enable comprehensive IAM reconnaissance, exactly what attackers need to map privilege escalation paths
4. **Notable Restriction:** The `iam:listaccesskeys` permission is limited to specific users (`Joel` and `Mike`), suggesting intentional scoping

---

Comprehensive IAM Landscape Enumeration

Expanding the Reconnaissance Scope

```
Pacu (cybr:imported-cybr) > run iam__enum_users_roles_policies_groups
  Running module iam__enum_users_roles_policies_groups...
[iam__enum_users_roles_policies_groups] Found 4 users
[iam__enum_users_roles_policies_groups] Found 14 roles
[iam__enum_users_roles_policies_groups] No Policies Found
[iam__enum_users_roles_policies_groups]   FAILURE: MISSING NEEDED PERMI
SSIONS
[iam__enum_users_roles_policies_groups] Found 2 groups
```

```
[iam__enum_users_roles_policies_groups] iam__enum_users_roles_policies_gr
oups completed.

[iam__enum_users_roles_policies_groups] MODULE SUMMARY:

  4 Users Enumerated
  14 Roles Enumerated
  0 Policies Enumerated
  2 Groups Enumerated
  IAM resources saved in Pacu database.
```

Enumeration Results Analysis:

- **4 Users:** A manageable user base suggesting either a small organization or a segmented environment
- **14 Roles:** Substantial role inventory indicating mature AWS usage with service integrations
- **0 Policies:** The permission failure here reveals a gap in our access, standalone policies require different permissions than attached policies
- **2 Groups:** Minimal group structure, suggesting either simple organization or role-based access patterns

---

Data Deep Dive and Intelligence Extraction

Examining the Complete IAM Dataset

The `data iam` command reveals the treasure trove of information our enumeration has collected:

```
Pacu (cybr:imported-cybr) > data iam
{
  "Groups": [
    {
      "Arn": "arn:aws:iam::014498641650:group/introduction-to-aws-iam-enum
eration-1760181664157-Developers",
      "CreateDate": "Sat, 11 Oct 2025 11:21:08",
      "GroupId": "AGPAQGYBPW3ZBWQ6SHJN4",
```

```
      "GroupName": "introduction-to-aws-iam-enumeration-1760181664157-Developers",
      "Path": "/"
    },
    {
      "Arn": "arn:aws:iam::014498641650:group/introduction-to-aws-iam-enumeration-1760181664157-Infrastructure",
      "CreateDate": "Wed, 31 Jul 2024 17:18:33",
      "GroupId": "AGPAQGYBPW3ZJVNLSC4EA",
      "GroupName": "introduction-to-aws-iam-enumeration-1760181664157-Infrastructure",
      "Path": "/"
    }
  ],
  "Policies": [],
  "Roles": [
    // Service-linked roles and custom roles...
  ],
  "Users": [
    {
      "Arn": "arn:aws:iam::014498641650:user/introduction-to-aws-iam-enumeration-1760181664157-Chris",
      "CreateDate": "Sat, 11 Oct 2025 11:21:10",
      "UserId": "AIDAQGYBPW3ZBMIA7K6HA",
      "UserName": "introduction-to-aws-iam-enumeration-1760181664157-Chris"
    },
    // Additional users: Joel, Mary, Mike...
  ]
}
```


Critical Security Findings and Attack Vectors

The **SupportRole** presents a critical privilege escalation opportunity because its assume role policy explicitly allows only the user `Mary` to assume this role. This creates a single high-value

target within the environment; compromising Mary's credentials or leveraging a flaw that allows role assumption as Mary effectively grants elevated access through the SupportRole.

> PS: The vulnerable SupportRole with its restrictive but critical assume role policy was identified in data retrieved from command `data iam`. This discovery highlights the importance of examining the full IAM dataset to uncover roles that serve as key privilege escalation targets within the AWS environment.


```
{
  "Arn": "arn:aws:iam::014498641650:role/SupportRole",
  "AssumeRolePolicyDocument": {
    "Statement": [
      {
        "Action": "sts:AssumeRole",
        "Condition": {
          "ArnEquals": {
            "aws:PrincipalArn": "arn:aws:iam::014498641650:user/introduction-to-
aws-iam-enumeration-1760181664157-Mary"
          }
        },
        "Effect": "Allow",
        "Principal": {
          "AWS": "arn:aws:iam::014498641650:root"
        }
      }
    ],
    "Version": "2012-10-17"
  },
  "CreateDate": "Sat, 11 Oct 2025 11:21:26",
  "Description": "Assumable role for internal support",
  "MaxSessionDuration": 3600,
  "Path": "/",
  "RoleId": "AROAQGYBPW3ZK4FCSE3HF",
  "RoleName": "SupportRole"
}
```

High-Value Targets Identified

1. **SupportRole with Conditional Access**: The `SupportRole` can only be assumed by user `Mary`, creating a clear privilege escalation target
2. **Cross-Account Trust Relationships**: Multiple roles trust external account `174005215664`, indicating federation or cross-account access patterns
3. **Service Integration Footprint**: Extensive AWS service roles reveal the organization's technology stack and potential lateral movement opportunities

Privilege Escalation Pathways

- **Target Mary's Credentials**: Compromising Mary's account grants access to the `SupportRole`
- **Cross-Account Enumeration**: The trusted external account represents an expanded attack surface
- **Service Role Exploitation**: Service-linked roles may have permissions beyond their intended scope

Reconnaissance Intelligence

- **Organization Structure**: The `Developers` and `Infrastructure` groups suggest team-based access patterns
- **Environment Age**: Creation dates reveal both recent setup (October 2025) and established infrastructure (July 2024)
- **Compliance Posture**: Presence of GuardDuty, CloudTrail, and support roles indicates security-conscious environment

---

Key Takeaways and Next Steps

This IAM enumeration exercise demonstrates the power of systematic reconnaissance in AWS environments. **PACU transforms what could be dozens of manual API calls into a streamlined intelligence-gathering operation** that reveals not just what exists, but how those resources interconnect to create security opportunities.

What We've Accomplished

✅ **Mapped the complete IAM landscape** of users, roles, groups, and their relationships

✅ **Identified specific privilege escalation targets** through role assumption analysis

✅ **Discovered cross-account trust relationships** that expand our potential attack surface

✅ **Documented comprehensive permission sets** that inform our next reconnaissance phases

Strategic Next Steps

1. **Enumerate Specific User Policies**: Focus on users like Mary who have special role assumptions
2. **Cross-Account Investigation**: Research the trusted account `174005215664` for additional attack vectors
3. **Service Role Deep Dive**: Investigate whether service roles have excessive permissions
4. **Credential Hunting**: Look for hardcoded credentials in code repositories or configuration files
5. **Lateral Movement Planning**: Use the service footprint to identify potential compromise targets

Remember: **effective cloud security assessment isn't just about finding vulnerabilities, it's about understanding how identity, permissions, and resources create pathways that determine what's possible within the environment.** This IAM enumeration provides the foundation map for everything that follows.

Continue building your AWS security expertise by practicing these techniques in controlled lab environments and always ensure proper authorization before conducting security assessments.