



5. Cloud Privilege Abuse Simulation Activities:

- **Tools:** Pacu, awscli, ScoutSuite.
- **Tasks:** Simulate privilege abuse in a cloud environment.

UserAInfoDelete

Summary

ARN
arn:aws:iam::767397746680:user/UserA

Console access
Disabled

Created
September 11, 2025, 14:37 (UTC+05:30)

Access key 1
AKIA3FLDYK74ICM2LS6N - Active
Never used. Created today.

Access key 2
Create access key

Permissions

Groups (1)

Tags (1)

Security credentials

Last Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

All types

Search

Policy name

Type

Attached via

AmazonEC2ContainerRegistryPowerUser

AWS managed

Group GroupA

UserBInfoDelete

Summary

ARN
arn:aws:iam::767397746680:user/UserB

Console access
Disabled

Created
September 11, 2025, 14:37 (UTC+05:30)

Access key 1
AKIA3FLDYK74FI4XXOFX - Active
Never used. Created today.

Access key 2
Create access key

Permissions

Groups (1)

Tags (1)

Security credentials

Last Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

All types

Search

Policy name

Type

Attached via

AmazonS3FullAccess

AWS managed

Group GroupB



- **Brief:**

- Privilege Abuse: Exploit a service principal or cross-tenant misconfiguration in AWS. Log:

Attack ID	Service	Misconfiguration	Notes
-----	-----	-----	-----
AID002	IAM	Overprivileged role	Escalated to admin

```
(root@kali)-[/home/kali/Desktop]
# aws iam list-attached-user-policies --user-name UserA
{
  "AttachedPolicies": [
    {
      "PolicyName": "IAMReadOnlyAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/IAMReadOnlyAccess"
    }
  ]
}
```

```
(root@kali)-[/home/kali/Desktop]
# aws iam list-attached-user-policies --user-name UserB
{
  "AttachedPolicies": [
    {
      "PolicyName": "IAMReadOnlyAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/IAMReadOnlyAccess"
    }
  ]
}
```



Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual | **JSON** | Actions ▾ |

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "iam:ListAttachedUserPolicies",
7       "Resource": "arn:aws:iam::767397746688:user/UserA"
8     }
9   ]
10 }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

Summary: Write a 50-word privilege abuse summary.

In the preceding example, UserA, a member of GroupA with EC2 full access permission and IAMreadonlyaccess, wishes to access UserB, a member of GroupB with IAMreadonlyaccess and S3access permission. If UserB has the aforementioned cross-tenant policy, UserA will be able to access the resources.