Lesson 12 Demo 02

Securing Terraform Credentials Using Checkov

Objective: To scan and secure Terraform credentials file using Checkov for ensuring security in Terraform

Tools required: Visual Studio Code

Prerequisites: Ensure you have created and implemented the AWS access key and secret key before starting this demo. Refer to Lesson 08, Assisted Practice 02, for detailed steps.

Steps to be followed:

1. Install Checkov
2. Set up credentials.tf
3. Review credentials.tf using Checkov

Step 1: Install Checkov

1.1 Make necessary updates using the following command:
sudo apt update

```
sakshiguptasimp@ip-172-31-22-2:~/demo$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 https://download.docker.com/linux/ubuntu jammy InRelease
Ign:6 https://pkg.jenkins.io/debian-stable binary/ InRelease
Hit:7 https://pkg.jenkins.io/debian-stable binary/ Release
Hit:8 https://deb.nodesource.com/node_14.x jammy InRelease
Hit:5 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.28/deb  InRelease
Get:9 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1824 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [329 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [2135 kB]
Hit:13 https://ppa.launchpadcontent.net/ansible/ansible/ubuntu jammy InRelease
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [364 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1102 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [256 kB]
Get:18 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1616 kB]
Get:19 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [272 kB]
Get:20 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2079 kB]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [355 kB]
Fetched 10.6 MB in 2s (4762 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
91 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

1.2 Ensure **pip** is installed by using the following command:

sudo apt install python3 python3-pip

```
sakshiguptasimp@ip-172-31-22-2:~/demo$ sudo apt install python3 python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.10.6-1~22.04).
python3 set to manually installed.
python3-pip is already the newest version (22.0.2+dfsg-1ubuntu0.4).
0 upgraded, 0 newly installed, 0 to remove and 91 not upgraded.
```

1.3 Install **Checkov** using the following command:

pip install checkov

```
sakshiguptasimp@ip-172-31-22-2:~/demo$ pip install checkov
```

```
n PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
  WARNING: The script bc_jsonpath_ng is installed in '/home/sakshiguptasimp/.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.
  WARNING: The scripts pyspdxtools and pyspdxtools3 are installed in '/home/sakshiguptasimp/.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.
  WARNING: The script policy_sentry is installed in '/home/sakshiguptasimp/.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.
  WARNING: The scripts detect-secrets and detect-secrets-hook are installed in '/home/sakshiguptasimp/.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.
  WARNING: The script openai is installed in '/home/sakshiguptasimp/.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.
  WARNING: The script jsonschema is installed in '/home/sakshiguptasimp/.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.
  WARNING: The script cloudsplaining is installed in '/home/sakshiguptasimp/.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 aiodns-3.2.0 aiohttp-3.9.5 aiomultiprocess-0.9.1 aiosignal-1.3.1 annotated-types-0.7.0 argcomplete-3.4.0 async-timeout-4.0.3 a
ttrs-23.2.0 bc-detect-secrets-1.5.15 bc-jsonpath-ng-1.6.1 bc-python-hcl2-0.4.2 beartype-0.18.5 beautifulsoup4-4.12.3 boolean.py-4.0 boto3-1.34.25 bot
ocore-1.34.25 cached-property-1.5.2 cachetools-5.4.0 cffi-1.16.0 charset-normalizer-3.3.2 checkov-3.2.190 click-8.1.7 click-option-group-0.5.6 clouds
plaining-0.6.2 configargparse-1.7 contextlib2-21.6.0 cyclonedx-python-lib-6.4.4 decorator-5.1.1 defusedxml-0.7.1 docker-7.1.0 dockerfile-parse-2.0.1
dpath-2.1.3 frozenlist-1.4.1 gitdb-4.0.11 gitpython-3.1.43 importlib-metadata-7.2.1 isodate-0.6.1 jmespath-1.0.1 jsonschema-4.23.0 jsonschema-specifi
cations-2023.12.1 junit-xml-1.9 lark-1.1.9 license-expression-30.3.0 markdown-3.6 multidict-6.0.5 networkx-2.6.3 numpy-2.0.0 openai-0.28.1 packageurl
-python-0.13.4 packaging-23.2 ply-3.11 policy-sentry-0.12.15 prettytable-3.10.2 py-serializable-1.1.0 pycares-4.4.0 pycep-parser-0.4.1 pycparser-2.22
 pydantic-2.8.2 pydantic-core-2.20.1 pyston-2.3.5 pyston-autoload-2.3.5 python-dateutil-2.9.0.post0 pyyaml-6.0.1 rdflib-7.0.0 referencing-0.35.1 rege
x-2024.5.15 requests-2.32.3 rpds-py-0.19.0 rustworkx-0.13.2 s3transfer-0.10.2 schema-0.7.5 semantic-version-2.10.0 smmap-5.0.1 sortedcontainers-2.4.0
 soupsieve-2.5 spdx-tools-0.8.2 tabulate-0.9.0 termcolor-2.3.0 tqdm-4.66.4 typing-extensions-4.12.2 unidiff-0.7.5 uritools-4.0.3 wcwidth-0.2.13 yarl-
1.9.4
sakshiguptasimp@ip-172-31-22-2:~/demo$
```

Step 2: Set up credentials.tf

2.1 Create a Terraform credentials file using the following command:

vi credentials.tf

```
sakshiguptasimp@ip-172-31-22-2:~/demo$ vi credentials.tf
sakshiguptasimp@ip-172-31-22-2:~/demo$
```

2.2 Set up **credentials.tf** by adding the following code:

```
provider "aws" {
 access_key = var.AWS_ACCESS_KEY
 secret_key = var.AWS_SECRET_KEY
 region     = "us-west-2"
}

variable "AWS_ACCESS_KEY" {}
variable "AWS_SECRET_KEY" {}
```

2.3 Set environment variables using the following command:

```
export AWS_ACCESS_KEY=AKIA5FR7SGZJLJGRZ5XY
export AWS_SECRET_KEY=ojnq/QIuoINe3bLDHwcDYI1iKn+3+6GVc18X+aoB
```

Note: Replace the access key and secret key with your actual values

Step 3: Review credentials.tf using Checkov

3.1 Find the directory path containing Checkov using the following command:
find $HOME/.local/bin -name checkov

```
sakshiguptasimp@ip-172-31-22-2:~/demo$ find $HOME/.local/bin -name checkov
/home/sakshiguptasimp/.local/bin/checkov
```

3.2 Run the following command to review the **credentials.tf** file:
$HOME/.local/bin/checkov -f credentials.tf

```
sakshiguptasimp@ip-172-31-22-2:~/demo$ $HOME/.local/bin/checkov -f credentials.tf
[ terraform framework ]: 100%|                    |[1/1], Current File Scanned=credentials.tf
[ secrets framework ]: 100%|                      |[1/1], Current File Scanned=credentials.tf

       _               _
   ___| |__   ___  ___| | _______   __
  / __| '_ \ / _ \/ __| |/ / _ \ \ / /
 | (__| | | |  __/ (__|   < (_) \ V /
  \___|_| |_|\___|\___|_|\_\___/ \_/

By Prisma Cloud | version: 3.2.190

terraform scan results:

Passed checks: 1, Failed checks: 0, Skipped checks: 0


        PASSED for resource: aws.default
        File: /credentials.tf:1-5
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/secrets-policies/bc-aws-secrets-5

sakshiguptasimp@ip-172-31-22-2:~/demo$
```

As shown in the above screenshot, **credentials.tf** has passed the checks.

By following these steps, you have successfully scanned and secured the Terraform credentials file using Checkov for ensuring security in Terraform.