Lab Exercise 18- Scanning IaC Templates for Vulnerabilities

Objective

- Learn how to scan Infrastructure as Code (IaC) templates for security vulnerabilities.
- Use open-source IaC security tools to detect misconfigurations.
- Understand common risks such as public access, unencrypted resources, and insecure network rules.

Prerequisites

- A Linux/Windows/Mac machine with:
  - Terraform installed (for sample IaC)
  - **Checkov** (pip install checkov) or **tfsec** (brew install tfsec or binary download)
- Git installed (optional, for version control of IaC templates)

```
D:\Terraform\.terraform>pip show checkov
Name: checkov
Version: 3.2.471
Summary: Infrastructure as code static analysis
Home-page: https://github.com/bridgecrewio/checkov
Author: bridgecrew
Author-email: meet@bridgecrew.io
License: Apache License 2.0
Location: C:\Users\DELL\AppData\Local\Programs\Python\Python313\Lib\site-packages
Requires: aiodns, aiohttp, aiomultiprocess, argcomplete, asteval, bc-detect-secrets, bc-jsonpath-ng, bc-python-hcl2, boto3, cachetools,
charset-normalizer, click, cloudsplaining, colorama, configargparse, cyclonedx-python-lib, docker, dockerfile-parse, dpath, gitpython, i
mportlib-metadata, jmespath, jsonschema, junit-xml, license-expression, networkx, packageurl-python, packaging, prettytable, pycep-parse
r, pydantic, pyyaml, requests, rustworkx, schema, spdx-tools, tabulate, termcolor, tqdm, typing-extensions, urllib3, yarl
Required-by:

D:\Terraform\.terraform>checkov --version
3.2.471
```

Step 1: Create an Insecure IaC Template

Create a file named main.tf with the following Terraform code:

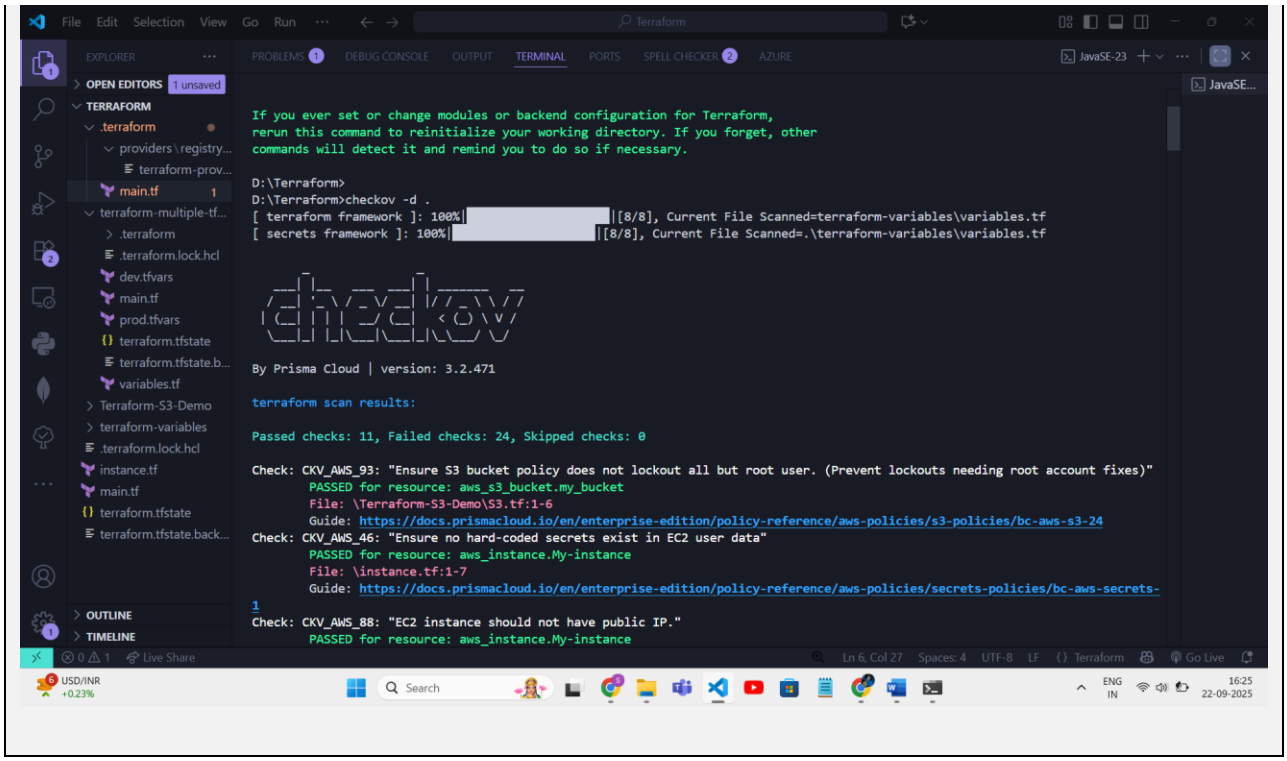
```
provider "aws" {

  region = "us-east-1"

}

resource "aws_s3_bucket" "insecure_bucket" {

  bucket = "my-insecure-bucket-lab"

  acl    = "public-read"

}

resource "aws_security_group" "insecure_sg" {

  name        = "insecure-sg"
```

```
  description = "Allow all inbound traffic"

  ingress {

    from_port   = 0

    to_port     = 65535

    protocol    = "tcp"

    cidr_blocks = ["0.0.0.0/0"]

  }

}
```

Step 2: Scan the Template with Checkov

Run Checkov on the current directory:

```
checkov -d .
```



Expected Findings:

- Public S3 bucket access (public-read)
- Security group open to all inbound traffic

Expected Findings:

- Warns about S3 bucket without encryption
- Flags open Security Group rules

Step 4: Review the Report

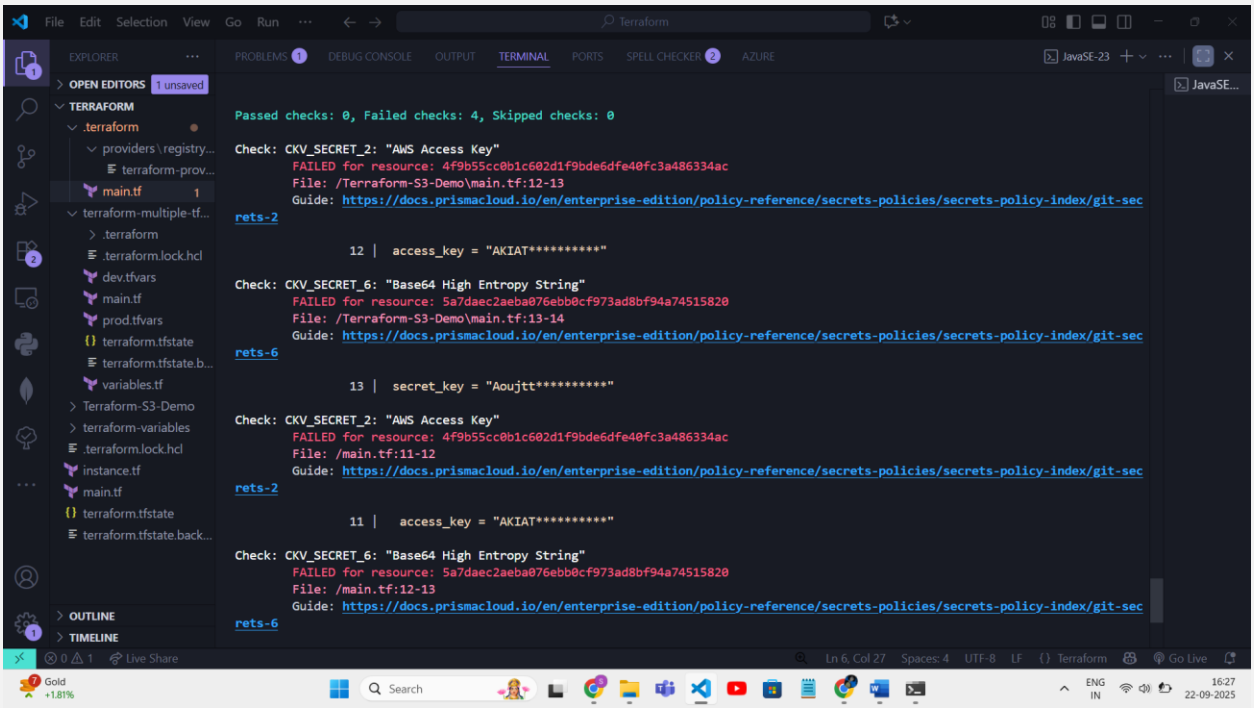
Example output (Checkov):

Check: CKV_AWS_20: "S3 Bucket allows public read access"

FAILED for resource: aws_s3_bucket.insecure_bucket

Check: CKV_AWS_260: "Security group allows ingress from 0.0.0.0/0"

FAILED for resource: aws_security_group.insecure_sg



Step 5: Apply Fixes (Optional)

Modify the IaC template to:

- Set S3 bucket ACL to private
- Enable encryption (AES256)
- Restrict Security Group to specific IP ranges

Step 6: Rescan the Template

Run the scan again:

```
checkov -d .
```

Now the findings should be **resolved or reduced**.

```
File association not found for extension .py
[ terraform framework ]: 100%|                    |[1/1], Current File Scanned=main.tf
[ secrets framework ]: 100%|                    |[1/1], Current File Scanned=.\main.tf
[ secrets framework ]: 100%|                    |[1/1], Current File Scanned=.\main.tf

 _  __  __  __  __  _ _____  _
| |/ _|| _|| _|| _|| |_   _|/ \
| ( (_ | ( | ( | ( | | | | ( o )
|_|\__|_|_|_|\__|_|_|_|_| \_/

By Prisma Cloud | version: 3.2.470

Terraform scan results:

Passed checks: 15, Failed checks: 8, Skipped checks: 0

Check: CKV_AWS_93: "Ensure S3 bucket policy does not lockout all but root user. (Prevent lockouts needing root account fixes)"
        PASSED for resource: aws_s3_bucket.insecure_bucket
        File: \main.tf:6-17
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/bc-aws-s3-24
Check: CKV_AWS_53: "Ensure S3 bucket has block public ACLS enabled"
        PASSED for resource: aws_s3_bucket_public_access_block.block
        File: \main.tf:20-26
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/bc-aws-s3-19
Check: CKV_AWS_54: "Ensure S3 bucket has block public policy enabled"
        PASSED for resource: aws_s3_bucket_public_access_block.block
        File: \main.tf:20-26
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/bc-aws-s3-20
Check: CKV_AWS_55: "Ensure S3 bucket has ignore public ACLs enabled"
        PASSED for resource: aws_s3_bucket_public_access_block.block
        File: \main.tf:20-26
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/bc-aws-s3-21
Check: CKV_AWS_56: "Ensure S3 bucket has 'restrict_public_buckets' enabled"
        PASSED for resource: aws_s3_bucket_public_access_block.block
        File: \main.tf:20-26
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/bc-aws-s3-22
Check: CKV_AWS_382: "Ensure no security groups allow egress from 0.0.0.0:0 to port -1"
        PASSED for resource: aws_security_group.insecure_sg
        File: \main.tf:29-54
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/bc-aws-382
Check: CKV_AWS_24: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 22"
        PASSED for resource: aws_security_group.insecure_sg
        File: \main.tf:29-54
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-1-port-security
Check: CKV_AWS_25: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 3389"
        PASSED for resource: aws_security_group.insecure_sg
        File: \main.tf:29-54
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-2
Check: CKV_AWS_260: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 80"
        PASSED for resource: aws_security_group.insecure_sg
        File: \main.tf:29-54
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-aws-security-groups-do-not-allow-ingress-from-00000-to-port-80
Check: CKV_AWS_277: "Ensure no security groups allow ingress from 0.0.0.0:0 to port -1"
        PASSED for resource: aws_security_group.insecure_sg
```

```
Command Prompt

        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-31

                29 | resource "aws_security_group" "insecure_sg" {
                30 |   name        = "restricted-sg"
                31 |   description = "Allow inbound traffic only from specific IPs"
                32 |
                33 |   ingress {
                34 |     from_port   = 22          # SSH
                35 |     to_port     = 22
                36 |     protocol    = "tcp"
                37 |     cidr_blocks = ["YOUR_IP/32"]   # Replace with your public IP
                38 |   }
                39 |
                40 |   ingress {
                41 |     from_port   = 80          # HTTP
                42 |     to_port     = 80
                43 |     protocol    = "tcp"
                44 |     cidr_blocks = ["YOUR_IP/32"]   # Replace with your public IP
                45 |   }
                46 |
                47 |   # Optional: allow HTTPS if needed
                48 |   ingress {
                49 |     from_port   = 443
                50 |     to_port     = 443
                51 |     protocol    = "tcp"
                52 |     cidr_blocks = ["YOUR_IP/32"]   # Replace with your public IP
                53 |   }
                54 | }

Check: CKV2_AWS_62: "Ensure S3 buckets should have event notifications enabled"
        FAILED for resource: aws_s3_bucket.insecure_bucket
        File: \main.tf:6-17
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/bc-aws-2-62

                6  | resource "aws_s3_bucket" "insecure_bucket" {
                7  |   bucket = "my-insecure-bucket-lab"
                8  |   acl    = "private"
                9  |
                10 |   server_side_encryption_configuration {
                11 |     rule {
                12 |       apply_server_side_encryption_by_default {
                13 |         sse_algorithm = "AES256"
                14 |       }
                15 |     }
                16 |   }
                17 | }

Check: CKV_AWS_21: "Ensure all data stored in the S3 bucket have versioning enabled"
        FAILED for resource: aws_s3_bucket.insecure_bucket
        File: \main.tf:6-17
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-16-enable-versioning

                6  | resource "aws_s3_bucket" "insecure_bucket" {
                7  |   bucket = "my-insecure-bucket-lab"
                8  |   acl    = "private"
                9  |
```

```
Check: CKV2_AWS_5: "Ensure that Security Groups are attached to another resource"
        FAILED for resource: aws_security_group.insecure_sg
        File: \main.tf:29-54
        Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-security-groups-are-attached-to-ec2-instances-or-elastic-network-interfaces-e
nis

                29 | resource "aws_security_group" "insecure_sg" {
                30 |   name        = "restricted-sg"
                31 |   description = "Allow inbound traffic only from specific IPs"
                32 |
                33 |   ingress {
                34 |     from_port   = 22          # SSH
                35 |     to_port     = 22
                36 |     protocol    = "tcp"
                37 |     cidr_blocks = ["YOUR_IP/32"]   # Replace with your public IP
                38 |   }
                39 |
                40 |   ingress {
                41 |     from_port   = 80          # HTTP
                42 |     to_port     = 80
                43 |     protocol    = "tcp"
                44 |     cidr_blocks = ["YOUR_IP/32"]   # Replace with your public IP
                45 |   }
                46 |
                47 |   # Optional: allow HTTPS if needed
                48 |   ingress {
                49 |     from_port   = 443
                50 |     to_port     = 443
                51 |     protocol    = "tcp"
                52 |     cidr_blocks = ["YOUR_IP/32"]   # Replace with your public IP
                53 |   }
                54 | }
```

Step 7: Document Findings

Create a simple findings log:

Resource	Issue / Vulnerability	Fix Applied	Status
aws_s3_bucket.insecure_bucket	S3 bucket public access (public-read)	ACL set to private	Resolved
aws_s3_bucket.insecure_bucket	S3 bucket not encrypted	Enabled server-side encryption (AES256)	Resolved
aws_s3_bucket.insecure_bucket	Public access block not configured	Added aws_s3_bucket_public_access_block	Resolved
aws_security_group.insecure_sg	Security group open to all IPs	Restricted cidr_blocks to specific IP range	Resolved
aws_s3_bucket.insecure_bucket	Versioning not enabled	Not implemented yet	Warning
aws_s3_bucket.insecure_bucket	Access logging not enabled	Not implemented yet	Warning
aws_s3_bucket.insecure_bucket	Cross-region replication not configured	Not implemented yet	Warning