## **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)

```
mohdanas@Mohds-MacBook-Air ~ % python3 -m pip install checkov

Collecting checkov

Downloading checkov-3.2.470-py3-none-any.whl.metadata (26 kB)

Collecting bc-python-hcl2==0.4.3 (from checkov)

Downloading bc_python_hcl2-0.4.3-py3-none-any.whl.metadata (4.2 kB)

Collecting bc-detect-secrets==1.5.45 (from checkov)

Downloading bc_detect_secrets-1.5.45-py3-none-any.whl.metadata (23 kB)

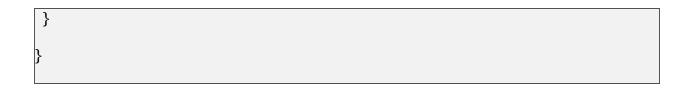
Collecting bc-jsonpath-ng==1.6.1 (from checkov)
```

• Git installed (optional, for version control of IaC templates)

#### **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" {
           = "insecure-sg"
name
description = "Allow all inbound traffic"
 ingress {
 from_port = 0
 to_port = 65535
 protocol = "tcp"
  \operatorname{cidr\_blocks} = ["o.o.o.o/o"]
```



## **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**.

```
By Prisma Cloud | version: 3.2.470
terraform scan results:
Passed checks: 7, Failed checks: 12, Skipped checks: 0
Check: CKV_AWS_93: "Ensure S3 bucket policy does not lockout all but root user. (Prevent lockouts ne eding root account fixes)"
         PASSED for resource: aws_s3_bucket.insecure_bucket
File: /main.tf:4-15

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
File: /main.tf:17-26
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:17-26
Check: CKV_AWS_41: "Ensure no hard coded AWS access key and secret key exists in provider"
         PASSED for resource: aws.default
Check: CKV_AWS_20: "S3 Bucket has an ACL defined which allows public READ access."
         PASSED for resource: aws_s3_bucket.insecure_bucket
         File: /main.tf:4-15
Check: CKV_AWS_19: "Ensure all data stored in the S3 bucket is securely encrypted at rest"
         PASSED for resource: aws_s3_bucket.insecure_bucket
File: /main.tf:4-15
Check: CKV_AWS_57: "S3 Bucket has an ACL defined which allows public WRITE access."
         PASSED for resource: aws_s3_bucket.insecure_bucket
File: /main.tf:4-15

Check: CKV_AWS_260: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 80"
FAILED for resource: aws_security_group.insecure_sg
File: /main.tf:17-26
```

## **Step 7: Document Findings**

Create a simple findings log:

# **Findings Log**

Check ID	Description	Status	Notes / Remediation	
CKV_AW S_260	SG allows ingress from 0.0.0.0/0 to port 80	X Failed	Restrict SG to specific IP ranges	
CKV_AW S_24	SG allows ingress from 0.0.0.0/0 to port 22	X Failed	Restrict SSH access to admin IP only	
CKV_AW S_25	SG allows ingress from 0.0.0.0/0 to port 3389	X Failed	Block or limit RDP access	
CKV_AW S_23	Missing SG rule descriptions	X Failed	Add descriptions to each rule	
CKV2_A WS_5	SG not attached to a resource	X Failed	Attach SG to EC2 or relevant resource	
CKV_AW S_18	S3 bucket logging not enabled	X Failed	Enable server access logging	
CKV_AW S_21	S3 bucket versioning not enabled	X Failed	Enable versioning for recovery	
CKV2_A WS_6	S3 public access block not configured	X Failed	Add aws_s3_bucket_public_acce	
CKV2_A WS_61	S3 bucket lifecycle not configured	X Failed	Add lifecycle rules for storage classes	
CKV_AW S_145	S3 not using KMS encryption	X Failed	Switch from AES256 to KMS	
CKV_AW S_144	S3 cross-region replication not enabled	X Failed	Configure replication if needed	
CKV2_A WS_62	S3 event notifications not enabled	X Failed	Add event notification configuration	