**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)

**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"]

}

}

A screenshot of a computer program

AI-generated content may be incorrect.

**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

A screenshot of a computer screen

AI-generated content may be incorrect.

**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

A screenshot of a computer screen

AI-generated content may be incorrect.

**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

A screenshot of a computer program

AI-generated content may be incorrect.

**Step 6: Rescan the Template**

Run the scan again:

checkov -d .

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

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

**Step 7: Document Findings**

Create a simple findings log:

**📝 Findings Log**

**Project:** Scanning IaC Templates for Vulnerabilities  
**Tool Used:** Checkov

**Initial Scan (main.tf - insecure version)**

* **Resource:** aws\_s3\_bucket.insecure\_bucket
  + ❌ Finding: S3 bucket allows **public read access** (CKV\_AWS\_20)
  + ❌ Finding: S3 bucket does **not have encryption enabled** (CKV\_AWS\_21)
* **Resource:** aws\_security\_group.insecure\_sg
  + ❌ Finding: Security group allows **all inbound traffic from 0.0.0.0/0** (CKV\_AWS\_260)

**Fixes Applied (Step 4)**

* Set S3 bucket ACL to **private**
* Enabled **AES256 server-side encryption** for S3 bucket
* Restricted security group ingress to a **specific IP** instead of 0.0.0.0/0

**Rescan Results (main.tf - fixed version)**

* ✅ No public access detected on S3 bucket
* ✅ S3 bucket encryption enabled (AES256)
* ✅ Security group restricted to specific IP range
* ✅ All previous findings resolved

**Conclusion**

* The insecure IaC template had critical misconfigurations exposing resources publicly.
* After applying fixes, all vulnerabilities were resolved, and the infrastructure meets security best practices.
* **Recommendation:** Always run IaC scans (Checkov/tfsec) as part of CI/CD pipelines to prevent misconfigurations before deployment.