**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

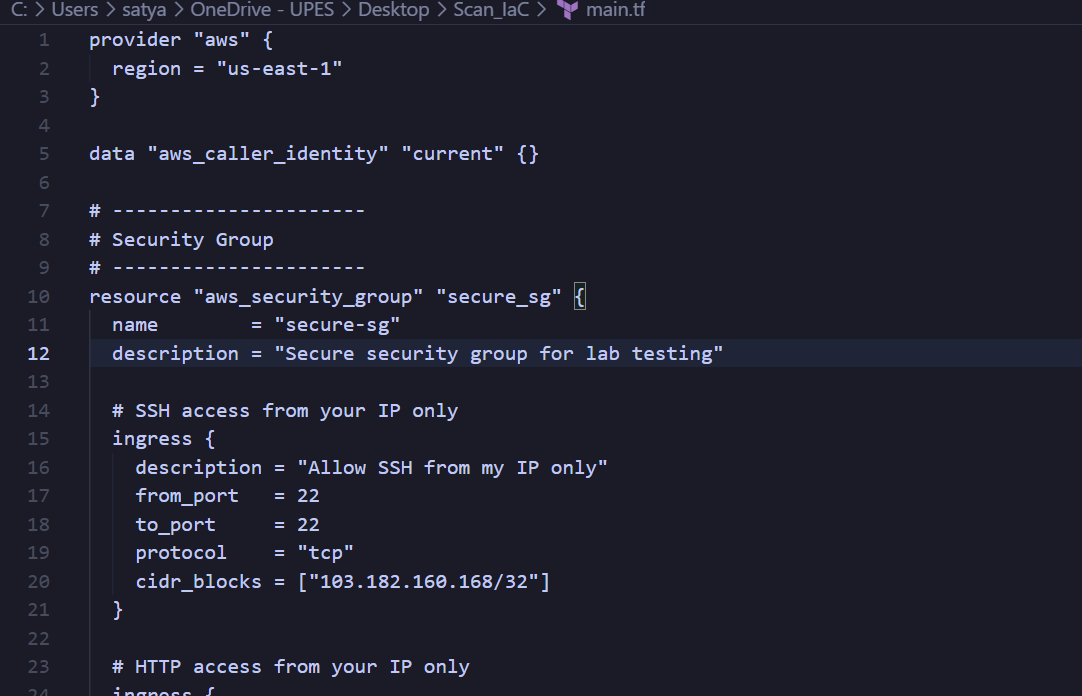
to\_port = 65535

protocol = "tcp"

cidr\_blocks = ["0.0.0.0/0"]

}

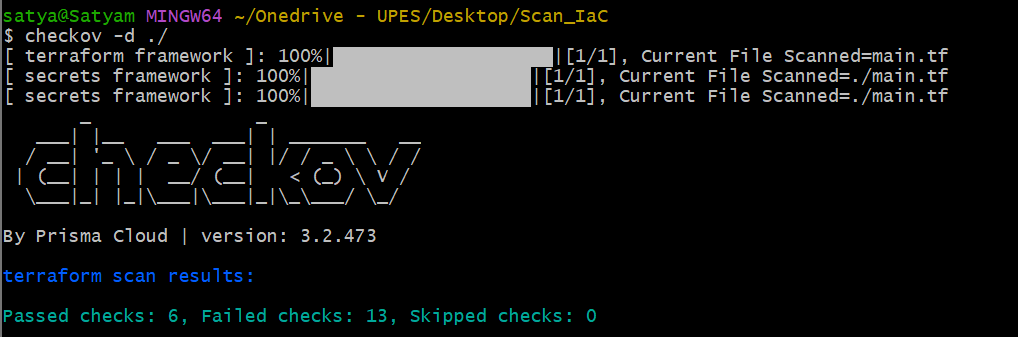
}



**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)**

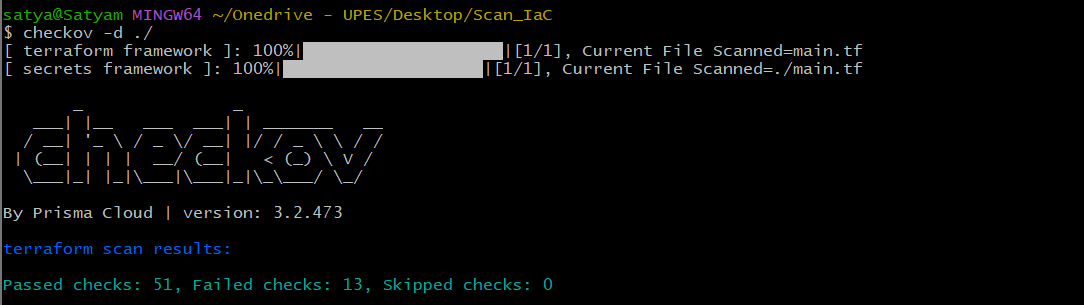
Modify the IaC template to:

* 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**.

**Step 7: Document Findings**

# **Checkov IaC Scan Finding Log:**

Scan Date: 2025-10-01

Directory Scanned: Scan\_IaC

Terraform File: main.tf

## Summary:

|  |  |  |
| --- | --- | --- |
| Result Type | Initial Scan | Last Scan |
| Passed Checks | 6 | 51 |
| Failed Checks | 13 | 13 |
| Skipped Checks | 0 | 0 |

## Failed Checks (Last Scan):

|  |  |  |  |
| --- | --- | --- | --- |
| Check ID | Description | Resource | Location |
| CKV\_AWS\_126 | Ensure that detailed monitoring is enabled for EC2 instances | aws\_instance.example | main.tf:244-256 |
| CKV\_AWS\_135 | Ensure that EC2 is EBS optimized | aws\_instance.example | main.tf:244-256 |
| CKV\_AWS\_79 | Ensure Instance Metadata Service Version 1 is not enabled | aws\_instance.example | main.tf:244-256 |
| CKV\_AWS\_8 | Ensure all data stored in the Launch configuration or instance Elastic Block Store is securely encrypted | aws\_instance.example | main.tf:244-256 |
| CKV2\_AWS\_62 | Ensure S3 buckets have event notifications enabled | aws\_s3\_bucket.secure\_bucket, aws\_s3\_bucket.log\_bucket, aws\_s3\_bucket.replica\_bucket | main.tf:97-183 |
| CKV2\_AWS\_6 | Ensure that S3 bucket has a Public Access block | aws\_s3\_bucket.secure\_bucket, aws\_s3\_bucket.log\_bucket, aws\_s3\_bucket.replica\_bucket | main.tf:97-183 |
| CKV\_AWS\_144 | Ensure that S3 bucket has cross-region replication enabled | aws\_s3\_bucket.log\_bucket, aws\_s3\_bucket.replica\_bucket | main.tf:130-183 |
| CKV2\_AWS\_61 | Ensure that an S3 bucket has a lifecycle configuration | aws\_s3\_bucket.secure\_bucket, aws\_s3\_bucket.log\_bucket, aws\_s3\_bucket.replica\_bucket | main.tf:97-183 |

## **Notes / Observations:**

Compared to the initial scan, most security misconfigurations with S3 and IAM have been fixed.  
  
Remaining failed checks are mainly related to EC2 instance configuration (monitoring, encryption, EBS optimization, metadata service) and S3 bucket operational best practices (event notifications, lifecycle rules, replication, public access block).