**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

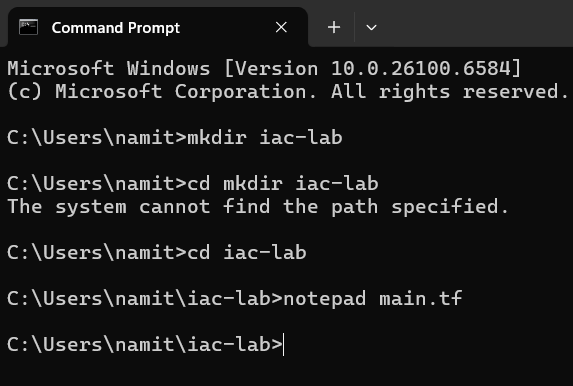
to\_port = 65535

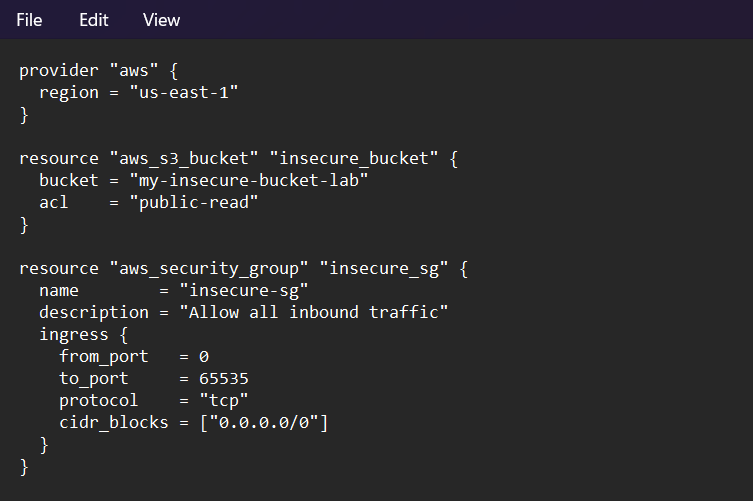
protocol = "tcp"

cidr\_blocks = ["0.0.0.0/0"]

}

}



****

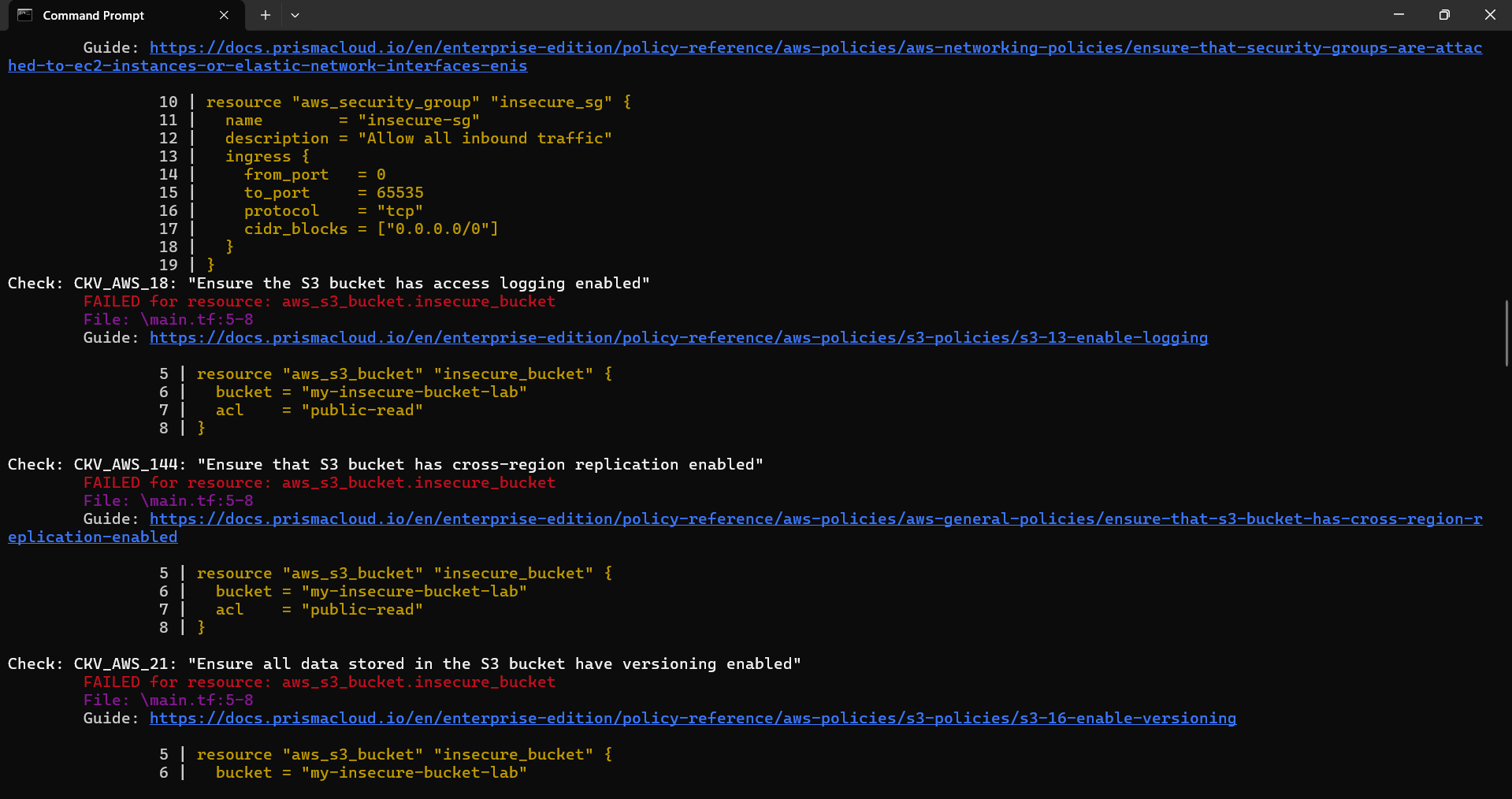
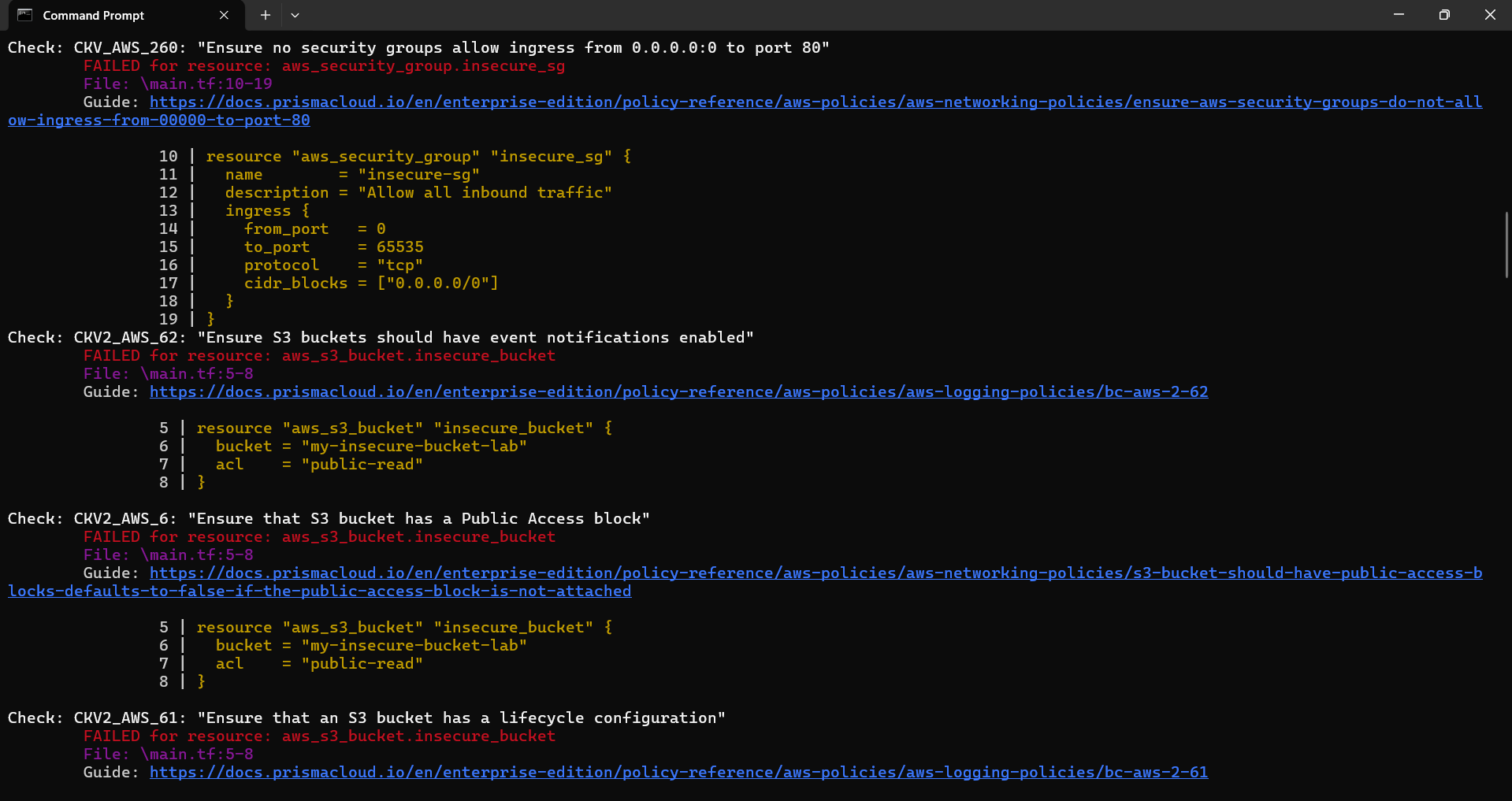
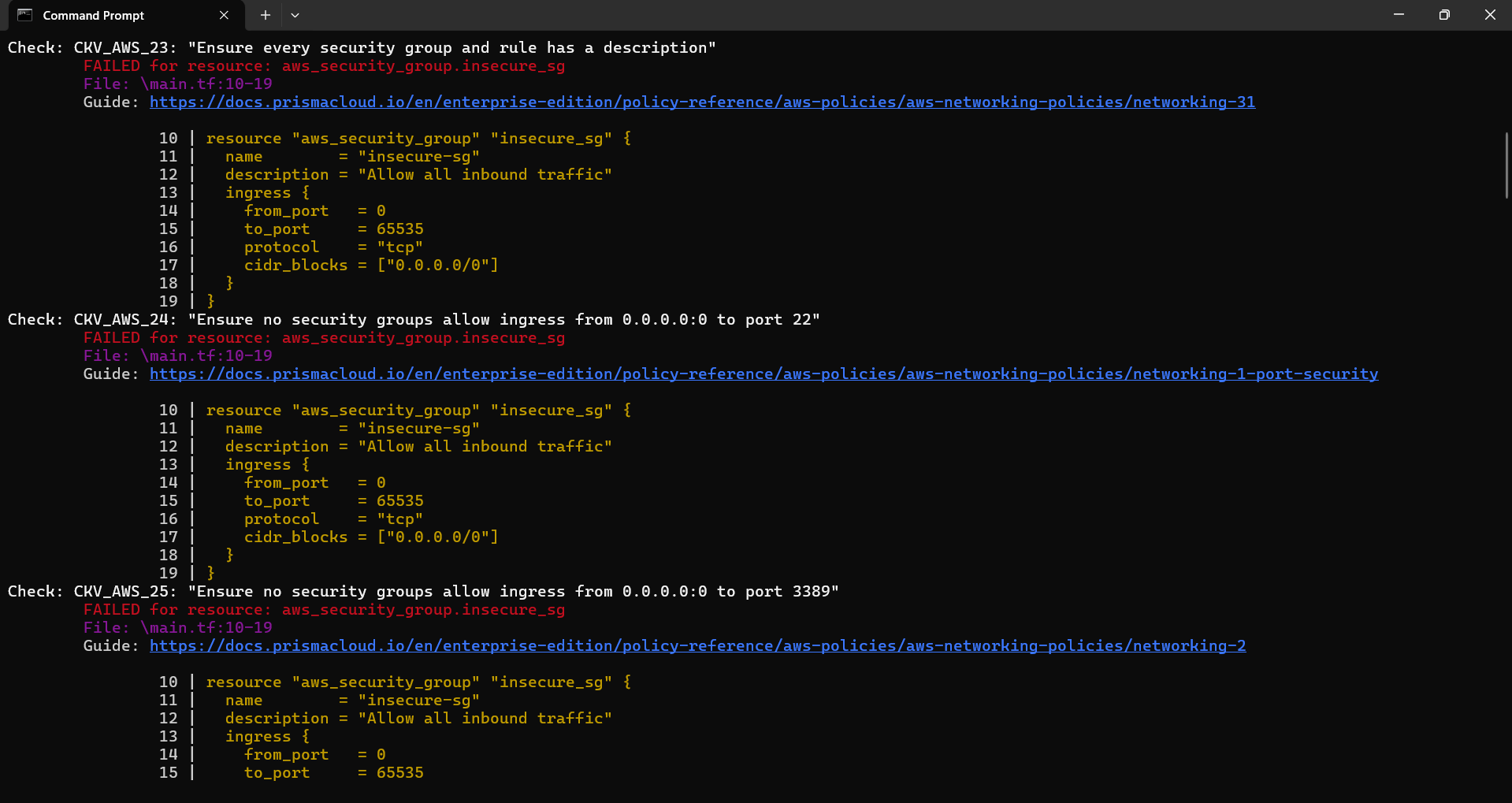
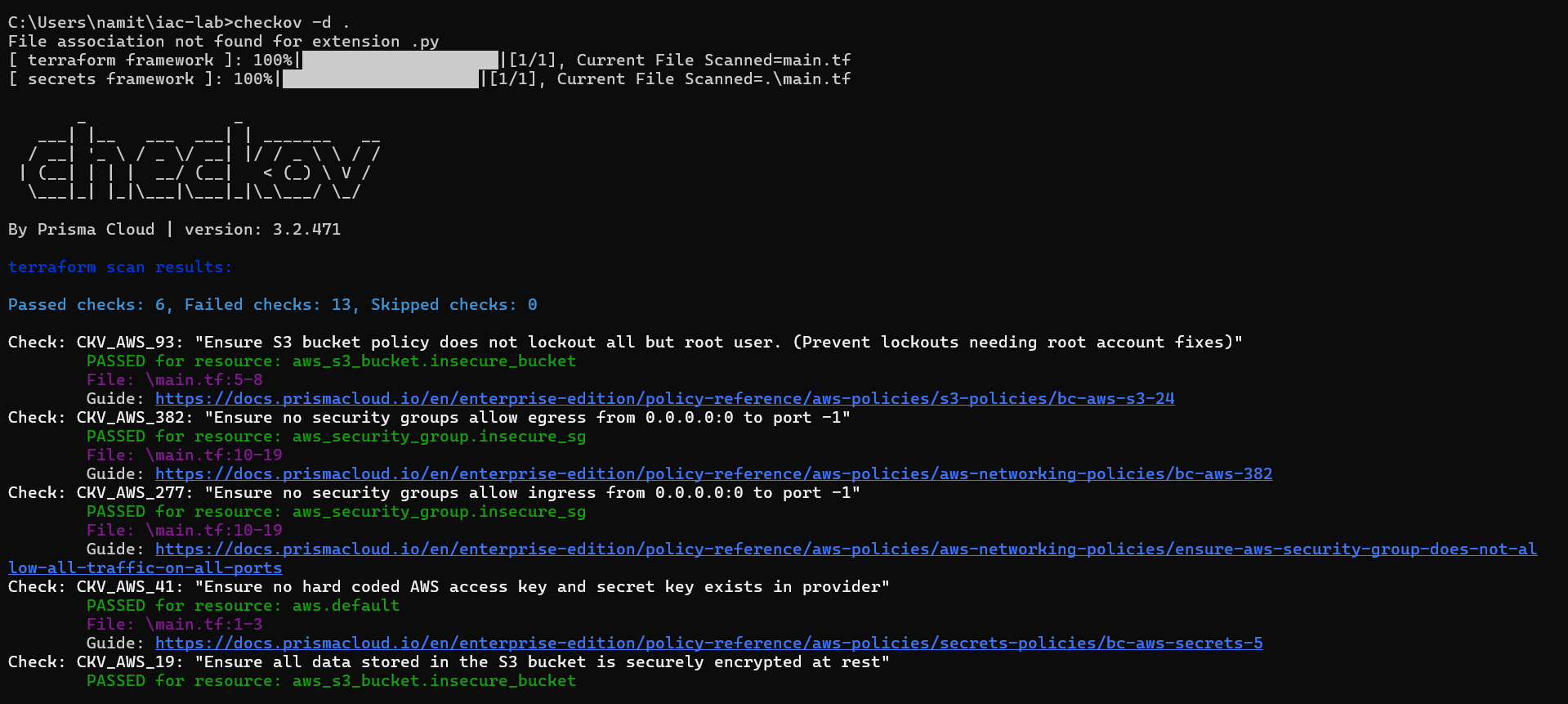
**Step 2: Scan the Template with Checkov**

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

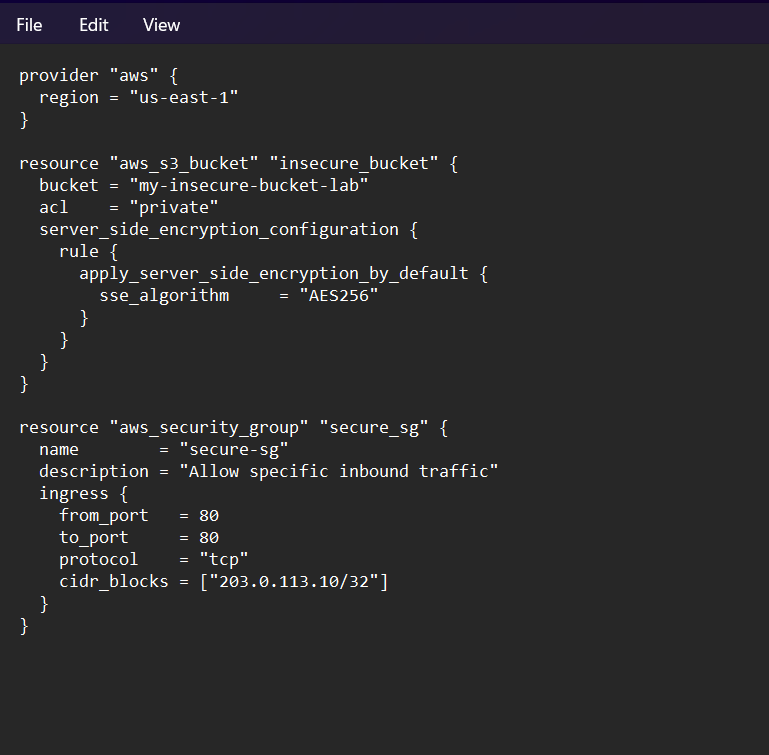
**Step 5: Apply Fixes (Optional)**

Modify the IaC template to:

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

**Changes Made to main.tf**

The Infrastructure as Code (IaC) template was modified to fix the security vulnerabilities found in the initial scan. The S3 bucket's public access was removed, and encryption was enabled. The security group was restricted to only allow specific inbound traffic, instead of all traffic from the internet.



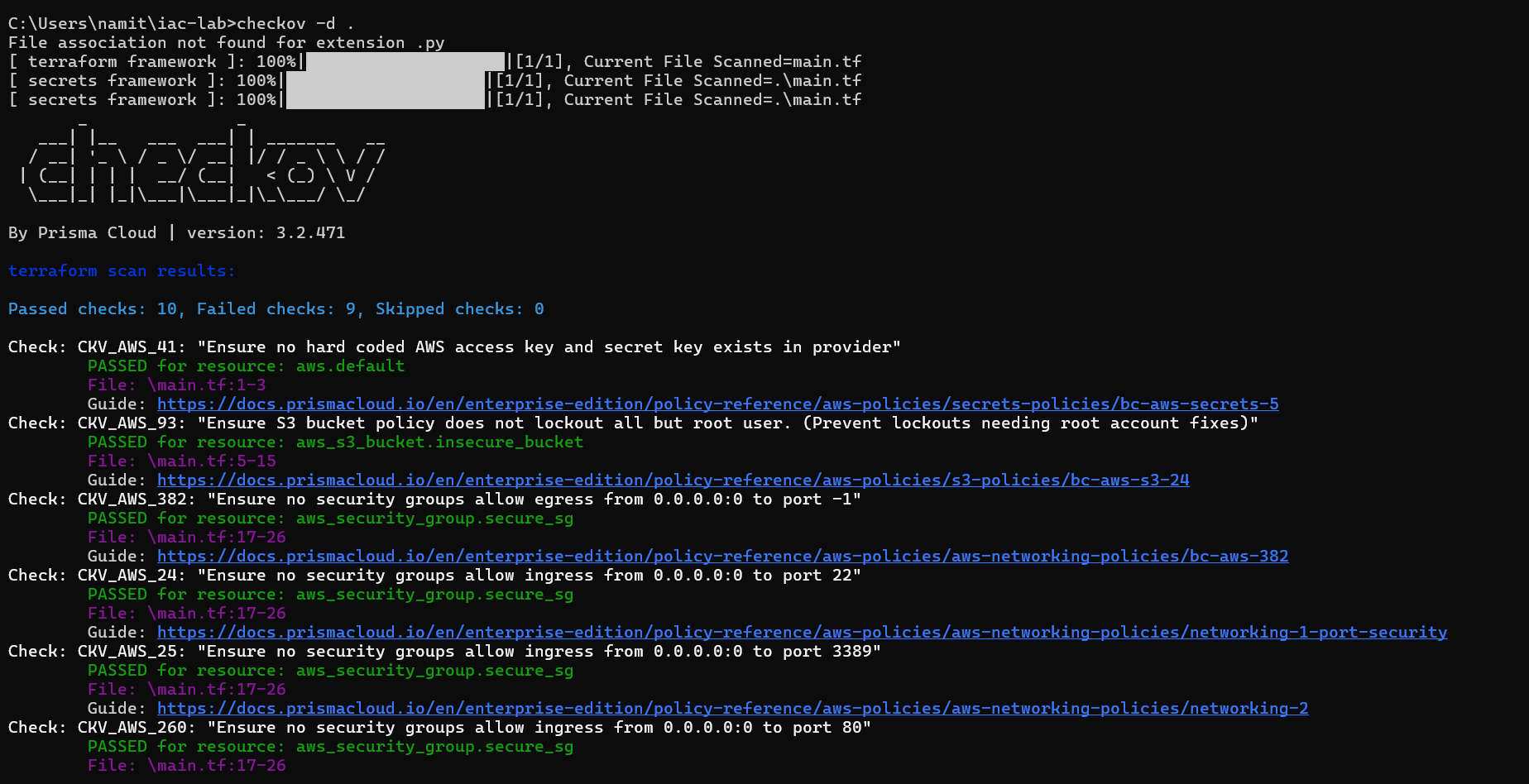
**Step 6: Rescan the Template**

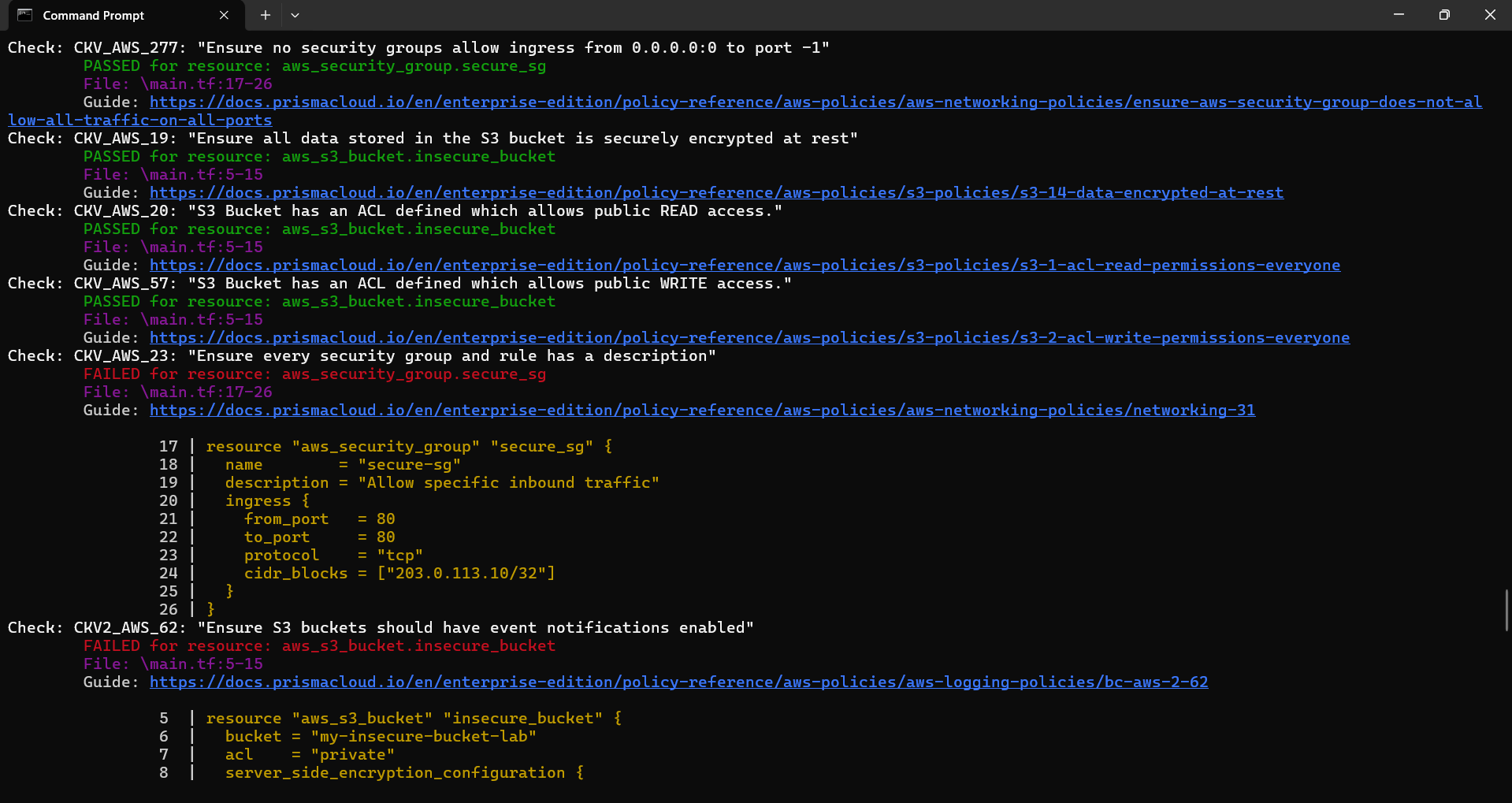
Run the scan again:

checkov -d .

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

After running the scan again, the errors were reduced -:





**Step 7: Document Findings**

**Final Findings Log -:**

|  |  |  |  |
| --- | --- | --- | --- |
| Check ID | Description | Resource | Status (After Fix) |
| CKV\_AWS\_20 | S3 bucket has an ACL which allows public READ access. | aws\_s3\_bucket.insecure\_bucket | **PASSED** |
| CKV\_AWS\_260 | Security group allows ingress from 0.0.0.0/0 to port 80. | aws\_security\_group.secure\_sg | **PASSED** |
| CKV\_AWS\_24 | Security group allows ingress from 0.0.0.0/0 to port 22. | aws\_security\_group.secure\_sg | **PASSED** |
| CKV\_AWS\_25 | Security group allows ingress from 0.0.0.0/0 to port 3389. | aws\_security\_group.secure\_sg | **PASSED** |
| CKV\_AWS\_57 | S3 bucket has an ACL which allows public WRITE access. | aws\_s3\_bucket.insecure\_bucket | **PASSED** |
| CKV\_AWS\_145 | S3 bucket is not encrypted with KMS by default. | aws\_s3\_bucket.insecure\_bucket | **FAILED** |
| CKV\_AWS\_23 | Security group does not have a description. | aws\_security\_group.secure\_sg | **FAILED** |
| CKV\_AWS\_18 | S3 bucket does not have access logging enabled. | aws\_s3\_bucket.insecure\_bucket | **FAILED** |
| CKV\_AWS\_21 | S3 bucket does not have versioning enabled. | aws\_s3\_bucket.insecure\_bucket | **FAILED** |