

**Pratik Agrawal**

**500123601**

**Devops B2**

## **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"]  
    }  
}
```

```

    terraform-multiple-tfvars — nano main.tf — 90x31
    UW PICO 5.09                               File: main.tf                               Modified
    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"]
      }
    }
  }
}

```

^G Get Help    ^O WriteOut    ^R Read File    ^Y Prev Pg    ^K Cut Text    ^C Cur Pos  
 ^X Exit        ^J Justify     ^W Where is    ^V Next Pg    ^U UnCut Text   ^T To Spell

## OUTPUT :-

---

### 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

# OUTPUT :-

```
[ 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

checkov

By Prisma Cloud | version: 3.2.471

terraform scan results:

Passed checks: 6, Failed checks: 13, Skipped checks: 0

Check: CKV_AWS_41: "Ensure no hard coded AWS access key and secret key exists in provider"
PASSED for resource: aws.default
File: \main.tf:1-3
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/secrets-policies/bc-aws-secrets-5

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:5-8
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/bc-aws-s3-24

Check: CKV_AWS_382: "Ensure no security groups allow egress from 0.0.0.0 to port -1"
PASSED for resource: aws_security_group.insecure_sg
File: \main.tf:10-19
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/bc-aws-382

Check: CKV_AWS_277: "Ensure no security groups allow ingress from 0.0.0.0 to port -1"
PASSED for resource: aws_security_group.insecure_sg
File: \main.tf:10-19
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-aws-security-group-does-not-allow-all-traffic-on-all-ports

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:5-8
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-i4-data-encrypted-at-rest

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:5-8
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-2-acl-write-permissions-everyone

Check: CKV_AWS_23: "Ensure every security group and rule has a description"
FAILED for resource: aws_security_group.insecure_sg
File: \main.tf:10-19
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-31

10 | resource "aws_security_group" "insecure_sg" {
11 |   name = "insecure-sg"
12 |   description = "Allow all inbound traffic"
```

```

14 |   from_port = 0
15 |   to_port   = 65535
16 |   protocol  = "tcp"
17 |   cidr_blocks = ["0.0.0.0/0"]
18 | }

```

Check: QKV\_AMS\_24: "Ensure no security groups allow ingress from 0.0.0.0/0 to port 22"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-1-port-security>

```

10 | resource "aws_security_group" "insecure_sg" {
11 |   name = "insecure-sg"
12 |   description = "Allow all inbound traffic"
13 |   ingress {
14 |     from_port = 0
15 |     to_port   = 65535
16 |     protocol  = "tcp"
17 |     cidr_blocks = ["0.0.0.0/0"]
18 |   }
19 | }

```

Check: QKV\_AMS\_25: "Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-1>

```

10 | resource "aws_security_group" "insecure_sg" {
11 |   name = "insecure-sg"
12 |   description = "Allow all inbound traffic"
13 |   ingress {
14 |     from_port = 0
15 |     to_port   = 65535
16 |     protocol  = "tcp"
17 |     cidr_blocks = ["0.0.0.0/0"]
18 |   }
19 | }

```

Check: QKV\_AMS\_26B: "Ensure no security groups allow ingress from 0.0.0.0/0 to port 80"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-aws-security-groups-do-not-allow-ingress-from-00000-to-port-80>

```

10 | resource "aws_security_group" "insecure_sg" {
11 |   name = "insecure-sg"
12 |   description = "Allow all inbound traffic"
13 |   ingress {
14 |     from_port = 0
15 |     to_port   = 65535
16 |     protocol  = "tcp"
17 |     cidr_blocks = ["0.0.0.0/0"]
18 |   }
19 | }

```

Check: QKV2\_AMS\_62: "Ensure S3 buckets should have event notifications enabled"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/for-aws-2-62>

```

5 | resource "aws_s3_bucket" "insecure_bucket" {
6 |   bucket = "my-insecure-bucket-lab"
7 |   acl    = "public-read"
8 | }

```

Check: QKV2\_AMS\_6: "Ensure that S3 bucket has a Public Access Block"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/s3-bucket-should-have-public-access-blocks-default-to-false-if-the-public-access-block-is-not-attached>

```

5 | resource "aws_s3_bucket" "insecure_bucket" {
6 |   bucket = "my-insecure-bucket-lab"
7 |   acl    = "public-read"
8 | }

```

Check: QKV\_AMS\_18: "Ensure the S3 bucket has access logging enabled"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-18-enable-logging>

## Step 5: Apply Fixes (Optional)

Modify the IaC template to:

```

Check: QKV_AMS_10A: "Ensure that S3 bucket has cross-region replication enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: /tmp/10-10
Guide: https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-that-s3-bucket-has-cross-region-replication-enabled

5 | resource "aws_s3_bucket" "insecure_bucket" {
6 |   bucket = "my-insecure-bucket-lab"
7 |   acl    = "public-read"
8 | }

```

Check: QKV\_AMS\_14B: "Ensure that S3 buckets are encrypted with KMS by default"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-that-s3-buckets-are-encrypted-with-kms-by-default>

```

5 | resource "aws_s3_bucket" "insecure_bucket" {
6 |   bucket = "my-insecure-bucket-lab"
7 |   acl    = "public-read"
8 | }

```

Check: QKV2\_AMS\_61: "Ensure that an S3 bucket has a lifecycle configuration"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/for-aws-2-61>

```

5 | resource "aws_s3_bucket" "insecure_bucket" {
6 |   bucket = "my-insecure-bucket-lab"
7 |   acl    = "public-read"
8 | }

```

Check: QKV\_AMS\_21: "Ensure all data stored in the S3 bucket have versioning enabled"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-16-enable-versioning>

```

5 | resource "aws_s3_bucket" "insecure_bucket" {
6 |   bucket = "my-insecure-bucket-lab"
7 |   acl    = "public-read"
8 | }

```

Check: QKV2\_AMS\_5: "Ensure that Security Groups are attached to another resource"

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-security-groups-are-attached-to-ec2-instances-or-elastic-network-interfaces-onis>

```

10 | resource "aws_security_group" "insecure_sg" {
11 |   name = "insecure-sg"
12 |   description = "Allow all inbound traffic"
13 |   ingress {
14 |     from_port = 0
15 |     to_port   = 65535
16 |     protocol  = "tcp"
17 |     cidr_blocks = ["0.0.0.0/0"]
18 |   }
19 | }

```

Check: QKV\_AMS\_20: "S3 Bucket has an ACL defined which allows public READ access."

File: /tmp/10-10  
 Guide: <https://docs.aws.amazon.com/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-3-acl-read-permissions-everyone>

```

5 | resource "aws_s3_bucket" "insecure_bucket" {
6 |   bucket = "my-insecure-bucket-lab"
7 |   acl    = "public-read"
8 | }

```

- 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**.

## OUTPUT :-

```
[ terraform framework ]: 100% [ [1/1], Current File Scanned*.main.tf ]
[ secrets framework ]: 100% [ [1/1], Current File Scanned*.main.tf ]

checkov
By Prisma Cloud | version: 3.2.471

terraform scan results:
Passed checks: 18, Failed checks: 9, 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.secure_bucket
File: *.main.tf:9-10
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/bc-aws-s3-24

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.secure_sg
File: *.main.tf:18-20
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.secure_sg
File: *.main.tf:18-20
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.secure_sg
File: *.main.tf:18-20
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.secure_sg
File: *.main.tf:18-20
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.secure_sg
File: *.main.tf:18-20
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-aws-security-group-does-not-allow-all-traffic-on-all-ports

Check: CKV_AWS_41: "Ensure no hard coded AWS access key and secret key exists in provider"
PASSED for resource: aws_default
File: *.main.tf:1-3
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/secrets-policies/bc-aws-secrets-5

Check: CKV_AWS_19: "Ensure all data stored in the S3 bucket is securely encrypted at rest"
PASSED for resource: aws_s3_bucket.secure_bucket
File: *.main.tf:9-10
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-14-data-encrypted-at-rest

Check: CKV_AWS_28: "S3 Bucket has an ACL defined which allows public READ access."
PASSED for resource: aws_s3_bucket.secure_bucket
File: *.main.tf:9-10
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-1-acl-read-permissions-everyone

Check: CKV_AWS_57: "S3 Bucket has an ACL defined which allows public WRITE access."
PASSED for resource: aws_s3_bucket.secure_bucket
File: *.main.tf:9-10
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-2-acl-write-permissions-everyone

Check: CKV_AWS_23: "Ensure every security group and rule has a description"
PASSED for resource: aws_security_group.secure_sg
File: *.main.tf:18-20
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-11

18 | resource "aws_security_group" "secure_sg" {
```

```

Check: CNV_AWS_13: "Ensure every security group and rule has a description"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-refnetworking-policies/allowing-s3

18 | resource "aws_security_group" "secure_sg" {
19 |   name = "secure-sg"
20 |   description = "Allow specific inbound traffic"
21 |
22 |   ingress {
23 |     from_port = 22
24 |     to_port = 22
25 |     protocol = "tcp"
26 |     cidr_blocks = ["203.0.113.0/24"]
27 |   }
28 |
29 |   ingress {
30 |     from_port = 80
31 |     to_port = 80
32 |     protocol = "tcp"
33 |     cidr_blocks = ["203.0.113.0/24"]
34 |   }
35 | }

Check: CNV_AWS_14: "Ensure S3 buckets should have event notifications enabled"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-reflogging-policies/for-iam-2-82

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

Check: CNV_AWS_15: "Ensure that S3 bucket has a Public Access Block"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-refnetworking-policies/s3-bucket-should-have-public-access-blocks-default-to-false-if-the-public-access-block-is-not-attached

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

Check: CNV_AWS_16: "Ensure that an S3 bucket has a lifecycle configuration"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-reflogging-policies/for-iam-2-61

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

Check: CNV_AWS_100: "Ensure that S3 bucket has cross-region replication enabled"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-general-policies/ensure-that-s3-bucket-has-cross-region-replication-enabled

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

Check: CNV_AWS_11: "Ensure all data stored in the S3 bucket have versioning enabled"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-general-policies/ensure-that-s3-bucket-has-versioning-enabled

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

```

## Step 7: Document Findings

```

8 |
9 |   server_side_encryption_configuration {
10 |     rule {
11 |       apply_server_side_encryption_by_default {
12 |         sse_algorithm = "AES256"
13 |       }
14 |     }
15 |   }
16 | }

Check: CNV_AWS_18: "Ensure the S3 bucket has access logging enabled"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/s3-policies/s3-logging-enabled
Guide: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/s3-policies/s3-logging-enabled

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

Check: CNV_AWS_5: "Ensure that Security Groups are attached to another resource"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-refnetworking-policies/ensure-that-security-groups-are-attached-to-ec2-instances-or-elastic-network-interfaces-units
Guide: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-refnetworking-policies/ensure-that-security-groups-are-attached-to-ec2-instances-or-elastic-network-interfaces-units

18 | resource "aws_security_group" "secure_sg" {
19 |   name = "secure-sg"
20 |   description = "Allow specific inbound traffic"
21 |
22 |   ingress {
23 |     from_port = 22
24 |     to_port = 22
25 |     protocol = "tcp"
26 |     cidr_blocks = ["203.0.113.0/24"]
27 |   }
28 |
29 |   ingress {
30 |     from_port = 80
31 |     to_port = 80
32 |     protocol = "tcp"
33 |     cidr_blocks = ["203.0.113.0/24"]
34 |   }
35 | }

Check: CNV_AWS_145: "Ensure that S3 buckets are encrypted with KMS by default"
File: /tmp/1f-18-19
Title: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-general-policies/ensure-that-s3-buckets-are-encrypted-with-kms-by-default
Guide: https://docs.aws.amazon.com/IAM/latest/reference/policy-reference/aws-policies/iam-general-policies/ensure-that-s3-buckets-are-encrypted-with-kms-by-default

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

```



```
UW PIC0 5.09                                     File: findings.txt

Initial Findings:
- S3 Bucket allows public read access
- S3 Bucket without encryption
- Security group allows all inbound traffic (0.0.0.0/0)

After Fixes:
- S3 Bucket ACL set to private
- Encryption enabled (AES256)
- Security group restricted to 192.168.1.0/24
```

Create a simple findings log: