

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.

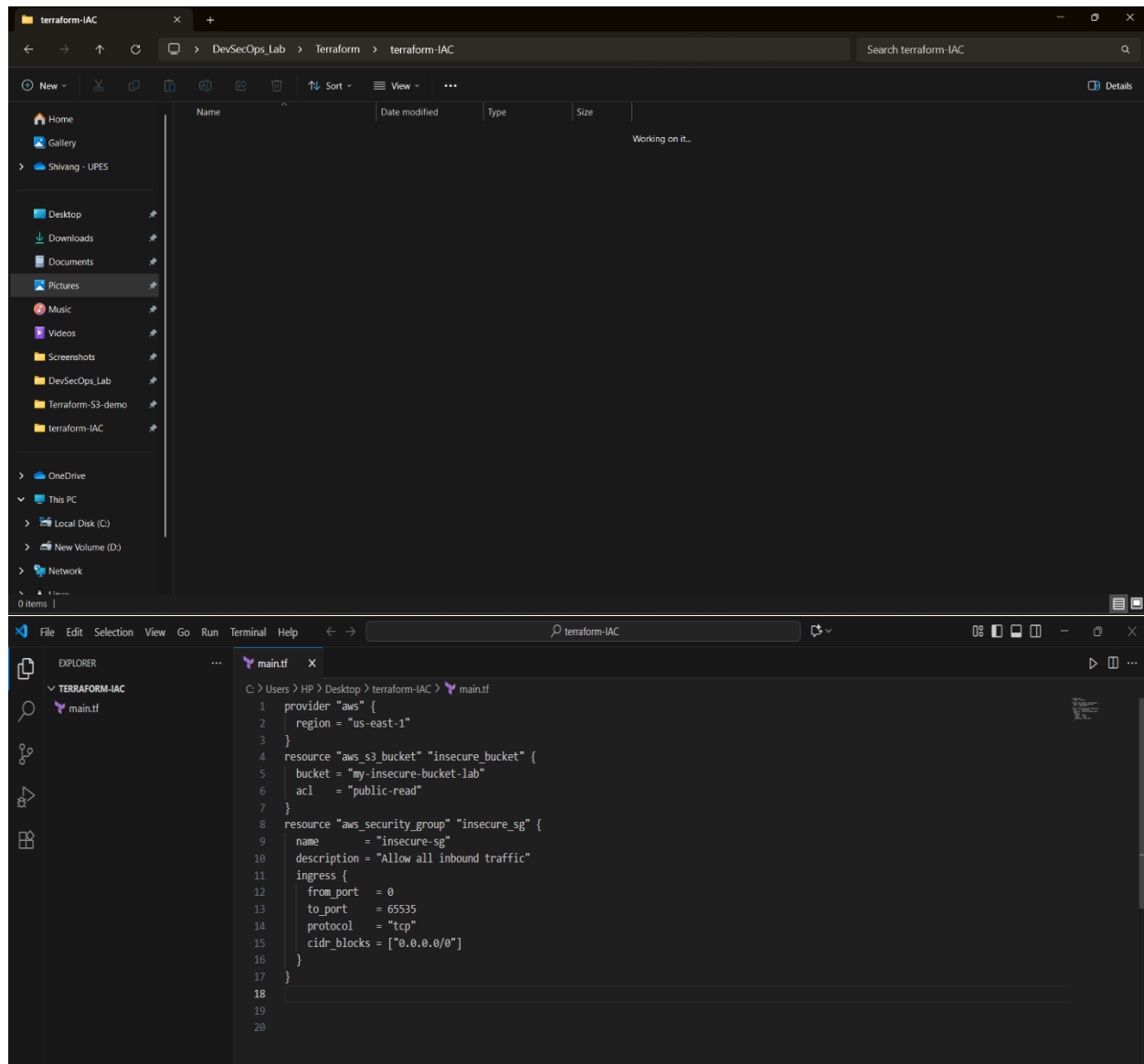
Prerequisites

- 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

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\HP\Desktop\DevSecOps_Lab\Terraform\terraform-IAC> checkov --version
3.2.470
PS C:\Users\HP\Desktop\DevSecOps_Lab\Terraform\terraform-IAC> checkov -d .
[ terraform framework ]: 100% [1/1], Current File Scanned=main.tf
[ secrets framework ]: 100% [1/1], Current File Scanned=.main.tf

By Prisma Cloud | version: 3.2.470

terraform scan results:

Passed checks: 6, Failed checks: 13, 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.insecure_bucket
File: \main.tf:4-7
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:8-17
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:8-17
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.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-l4-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:4-7
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:8-17
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-31

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

Check: CKV_AWS_24: "Ensure no security groups allow ingress from 0.0.0.0 to port 22"
FAILED For resource: aws_security_group.insecure_sg
File: \main.tf:8-17
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-1-port-security

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

```
Windows PowerShell X + v

Check: CKV_AWS_25: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 3389"
FAILED for resource: aws_security_group.insecure_sg
File: \main.tf:8-17
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-2

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

Check: CKV_AWS_268: "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:8-17
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

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

Check: CKV2_AWS_62: "Ensure S3 buckets should have event notifications enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/bc-aws-2-62

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

Check: CKV2_AWS_6: "Ensure that S3 bucket has a Public Access block"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/s3-bucket-should-have-public-access-blocks-defaults-to-false-if-the-public-access-block-is-not-attached

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

Check: CKV2_AWS_61: "Ensure that an S3 bucket has a lifecycle configuration"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/bc-aws-2-61

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

Check: CKV2_AWS_5: "Ensure that Security Groups are attached to another resource"
FAILED for resource: aws_security_group.insecure_sg
File: \main.tf:8-17
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-security-groups-are-attached-to-ec2-instances-or-elastic-network-interfaces-enis

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

Check: CKV_AWS_18: "Ensure the S3 bucket has access logging enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-l3-enable-logging

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

Check: CKV_AWS_144: "Ensure that S3 bucket has cross-region replication enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-that-s3-bucket-has-cross-region-replication-enabled

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

Check: CKV_AWS_21: "Ensure all data stored in the S3 bucket have versioning enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-l6-enable-versioning

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

Check: CKV_AWS_145: "Ensure that S3 buckets are encrypted with KMS by default"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-that-s3-buckets-are-encrypted-with-kms-by-default

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

Check: CKV_AWS_20: "S3 Bucket has an ACL defined which allows public READ access."
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-l-acl-read-permissions-everyone

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

PS C:\Users\HP\Desktop\DevSecOps_Lab\Terraform\terraform-IAC>
```

Step 3: Review the Report

Example output (Checkov):

Check: CKV_AWS_20: "S3 Bucket allows public read access"

FAILED for resource: aws_s3_bucket.insecure_bucket

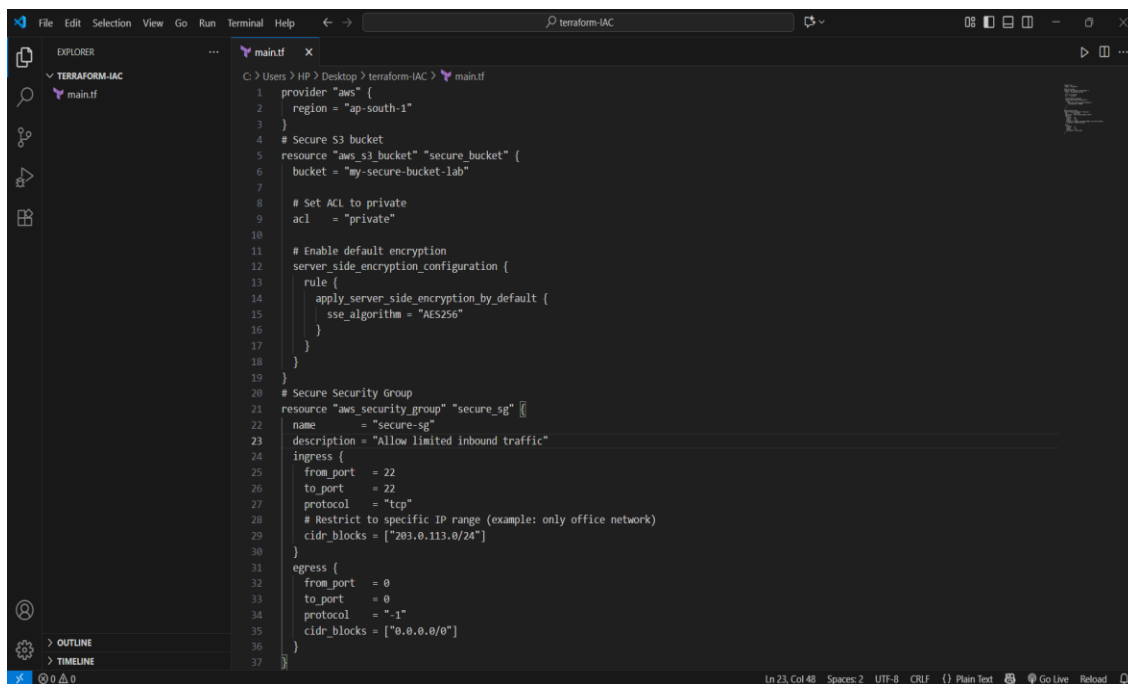
Check: CKV_AWS_260: "Security group allows ingress from 0.0.0.0/0"

FAILED for resource: aws_security_group.insecure_sg

Step 4: Apply Fixes (Optional)

Modify the IaC template to:

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



```
1 provider "aws" {
2   region = "ap-south-1"
3 }
4 # Secure S3 bucket
5 resource "aws_s3_bucket" "secure_bucket" {
6   bucket = "my-secure-bucket-lab"
7
8   # Set ACL to private
9   acl = "private"
10
11   # Enable default encryption
12   server_side_encryption_configuration {
13     rule {
14       apply_server_side_encryption_by_default {
15         sse_algorithm = "AES256"
16       }
17     }
18   }
19 }
20 # Secure Security Group
21 resource "aws_security_group" "secure_sg" {
22   name = "secure-sg"
23   description = "Allow limited inbound traffic"
24   ingress {
25     from_port = 22
26     to_port = 22
27     protocol = "tcp"
28     # Restrict to specific IP range (example: only office network)
29     cidr_blocks = ["203.0.113.0/24"]
30   }
31   egress {
32     from_port = 0
33     to_port = 0
34     protocol = "-1"
35     cidr_blocks = ["0.0.0.0/0"]
36   }
37 }
```

Step 5: Rescan the Template

Run the scan again:

checkov -d .

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

```
PS C:\Users\HP\Desktop\DevSecOps_Lab\Terraform\terraform-IAC> checkov -d .
[ 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: 3.2.470



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:4-7
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.insecure_sg
File: \main.tf:8-17
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 0.0.0.0:0 to port -1"
PASSED for resource: aws_security_group.insecure_sg
File: \main.tf:8-17
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:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-14-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:4-7
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:8-17
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-31

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

Step 6: Document Findings

Create a simple findings log:

Findings Log – Terraform IaC

ID	Resource	Issue Detected	Risk	Fix Applied
1	aws_s3_bucket.insecure_bucket	S3 bucket ACL set to public-read	Public exposure of data	Changed ACL to private
2	aws_s3_bucket.insecure_bucket	No encryption configured	Data at rest not protected	Enabled AES256 server-side encryption

ID	Resource	Issue Detected	Risk	Fix Applied
3	aws_security_group.insecure_sg	Ingress allows 0.0.0.0/0 on all TCP ports	Full internet exposure (critical risk)	Restricted ingress to specific CIDR (203.0.113.0/24) and limited to port 22

