

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)

```
C:\Users\hp\Desktop\Notes\DevSecOps-Lab\terraform-demo\lab-18>python3 -m pip install checkov
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: checkov in c:\users\hp\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (3.2.471)
Requirement already satisfied: bc-python-hcl2==0.4.3 in c:\users\hp\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from checkov) (0.4.3)
Requirement already satisfied: bc-detect-secrets==1.5.45 in c:\users\hp\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from checkov) (1.5.45)
```

- 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

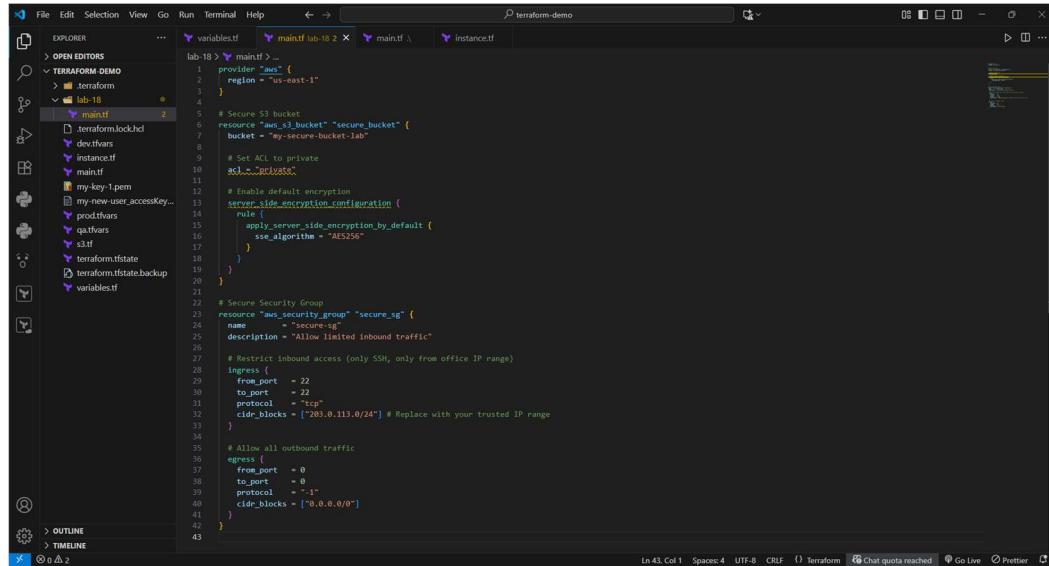
```
Check: CKV_AWS_20: "Ensure no security groups allow ingress from 0.0.0.0 to port 22"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/networking/networking-1-sec-security
10 | resource "aws_security_group" "insecure_sg" {
11 |   ingress {
12 |     type        = "ingress"
13 |     description = "Allow all inbound traffic"
14 |     ingress {
15 |       protocol  = "tcp"
16 |       port      = 22
17 |       cidr_blocks = ["0.0.0.0/0"]
18 |     }
19 |   }
20 | }
21 |
22 | Check: CKV_AWS_25: "Ensure no security groups allow ingress from 0.0.0.0 to port 3389"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/networking/networking-1-sec-security
23 | resource "aws_security_group" "insecure_sg" {
24 |   ingress {
25 |     type        = "ingress"
26 |     description = "Allow all inbound traffic"
27 |     ingress {
28 |       protocol  = "tcp"
29 |       port      = 3389
30 |       cidr_blocks = ["0.0.0.0/0"]
31 |     }
32 |   }
33 | }
34 |
35 | Check: CKV_AWS_260: "Ensure no security groups allow ingress from 0.0.0.0 to port 80"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/networking/networking-1-sec-security
36 | resource "aws_security_group" "insecure_sg" {
37 |   ingress {
38 |     type        = "ingress"
39 |     description = "Allow all inbound traffic"
40 |     ingress {
41 |       protocol  = "tcp"
42 |       port      = 80
43 |       cidr_blocks = ["0.0.0.0/0"]
44 |     }
45 |   }
46 | }
47 |
48 | Check: CKV_AWS_40: "Ensure S3 buckets should have event notifications enabled"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/storage/storage-1-s3-best-practices
49 | resource "aws_s3_bucket" "insecure_bucket" {
50 |   bucket        = "my-insecure-bucket"
51 |   encryption_type = "AES256"
52 |   notification {
53 |     events = ["s3:ObjectCreated:Put"]
54 |     target = "arn:aws:sns:us-east-1:123456789012:my-notification-topic"
55 |   }
56 | }
57 |
58 | Check: CKV_AWS_41: "Ensure that an S3 bucket has a lifecycle configuration"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/storage/storage-1-s3-best-practices
59 | resource "aws_s3_bucket" "insecure_bucket" {
60 |   bucket        = "my-insecure-bucket"
61 |   lifecycle_rule {
62 |     id          = "old-data"
63 |     rule {
64 |       filter {
65 |         prefix = "old-data"
66 |       }
67 |       status    = "Enabled"
68 |       transition = "Delete"
69 |       days     = 30
70 |     }
71 |   }
72 | }
73 |
74 | Check: CKV_AWS_51: "Ensure that Security Groups are attached to another resource"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/networking/networking-1-sec-security
75 | resource "aws_security_group_attachment" "insecure_sg_attachment" {
76 |   security_group_id = "sg-01234567890123456"
77 |   resource_id       = "i-01234567890123456"
78 |   group_name        = "Insecure SG"
79 | }
80 |
81 | Check: CKV_AWS_55: "Ensure the S3 bucket has access logging enabled"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/storage/storage-1-s3-best-practices
82 | resource "aws_s3_bucket" "insecure_bucket" {
83 |   bucket        = "my-insecure-bucket"
84 |   logging {
85 |     target      = "arn:aws:s3:::my-insecure-bucket-access-logs"
86 |     prefix      = "my-insecure-bucket"
87 |   }
88 | }
89 |
90 | Check: CKV_AWS_100: "Ensure S3 buckets have cross-region replication enabled"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/storage/storage-1-s3-best-practices
91 | resource "aws_s3_bucket" "insecure_bucket" {
92 |   bucket        = "my-insecure-bucket"
93 |   replication {
94 |     role      = "S3FullAccess"
95 |     destination = "arn:aws:s3:::my-insecure-bucket-us-west-2"
96 |   }
97 | }
98 |
99 | Check: CKV_AWS_101: "Ensure all data stored in the S3 bucket have versioning enabled"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/storage/storage-1-s3-best-practices
100 | resource "aws_s3_bucket" "insecure_bucket" {
101 |   bucket        = "my-insecure-bucket"
102 |   versioning {
103 |     enabled = true
104 |   }
105 | }
106 |
107 | Check: CKV_AWS_105: "Ensure that S3 buckets are encrypted with KMS by default"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/storage/storage-1-s3-best-practices
108 | resource "aws_s3_bucket" "insecure_bucket" {
109 |   bucket        = "my-insecure-bucket"
110 |   encryption_type = "awsKmsKey"
111 | }
112 |
113 | Check: CKV_AWS_106: "Ensure that S3 bucket has a Public Access Block"
Guide: https://www.owasp.org/www-project/owasp-aws-guide/latest/references/policy/storage/storage-1-s3-best-practices
114 | resource "aws_s3_bucket_public_access_block" "insecure_bucket" {
115 |   bucket        = "my-insecure-bucket"
116 |   block_all_public = true
117 | }
```

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



```

file: main.tf
provider "aws" {
  region = "us-east-1"
}

# Secure S3 bucket
resource "aws_s3_bucket" "secure_bucket" {
  bucket = "my-secure-bucket-lab"
}

# Set ACL to private
acl = "private"

# Enable default encryption
server_side_encryption_configuration {
  rule {
    apply_server_side_encryption_by_default {
      sse_algorithm = "AES256"
    }
  }
}

# Secure Security Group
resource "aws_security_group" "secure_sg" {
  name        = "secure-sg"
  description = "Allow limited inbound traffic"
}

# Restrict inbound access (only SSH, only from office IP range)
ingress {
  from_port   = 22
  to_port     = 22
  protocol    = "tcp"
  cidr_blocks = ["203.0.113.0/24"] # Replace with your trusted IP range
}

# Allow all outbound traffic
egress {
  from_port   = 0
  to_port     = 0
  protocol    = "-*-"
  cidr_blocks = ["0.0.0.0/0"]
}

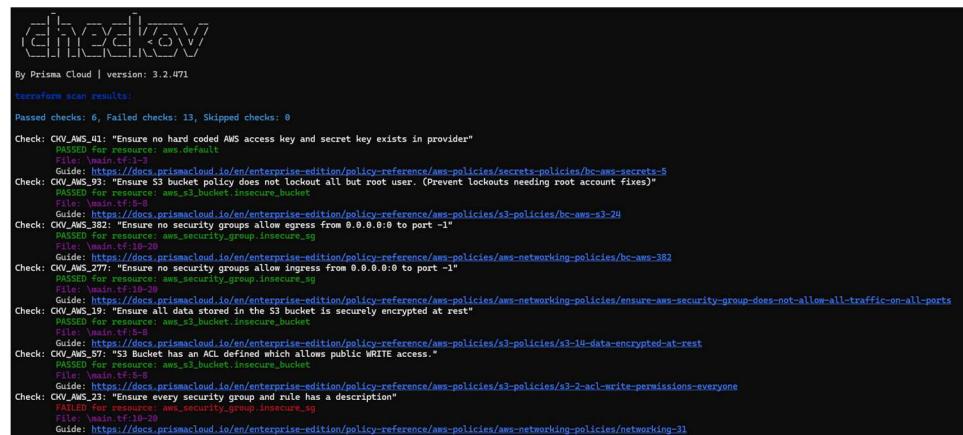
```

Step 6: Rescan the Template

Run the scan again:

```
checkov -d .
```

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



```

By Prisma Cloud | version: 3.2.471
Terraform scan results:
Passed checks: 6, Failed checks: 13, Skipped checks: 0

Check: CHV_AWS_41: "Ensure no hard coded AWS access key and secret key exists in provider"
  FAILED 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: CHV_AWS_93: "Ensure S3 Bucket policy does not lockout all but root user. (Prevent lockouts needing root account fixes)"
  FAILED For resource: aws_s3_bucket.secure_bucket
  File: /main.tf:8-10
  Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/bc-aws-s3-24
Check: CHV_AWS_382: "Ensure no security group allow egress from 0.0.0.0 to port -1"
  FAILED For resource: aws_security_group.secure_sg
  File: /main.tf:10-20
  Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-networking-policies/bc-aws-382
Check: CHV_AWS_277: "Ensure no security group allow ingress from 0.0.0.0/0 to port -1"
  FAILED For resource: aws_security_group.secure_sg
  File: /main.tf:10-20
  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: CHV_AWS_19: "Ensure all data stored in the S3 bucket is securely encrypted at rest"
  FAILED For resource: aws_s3_bucket.secure_bucket
  File: /main.tf:8-8
  Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-14-data-encrypted-at-rest
Check: CHV_AWS_57: "S3 Bucket has an ACL defined which allows public WRITE access."
  FAILED For resource: aws_s3_bucket.secure_bucket
  File: /main.tf:8-8
  Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-2-acl-write-permissions-everyone
Check: CHV_AWS_23: "Ensure every security group and rule has a description"
  FAILED For resource: aws_security_group.secure_sg
  File: /main.tf:10-10
  Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-31

```

Step 7: Document Findings

Findings Log:

Fixed Vulnerabilities:

ID	Resource	Issue Detected	Risk	Fix Applied
1	aws_s3_bucket.secure_bucket	S3 bucket ACL was public-read	Public exposure of data	Changed ACL to private
2	aws_s3_bucket.secure_bucket	No encryption configured	Data at rest not protected	Enabled AES256 server-side encryption
3	aws_security_group.secure_sg	Ingress allowed 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 (SSH)

Remaining Issues:

Check ID	Description	Status	Notes
CKV_AWS_23	Missing SG rule descriptions	✗ Failed	Add descriptions to each rule
CKV_AWS_382	SG allows egress 0.0.0.0/0 on all ports	✗ Failed	Restrict egress to only required destinations
CKV2_AWS_5	SG not attached to a resource	✗ Failed	Attach SG to EC2 or relevant resource
CKV_AWS_18	S3 bucket logging not enabled	✗ Failed	Enable server access logging
CKV_AWS_21	S3 bucket versioning not enabled	✗ Failed	Enable versioning for recovery
CKV2_AWS_6	No public access block on S3 bucket	✗ Failed	Add aws_s3_bucket_public_access_block resource

CKV2_AWS_61	No lifecycle configuration on S3 bucket	✗ Failed	Add lifecycle rules for storage classes
CKV_AWS_145	S3 not using KMS encryption	✗ Failed	Switch from AES256 to KMS CMK
CKV_AWS_144	No cross-region replication configured	✗ Failed	Configure replication if needed
CKV2_AWS_62	No event notifications configured	✗ Failed	Add event notification configuration