SecOps Assessment

by: Ahmed Tarek Khedr

Task1:

1. Introduction

1.1 Objective

The objective of this security audit is to assess the security posture of an application deployed on the Ghaymah Cloud platform. The audit focuses on five key security domains:

- Container Security
- Network Security
- OWASP Top 5
- Data Security
- Identity and Access Management (IAM)

The goal is to identify potential security weaknesses and recommend best practices to reduce security risk.

---

2. Security Audit Checklist

A. Container Security

1. Scan Container Images for Vulnerabilities

> All Docker images should be scanned before deployment as old packages may contain known CVEs.

How to apply on Ghaymah

Before deploying the image to Ghaymah:

- Scan image using Trivy.
- Fix High and Critical vulnerabilities.
- Only deploy clean image

2. Run Containers as Non-root

> Containers should never run with root privileges as if an attacker escapes the application, they will gain root access inside the container

3. Store Secrets Securely

> Never hardcode passwords or API keys inside the Docker image.

How to apply on Ghaymah

Use:

- Environment Variables
- Secret Management
- Encrypted configuration

B. Network Security

4. Allow Only Required Ports

Expose only necessary ports by Configuring Security Groups / Firewall Rules

5. Enforce HTTPS

All traffic must use HTTPS since it protects credentials and user data.

How to apply it:

We can install an SSL certificate and redirect HTTP → HTTPS

6. Restrict Internal Network Communication

Database should never be publicly accessible we will accomplish this by Network Policies concept to isolate workloads.

C. OWASP Top 5

7. Prevent Broken Access Control

Users should only access authorized resources by Role-Based Access Control (RBAC).

8. Prevent Injection

Use parameterized queries

9. Encrypt Sensitive Data

Passwords

↓

Hash using bcrypt

Sensitive files

↓

AES Encryption

HTTPS

↓

TLS

10. Secure Configuration

Disable

- Debug Mode
- Default Passwords
- Directory Listing

And update configuration regularly

11. Keep Components Updated

Always update:

- Docker Images
- Libraries
- Operating System

Use Trivy to detect outdated packages.

D. Data Security

12. Encrypt Data at Rest

All stored data should be encrypted.

E.G.

- Block Storage
- Database
- Backups

13. Backup Critical Data

Implement automatic backups.

- Daily Backup
- Weekly Full Backup
- Off-site Backup

E. Identity & Access Management

14. Enable Multi-Factor Authentication (MFA)

Administrators should authenticate using

- Password
- OTP / Authenticator App

---

15. Apply Least Privilege Principle

Every user receives only the permissions they actually need.