TCS iON RIO Project: Docker-Based Lab

**Project Overview**

This project is part of the TCS iON RIO program. It involves setting up a Docker-based lab environment on AWS EC2 using Ubuntu. The lab hosts a web server and MySQL service, configures a private network, and

includes basic cybersecurity testing tools like Nmap

**Technologies Used**

* Docker & Docker Compose
* Ubuntu 24.04 on AWS EC2 (Free Tier)
* Apache Web Server (httpd)
* MySQL 5.7
* Cybersecurity Tools: Nmap (basic), others.

**Setup Details**

**Docker Services:**

**Web Server:**

Image: httpd:latest

Port: 80:80

Static IP: 172.16.0.100

**Database Server:**

Image: mysql:5.7

Port: 3306

Environment: MYSQL\_ROOT\_PASSWORD

Static IP: 172.16.0.101

**Network:**

networks:

app\_net:

driver: bridge

ipam:

config:

- subnet: 172.16.0.0/24

**How to Run the Project**

**1. Clone the Repo**

git clone https://github.com/Afra-Dev-ai/TCS-iON-RIO-Docker-Lab.git

cd TCS-iON-RIO-Docker-Lab

**2. Start the Docker Containers**

sudo docker-compose up -d

**3. Test the Services**

# Test Apache Web Server

curl http://localhost

# Access MySQL

sudo docker exec -it mysql\_db mysql -uroot -p

**Vulnerability Scanning**

**Nmap Usage:**

sudo apt install nmap -y

nmap -sV 172.20.0.0/24

This identifies open ports (22, 80, 3306) and service versions

**Screenshots Included**

Docker Compose File & Run Output

Apache Web Server Test via curl

MySQL Access via docker exec

Nmap Vulnerability Scan Result

All images are available in the /screenshots/ folder

**Documentation**

The complete report is available in Project\_Report.docx . It includes: - Objective & Approach - System

Architecture - Configuration Steps - Vulnerability Test Logs - Learnings & Enhancements