

Docker Lab 8 — Docker CIS Benchmark & Security Hardening

Author: Dr. Sandeep Kumar Sharma

Lab Description

Lab 8 focuses on performing **Docker CIS Benchmark checks** and applying security hardening practices using Docker Bench for Security. This lab walks through how to audit Docker hosts, containers, images, and configurations using official CIS standards.

Topics Covered

- What is Docker CIS Benchmark?
 - Installing Docker Bench for Security
 - Running CIS scans
 - Reading and interpreting CIS reports
 - Performing recommended hardening (daemon configs, user namespace, logging config, etc.)
-

Learning Objectives

- Understand industry security benchmarks for Docker
 - Perform security audits using automated tools
 - Apply hardening recommendations
-

Learning Outcomes

- Ability to secure Docker hosts and containers to enterprise standards
 - Ability to evaluate compliance reports
-

Section 1 — Install Docker Bench for Security

```
git clone https://github.com/docker/docker-bench-security.git
cd docker-bench-security
sudo sh docker-bench-security.sh
```

Report will show: - Host configuration - Docker daemon settings - Container runtime security - Logging and monitoring

Section 2 — Apply Basic Hardening

Enable user namespace:

```
sudo nano /etc/docker/daemon.json
```

Add:

```
{
  "userns-remap": "default"
}
```

Restart Docker:

```
sudo systemctl restart docker
```

Section 3 — Logging and Audit Config

Configure auditd:

```
sudo apt install auditd -y
sudo auditctl -w /usr/bin/dockerd -k docker
```

Section 4 — Re-run CIS Scan

```
sudo sh docker-bench-security.sh
```

Verify improvements.

Section 5 — Cleanup

```
rm -rf docker-bench-security
```

Summary

You successfully ran CIS benchmarks and applied recommended hardening practices.