Docker Lab 9 — Secrets Management with Docker Swarm

Author: Dr. Sandeep Kumar Sharma

Lab Description

Lab 9 teaches **secure secrets management** using Docker Swarm. You will store and use sensitive data such as passwords, API keys, and certificates securely using Docker Swarm Secrets.

Topics Covered

- What are Docker secrets?
- How Swarm secures secrets (encryption-at-rest & in-transit)
- Creating and storing secrets
- Accessing secrets inside containers

Learning Objectives

- Understand the secure lifecycle of secrets in Docker
- Store secrets securely without environment variables
- Use secrets in services

Learning Outcomes

- Ability to securely manage sensitive data in production environments
- Ability to design secure microservice deployments

Section 1 — Initialize Swarm

```
docker swarm init
```

Section 2 — Create a Secret

```
echo "MySandeepPassword123" | docker secret create sandeep-secret -
```

List secrets:

```
docker secret ls
```

Section 3 — Use Secret in a Service

```
docker service create
  --name sandeep-app-secret
  --secret sandeep-secret
  ubuntu sleep infinity
```

Enter the container:

```
CID=$(docker ps | grep sandeep-app-secret | awk '{print $1}')
docker exec -it $CID bash
```

Access secret:

```
cat /run/secrets/sandeep-secret
```

Section 4 — Rotate Secret

```
echo "NewSecurePassword!" | docker secret create sandeep-secret-v2 -
```

Update service:

```
docker service update --secret-rm sandeep-secret --secret-add sandeep-secret-v2
sandeep-app-secret
```

Section 5 — Cleanup

```
docker service rm sandeep-app-secret
```

```
docker secret rm sandeep-secret sandeep-secret-v2
```

```
docker swarm leave --force
```

Summary

You successfully created, consumed, rotated, and removed Docker secrets using Swarm.