



Docker Deep Dive

Introduction to Docker Security

Docker Security 101

Docker platform
technologies

Secrets Management

Docker Content Trust

Security Scanning

Swarm Mode

OS (Linux)
technologies

Seccomp

Mandatory Access Control

Capabilities

Control Groups

Kernel Namespaces



Linux Academy



Docker Deep Dive

Namespaces

- Docker on Linux Namespaces:
 - Process ID (pid)
 - Network (net)
 - Filesystem/mount (mount)
 - Inter-process Communication (ipc)
 - User (user)
 - UTS (uts)



Docker Swarm

- Cryptographic node IDs
- Mutual authentication via TLS
- Secure join tokens
- CA configuration with automatic certificate rotation
- Encrypted cluster store
- Encrypted networks



Docker Secrets

Secrets Workflow:

- A secret is created and posted to the Swarm.
- The secret is encrypted and stored.
- A service is created and the secret is attached.
- Secrets are encrypted in-flight.
- The secret is mounted into the container of a service.
- When the task is complete, the in-memory is torn down.



Docker Security 101 (cont.)

