Docker Certified Associate

Security – Docker Engine and Swarm

Docker Engine Security

Docker Engine security involves the consideration of four areas:

1. The host’s kernel support of namespaces and cgroups.
2. Limited ‘attack surface’ of the Docker daemon.
3. Customization of container configuration profiles.
4. Hardening features of the kernel and their interaction with underlying containers.

Namespaces provide isolation to running containers so they cannot see or affect other processes on the host. Namespaces provide an isolated process, network, and volume stacks to enable that isolation.

Control groups implement resource management (allocating and reporting) to further minimize the effect of a container on a host. As a result, both play a role in minimizing (or mitigating completely) various security risks, such as the denial of service attacks on a container, privilege escalation exploits, etc.

Docker Engine Security

Docker Engine security involves the consideration of four areas:

1. The host’s kernel support of namespaces and cgroups.
2. Limited ‘attack surface’ of the Docker daemon.
3. Customization of container configuration profiles.
4. Hardening features of the kernel and their interaction with underlying containers.

The ‘attack surface’ is affected by the fact that the daemon requires ROOT account privileges, so more care than normal should be applied when changing parameters and/or known secure default configurations.

Even when ‘trusted users’ are given access to the daemon for control, unknowingly malicious images with ‘docker load’ type commands is a concern. The addition of Docker Enterprise Edition features with UCP, DTR, and Docker Content Trust can address some of those risks.

Docker Swarm

In addition to Docker Engine security protections, Docker Swarm makes heavy use of the Overlay Network Model.

This model comes prepared with security and support for communication encryption (using the –opt encrypted option when creating the network for use).

NOTE: This does NOT extend to Windows, where encryption is not supported.