What is container security?

Container security is the practice of keeping containers isolated from each other and from the host they run on. Unlike a virtual machine, a container shares the host kernel, so the boundary is enforced by Linux features (namespaces, cgroups, capabilities, seccomp) rather than a hypervisor. When those are misconfigured, an attacker who lands in one container can escape to the host or the wider cluster. It spans the image, the runtime, and the orchestrator (Kubernetes).

HOW IT WORKS

01 Why it is different from a VM

A virtual machine has its own kernel and is separated by a hypervisor, a hard boundary. A container shares the host kernel with every other container, so the separation is softer and depends entirely on configuration.

That is why a single risky flag (privileged mode, a mounted host path, a shared namespace) can collapse the boundary in a way that has no equivalent on a properly configured VM. See container vs virtual machine.

02 The three layers attackers target

Container risk lives in three places:

- The image: secrets baked into layers, outdated packages, or a poisoned base image. See image security.
- The runtime: dangerous run flags such as privileged containers, a mounted Docker socket, or host namespace sharing that enable a container escape.
- The orchestrator: Kubernetes misconfigurations such as an exposed kubelet, weak RBAC, or an over-permissioned service account token.

03 How a pentest tests it

A container and Kubernetes penetration test starts inside a low-privilege pod and tries to break out exactly as an attacker would: escape to the node, read other workloads, reach the cluster control plane, and pivot into the cloud account. The deliverable is the real escape path with reproducible evidence and a fix for each step.

SOURCES

[1] MITRE ATT&CK: Containers Matrix

[2] NIST SP 800-190 Application Container Security Guide

SHARED KERNEL, SOFTER WALL

The one idea that explains most container attacks: containers share the host kernel, so isolation is a matter of configuration, not hardware. Get the config wrong and the wall comes down.

Find the container escape paths before an attacker does.

securelayer7.net/learn/containers/what-is-container-security

Open online