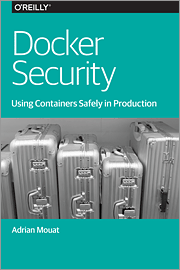
**Kernel exploits**

Unlike in a VM, the kernel is shared among all containers and the host, magnifying the importance of any vulnerabilities present in the kernel. Should a container cause a kernel panic, it will take down the whole host. In VMs, the situation is much better: an attacker would have to route an attack through both the VM kernel and the hypervisor before being able to touch the host kernel.

**EBOOK**

[](https://shop.oreilly.com/product/0636920044321.do)

[**Docker Security**](https://shop.oreilly.com/product/0636920044321.do)

By [Adrian Mouat](https://shop.oreilly.com/product/0636920044321.do)

[Shop now](https://shop.oreilly.com/product/0636920044321.do)

**Denial-of-service attacks**

All containers share kernel resources. If one container can monopolize access to certain resources–including memory and more esoteric resources such as user IDs (UIDs)—it can starve out other containers on the host, resulting in a denial-of-service (DoS), whereby legitimate users are unable to access part or all of the system.

**Container breakouts**

An attacker who gains access to a container should not be able to gain access to other containers or the host. By default, users are not namespaced, so any process that breaks out of the container will have the same privileges on the host as it did in the container; if you were root in the container, you will be root on the host.[2](https://www.oreilly.com/ideas/five-security-concerns-when-using-docker#fn:2) This also means that you need to worry about potential *privilege escalation* attacks–whereby a user gains elevated privileges such as those of the root user, often through a bug in application code that needs to run with extra privileges. Given that container technology is still in its infancy, you should organize your security around the assumption that container breakouts are unlikely, but possible.

**Poisoned images**

How do you know that the images you are using are safe, haven't been tampered with, and come from where they claim to come from? If an attacker can trick you into running his image, both the host and your data are at risk. Similarly, you want to be sure that the images you are running are up-to-date and do not contain versions of software with known vulnerabilities.