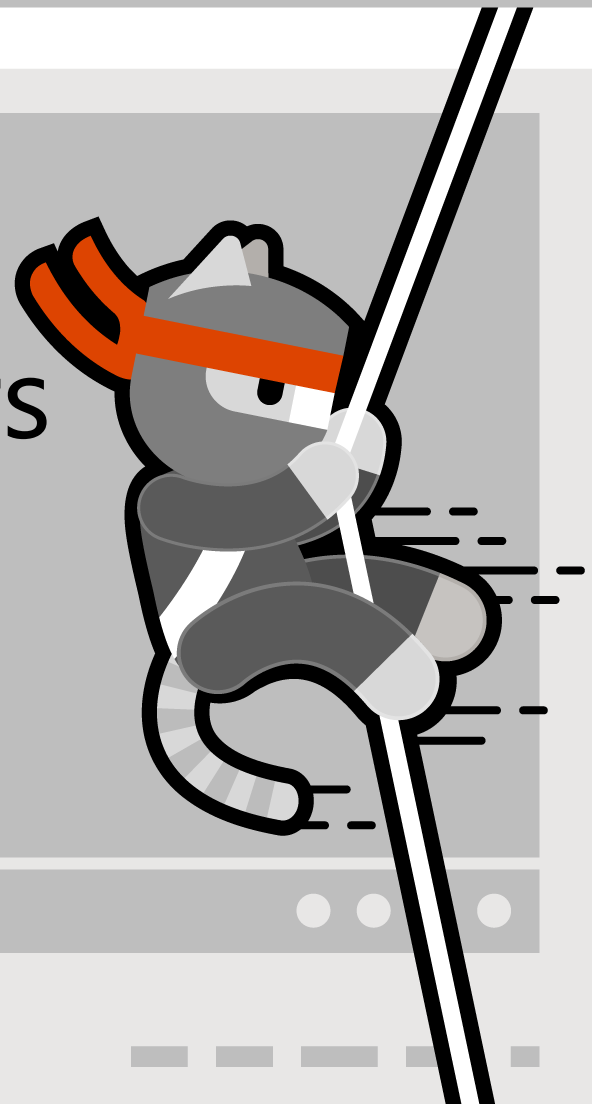
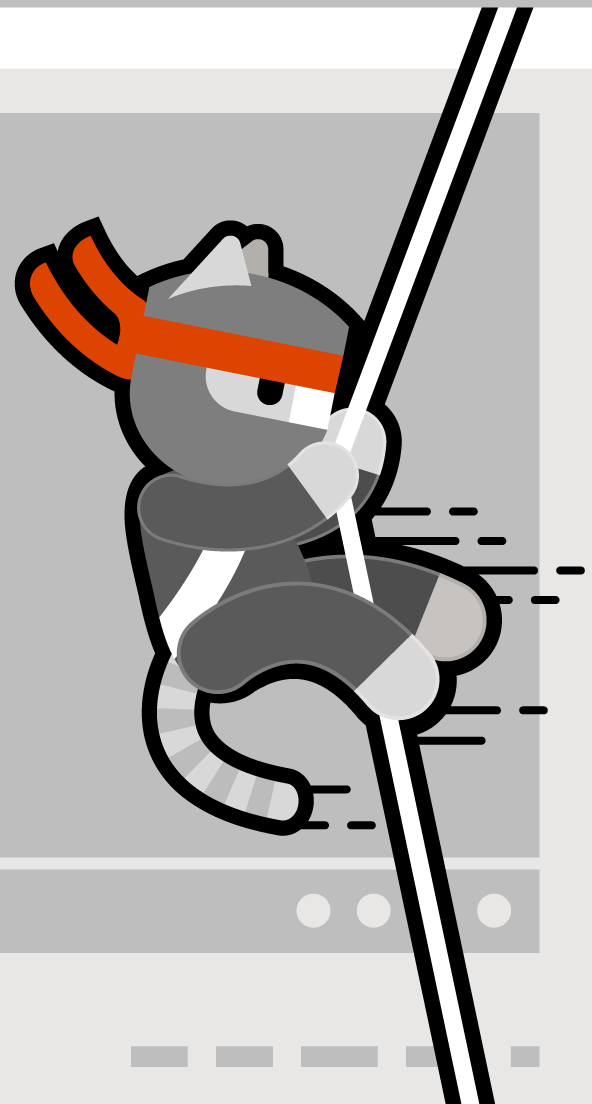
Hacking Containers
Linux Containers



Eng Teong Cheah
Microsoft MVP



Linux Containers

An image format compliant with the Open Container Initiative (OCI)

An OCI-compliant runtime

An OCI-compliant distribution

Chroot, which is technology that changes the root directory for a process and its children

Union mount file systems, such as Overlay2, Overlay, and Aufs

Container Internals

Not based on any standard when they were first conceived of

In fact, the Open Container Initiative (OCI) was established in 2015 by the Docker company.

Many frameworks created their own standards for how to interact with the kernel. This has led to many different types of container runtimes in one form or another over the last several years.

Regardless of the differences in Linux containers, many of the initial constructs remain the same.

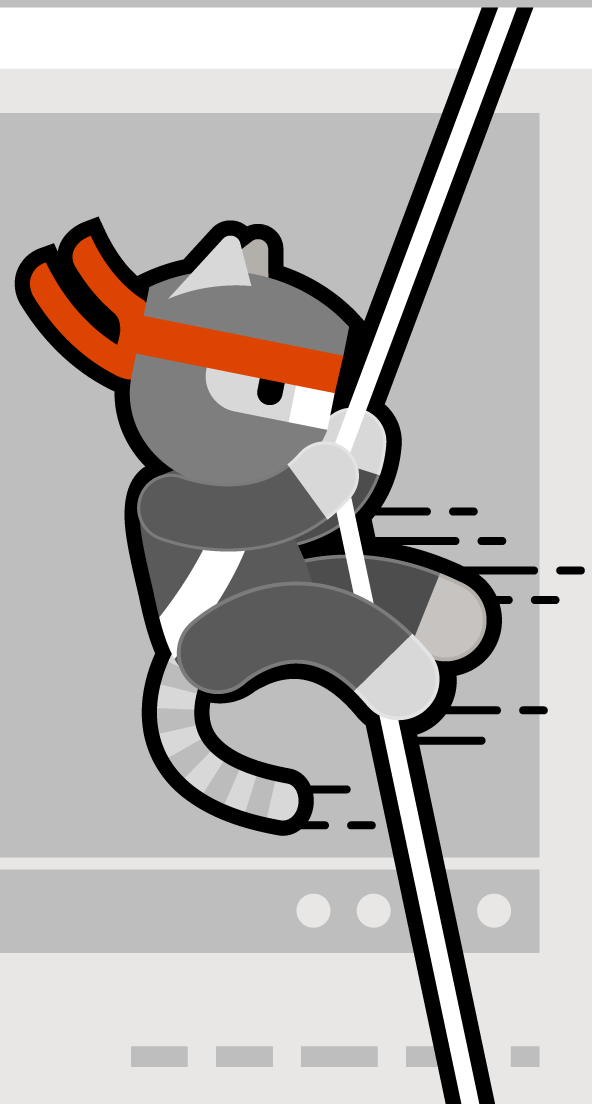
Cgroups

Starting in version 2.6.24 of the Linux Kernel, a functionality know as control groups, or *cgroups* for short, was released.

The latest release of cgroups (cgroups v2) was introduced in Kernel 4.5 and brings security enhancements to the systems.

Controls groups are a series of kernel-level resource controls for processes that can include the ability to limit a series of kernel-level resource controls for processes that can include the ability to limit resources, such as CPU, network, and disk, and isolate those resources from one another.

Demo
Setup of our Environment



References

Gray Hat Hacking, Sixth Edition