

Jails Lecture notes

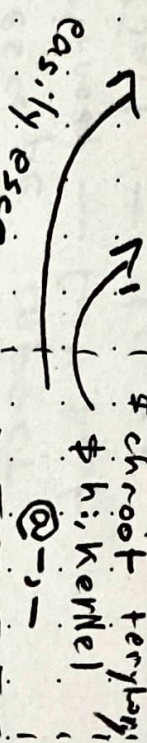
chroot - changes your root fs to another thing

↳ chroot - pretend this folder is /

- not designed for security
- bc root processes can easily exit the chroot

• this was not for security in the 1st place

/aaa /bbb /zendaya



then you can move freely through the system like an electron in metallic band.

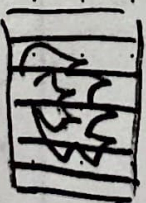
chroot is like changing the valence band



Jails, on the other hand

/aaa /bbb /zendaya

- ! limit fs
 - ! limit syscalls
 - ! limit network
- assuming unsafe kernel are there



↳ same kernel, tho
↳ And BSD-only

Bsd Jail = Linux namespaces + cgroups + capabilities + seccomp

Comparing Isolations

	sep. kern.	sep. fs.	sep. processes	sep. net	sys calls block
chroot	no	yes	no	no	no
containers	no	yes	yes	yes	yes
Jail	no	yes	yes	yes	yes
VM	yes	yes	yes	yes	yes

cost of performance



setup complexity



- escape impact
- chroot — full host
 - Jail — if soke
 - cont. — if soke
 - VM — don't worry

Jails make Antrening happy. why.