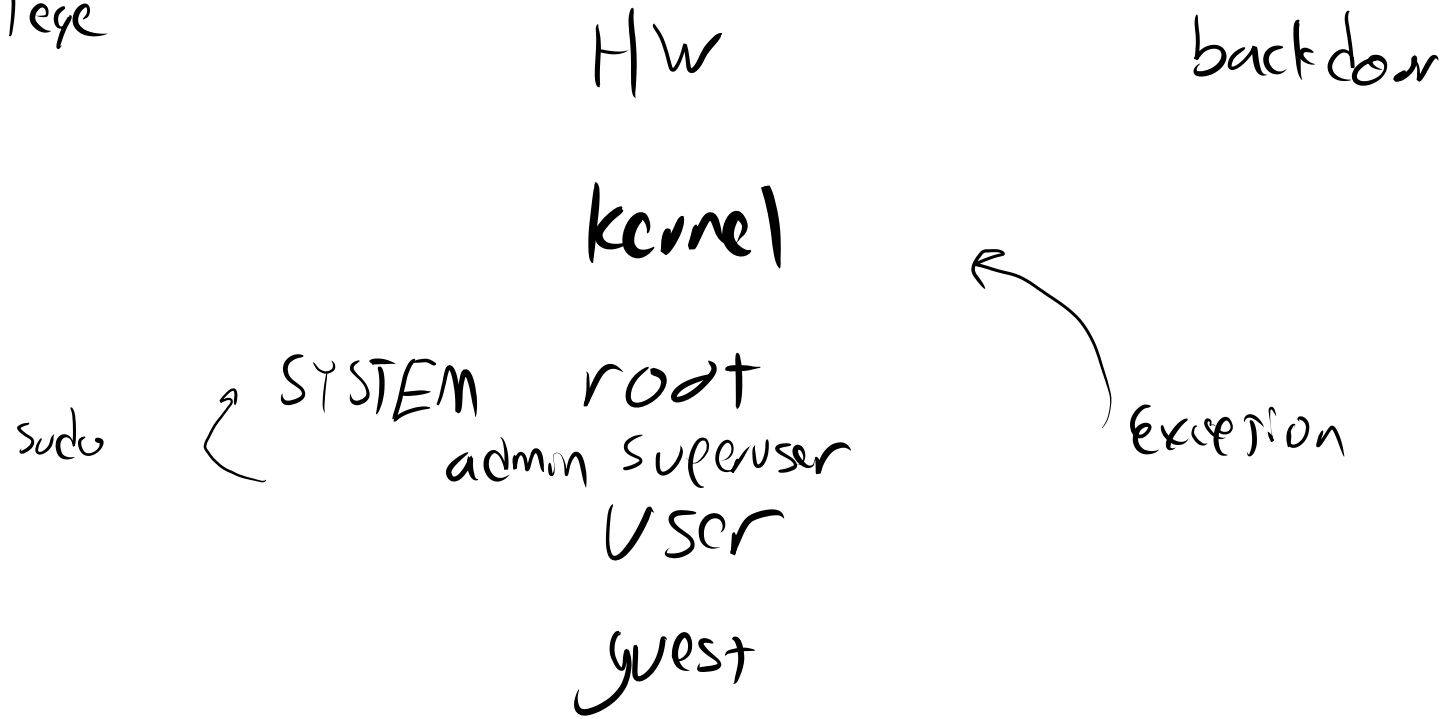


Principle of least privilege



→ Sandbox / Jail

Control input

data input ← buffer overflow

non-tech

Config
files

device
drivers

User

root

kernel

daemons

Avoid

- write good code
- permissions - minimal amount
 - protect resources
- don't stay lazy
 - ls - during dev
 - /bin/ls - release
- don't assume niceness
 - check everything?

.. / foo

✓ .. / .. / grades / mspk

Phishing