# Linux capabilities

Linux subdivides root's privileges into  40 capabilities, e.g.

- `cap_net_admin` – configure network interfaces (IP address, etc.)
- `cap_net_raw` – use raw sockets (bypassing UDP/TCP)
- `cap_sys_boot` – reboot
- `cap_sys_time` – adjust system clock

For instance ping needs raw network access, not ability to delete all files

```
$ ls -al /usr/bin/ping
-rwxr-xr-x 1 root root 61168 Nov 15 23:57 /usr/bin/ping
$ getcap /usr/bin/ping
/usr/bin/ping = cap_net_raw+ep
```

See also: `getcap(8)`, `setcap(8)`, `capsh(1)`

# Other permissions

When can process A send a signal to process B with kill?

- Allow if sender and receiver have same effective UID
- But need ability to kill processes you launch even if `setsuid`, so allow if real UIDs match, as well

Debugger system call `ptrace` - lets one process modify another's memory

- `setuid` gives a program more privilege than invoking user
  so do not let a process ptrace a more privileged process
  e.g. require sender to match real & effective UID of target
- Also disable/ignore `setuid` if ptraced target calls exec
- Exception - root can ptrace anyone