Про sandbox в macOS:

Code Signing = com.apple.driver.AppleMobileFileIntegrity.kext + /usr/libexec/amfid

– Entitlements = set fine-grained "rights"

Gatekeeper = on first launch: full check of all resources, check notarization (extra signature generated by Apple); on application launch: limited codesigning check (code only!)

Hardened Runtime (macOS Mojave 10.14) = protects against various forms of process injection;

Allowlist = syscalls a process can perform com.apple.security.sandbox.kext (since OS X 10.5) and /usr/libexec/sandboxd (since OS X 10.7)

=> sandbox based on profiles written in Scheme language; sandbox has hooks in all syscalls, across the entire kernel tree; redefines $HOME to ~/Library/Containers/<Bundle ID>/Data

System Integrity Protection = restricts file modifications, kernel/system extension loading and process debugging; actually it's just sandbox profile;

Sandbox: limit what functionality a process can use

SIP: limit which processes can use certain functionality

Dynamic Sandbox (macOS Mojave 10.14)

Signed System Volume = prevents modification of system files

TCC = handles user controlled permissions

Степень изоляции в Sandbox и Docker контейнерах?

Идея в том, что на macOS повышенный уровень изоляции для Docker контейнеров достигается за счет использования виртуальной машины на уровне операционной системы. При запуске Docker контейнеров на macOS Docker Desktop for Mac создает виртуальную машину на базе гипервизора, где запускается Docker Engine, и все Docker контейнеры запускаются внутри этой виртуальной машины.

Можно ли из докера запустить нативные маковские команды (написать докерфайл для os x)?

Нет, нельзя. Потому что docker запрограммирован таким образом, чтобы специально работать поверх ядра линукс. Docker контейнеры внутри macOS работают в Linux VM,

References

1. Docker on MacOS is slow and how to fix it: https://www.cncf.io/blog/2023/02/02/docker-on-macos-is-slow-and-how-to-fix-it/
2. Under the Hood: Demystifying Docker Desktop for Mac: https://collabnix.com/how-docker-for-mac-works-under-the-hood/
3. Hyperkit: https://github.com/moby/hyperkit
4. xhyve: https://github.com/machyve/xhyve
5. The Magic Behind the Scenes of Docker Desktop (Docker uses QEMU): https://www.docker.com/blog/the-magic-behind-the-scenes-of-docker-desktop/
6. Deep Dive Into the New Docker Desktop file sharing Implementation Using FUSE: https://www.docker.com/blog/deep-dive-into-new-docker-desktop-filesharing-implementation/
7. Virtualization Framework on macOS: https://developer.apple.com/documentation/virtualization
8. VirtioFS: https://virtio-fs.gitlab.io/
9. VPNKit: https://github.com/moby/vpnkit
10. DataKit: https://github.com/moby/datakit
11. Hypervisor: https://developer.apple.com/documentation/hypervisor
12. Rancher Desktop (Open Source): https://rancherdesktop.io/
13. Colima (Open Source): https://github.com/abiosoft/colima/
14. What is Hypervisor? https://www.vmware.com/topics/glossary/content/hypervisor.html
15. Podman vs Docker: What are the differences? https://www.imaginarycloud.com/blog/podman-vs-docker/
16. Podman vs Docker. All you need to know! https://www.lambdatest.com/blog/podman-vs-docker/
17. What is Enhanced Container Isolation? https://docs.docker.com/desktop/hardened-desktop/enhanced-container-isolation/

18. Virtualization.Framework vs Hyperkit.Framework: https://zarinfam.medium.com/what-are-the-advantages-of-the-new-virtualization-framework-in-macos-big-sur-7685c3aca0f7
19. Apple Extends macOS Virtualization Capabilities and Introduces Rosetta for Linux Binaries: https://www.infoq.com/news/2022/06/apple-virtualization-framework/
20. Are Docker containers really secure? https://opensource.com/business/14/7/docker-security-selinux
21. Docker Namespaces and Cgroups: https://medium.com/@kasunmaduraeng/docker-namespace-and-cgroups-dece27c209c7
22. LXC vs Docker: https://earthly.dev/blog/lxc-vs-docker/
23. 2022 - macOS local security: escaping the sandbox and bypassing TCC: https://youtu.be/vMGiplQtjTY
24. App Sandbox: https://developer.apple.com/documentation/security/app_sandbox
25. Uncovering a macOS App Sandbox escape vulnerability: A deep dive into CVE-2022-26706: https://www.microsoft.com/en-us/security/blog/2022/07/13/uncovering-a-macos-app-sandbox-escape-vulnerability-a-deep-dive-into-cve-2022-26706/
26. Attacking & Auditing Docker Containers Using Open Source (Namespaces): https://madhuakula.com/content/attacking-and-auditing-docker-containers-using-opensource/attacking-docker-containers/namespaces.html