Docker Security

황상철

espressobook

"도커가 위험하다고 생각하는 이유는 (내가) 잘 모르기 때문은 아닐까"

1.도커 호스트 서버
2.이미지
3.컨테이너

도커 호스트 서버

- 도커 데몬은 신뢰할 수 있는 사용자만 접근 가능해야 한다.
  - 도커 데몬은 root 권한으로 실행된다.
- 도커 호스트 서버에 어드민 관리 도구를 실행하지 마라.
- REST API는 TCP 소켓대신 UNIX 소켓을 사용한다.

도커 이미지

- 도커 이미지는 안전한 위치에 저장되어야 하며 체크섬을 가져야 한다.
- 배포전에 보안패치를 빌드해야 한다.
  - on build 옵션
- --privileged 사용하지 않는다.

도커 컨테이너

- 컨테이너에서 실행되는 프로세스는 다른 컨테이너의 프로세스에 영향을 줄 수 없다.
- 컨테이너는 자신만의 네트워크 스택을 갖는다.
  - 브릿지

https://docs.docker.com/engine/security/security/

컨테이너가 폭주하면

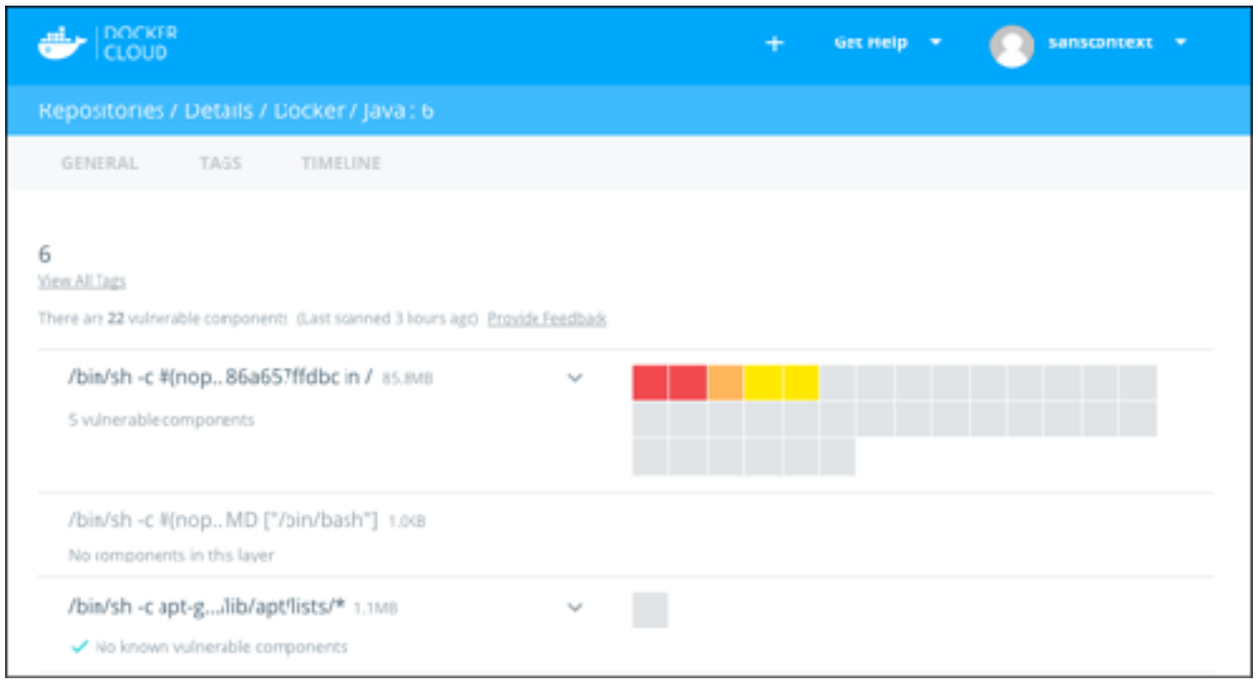
- 컨테이너는 메모리,CPU,I/O 자원을 공유한다.
- 컨테이너는 호스트 서버 모든 자원을 소진할 수 없다.
- Kernal panic과 DoS 방지

https://docs.docker.com/engine/security/security/

이런 이슈를 한방에
해결해주는 도구는 없나요

Docker Security Scanning

레지스트리에 애드온되어 이미지 보안 취약점을 스캔해서 알려준다.



https://docs.docker.com/docker-cloud/builds/image-scan/

Login to Docker Cloud

Sangcheol

https://cloud.docker.com/login

Welcome to Docker Cloud

Login with your **Docker ID**

Docker ID

Password

Login

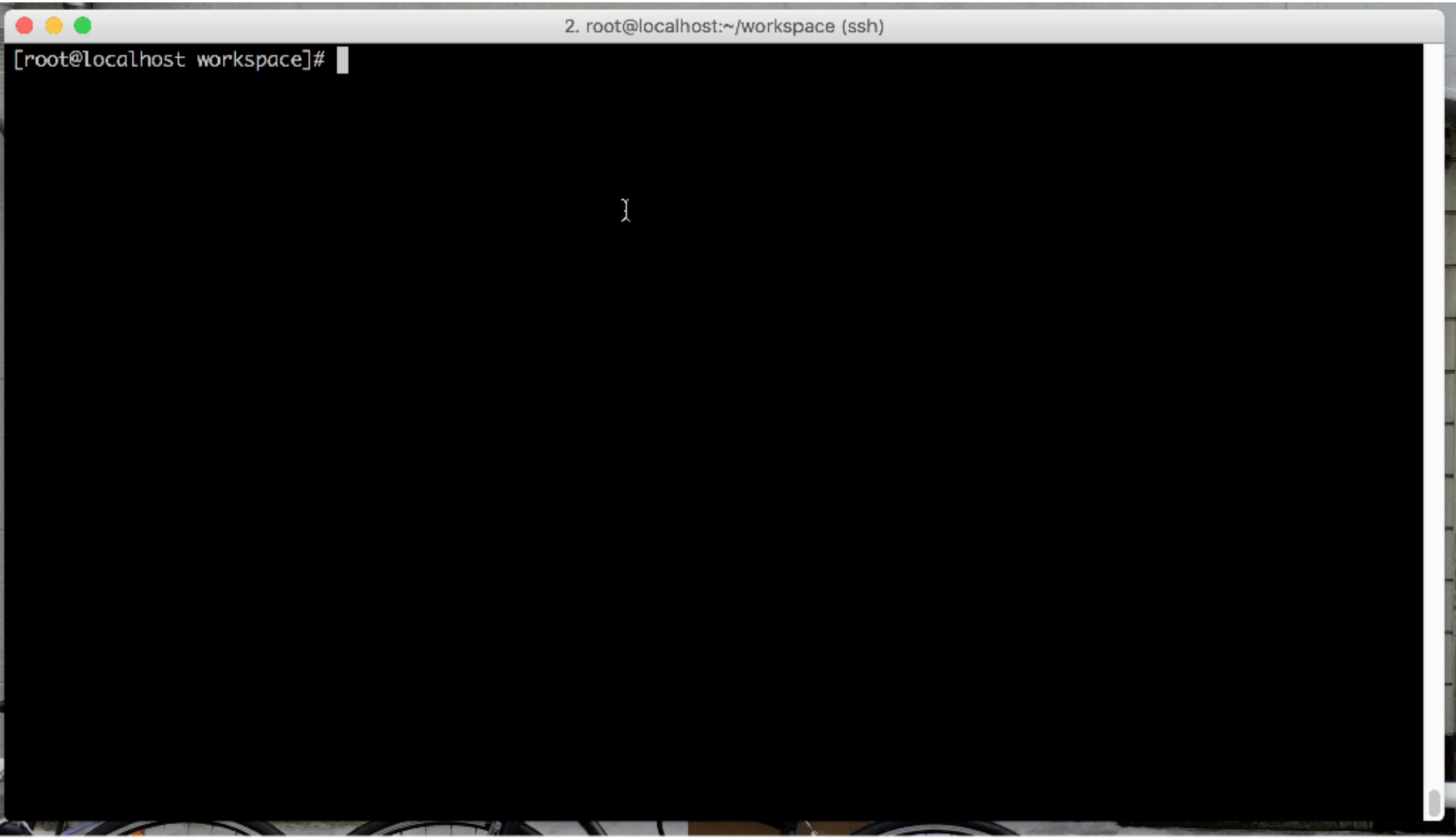
Forgot Password? | Create Account

Docker Bench

도커 호스트와 컨테이너에 대한 보안 취약점을 체크해주는 스크립트

- https://github.com/docker/docker-bench-security

- https://benchmarks.cisecurity.org/tools2/docker/CIS_Docker_1.11.0_Benchmark_v1.0.0.pdf


2. root@localhost:~/workspace (ssh)
[root@localhost workspace]#