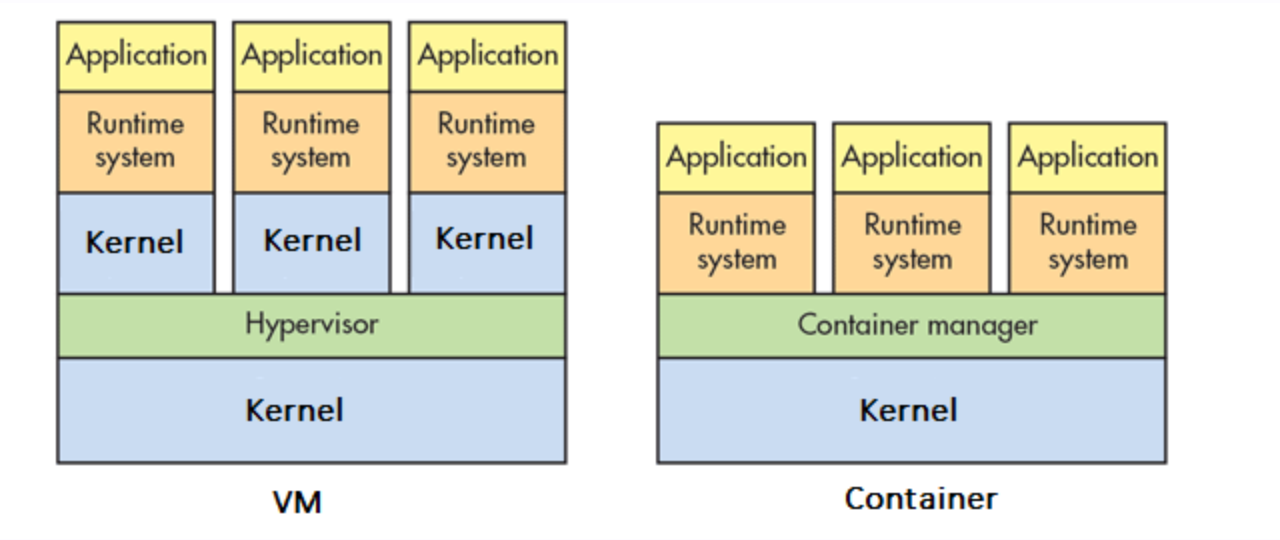
Born to be Root

How we can protect our Infrastructure

Architecture of Docker

Share kernel Host



0 - Keep Host and Docker up to date

1 - Set a user

File: Dockerfile

```
1  FROM alpine
2  RUN addgroup -S myuser && adduser -S myuser -G myuser
3  RUN apk add cowsay --repository=http://dl-cdn.alpinelinux.org/alpine/edge/testing/
4  USER myuser
```

```
➜  set-user docker run -it --rm alpine-root
/ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
/ # cowsay Born to be Root
 ________________
< Born to be Root >
 ----------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
/ # exit
➜  set-user docker run -it --rm alpine-myuser
/ $ id
uid=100(myuser) gid=101(myuser) groups=101(myuser)
/ $ cowsay Born to be standard user
 ________________________
< Born to be standard user >
 ------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
/ $ exit
➜  set-user
```

2 - Limit resources

```
28              - name: http
29                containerPort: 8080
30            readinessProbe:
31              httpGet:
32                path: /health
33                port: http
34            livenessProbe:
35              httpGet:
36                path: /health
37                port: http
38            resources:
39              # Limits impose a restriction on how much of a given compute resource
40              # the container can get. If the limit is surpassed, the container
41              # might be terminated, depending on  the cluster available resources
42              limits:
43                cpu: <value>
44                memory: <value>
45              # Resources specify that a container will reserve the given amount of
46              # the given compute resource for itself. Those resources are not available
47              # for any other container in the whole cluster, even if not used
48              requests:
49                cpu: <value>
50                memory: <value>
```

3 - Set filesystem and volumes to read-only

```
➜  set-filesystem docker run -it --rm --read-only --tmpfs /tmp alpine
/ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
/ # ls
bin    dev    etc    home   lib    media  mnt    opt    proc   root   run    sbin   srv    sys    tmp    usr    var
/ # mkdir holamundo
mkdir: can't create directory 'holamundo': Read-only file system
/ # cd tmp/
/tmp # touch holamundo
/tmp # ls
holamundo
/tmp #
```

4 - Use static analysis tools

```
➜  set-filesystem trivy image alpine-myuser
2022-11-17T14:11:28.303+0100    INFO    Vulnerability scanning is enabled
2022-11-17T14:11:28.303+0100    INFO    Secret scanning is enabled
2022-11-17T14:11:28.303+0100    INFO    If your scanning is slow, please try '--security-checks vuln' to disable secret scanning
2022-11-17T14:11:28.303+0100    INFO    Please see also https://aquasecurity.github.io/trivy/v0.34/docs/secret/scanning/#recommendatio
n for faster secret detection
2022-11-17T14:11:28.727+0100    INFO    Detected OS: alpine
2022-11-17T14:11:28.727+0100    INFO    Detecting Alpine vulnerabilities...
2022-11-17T14:11:28.728+0100    INFO    Number of language-specific files: 0

alpine-myuser (alpine 3.16.2)

Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)
```

```
→  set-filesystem trivy image adoptopenjdk:11-jre-hotspot
2022-11-17T15:21:41.937+0100    INFO    Vulnerability scanning is enabled
2022-11-17T15:21:41.937+0100    INFO    Secret scanning is enabled
2022-11-17T15:21:41.937+0100    INFO    If your scanning is slow, please try '--security-checks vuln' to disable secret scanning
2022-11-17T15:21:41.937+0100    INFO    Please see also https://aquasecurity.github.io/trivy/v0.34/docs/secret/scanning/#recommendation for faster secret detection
2022-11-17T15:21:43.800+0100    INFO    Detected OS: ubuntu
2022-11-17T15:21:43.800+0100    INFO    Detecting Ubuntu vulnerabilities...
2022-11-17T15:21:43.802+0100    INFO    Number of language-specific files: 0

adoptopenjdk:11-jre-hotspot (ubuntu 20.04)

Total: 181 (UNKNOWN: 0, LOW: 81, MEDIUM: 94, HIGH: 6, CRITICAL: 0)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
bash	CVE-2022-3715	MEDIUM	5.0-6ubuntu1.1		bash: a heap-buffer-overflow in valid_parameter_transform https://avd.aquasec.com/nvd/cve-2022-3715
	CVE-2019-18276	LOW		5.0-6ubuntu1.2	bash: when effective UID is not equal to its real UID the... https://avd.aquasec.com/nvd/cve-2019-18276
bsdutils	CVE-2021-3995	MEDIUM	2.34-0.1ubuntu9.1	2.34-0.1ubuntu9.3	util-linux: Unauthorized unmount of FUSE filesystems belonging to users with similar uid... https://avd.aquasec.com/nvd/cve-2021-3995
	CVE-2021-3996				util-linux: Unauthorized unmount of filesystems in libmount https://avd.aquasec.com/nvd/cve-2021-3996
coreutils	CVE-2016-2781	LOW	8.30-3ubuntu2		coreutils: Non-privileged session can escape to the parent session in chroot https://avd.aquasec.com/nvd/cve-2016-2781
curl	CVE-2022-22576	MEDIUM	7.68.0-1ubuntu2.7	7.68.0-1ubuntu2.10	curl: OAUTH2 bearer bypass in connection re-use https://avd.aquasec.com/nvd/cve-2022-22576
	CVE-2022-27774				curl: credential leak on redirect https://avd.aquasec.com/nvd/cve-2022-27774
	CVE-2022-27782			7.68.0-1ubuntu2.11	curl: TLS and SSH connection too eager reuse https://avd.aquasec.com/nvd/cve-2022-27782

5 - Lint the Dockerfile at build time

Demo Time

Review

- Keep Host and Docker up to date
- Set a user
- Limit resources
- Set filesystem and volumes to read-only
- Use static analysis tools
- Lint the Dockerfile at build time

Thanks! 👋