```
CONTAINER ID   NAME             CPU %     MEM USAGE / LIMIT     MEM %     NET I/O         BLOCK I/O        PIDS
b799d87783c5   test-container   0.00%     10.35MiB / 7.437GiB   0.14%     1.17kB / 126B   197kB / 12.3kB   13
```

```
marti@HONORDeMartin:~/ece-container-security-BAS$ docker run --rm --cap-add=SYS_ADMIN alpine sh -c \
  "apk add -U libcap >/dev/null 2>&1 && \
   v=\$(grep CapEff /proc/self/status | awk '{print \$2}'); \
   capsh --decode=\$v"
0x00000000a82425fb=cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chro
ot,cap_sys_admin,cap_mknod,cap_audit_write,cap_setfcap
```

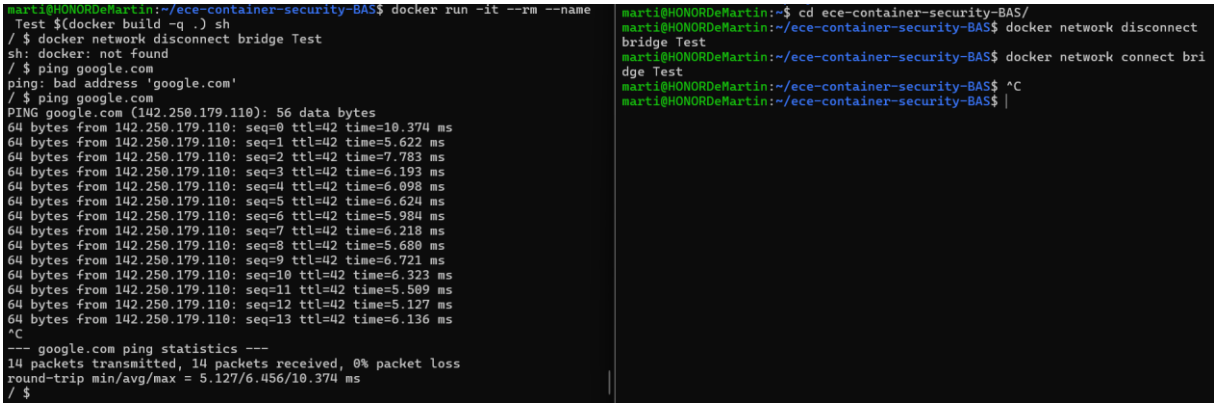
```
marti@HONORDeMartin:~/ece-container-security-BAS$ docker run --rm --privileged alpine sh -c 'echo hello from privileged mode'
hello from privileged mode
marti@HONORDeMartin:~/ece-container-security-BAS$
```

Lancer un containeur en mode privilégier le rapproche beaucoup d'un accès root : à la moindre faille de sécurité, il donne accès à beaucoup de périphériques de l'hôte normalement bloqués (disques mémoire, réseaux etc...)

```
marti@HONORDeMartin:~/ece-container-security-BAS$ docker run --rm -v /:/mnt alpine sh -c 'ls -la /mnt'
total 2808
drwxr-xr-x   23 root     root          4096 Feb  4 13:05 .
drwxr-xr-x    1 root     root          4096 Feb  4 14:33 ..
drwxr-xr-x    3 root     root          4096 Oct 29 12:39 Docker
lrwxrwxrwx    1 root     root             7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x    2 root     root          4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x    2 root     root          4096 Apr 22  2024 boot
drwxr-xr-x   15 root     root          3940 Feb  4 13:05 dev
drwxr-xr-x   89 root     root          4096 Feb  4 13:18 etc
drwxr-xr-x    3 root     root          4096 Sep 17 12:32 home
-rwxr-xr-x    1 root     root       2781568 Dec 12 01:58 init
lrwxrwxrwx    1 root     root             7 Apr 22  2024 lib -> usr/lib
drwxr-xr-x    2 root     root          4096 Apr  8  2024 lib.usr-is-merged
lrwxrwxrwx    1 root     root             9 Apr 22  2024 lib64 -> usr/lib64
drwx------    2 root     root         16384 Sep 17 12:31 lost+found
drwxr-xr-x    2 root     root          4096 Aug  5  2025 media
drwxr-xr-x    6 root     root          4096 Sep 17 12:32 mnt
drwxr-xr-x    3 root     root          4096 Dec 23 14:43 opt
dr-xr-xr-x  312 root     root             0 Feb  4 13:05 proc
drwx------    6 root     root          4096 Oct 29 12:39 root
drwxr-xr-x   20 root     root           680 Feb  4 13:05 run
lrwxrwxrwx    1 root     root             8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x    2 root     root          4096 Mar 31  2024 sbin.usr-is-merged
drwxr-xr-x    2 root     root          4096 Sep 17 12:32 snap
drwxr-xr-x    2 root     root          4096 Aug  5  2025 srv
dr-xr-xr-x   13 root     root             0 Feb  4 13:04 sys
drwxrwxrwt    9 root     root          4096 Feb  4 13:28 tmp
drwxr-xr-x   12 root     root          4096 Aug  5  2025 usr
drwxr-xr-x   13 root     root          4096 Sep 17 12:32 var
marti@HONORDeMartin:~/ece-container-security-BAS$
```

En montant la racine de l'hôte dans /mnt, on donne au containeur accès à toute la mémoire de l'hote, la rendant extrêmement vulnérable.

```
/ $ id
uid=1000(appuser) gid=1000(appuser) groups=1000(appuser)
/ $ exit
marti@HONORDeMartin:~/ece-container-security-BAS$
```



En effet, après la commande docker network disconnect bridge Test (ici le nom du containeur), le ping de google.com est impossible tant que la commande docker network connect bridge Test n'est pas entrée.

```
marti@HONORDeMartin:~/ece-container-security-BAS$ trivy image vulnerables/web-dvwa | grep "CRITICAL"
2026-02-04T17:08:37+01:00       INFO    Vulnerability scanning is enabled
2026-02-04T17:08:37+01:00       INFO    Secret scanning is enabled
2026-02-04T17:08:37+01:00       INFO    If your scanning is slow, please try '--scanners vuln' to disable
 secret scanning
2026-02-04T17:08:37+01:00       INFO    Please see also https://aquasecurity.github.io/trivy/v0.52/docs/s
canner/secret/#recommendation for faster secret detection
2026-02-04T17:08:37+01:00       INFO    Detected OS     family="debian" version="9.5"
2026-02-04T17:08:37+01:00       INFO    [debian] Detecting vulnerabilities...   os_version="9" pkg_num=21
5
2026-02-04T17:08:37+01:00       INFO    Number of language-specific files       num=0
2026-02-04T17:08:38+01:00       WARN    This OS version is no longer supported by the distribution      f
amily="debian" version="9.5"
2026-02-04T17:08:38+01:00       WARN    The vulnerability detection may be insufficient because security
updates are not provided
Total: 1575 (UNKNOWN: 12, LOW: 116, MEDIUM: 642, HIGH: 551, CRITICAL: 254)
| apache2                 | CVE-2019-10082   | CRITICAL | fixed        | 2.4.25-3+deb9u5           | 2
.4.25-3+deb9u8                  | httpd: read-after-free in h2 connection shutdown          |
| apache2-bin             | CVE-2019-10082   | CRITICAL |              |                           | 2
.4.25-3+deb9u8                  | httpd: read-after-free in h2 connection shutdown          |
| apache2-data            | CVE-2019-10082   | CRITICAL |              |                           | 2
.4.25-3+deb9u8                  | httpd: read-after-free in h2 connection shutdown          |
| apache2-utils           | CVE-2019-10082   | CRITICAL |              |                           | 2
.4.25-3+deb9u8                  | httpd: read-after-free in h2 connection shutdown          |
| bzip2                   | CVE-2019-12900   | CRITICAL |              | 1.0.6-8.1                 |
                                | bzip2: bzip2: Data integrity error when decompressing (with  |
| dpkg                    | CVE-2022-1664    | CRITICAL |              | 1.18.25                   | 1
.18.26                          | Dpkg::Source::Archive in dpkg, the Debian package management |
| inetutils-ping          | CVE-2020-10188   | CRITICAL |              | 2:1.9.4-2+b1              | 2
:1.9.4-2+deb9u1                 | telnet-server: no bounds checks in nextitem() function    |
| libapache2-mod-php7.0   | CVE-2017-8923    | CRITICAL | will_not_fix | 7.0.30-0+deb9u1           |
                                | php: Overflowing the length of string causes crash        |
| libbsd0                 | CVE-2019-20367   | CRITICAL | fixed        | 0.8.3-1                   | 0
.8.3-1+deb9u1                   | nlist.c in libbsd before 0.10.0 has an out-of-bounds read |
| libc6                   | CVE-2017-18269   | CRITICAL |              |                           |
                                | glibc: memory corruption in memcpy-sse2-unaligned.S       |
```

254 vulnérabilités sont relevées par trivy

```
marti@HONORDeMartin:~/ece-container-security-BAS$ grype alpine:latest
 ✔ Vulnerability DB                [updated]
 ✔ Loaded image                                                                    alpine:latest
 ✔ Parsed image                    sha256:a40c03cbb81c59bfb0e0887ab0b1859727075da7b9cc576a1cec2c771f38c
 ✔ Cataloged contents                 ceedcaa851833940d364da9a0a99b8c50699bef7776439e2fb3d923a60a6638b
   ├── ✔ Packages                        [16 packages]
   ├── ✔ Executables                     [17 executables]
   ├── ✔ File metadata                   [79 locations]
   └── ✔ File digests                    [79 files]
 ✔ Scanned for vulnerabilities     [3 vulnerability matches]
   ├── by severity: 0 critical, 0 high, 3 medium, 0 low, 0 negligible
NAME           INSTALLED   TYPE  VULNERABILITY   SEVERITY  EPSS           RISK
busybox        1.37.0-r30  apk   CVE-2025-60876  Medium    < 0.1% (16th)  < 0.1
busybox-binsh  1.37.0-r30  apk   CVE-2025-60876  Medium    < 0.1% (16th)  < 0.1
ssl_client     1.37.0-r30  apk   CVE-2025-60876  Medium    < 0.1% (16th)  < 0.1
A newer version of grype is available for download: 0.107.1 (installed version is 0.107.0)
marti@HONORDeMartin:~/ece-container-security-BAS$
```

Tandis que Grype ne trouve que 3 vulnérabilités de niveau MEDIUM

```
marti@HONORDeMartin:~/ece-container-security-BAS$ rm Dockerfile
marti@HONORDeMartin:~/ece-container-security-BAS$ nano Dockerfile
marti@HONORDeMartin:~/ece-container-security-BAS$ docker run -it --rm --name Test $(docker build -q .) sh
/app $
/app $
/app $ whoami
appuser
/app $
```

```
marti@HONORDeMartin:~/ece-container-security-BAS$ docker run --rm monapp-distroless
ECE, 2K26!
marti@HONORDeMartin:~/ece-container-security-BAS$ docker run --rm monapp-full
ECE, 2K26!
marti@HONORDeMartin:~/ece-container-security-BAS$ docker images | grep monapp
monapp-distroless             latest    3496c8f1b348   2 minutes ago    9.15MB
monapp-full                   latest    8e54857b2cc0   2 minutes ago    1.53GB
marti@HONORDeMartin:~/ece-container-security-BAS$
```

On constate que l'image distroless est environ 150 fois moins volumineuse que l'image full.