链滴

Docker 暴重大安全漏洞：外部网络可直接访问映射到 127.0.0.1 的本地服务

作者：JayGao

原文链接：https://ld246.com/article/1657246819290

来源网站：链滴

问题概述

这两天 Hacker News 上面有一个贴子 ^[1]^ 火了，这是一封发给 Docker 安全团队的邮件，主要讲是 Docker 有一个非常离谱的安全隐患。 **即使你通过像 -p 127.0.0.1:80:80 这样的参数将端口暴露回环地址，外部仍然可以访问该服务** ，怎么回事呢?

产生原因

原因其实很简单，Docker 添加了这样一条 Iptables 规则：

```
:whale:  → iptables -nvL DOCKER
Chain DOCKER (2 references)
 pkts bytes target prot opt in       out     source    destination
    0 0     ACCEPT tcp  --  !docker0 docker0 0.0.0.0/0 172.17.0.2  tcp dpt:80
```

只要外部攻击者通过这台主机将流量发送到 172.17.0.2:80，就会匹配这条规则并成功访问容器中的务，127.0.0.1 并没有什么卵用。

尴尬的是，选择将端口映射到 127.0.0.1 的用户基本上都是觉得这样很安全，以至于他们不再想采取一步的安全措施。现在问题来了，映射到 127.0.0.1 **不能说是非常安全吧，只能说是与安全毫不相干**。。。

概念验证

下面通过一个例子来验证。

① 在 A 机器上运行一个 PostgreSQL 容器，并将端口映射到 127.0.0.1。

```
# IP: 192.168.0.100
:whale:  → docker run -e POSTGRES_PASSWORD=password -p 127.0.0.1:5432:5432 postgres
```

② 同一个局域网中的 B 机器添加路由表，将所有访问 172.16.0.0/12 的流量指向 A 机器。

```
# IP: 192.168.0.200
:whale: → ip route add 172.16.0.0/12 via 192.168.0.100
```

③ 在 B 机器中扫描 A 机器的端口。

```
:whale: → nmap -p5432 -Pn --open 172.16.0.0/12
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-05 15:00 CDT
Nmap scan report for 172.17.0.2
Host is up (0.00047s latency).

PORT     STATE SERVICE
5432/tcp open  postgresql
```

④ 在 B 机器中直接连接 PostgreSQL。

```
:whale: → psql -h 172.17.0.2 -U postgres
Password for user postgres:
```

解决方案

事实上不仅仅是 127.0.0.1，你将容器端口映射到主机的任何一个地址，外部都可以访问到，这就离大谱了！

邮件作者给 Docker 团队提出了一个解决方案，希望能优化 Docker 的 iptables 规则：

① 首先要严格限制允许访问容器端口的源地址和网络接口，例如 docker run -p 127.0.0.1:5432:5432 的**原** iptables 规则如下：

```
Chain DOCKER (2 references)
 pkts bytes target prot opt in       out     source    destination
    0 0     ACCEPT tcp  --  !docker0 docker0 0.0.0.0/0 172.17.0.2  tcp dpt:5432
```

改进后的 iptables 规则如下：

```
Chain DOCKER (2 references)
 pkts bytes target prot opt in out     source      destination
    0 0     ACCEPT tcp  --  lo docker0 127.0.0.1/8 172.17.0.2 tcp dpt:5432
```

同理，如果主机的地址为 192.168.0.100，掩码为 24，那么 docker run -p 192.168.0.100:5432:5432 的 iptables 规则就应该是：

```
Chain DOCKER (2 references)
 pkts bytes target prot opt in   out     source         destination
    0 0     ACCEPT tcp  --  eth0 docker0 192.168.0.0/24 172.17.0.2 tcp dpt:5432
```

② 最后要修改默认行为，如果使用 -p 参数时没有指定任何 IP 地址，就默认映射到 127.0.0.1。

虽然评论区也有很多人给出了添加 iptables 规则来进行限制的方案，但这是不现实的，目前全世界有千上万的用户在使用 -p 参数将容器端口映射到 127.0.0.1，攻击者估计早就发现了这个漏洞，我们不期望用户自己添加 iptables 规则来限制外部访问，最靠谱的方式还是等 Docker 官方修复这个 bug 后升级吧。

引用文章

Hacker News 上面有一个贴子: https://news.ycombinator.com/item?id=31839936

github issues

Docker Network bypasses Firewall, no option to disable · Issue #22054 · moby/moby (github.om)