网络安全工具 TCP Wrapper

作者：leekeggs
原文链接：https://ld246.com/article/1544333777441
来源网站：链滴

1. 什么是TCP Wrapper

TCP Wrapper是一个基于主机的网络访问控制表系统，用于过滤对类Unix系统（如Linux或BSD）的络访问。

当网络请求到达我们的服务器时，TCP Wrapper使用hosts.allow和hosts.deny（按此顺序）来确定户端能否访问给定的服务。

需要注意的是，并非所有网络服务都支持使用TCP Wrapper,我们可以下面的命令确认网络服务是否持TCP Wrapper

```
$ ldd /path/to/binary | grep libwrap
```

如果上述命令有结果输入，则表示该服务支持TCP Wrapper。

注意：/path/to/binary是指网络服务的绝对路径

我们以sshd和vsftpd服务为例：

```
[wxyuan@node1 ~]$ ldd $(which sshd) | grep libwrap
        libwrap.so.0 => /lib64/libwrap.so.0 (0x00007f3b1b1e4000)
[wxyuan@node1 ~]$
[wxyuan@node1 ~]$ ldd $(which vsftpd) | grep libwrap
        libwrap.so.0 => /lib64/libwrap.so.0 (0x00007fcde2dfd000)
```

可以看到sshd和vsftpd服务都支持TCP Wrapper.

2. 如何使用TCP Wrappers限制对服务的访问

TCP Wrappers对网络服务的访问控制基于下面两个文件：

- /etc/hosts.allow
- /etc/hosts.deny

当客户端尝试连接到远程系统上的网络服务时，这两个文件用于确定是允许还是拒绝客户端访问。

使用/etc/hosts.allow和/etc/hosts.deny定义访问规则，控制客户端对网络服务的访问。

两个文件的语法是相同的：

```
<services> : <clients> [: command : command : ...]
```

参数说明：

- services:应用当前规则的逗号分隔的服务列表。，关键字　ALL表示所有服务
- clients:表示受该规则影响的逗号分隔的主机名或IP地址列表，关键字　ALL表示所有的客户端
- command:冒号分隔动作的可选列表指示触发给定规则时应该发生什么

要允许客户端访问，请在/etc/hosts.allow中添加客户端主机名或IP地址。要拒绝客户端访问，请在/et/hosts.deny中添加其名称或IP地址。

请注意：/etc/hosts.allow中允许的规则优先于/etc/hosts.deny中禁止的规则。

当服务器接收到对指定网络服务的请求时，规则匹配过程如下：

首先读取/etc/hosts.allow文件，并从上到下读取。将网络服务（services）和客户端（clients），

文件中的第一行进行对比，如果匹配，则授予访问权限。

如果该行不匹配，则读取下一行并执行相同的检查。如果读取所有行并且不匹配，则从顶部开始读取/tc/hosts.deny文件。

如果在hosts.deny文件中找到匹配行，则拒绝访问。如果在两个文件中都找不到匹配行，或者两个文都不存在，则授予对服务的访问权限。

举两个例子：

(1) 只允许192.168.1.101、192.168.1.102和192.168.1.103访问sshd服务，拒绝其它客户端对sshd务的访问。首先在/etc/hosts.allow文件中添加如下内容：

```
sshd:192.168.1.101,192.168.1.102,192.168.1.103
```

在/etc/hosts.deny添加如下内容：

```
sshd:ALL
```

注意：由于首先应用hosts.allow中的访问规则，所以它们优先于hosts.deny中指定的规则。因此，果hosts.allow中允许访问服务，则会忽略hosts.deny中相同服务的规则。

(2) 允许192.168.1.0/24子网的客户端访问vsftpd服务，拒绝其它客户端对vsftpd服务的访问。首先在etc/hosts.allow文件中增加如下内容

```
vsftpd:192.168.1.*
```

在/etc/hosts.deny添加如下内容：

```
sshd:ALL
```

从这个例子可以看到，/etc/hosts.allow和/etc/hosts.deny支持使用通配符来配置规则

(3) 允许example.com子域中的主机访问sshd和vsftpd服务，在/etc/hosts.allow文件中增加如下内：

```
sshd,vsftpd:.example.com
```

从这个例子可以看到，/etc/hosts.allow和/etc/hosts.deny支持使用域名来配置规则