

longyu\_wlz

已于 2022-08-13 07:20:59 修改

1641

收藏 5

分类专栏:

securitylinux security

文章标签:

linuxdebianserver

 security

同时被 2 个专栏收录 \*

0 订阅

3 篇文章

订阅专栏

这两天在学习 Linux capabilities 权限相关内容，无意中发现 ping 命令原来需要一个特殊的 capability 权限才能够正常使用，root 用户当然可以 [bypass](#) 这个权限，然而普通用户却不能直接获取到这个权限，这意味着普通用户不能使用 ping 命令来发送 icmp 请求。

可是在主流的发行版中并没有这个限定，普通用户能够正常使用 ping，这背后着实有些机关，本文将探讨其背后的原理。

### man ping 得到的信息

man 一下，获取到如下信息：

```
1 SECURITY
2     ping requires CAP_NET_RAW capability to be executed 1) if the program is used for non-echo queries (See
3     sockets, or 3) if the user is not allowed to create an ICMP echo socket. The program may be used as set-
4     .....
5 AVAILABILITY
6     ping is part of iputils package.
```

如上信息表明，在下面几种场景中 ping 命令需要 CAP\_NET\_RAW 权限来执行：

- ping 命令被用于非 echo 请求
- 内核不支持非原生 ICMP 套接字
- 用户不能创建一个 ICMP echo 套接字

为了支持如上场景，可以给 ping 命令添加 [suid](#) root 权限，这样普通用户在执行 ping 命令时就会拥有与 root 相同的权限，就能够正常使用了。

写到这里好像已经破案了，但我查看 debian11 中 ping 命令的权限却发现并没有 suid 位的设定，相关内容如下：

```
1 [longyu@debian:07:45:02] tmp $ ls -lh /usr/bin/ping
2 -rwxr-xr-x 1 root root 76K Feb  3  2021 /usr/bin/ping
```

可以看到，ping 命令并没有设定 suid 位，此时应该不能正常使用 ping，可事实证明普通用户确实能够正常使用，看来这里有些机关。

### Linux capabilities 与 CAP\_NET\_RAW 权限

如果你研究过 Linux capabilities，可能马上能够 get 到其中的机关。对于小白来说，可以先执行如下命令查看 ping 命令的 capabilities 权限：

```
1 [longyu@debian:21:51:13] linux-git $ sudo getcap /bin/ping
2 [sudo] password for longyu:
3 /bin/ping cap_net_raw=ep
```

getcap 命令用于获取一个文件的 Linux capabilities 属性，上面的输出表明 ping 命令具有 cap\_net\_raw 权限，这样当普通用户执行 ping 命令时，在 execve 时就能够获取到 CAP\_NET\_RAW 权限，就能够正常使用 ping 命令。

那么这个权限又是谁添加的呢？

### debian11 iputils 安装包的配置过程

ping 命令属于 iputils 安装包，执行 sudo apt-get source iputils 下载安装包源码，然后查看 iputils-20210202/debian/putils-ping.postinst 文件，此文件为 iputils 包部署 ping 命令后执行的配置操作。

其中设置 ping 命令权限的操作代码如下：

```
1 if [ "$1" = configure ]; then
2     # If we have setcap installed, try setting cap_net_raw=ep,
3     # which allows us to install our binaries without the setuid
4     # bit.
5     if command -v setcap > /dev/null; then
6         if setcap cap_net_raw=ep $PROGRAM; then
7             chmod u-s $PROGRAM
8         else
9             echo "Setcap failed on $PROGRAM, falling back to setuid" >&2
10            chmod u+s $PROGRAM
11        fi
12    else
13        echo "Setcap is not installed, falling back to setuid" >&2
14        chmod u+s $PROGRAM
15    fi
16 fi
```

当系统中安装了 setcap 命令时，此脚本优先使用 setcap 命令给 ping 命令添加 cap\_net\_raw 权限，添加成功则去掉 suid 位，添加失败、setcap 命令未安装则添加 suid 位。

好了，机关到此揭晓！其实是发行版在安装 ping 命令时单独给 ping 命令添加了需要的权限。

### 为什么要使用 setcap 单独给 ping 命令添加特定权限？

使用传统的 suid root 权限也能够实现普通用户使用 ping 的功能，可是这样的实现并不安全。按照最小权限的原则，普通用户要执行 ping 命令只需要添加 CAP\_NET\_RAW 权限，不需要其它的特殊权限，而 suid 这种方式却会拥有与 root 相同的权限执行程序，安全性没有保障，于是现在的主流发行版基本都优先使用 setcap 来给 ping 命令单独添加 CAP\_NET\_RAW 权限。

### 去掉 CAP\_NET\_RAW 权限后普通用户执行 ping 命令的输出

```
1 [longyu@debian:08:09:28] tmp $ sudo setcap cap_net_raw=ep /usr/bin/ping
2 [longyu@debian:08:09:46] tmp $ ping www.baidu.com
3 ping: socket: Operation not permitted
4 [longyu@debian:08:09:52] tmp $ strace ping www.baidu.com 2>&1 | grep socket
5 socket(AF_INET, SOCK_DGRAM, IPPROTO_ICMP) = -1 EACCES (Permission denied)
6 socket(AF_INET, SOCK_RAW, IPPROTO_ICMP) = -1 EPERM (Operation not permitted)
7 socket(AF_INET6, SOCK_DGRAM, IPPROTO_ICMPV6) = -1 EACCES (Permission denied)
8 socket(AF_INET6, SOCK_RAW, IPPROTO_ICMPV6) = -1 EPERM (Operation not permitted)
9 write(2, "socket", 6socket) = 6
```

当使用 setcap 去掉 ping 命令的 CAP\_NET\_RAW 权限后，普通用户无法正常执行 ping 命令，使用时会报 socket: Operation not permitted 的错误信息，使用 strace 跟踪能够看到在创建 [ICMP](#) 协议族 socket 套接字的时候会因为没有权限而失败，这个权限就是 CAP\_NET\_RAW 权限。

最后不要忘记在测试环境中将权限还原，可以执行 sudo setcap cap\_net\_raw=ep /usr/bin/ping 命令。

### 参考链接

<https://k3a.me/linux-capabilities-in-a-nutshell/>

 文章知识点与官方知识档案匹配，可进一步学习相关知识

CS入门技能树 > Linux进阶 > 新增用户 35230 人正在系统学习中

### Linux ping命令用法详解

01-09

Linux ping命令 Linux ping命令用于检测主机。执行ping指令会使用ICMP传输协议，发出要求回应的信息，若远端主机的网络功能没有问题，就会回应该...

### Debian GNU Linux 安装手册

04-05

Debian GNU Linux 安装手册 和系统介绍

### 1 条评论

 jkilly111 感谢大哥教我购命...愁了好久的问题得到解答

与评论

Debian/Ubuntu安装ps.ping,telnet,netstat命令\_debian ping-CSDN博..

9-22

man ping 得到的信息

Linux capabilities 与 CAP\_NET\_RAW 权限


debian11 iputils 安装包的配置过程

为什么要使用 setcap 单独给 ping 命令...


去掉 CAP\_NET\_RAW 权限后普通用户执...

参考链接


分类专栏

 Linux


141 篇

 云原生


5 篇

 UNPV2


6 篇

 VPP


1 篇

 macos


2 篇

 security


3 篇

 linux security


4 篇

 python


1 篇

 工作问题案例


31 篇

 dpdk 问题定位


28 篇

 ssh


1 篇

 开源工具


1 篇

 elf


14 篇

 读书与思考


12 篇

 性能优化


2 篇

 bpf


7 篇

 包管理器


2 篇

 openEuler


3 篇

 笔记

2 篇

 写给你的情书


1 篇

 图形


1 篇

 数据手册阅读


2 篇

 安卓


1 篇

 network


22 篇

 dpdk


88 篇

 嵌入式学习


25 篇

 龙谕的 RTOS 视点


6 篇

 LINUX KERNEL


40 篇

 linux command


39 篇

 c语言


13 篇

 策略


23 篇

 awk


12 篇

 C++


6 篇

 Unix


6 篇

 APUE

6 篇

 sed

4 篇

 perl

2 篇

原创周排名总排名访问等级

77302513192551466

积分粉丝获赞评论收藏

私信关注

创作者简介

创作稿酬 200元/篇

供稿得现金奖励，多劳多得

点此查看详情

发布首篇原创文章，  
原力分+10分，点亮新秀勋章

去发布

搜博文

博文

热门文章

Debian 10 安装与配置 @ 26595

解决 canberra-gtk-module 加载失败的问题 @ 20837

max file descriptors [4096] for elasticsearch process is too low 问题定位 @ 18252

patchelf 的功能以及使用 patchelf 修改 rpath 以解决动态库问题 @ 15572

linux 突然无法识别芯片的问题 @ 14535

最新评论

从 seccomp filter 学习内核 bpf 自定义 h...  
longyu\_wlzl 准备中

使用 nmon 驱动抓取 netlink 报文的原理  
longyu\_wlzl 感谢提醒，已经修改 🤔 \_

网卡手册阅读：tgbe 发包流程研究  
longyu\_wlzl 填的是报文的总线地址，一般指的就是报文的物理地址，手册中是有确...  
ELF file OS ABI invalid 问题与 chroot 解...  
ajievip: chroot 确实是救命的技能了！  
使用 nmon 驱动抓取 netlink 报文的原理  
Matrix9527930: 引用 [find] 應該是king

您愿意向朋友推荐“博客详情”吗？

强烈不推荐不推荐一般般推荐强烈推荐

最新文章

linux 发行版中在容器内访问热插拔 U 盘的分  
区内容

UOS 如何实现自动将 U 盘挂载到指定目录  
中？

从 seccomp filter 学习内核 bpf 自定义 hook  
点的设计实现

2023年 5篇

2022年 78篇

2021年 92篇

2020年 135篇

2019年 76篇

2018年 46篇

2017年 6篇

ps 命令所在的安装包名字为procps 可在Debian/Centos 中使用命令apt-file search /bin/ps | grep -w "bin/ps" 搜索命令对应安装包的名字 安装 apt-get upd... 9-11

Debian/Ubuntu安装ps ping.telnet.netstat命令 rockstics的博客 @ 1万+  
ps 命令所在的安装包名字为procps 可在Debian/Centos 中使用命令apt-file search /bin/ps | grep -w "bin/ps" 搜索命令对应安装包的名字 安装 apt-get upd... 9-11

Debian/Ubuntu安装ps ping.telnet.netstat命令 rockstics的博客 @ 1万+  
ps 命令所在的安装包名字为procps 可在Debian/Centos 中使用命令apt-file search /bin/ps | grep -w "bin/ps" 搜索命令对应安装包的名字 安装 apt-get upd... 9-11

linux新建可以ping用户及组Linux基础操作 weixin\_39645268的博客 @ 65  
一、自录处命令ls [选项[参数]] -ldd路径 /bin/ls -a 所有文件，包括隐藏文件，以“.”开头的文件是隐藏文件(all)-l 长格式显示-h 人性化显示文件大小-d 查看... 9-11

debian查看ip地址命令、设备调试、维护最实用网络命令\_weixin\_39645268的... 9-4  
② ping 本机IP地址 如果测试不成功,则表示本地配置或安装存在问题,应当对网络设备和通讯介质进行测试、检查并排除。③ ping局域网内其他IP 如果测... 9-4

debian下ping命令向目的主机发送ICMP报文的实现代码\_debin 开启icmp\_上... 9-16  
17 typedef struct pingm\_packet { 19 struct timeval tv\_begin; //发送的时间 20 struct timeval tv\_end; //接收到的时间 21 short seq; //序号 22 int flag; //1... 9-16

linux raw 模块\_linux Capabilities简介-#setcap cap\_net\_raw.cap\_net\_admin=elip /a.out weixin\_29630465的博客 @ 661  
Linux是一种安全操作系统，它给普通用户尽可能低的权限，而把全部的系统权限赋予一个单一的帐户~root。root帐户用来管理系统、安装软件、管理帐户... 9-13

Debian系统与开发板之间互ping以及ssh指令的使用\_debian ping端口\_Br... 9-13  
2. vi /etc/network/interfaces ,添加ens33的配置信息。或者使用ifconfig命令修改IP 3. 然后执行重启网卡命令 ifconfig eth0 up 4. 重启网络服务 restart 在root用户模式... 9-13

k8s容器安装ifconfig.netstat.telnet.vim.ping命令工具 9-22  
/mirrors.aliyun.com/debian stable-updates main contrib non-free deb-src http://mirrors.aliyun.com/debian stable main contrib non-free deb-src http://m... 9-22

ping在Java中Linux中执行ping的服务器-客户端实现 05-04  
ping 在Java中Linux中执行ping的服务器-客户端实现=====系统要求运行该应用程序的系统必须已安装Java 8, ===== 05-04

如何在Linux中禁用ping命令.pdf 09-07  
如何在Linux中禁用ping命令.pdf 09-07

在android手机chroot的debian linux下无权执行ping命令的问题\_android... 9-10  
今天无意中解决了一个困惑已久的问题:我一直喜欢在我的android里通过chroot方式安装一个debian linux.这样可以随时携带一个完整的linux.但上次升级... 9-10

...静态IP、局域网DNS等\_debian安装桌面\_lggirls的博客 9-21  
1.命令行桌面环境 taskset 1.2 纯粹的命令行安装.这里仅仅以xfce4的安装为例 apt install-x-window-system-xfce4 reboot # Debian11 安装最轻量化的xde桌... 9-21

linux中c语言实现多线程ping命令，既可以ping单个ip也可以ping网段 02-10  
linux中c语言实现多线程ping命令，既可以ping单个ip也可以ping网段。网段格式为：./XX 14.215.177.38 - 45，最后还能统计网段信息，在线数量离线数... 02-10

Linux普通用户无法ping Linux系统下普通用户无法正常使用ping weixin\_39667452的博客 @ 1316  
https://www.cndba.cn/Expect-4e/article/167Linux系统下，普通用户使用ping命令返回#pingwww.baidu.comping icmpopensocket:Operationnotpermitted但... 1316

linux Capabilities简介-#setcap cap\_net\_raw.cap\_net\_admin=elip /a.out 热门推荐 Eighty\_Nine的博客 @ 2万+  
转自：https://zhidao.baidu.com/question/459061673954720405.htmlLinux是一种安全操作系统，它给普通用户尽可能低的权限，而把全部的系统权限赋... 2万+

Dell 服务器安装debian 操作系统后ping 不通 最新发布 shelbytlr的博客 @ 235  
dell 服务器没有固件支持，重装系统之后，网络ping 不通 235

Docker的Ubuntu镜像安装的容器无ifconfig命令和ping命令 wiseMale的博客 @ 625  
apt-get update apt install net-tools # ifconfig apt install iputils-ping # ping 625

Debian中fping应用丢失之重新安装方法 @ 252  
debian fping 252

Debian 11 安装，超详细！ dahaidoushishuia的博客 @ 1万+  
华为云中心下载镜像3A服务器的虚拟机。 1万+

计算机网络：九大命令！解决网络故障新思路 IT技术分享社区 @ 3255  
一：ping命令ping是个使用频率极高的实用程序，主要用于确定网络的连通性。这对确定网络是否正确连接，以及网络连接的状况十分有用。简单的说，pl... 3255

借助 Linux 用户命名空间来增强容器安全性 Docker 的专栏 @ 273  
之前在 Netflix 技术博客中也介绍过，Tlusz(1)是我们自研的一套容器编排系统。我们通过它来承载着公司各个部门的各种工作负载 —— 从 netflix.com 的前... 273

Linux：ping 删除cap\_net\_raw后欲使之ping不通，结果却能ping通？ weixin\_42072280的博客 @ 1372  
问题：ping 删除cap\_net\_raw后欲使之ping不通，结果却能ping通？ 原因：不光要设置进程的权限 还要设置文件(ping)的权限 女神阳告诉我的 ... 1372

虚拟机和主机互相ping不通 debian luminous\_you的博客 @ 379  
输入 vi /etc/network/interfaces , vi为进入编辑器命令，打开kali虚拟机命令行，输入sudo -i, 输入密码，进入root权限。在命令行输入/etc/init.d/networki... 379

linux中ping命令 03-16  
ping命令是在Linux系统中常用来测试网络连通性的命令。它的基本格式是：ping 目标地址。例如：ping www.baidu.com。运行该命令后，系统会向目标地... 03-16

“相关推荐”对你有帮助？  
👎 非常没帮助 👎 没帮助 😐 一般 😊 有帮助 😊 非常有帮助

关于我们 招贤纳士 商务合作 寻求报道 ☎ 400-660-0108 ✉ kefu@csdn.net 🗣 在线客服 工作时间 8:30-22:00

longyu\_wlzl 关注

👍 2 🗨 5 ⭐ 5 📄 1 📁 专栏目录