技巧放送:处理Linux内核安全详解Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E6_8A_80_E5_B7_A7_E6_94_BE_E9_c103_645096.htm 对于电脑用户来说，Windows的强大功能服务了广大用户， 不过Windows安全问题还是让很多人头疼，所以很多人开始应用Linux，不过Linux内核安全也不知大疏忽，今天就讲讲Linux内核安全问题清理。 Windows的安全问题比谷仓里的跳蚤还要多，但Linux也未必就对自身的安全漏洞免疫。最近有两个明显的bug被发现，不过很快就修好了。为了保证你不受困扰，你需要尽快地为你的内核打上补丁。 修复列表上的第一个bug是一个远程DDos（分布式拒绝服务）缺陷，可能让潜在的攻击者通过发送一个非法的大型IPv4 TCP/IP包来崩溃你的服务器。那些网络管理员可能会想：“ 等等，曾经听说过这个东东吗？ ”没错，你听说过。 一个古老的 ping到死 DDoS 攻击又回来了. 到底发生了什么呢, 根据Linux kernel讨论列表, 在Linux kernel 2.6.28.10到2.6.29发布之间的某个地方，有人犯了一个编码上的错误，导致了这个古老的攻击方式又卷土重来。百考试题－全国最大教育类网站(100test.com) 幸运的是--这里终究还是开源的--这个bug在别有用心的坏人有机会通过“ ping到死 ”攻击你的系统之前就被迅速地发现而且修复了。如果你使用 的不是Linux内核的2.6.28.1x版本，那么你本就是安全的。不确定你用的是什么版本？最简单的办法是在命令提示符下面运行下面这个命令： uname -a 另一个bug在本质上要麻烦得多，因为它会导致你的系统玩完。不过话说回来，你只有在作为一个本地用户的情况下才能完成这一切，所

以，就我个人来说，我认为它并不比一个可以通过因特网发起的攻击来的更重要。 这个bug跟Ext4文件系统有关， 在2.6.28版本的内核中Ext4已经成为了一个官方维护的部分。 该bug来自三个小的 Ext4 问题, 会导致一个普通的本地用户覆盖掉本来只拥有读权限的文件。因此，一个恶意的用户可以覆盖掉原本正常的Unix/Linux用户密码文件，/etc /passwd，而不管这是不是他们所需要的。这一点都不好玩。 这个问题也已经被修复。你通常的Linux更新操作必须注意到这个问题。那就是你确保你的习惯性更新都做好了吗？ 对于Ubuntu. Red Hat. Fedora和 openSUSE，修复这些问题还有另外的细节。但是，除非你想深入了解代码上的细节，你不需要过多地关注这些杂七杂八的事情。你只需要保证正常更新你的系统就可以了，一切都会好起来的。 完成了Linux内核的处理，你就能轻松应用电脑了。 编辑特别推荐: Linux内核中流量控制(1) Linux内核中流量控制(2) Linux内核中流量控制(3) Linux内核中流量控制(4) Linux内核中流量控制(5) 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com