深入浅出分析Linux系统内核漏洞的问题（1） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E6_B7_B1_E5_85_A5_E6_B5_85_E5_c103_144396.htm 与Windows相比，Linux被认为具有更好的安全性和其他扩展性能。这些特性使得Linux在操作系统领域异军突起，得到越来越多的重视。随着Linux应用量的增加，其安全性也逐渐受到了公众甚或黑客的关注。那么，Linux是否真的如其支持厂商们所宣称的那样安全呢？ Linux内核精短、稳定性高、可扩展性好、硬件需求低、免费、网络功能丰富、适用于多种cpu等特性，使之在操作系统领域异军突起。其独特的魅力使它不仅在pc机上占据一定的份额，而且越来越多地被使用在各种嵌入式设备中，并被当作专业的路由器，防火墙，或者高端的服务器OS来使用。各种类型的Linux发行版本也如雨后春笋般冒了出来，国内更是掀起了Linux的使用热潮，很多政府部门因安全需要也被要求使用Linux。正是因为Linux被越来越多地使用，其安全性也渐渐受到了公众的关注，当然，也更多地受到了黑客的关注。通常，我们讨论Linux系统安全都是从Linux安全配置的角度或者Linux的安全特性等方面来讨论的，而这一次我们转换一下视角，从Linux系统中存在的漏洞与这些漏洞产生的影响来讨论Linux的安全性。 首先来说明一下这次我们讨论Linux系统安全的范围，其实通常我们所说的Linux是指GNU/Linux系统，Linux是系统中使用的操作系统内核。这一次我们重点从Linux系统内核中存在的几类非常有特点的漏洞来讨论Linux系统的安全性。 权限提升类漏洞 一般来说，利用系统上一些程序的逻辑缺陷或缓冲区溢出的手段，攻击

者很容易在本地获得Linux服务器上管理员权限root；在一些远程的情况下，攻击者会利用一些以root身份执行的有缺陷的系统守护进程来取得root权限，或利用有缺陷的服务进程漏洞来取得普通用户权限用以远程登录服务器。目前很多Linux服务器都用关闭各种不需要的服务和进程的方式来提升自身的安全性，但是只要这个服务器上运行着某些服务，攻击者就可以找到权限提升的途径。下面是一个比较新的导致权限提升的漏洞。