分析Unix主机系统安全漏洞存在的必然性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_ti2020/644/2021_2022__E5_88_86_E6_9E_90Unix_c103_644736.htm ◆操作系统体系结构的安全隐患 这是计算机系统脆弱性的根本原因。如Unix系统的许多版本升级开发都是采用打补丁(Patch)的方式进行的，这种方式黑客同样也可以使用。另外，操作系统的程序可以动态链接，包括I/O驱动程序与系统服务，但这同样为黑客提供了可乘之机。如黑客可将磁带设备的软链接点/dev/rmt/0进行修改，添加某种后门程序，那么当用户执行tar cvf /dev/rmt/0 *这类命令的时候，可能激活该后门程序从而导致漏洞的产生。可是操作系统支持程序动态链接和数据动态交换又是现代操作系统集成和扩展必备的功能，因而出现了自相矛盾之处。百考试题论坛 ◆进程创建和远程过程调用(RPC)的安全隐患 一方面，Unix操作系统支持远程加载程序，另一方面，它又可以创建进程，支持在网络节点上创建和激活远程进程，并且被创建的进程能够继承父进程的权限。这两点结合在一起就为黑客在远程服务器上安装"间谍"软件提供了可能。 ◆系统守护进程的安全隐患 守护进程实际上是一组系统进程，它们总是等待相应条件的出现，一旦条件满足，进程便继续进行下去。这些进程特性是黑客能够利用的。值得注意的是，关键不是守护程序本身，而是这种守护进程是否具有与操作系统核心层软件同等的权利。 实际上，在Unix刚刚开发出来的时候，安全性还并不是它主要关注的因素。它的安全模型是为局域网环境下的小型或中等规模的工作组所设计的。 1988年的Internet蠕虫事件就是一个明显的证据：在系统级别上的安

全措施是非常不够的。尽管蠕虫事件导致Carnegie Mellon大学计算机紧急情况反应小组(Computer Emergence Response Team，CERT)的成立，并加强了系统供应商和系统管理员的安全意识，但现在人们对于安全问题的认识和准备还是远远落后于各种专业或业余黑客的能力和决心。幸运的是，现在有很多的OEM附加安全部件和第三方产品可以为承担风险的WWW、FTP、Email Unix服务器提供足够的保障。◆应用软件在安全设计上的滞后性 目前Internet上运行的很多应用软件在最初设计的时候根本或很少考虑到要抵挡黑客的攻击。为局域网设计的Client/Server结构的应用程序在未做任何修改的情况下，直接联到了Internet环境下，然后便面临着被攻击。即使这些软件获得了防火墙和其他安全手段的保护，这种危险依旧存在。实践表明，不管一个应用软件看起来可能会有多么安全，由于用来开发和运行这个程序的工具甚至用来保护它的组件都可能具有安全漏洞，使得该软件的安全可能变得非常脆弱。也就是说，软件安全是一个系统工程，系统各相互作用的组件必须放在安全这个统一的标尺去衡量、开发和使用维护。比如对于系统调用函数get()，如果孤立地去考察它，并没有致命的安全漏洞。但是当黑客借助特权程序利用get()函数不检查参数长度的缺陷，制造缓冲区溢出，并转而执行一个Shell，则普通用户就变成了root用户。可见，在一个相互作用的系统里，小小的设计缺陷可能导致致命的漏洞。◆应用软件在安全评估上的困难性 由于在Internet上运行的诸如WWW、Email等服务软件代码规模较大、设计复杂，要从理论上证明这类复杂程序的安全性，以目前的技术手段，还是一个有待突破的世界难题。现在评估软件安全性的常

用方法，就是在具体使用中去检测，甚至借助黑客们的攻击来发现软件的安全漏洞并加以修补。 编辑特别推荐: Linux系统通过手机GPRS上网设置简介 提高Apache服务器性能的四个建议 Linux认证能帮助你找到一份好工作吗 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