

面对网络Unix和Linux真的安全吗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__E9_9D_A2_E5_AF_B9_E7_BD_91_E7_c103_644755.htm 长久以来

，Windows系统的漏洞层出不穷，病毒、木马以及黑客攻击泛滥，其安全性之差让大家有苦难言，都有“鸡肋”的感觉。很多用户不愿忍受这样长期的折磨，演变为对其他操作系统的期待，对于服务器来说Unix已经成为不错的选择，个人用户对Linux的兴趣也与日俱增，相信SUN要为政府开发专用的Linux版本并提供内核代码的消息，不是空穴来风，难道Unix和Linux真的很安全吗？一、开放源码就更安全吗？由于很多Unix和Linux的版本都是开放源代码的，因此很多人坚信其安全性是受到全世界程序员监控的，它们的任何漏洞和后门都会被发现，所以很多人主观上愿意相信它们比微软至今未公开内核的Windows更加安全。面对Unix和Linux的挑战，微软也曾经与中国政府签署了“政府安全计划源代码协议”，协议中商定，经过相关部门批准的政府部门可以查阅部分的Windows系统源码，随着操作系统的安全关系到国家安全的意识的加深，微软这样“慷慨”的行为，也就不足为怪了！不可否认，开放源代码对于软件的发展以及其安全性的加强都会有一定的促进作用。如果从纯技术的角度来说，在如此庞大的操作系统中，经过精心隐藏的后门，也许只有开发者能够懂得和利用，不论是Windows，还是Unix或Linux都无法回避这个事实。在你感兴趣的前提下，Linux的源码你可以尽情下载和阅读，但通常大家所关注的都是那些知名的程序，其他数量庞大(8-9成)的程序你也许根本没有兴趣或没有时间

去仔细研究一遍，即使是安全专家也不一定能将其中的漏洞一网打尽。很多厂商对Unix和Linux进行改写的过程中，都会对其进行性能和安全方面的测试，但是，单凭一家之力发现安全漏洞的几率微乎其微。曾经有人(不记得名字了，Sorry)就曾经下过定论：没有哪个系统绝对安全，Unix和Linux当然也不例外。

二、哪个更安全？Windows的确存在很多漏洞，总给人以不够安全的印象，不过平心而论，针对它的攻击实在太多了，所以它的漏洞更多、更容易地被大家发现，我想这与它尚未公开内核程序不无关系。大多数安全专家和厂商认为，就三种类型的操作系统安全性而言，Unix的安全性最好、Linux其次、垫底的是Windows。但对于Linux的安全机制，人们仍然存在争议。不过从对安全漏洞的补救来看，Linux的补救速度往往比其他商业操作系统要快，因为开放源代码社区可以非常及时地发布补丁程序，甚至用户自己也可以修改Linux的源代码，弥补安全漏洞。对于普通的商业应用来说，Linux的安全性已经足够，而其实在此类应用中，Windows的安全性也已经足够。

三、事实胜于雄辩：其实早在1988年，Unix平台上就已经释放出了第一个大型的蠕虫，但这些就如同当时的Unix系统本人一样，还不为人所知。随着Klez病毒在Linux平台上传染的通告，才使人们渐渐认识到，原来Unix和Linux也存在安全问题。接下来的病毒就更多了，如：Lion.worm、OSF.8759、Slapper、Scalper、Linux.Svat和BoxPoison等等病毒。有一个奥地利的学生，甚至编写了一本如何在Linux平台上编写ELF病毒的指南，但即使这样，很多病毒还是不被大家所熟悉。至今被病毒侵害过Unix/Linux已经很多了，Unix的有：FreeBSD、HP/UX、IBM AIX、SCO

Unixware、SCO OpenServer、Sun Solaris以及SunOS等，Linux的有：SuSE Linux、Mandrake Linux、Red Hat Linux、Debian GNU Linux、Slackware Linux。WINE是一个开源代码的兼容软件包，能让UNIX平台运行Windows应用软件。虽然这似乎是个不错的选择，然而，使用WINE的 Unix/Linux系统特别容易受到病毒的攻击。因为它们会使无论是对UNIX的还是对Windows的病毒、蠕虫和木马都能对系统产生威胁。其实，无论是Unix/Linux还是Windows，病毒和木马的工作原理都是大同小异的，我们可以将病毒简单的理解为不经过你的同意而感染和摧毁其他程序的程序，蠕虫则看成是一个不经过你的同意而自我复制的代码块，虽然有些系统Bug也会存在复制的行为，但其无意识的行为和病毒、蠕虫、木马的有意识的主动行为还是有区别的。在Unix系统中，一个将名字伪装成tar或df的木马，甚至可以移除整个文件系统，这显然是非常可怕的。

四、实例为证：为了进一步了解在Unix/Linux环境下，病毒的工作原理和过程，最好还是结合病毒实例进行讲述。在Unix/Linux系统中使用Apache作为WEB服务器的用户是相对较多的，而Linux.Slapper worm. Slapper正是针对其攻击的，此蠕虫通过HTTP协议向WEB的80端口发出GET请求，从而获得Apache的版本，它一旦发现容易攻击的版本时，便连接到服务器的443端口，利用一个缓冲区溢出漏洞来采用合适的蠕虫包替换服务器中相应的文件。替换成功后，该蠕虫会利用一个本地编译器(如：GCC)编译自身，将编译后的二进制结果从/tmp目录开始扩散，监听UDP端口，以接受更长远的分布式拒绝服务(DDoS)攻击的指示。最后，DDoS攻击制造TCP洪流令系统瘫痪。某些Slapper病毒的变异体还会

扫描整个B类网络寻找容易攻击的Apache服务器。 另外还有一个典型的例子，Linux Lion worm蠕虫。它就是通过扫描B类网络的53端口，从中寻找易攻击的DNS服务器(基于Unix/Linux平台)，若寻找到目标服务器，它将清除日志文件，接着种植各种木马文件以隐藏它的真实企图。它复制的这些文件几乎看不什么破绽，它还会删除一些系统文件以达到更好的隐藏目的。一旦整个部署过程完成后，它会把密码文件发送给预先设定的远程计算机，其他Lion的变种可以通过嗅探器来嗅探活动连接中的密码信息。通过获得系统访问权限，病毒黑客们能利用远程系统进行DDoS攻击，窃取信用卡号，或者窃取和破坏机密文件、纪录。 结束语：要想使你的Unix/Linux系统更加安全，选择合适的防毒产品是必须要考虑的问题，一些Unix/Linux被设计安装在防火墙上，或部署在消息和群件服务器上。在拥有Unix/Linux服务器的网络中，保护服务器的安全就显得尤为重要，仍需要厂商和广大的程序员们不懈地努力! 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