铲除病毒攻击两大威胁 走近Linux防护 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E9_93_B2_E9_99_A4_E7_97_85_E6_c103_260898.htm 所谓“ 棒打出头鸟 ”一点都不错。当我们还在努力学习什么是Linux时，绝然不会想到如今的Linux系统也成为了黑客口口声声要攻破的热门话题。相比 Windows系统而言，Linux系统稳定、成本低廉，最重要的是它相对安全。于是，Linux忽如一夜春风来，为形形色色各种人群所用，花开千万树。当然随之而来的也不仅仅是开源软件的大肆发展，还有越来越多的安全问题。 作为极受欢迎的开源软件，每当Linux出现安全漏洞时总是会有很多人主动将其修复，不过随着问题的逐渐增多，及时地修补已很难实现。不过，一般认为，计算机网络威胁主要来源于计算机病毒和黑客攻击两个方面，那么就让我们也从这两方面入手，更加有目的性地进行Linux系统的安全防护工作。 拒绝来自病毒的威胁 病毒是任何系统都会首先遭遇的安全威胁。尽管我们熟知的很多Linux病毒并不会真正破坏Linux系统，但是它会感染到与之相邻的Windows系统，同样可以造成系统无法正常工作。 目前Linux下的防病毒软件主要分为基于开放源代码的防病毒软件和商业防毒软件两大部分，前者有德国SEBASTIAN、H BEDV AntiVir/X公司的Anti Vir Linux，后者包括GeCAD Software 的RAV Anti Virus Desktop For Linux v8等。 在上述的防病毒软件中，最常用的产品是AntiVir Linux。软件本身是基于命令行的工具，因此在一些高级参数配置上需要管理员较高的水平。在桌面级产品中，RAV Anti Virus Desktop For Linux v8是颇受用户青睐的产品。 怎样抵御黑客

攻击 安装系统时的分区 在各种常见的攻击中，以缓冲区溢出为典型的安全漏洞攻击数量最高。这种攻击使得任何一个网络用户可能获得主机的控制权。所以我们在安装系统时就要注意分区的问题。 如果用root分区纪录数据，如log文件和电邮，可能因为拒绝服务产生大量日志或垃圾邮件导致系统崩溃。所以建议为/var开辟单独的分区，用来存放日志和邮件，以避免root分区被溢出。最好为特殊的应用程序单独开一个分区，特别是可以产生大量日志的程序。另外建议为/home单独分一个区，这样它们就无法填满/分区，从而避免了部分针对Linux分区溢出的恶意攻击。 BIOS的设置 在BIOS设置中设定密码，不接受软盘启动系统。此举可阻止那些试图用专门的启动盘来进入系统的黑客。 用户口令 这是一个老生常谈的话题。无论什么系统，用户口令都是最基本的安全起点。虽然从理论上说，只要有足够的时间和资源可以利用，就没有不能破解的口令，但是一串奇特的字符也许就能帮你抵御外部威胁，何乐而不为？ 默认帐号、服务 在第一次安装Linux系统时我们就应该删除那些用不到的帐户。你暴露的信息越多，受到的伤害就越大。 Linux是一个强大的系统，它给用户提供了很多服务，但并不是每一个服务都是你的所需。这个文件就是/etc/inetd.conf，它制定了/usr/sbin/inetd将要监听的服务，你可能只需要其中的两个：telnet和 ftp，其它的类如shell、login、exec、talk等等，除非你真的有必要，否则统统关闭。 来自外界的Ping请求 网管可以加上“ echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all ”这样一个命令行到，/etc/rc.d/rc.local当系统每次启动后，它会自动帮你阻止来自外界的Ping请求。 加强日志管理 按理说，默认的Linux日志管理

已经非常完善，但是在所有的行为记录中，却不包括 ftp连接记录。网管们可以通过修改/etc/ftpaccess 或者/etc/inetd.conf，来保证每一个ftp连接日志都能够纪录下来。详细掌握系统的每一个行为，有助于网管抵御任何一个可能的攻击。 Telnet 服务 用户可利用Telnet远程登陆Linux，不过在登陆的同时，操作系统和版本信息容易暴露，这时候可以修改Telnet命令行使Telnet命令行不显示系统信息，以避免有针对性的攻击。 对于网管来说，保护系统安全还有一个最简单有效的方法，那就是到系统发行商那里下载最新的安全补丁（只是，这些补丁的发现也极有可能是黑客的功劳，也许是他们发现了系统漏洞所在）。 建立良好的安全意识，从最简单的安全设置开始，合理利用安全工具，对于Linux管理员来说，这一切看似简单。但是保护Linux，正是要从简单开始。 