 缓冲区溢出攻击是目前黑客最常用的攻击手段之一，为了应对不断涌现的缓冲区溢出攻击，我们研究了在Linux系统下防范缓冲区溢出的方法，通过研究，总结了在Linux平台下防范缓冲区溢出攻击的安全策略，这些安全策略可以应用于一般企业内部服务器，包括web服务器、mail服务器、samba服务器、ftp服务器以及proxy服务器等。在实际使用中，我们发现通过这些安全策略的配置能够对缓冲区溢出攻击起到很好的防范措施。 在对计算机系统安全的研究中，有一种系统安全漏洞引起了我们的关注。一方面是由于这种安全漏洞的广泛性--几乎使所有的操作系统平台都受到影响。另一方面，我们为黑客基于此类安全漏洞所编写的攻击程序的隐蔽性和强大威力所吸引。这就是缓冲区溢出技术。它可以使看似安全的，正在运行常规服务（如 DNS、ftpd等）的主机在几秒钟内失去控制权。缓冲区溢出攻击是目前黑客最常用的攻击手段。在当前CERT和CIAC等发布的Internet安全事件报告中, 缓冲区溢出已成为常见的用语。缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能。这样可以让攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。 为了应对不断涌现的缓冲区溢出攻击，我们研究了在Linux系统下防范缓冲区溢出的方法，之所以选择Linux平台，主要有两方面的原因：（1）Linux是一个开放源码的平台，有利于我们在研究的过程中深入技术细节，由于Linux及其上面的大量应用都是基于

开放源码，有很多黑客在其上进行了大量的工作，可以说Linux上的网络攻击水平代表了整个网络攻击的最高水平。（2）Linux是一个类Unix系统，同时也是在Internet中大量使用的操作系统平台，选择Linux作为研究缓冲区溢出技术的平台是非常具有代表性的，在Linux平台上取得的经验可以非常容易地移植到其他Unix或者类Unix平台上。 通过研究，我们总结了在Linux平台下防范缓冲区溢出的安全策略，这些安全策略可以应用于一般企业内部服务器，包括web服务器、mail服务器、samba服务器、ftp服务器以及proxy服务器等。我们所总结的这些安全策略如下所示： 1． 不显示系统提示信息 如果不想让远程登录的用户看到系统的提示信息，可以改变"/etc/inetd.conf"文件中的telnet设置： telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd -h 在末尾加上"-h"参数可以让daemon不显示任何系统信息，只显示登录提示。当然，只有在服务器上装了telnet服务器才有这样做的必要。 2． 处理"rc.local"文件 在默认情况下，当登录装有Linux系统的计算机时，系统会告诉你Linux发行版的名字、版本号、内核版本和服务器名称。这泄露了太多的系统信息。出于安全的考虑，最好只显示一个"Login:"的提示信息。处理方法如下：（1）编辑"/etc/rc.d/rc.local"文件，在下面这些行的前面加上"#"：…… # This will overwrite /etc/issue at every boot. So, make any changes you # want to make to /etc/issue here or you will lose them when you reboot. #echo "" > /etc/issue #echo "$R" >> /etc/issue #echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue # #cp -f /etc/issue /etc/issue.net #echo >> /etc/issue …… （2）删除"/etc"目录下的"issue.net"和"issue"文件： [root@snow]# rm -f /etc/issue

[root@snow]# rm -f /etc/issue.net "/etc/issue.net"文件是用户从网络登录计算机时（例如：telnet、SSH）看到的登录提示。同样在"/etc"目录下还有一个"issue"文件，是用户从本地登录时看到的提示。这两个文件都是文本文件，可以根据需要改变。但是，如果想删掉这两个文件，必须向上面介绍的那样把"/etc/rc.d/rc.local"脚本中的那些行注释掉，否则每次重新启动的时候，系统又会重新创建这两个文件。 3. 禁止提供finger 服务 在Linux系统下，使用finger命令可以显示本地或远程系统中目前已登录用户的详细信息，黑客可以利用这些信息，增大侵入系统的机会。为了系统的安全，最好禁止提供finger服务，即从/usr/bin下删除finger 命令。如果要保留finger服务，应将finger文件换名，或修改其权限，使得只允许root用户执行finger命令。 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