Linux系统安全工具之:Sxid和SkeyLinux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_Linux_E7_B3_BB_E7_BB_c103_644677.htm 下面介绍一些可以用于 Linux 的安全工具，这些工具对于固化您的服务器将起到一定的作用，可以解决各方面的问题。我们的重点只是想让您了解这些工具，对安装配置以及使用不会给出很详细的介绍。一些安全问题例如 suid 是什么，缓冲溢出是什么等概念性的东西也不属于本文讨论的范围。 介绍这些工具的目的只是给您一个提示的方向，并不是让您拘泥于这些工具。毕竟安全是一个过程，不是一个产品。 一、Sxid sxid 是一个系统监控程序。它可以监视系统中 suid，sgid 文件以及没有属主的变化。并且以可选的形式报告这些改变，你可以在配置文件中设置用 email 的形式通知这些改变，也可以不使用 email 而直接在标准输出上显示这些变化。Suid，sgid 文件以及没有属主的文件很有可能是别人放置的后门程序，这些都是您所要特别注意的。 你可以从下面的网址获得 sxid:ftp://marcus.seva.net/pub/sxid/ 如果您安装过其他工具，那么您一定也会安装这个工具，它在安装上没有什么特别的地方。 缺省安装的时候，配置文件为 /usr/local/etc/sxid.conf，这个文件中有很明显的注释很容易看懂。在这个文件中定义了 sxid 的工作方式。日志文件缺省为 /var/log/sxid.log，日志文件的循环次数在 sxid.conf 文件中定义。您可以在配置固定后把 sxid.conf 设置为不可改变，把 sxid.log 设置为只可添加(使用 chattr 命令)。 您可以用 sxid -k 加上 -k 选项来进行检查，这时检查很灵活，既不记入日志，也不会发出 email。这样您就可

以随时做检查。但是我还是建议您把检查放入 crontab 中，使用 crontab -e 编辑加入下面的条目： 0 4 * * * /usr/bin/sxid 表示每天上午 4 点执行这个程序。 如果您还想了解更详细的信息，可以参考： man sxid man 5 sxid.conf 二、Skey 您认为您的密码安全吗?即使您的密码很长，有很多特殊字符，解密工具很难破解，但您的密码在网络中传送时是以明文形式的，在以太网中随便一个嗅探器就可以截取您的密码。现在在交换环境中也能实现这种技术。在这种情况下，skey 对您来说是一个选择。 Skey 是一次性口令的一个工具。它是一个基于客户服务器的应用程序。首先在服务器端可以用 keyinit 命令为每个用户建立一个 skey 客户，这个命令需要指定一个秘密口令，然后就可以为客户端的用户产生一次性口令列表。当用户通过 telnet，ftp 等与服务器进行连接时就可以按照一次性口令列表中的口令顺序输入自己的密码，下次再连接时候密码就换成了列表中的下一个。 可以从下面的网址获得 skey:ftp://ftp.cc.gatech.edu/ac121/Linux/system/network/sunacm/other/skey skey 的服务器端使用有下面的步骤： 1.使用下面的命令初始化用户 mary: keyinit mary keyinit 每次为用户生成 99 个一次性口令，这时就会在 /etc/skeykeys 文件建立这个用户，该文件中保存了服务器端计算下一个一次性口令的一些信息。用上面的 keyinit 命令时就会在 /etc/skeykeys 中有下面的记录： mary 0099 to25065 be9406d891ac86fb Mar 11, 2001 04:23:12 上面的记录中从左到右依次是用户名，要使用的一次性口令序号，口令的种类，16 进制表示的口令，日期和时间。 2.将一次性口令列表提供给 mary 您可以打印出口令列表然后送给 mary。这样比较安全，密码不会在网络中传递。 3.为 mary 修

改缺省的登陆 shell 为 /usr/local/bin/keysh 由于 PAM 的作用，mary 登陆时要输入密码，她输入这个一次性口令后服务器端要对这个口令进行校验，校验通过连接就被许可了。 可能有些用户不喜欢书面的口令列表，用户可以使用 key 命令在自己的客户端得到一次性口令。您可以通过开两个窗口，一个对服务器进行连接获得一次性口令的种类和序号，然后在另一个窗口用 key 命令根据口令的种类和序号获得所要的密码。但是必须提醒您，您这样的方便是以一定的危险性为代价的。 如果您的缺省的 99 个口令用完了，您可以使用 keyinit -s 刷新口令列表。 在 /usr/src/skey/misc 目录中有许多其他的替换 keysh 的提供其他服务的程序，例如：su,login,ftp 等等。这样您可以应付不同的服务的连接请求了。 为了安全，您最好设置一下/etc/skeykeys 文件的属性和权限。 