Linux操作系统下查找漏洞的N种兵器（1） PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/144/2021_2022_Linux_E6_93_8D_E4_BD_c103_144462.htm 阅读本文之前，我们还需要对Linux系统的基本安全特性有一定的了解 Linux操作系统是一个开放源代码的免费操作系统，它不仅安全、稳定、成本低，而且很少发现有病毒传播，因此，Linux操作系统一直被认为是微软Windows系统的劲敌。近年来，随着Linux操作系统在我国的不断普及，随着越来越多的服务器、工作站和个人电脑开始使用Linux软件，当然，越来越多的安全发烧友也开始对这个操作系统发生了浓厚的兴趣。本文的目的是希望用户以最快的速度对Linux下的精品Hack软件功能及使用方法有一个比较细致全面的了解。今天我们先了解寻找肉鸡的N种兵器。 漏洞扫描器是一种自动检测远程或本地主机安全性弱点的程序。和Windows系统一样，当黑客得到目标主机的清单后，他就可以用一些Linux扫描器程序寻找这些主机的漏洞。这样，攻击者可以发现服务器的各种TCP端口的分配、提供的服务、Web服务软件版本和这些服务及安全漏洞。而对系统管理员来说，如果能够及时发现并阻止这些行为，也可以大大减少入侵事件的发生率。按常规标准，可以将漏洞扫描器分为两种类型：主机漏洞扫描器（Host Scanner）和网络漏洞扫描器（Network Scanner）。主机漏洞扫描器是指在系统本地运行检测系统漏洞的程序；网络漏洞扫描器则是指基于Internet远程检测目标网络和主机系统漏洞的程序，下面，我们选取一些典型的软件及实例进行介绍。 1、基于主机的实用扫描软件 （1） sXid sXid是一个系统监控程序，软件下

载后，使用“ make install ”命令即可安装。它可以扫描系统中suid和sgid文件和目录，因为这些目录很可能是后门程序，并可以设置通过电子邮件来报告结果。缺省安装的配置文件为/etc/sxid.conf，这个文件的注释很容易看懂，它定义了sxid的工作方式、日志文件的循环次数等；日志文件缺省为/var/log/sxid.log。出于安全方面的考虑，我们可以在配置参数后把sxid.conf 设置为不可改变，使用 chattr 命令把sxid.log文件设置为只可添加。此外，我们还可以随时用sxid -k加上 -k 选项来进行检查，这种检查方式很灵活，既不记入日志，也不发出 email。如图1所示。 图1 