使用BackTrack检查Linux安全漏洞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_ti2020/645/2021_2022__E4_BD_BF_E7_94_A8Back_c103_645028.htm 无论你是否用过Bastille UNIX工具，以便手动加固你的Linux系统，或者只是想对目前系统的状态进行快照，你需要使用BackTrack。这是款基于Slackware Linux的版本，通过启动CD或虚拟机镜像(VMI)运行。在官方的第三个版本(如果你计算最新发布的就是第四版)，BackTrack含有方便的安全工具，用于检测Linux系统里的漏洞。本着“ 黑客入侵 ”的精神，BackTrack集成这种通常的安全测试方法： BackTrack包含利基安全工具，很难下载、编译和安装。无论你是Linux技术专家或新手，很难下载完整版本的Linux与安全测试工具。BackTrack的主要接口 使用BackTrack测试内部Linux系统的常用安全评估情景如下： 使用fping识别活动主机 使用nmap识别操作系统和检测打开的端口 使用amap识别正在运行的应用 使用SAINT查找操作系统里的漏洞 使用Metasploit开发操作系统和应用漏洞来源：考试大的美女编辑们 Linux的集中可能性是无穷的。此外，BackTrack包括广泛的数据库、Web和无缝工具的设置，用于查找和挖掘Linux宣称之外的系统缺陷。它甚至包含内置的HTTP、TFTP、SSH和VNC设备，在漏洞验证和分析期间使用。并且，如果你有这样的需求，BackTrack也能集成数字取证工具。事实上，使用Autopsy和Sleuthkit这样的工具对于“ 倒回 ”黑客技术，进一步坚强的你安全技能是很好的。 我一直是使用好的商业安全测试工具的支持者，不过你可能不再使用付费工具。实际上，BackTrack工具不止是够好，她其

实非常不错，尤其是精心的报道和正在遭遇漏洞的管理不是你首要考虑的。我将继续在安全评估方面使用商业工具。 编辑特别推荐: Linux内核中流量控制(1) Linux内核中流量控制(2) Linux内核中流量控制(3) Linux内核中流量控制(4) Linux内核中流量控制(5) 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