

Linux操作系统如何据敌于千里之外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_Linux_E6_93_8D_E4_BD_c103_645366.htm Linux操作系统作为开源的操作系统对于其他系统来说是安全性能绝对没的说。但是有些时候他还是会出现一些小问题，接下来我们就看看出现问题的时候如何解决。在刚刚结束的Pwn2Own大会上，几乎所有的系统都遭遇到了黑客们的“嘲笑”，对比大赛前众家拼命的缝缝补补，黑客们用行动证明了厂商们做的“无用功”。不过黑客归黑客，平时Linux操作系统相对还算是安全的系统，当然也会有很多朋友遇见服务器被黑的问题，这里经过搜集和整理相关的相关的材料，在这里本人给大家找到了Linux操作系统服务器被黑的解决方法，希望大家看后会有不少收获。如果你安装了所有正确的补丁，拥有经过测试的防火墙，并且在多个级别都激活了先进的入侵检测系统，那么只有在一种情况下你才会被黑，那就是，你太懒了以至没去做该做的事情，例如，安装BIND的最新补丁。一不留神而被黑确实让人感到为难，更严重的是某些脚本小鬼还会下载一些众所周知的“rootkits”或者流行的刺探工具，这些都占用了你的CPU，存储器，数据和带宽。这些坏人是从那里开始着手的呢？这就要从rootkit开始说起。一个rootkit其实就是一个软件包，黑客利用它来提供给自己对你的机器具有root级别的访问权限。一旦这个黑客能够以root的身份访问你的机器，一切都完了。唯一可以做就是用最快的效率备份你的数据，清理硬盘，然后重新安装操作系统。无论如何，一旦你的机器被某人接管了要想恢复并不是一件轻而易举的事情。你能

信任你的ps命令吗？找出rootkit的首个窍门是运行ps命令。有可能对你来说一切都看来很正常。图示是一个ps命令输出的例子。真正的问题是，“真的一切都正常吗？”黑客常用的一个诡计就是把ps命令替换掉，而这个替换上的ps将不会显示那些正在你的机器上运行的非法程序。为了测试个，应该检查你的ps文件的大小，它通常位于/bin/ps。在我们的Linux操作系统机器里它大概有60kB。我最近遇到一个被rootkit替换的ps程序，这个东西只有大约12kB的大小。另一个明显的骗局是把root的命令历史记录文件链接到/dev/null。这个命令历史记录文件是用来跟踪和记录一个用户在登录上一台Linux机器后所用过的命令的。黑客们把你的历史纪录文件重定向到/dev/null的目的在于使你不能看到他们曾经输入过的命令。你可以通过在shell提示符下敲入history来访问你的历史记录文件。假如你发现自己正在使用history命令，而它并没有出现在之前使用过的命令列表里，你要看一看你的~/.bash_history文件。假如这个文件是空的，就执行一个ls-l~/.bash_history命令。在你执行了上述的命令后你将看到类似以下的输出：
-rw----- 1 jd jd 13829 Oct 10 17:06 /home/jd/.bash_history 又或者，你可能会看到类似以下的输出：lrwxrwxrwx 1 jd jd 9 Oct 10 19:40 /home/jd/.bash_history - 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