

教你判断Linux系统是否被黑的方法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_ti2020/555/2021_2022__E6_95_99_E4_BD_A0_E5_88_A4_E6_c103_555854.htm 俗称“脚本小鬼”的家伙是属于那种很糟糕的黑客，因为基本上他们中的许多和大多数人都是如此的没有技巧。可以这样说，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“root kits”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root kit开始说起。一个root kit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root kit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机器里它大概有60kB。我最近遇到一个被root kit替换的ps程序，这

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 -> /dev/null假如你看到的是第二种，就表明这个.bash_history文件已经被重定向到/dev/null。这是一个致命的信息，现在就立即把你的机器从Internet上断掉，尽可能备份你的数据，并且开始重新安装系统。寻找未知的用户账号在你打算对你的Linux机器做一次检测的时候，首先检查是否有未知的用户账号无疑是明智的。在下一次你登录到你的Linux机器时，敲入以下的命令：grep :x:0: /etc/passwd只有一行，我再强调一遍，在一个标准的Linux安装里，grep命令应该只返回一行，类似以下：

```
root:x:0:0:root:/root:/bin/bash
```

假如在敲入之前的grep命令后你的系统返回的结果不止一行，那可能就有问题了。应该只有一个用户的UID为0，而如果grep命令的返回结果超过一行，那就表示不止一个用户。认真来说，虽然对于发现黑客行为，以上都是一些很好的基本方法。但这些技巧本身并不能构

成足够的安全性，而且其深度和广度和在文章头提到的入侵检测系统比起来也差得远。我的建议是，假如你怀疑你的系统真的出了问题，打电话给一个Linux的安全专家，参考他的意见。毕竟Linux的安全不是一下子就可以弄好的。更多优质资料尽在百考试题论坛 百考试题在线题库 linux认证更多详细资料 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