在现在这个世道中，保障基于 Linux 的系统的安全是十分重要的。但是，你得知道怎么干。一个简单反恶意程序软件是远远不够的，你需要采取其它措施来协同工作。那么 Linux 的系统的安全如何保障？今天小编就为大家总结九个常用方法来保护 Linux 系统安全，希望能帮助到大家。

1. 使用 SELinux

SELinux 是用来对 Linux 进行安全加固的，有了它，用户和管理员们就可以对访问控制进行更多控制。SELinux 为访问控制添加了更细的颗粒度控制。与仅可以指定谁可以读、写或执行一个文件的权限不同的是，SELinux 可以让你指定谁可以删除链接、只能追加、移动一个文件之类的更多控制。(LCTT 译注：虽然 NSA 也给 SELinux 贡献过很多代码，但是目前尚无证据证明 SELinux 有潜在后门

2 禁用不用的服务和应用

通常来讲，用户大多数时候都用不到他们系统上的服务和应用的一半。然而，这些服务和应用还是会运行，这会招来攻击者。因而，最好是把这些不用的服务停掉。(LCTT 译注：或者干脆不安装那些用不到的服务，这样根本就不用关注它们是否有安全漏洞和该升级了。

3 订阅漏洞警报服务

安全缺陷不一定是在你的操作系统上。事实上，漏洞多见于安装的应用程序之中。为了避免这个问题的发生，你必须保持你的应用程序更新到最新版本。此外，订阅漏洞警报服务，如 SecurityFocus。

4 使用 Iptables

Iptables 是什么?这是一个应用框架，它允许用户自己为系统建立一个强大的

防火墙。因此，要提升安全防护能力，就要学习怎样一个好的防火墙以及怎样使用 Iptables 框架。

5 检查系统日志

你的系统日志告诉你在系统上发生了什么活动，包括攻击者是否成功进入或试着访问系统。时刻保持警惕，这是你第一条防线，而经常性地监控系统日志就是为了守好这道防线。

6 考虑使用端口试探

设置端口试探(Port knocking)是建立服务器安全连接的好方法。一般做法是发生特定的包给服务器，以触发服务器的回应/连接(打开防火墙)。端口敲门对于那些有开放端口的系统是一个很好的防护措施。

7. 默认拒绝所有

防火墙有两种思路：一个是允许每一点通信，另一个是拒绝所有访问，提示你是否许可。第二种更好一些。你应该只允许那些重要的通信进入。(LCTT 译注：即默认许可策略和默认禁止策略，前者你需要指定哪些应该禁止，除此之外统统放行;后者你需要指定哪些可以放行，除此之外全部禁止。)

8.使用全盘加密

加密的数据更难窃取，有时候根本不可能被窃取，这就是你应该对整个驱动器加密的原因。采用这种方式后，如果有某个人进入到你的系统，那么他看到这些加密的数据后，就有得头痛了。根据一些报告，大多数数据丢失源于机器被盗。

9.使用入侵检测系统

入侵检测系统，或者叫 IDS，允许你更好地管理系统上的通信和受到的攻击。Snort 是目前公认的 Linux 上的最好的 IDS。

以上就是保护 Linux 系统安全的九个常用方法，希望能帮助到大家！