Linux系统下ssh安全设置指南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_ti2020/586/2021_2022_Linux_E7_B3_BB_E7_BB_c103_586584.htm 如果您仍然使用 telnet, 而不是 ssh, 则需要改变对本手册的阅读方式. 应当用 ssh 来取代所有的 telnet 远程登录。任何时候通过嗅探互联网通讯来获取明文密码都是相当简单的, 您应该采用使用加密算法的协议. 那么, 现在在你的系统上执行 apt-get install ssh。 鼓励您系统上的所有用户使用 ssh 取代 telnet, 或者更进一步, 卸载 telnet/telnetd. 另外您应该避免使用 ssh 以 root 身份登录, 其替代的方法是使用 su 或 sudo 转换成 root 用户。最后, /etc/ssh 目录下的 sshd_config 文件, 应当作如下修改, 以增强安全性： ListenAddress 192.168.0.1 使得 ssh 只监听一个指定的接口, 如果你有多个(并不想在其上边获得 ssh 服务)接口, 或者将来会增加一块新网卡(但并不想通过它连接ssh服务). PermitRootLogin no 尝试任何情况先都不允许 Root 登录. 如果有人想通过 ssh 成为 root, 需要两次登录, 并且root的密码现在仍不可能通过SSH暴力破解. Listen 666 改变监听端口, 这样入侵者不能完全确定是否运行了sshd守护进程(事先警告，这是模糊安全的). PermitEmptyPasswords no 空密码是对系统安全的嘲弄. AllowUsers alex ref me@somewhere 只允许某些用户通过 ssh 访问主机. user@host 也可用于限制指定用户通过指定主机访问. AllowGroups wheel admin 仅允许某个组的成员通过 ssh 访问主机. AllowGroups 和 AllowUsers 对于拒绝访问主机有同样的效果. 当称它们为 "DenyUsers" 和 "DenyGroups" 时不要觉得奇怪. PasswordAuthentication yes 这完全取决于您的选择. 仅仅允许用

户使用置于 ~/.ssh/authorized_keys 文件中的 ssh-keys 登录主机将更加安全. 如果要达到这种效果，将其设为 "no". 禁用所有的您不需要的认证方式, 如果您用不到, 例如 RhostsRSAAuthentication, HostbasedAuthentication, KerberosAuthentication 或 RhostsAuthentication(例如), 您应该将其禁用, 即使它们是缺省设置(参阅联机帮助 sshd_config(5)). Protocol 2 禁用版本1协议, 因为其设计缺陷, 很容易使密码被黑掉. 更多信息, 参阅 ssh协议问题报告 或 Xforce 通告. Banner /etc/some_file 为用户连接到 ssh 服务器增加一个标题(它将从文件读取), 在一些国家, 登入给定系统前, 给出未经授权或者用户监视警告信息, 将会受到法律的保护. 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