用SRP建立安全的Linux下FTP服务器 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/145/2021_2022__E7_94_A8SRP_E5_BB_BA_E7_c103_145040.htm 在中小型异构网络中，很多用户选择Linux作为网络操作系统，利用其简单的配置和用户熟悉的图形界面提供Internet服务，FTP便是其提供的服务之一。在众多网络应用中，FTP（文件传输协议）有着非常重要的地位。互联网一个十分重要的资源就是软件资源，而各种各样的软件资源大多数都放在FTP服务器中。与大多数互联网服务一样，FTP也是一个客户机/服务器系统。 FTP是传统的网络服务程序，在本质上是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就可以截获这些口令和数据。而且，这些服务程序的安全验证方式也是有其弱点的，就是很容易受到“ 中间人 ”（man-in-the-middle）这种方式的攻击。所谓“ 中间人 ”的攻击方式，就是“ 中间人 ”冒充真正的服务器接收你传给服务器的数据，然后再冒充你把数据传给真正的服务器。服务器和你之间的数据传送被“ 中间人 ”转手后做了手脚之后，就会出现很严重的问题。 截获这些口令的方式主要为暴力破解。另外使用sniffer程序监视网络封包捕捉FTP开始的会话信息，便可顺手截获root密码。 SSH（Secure Shell）是以远程联机服务方式操作服务器时的较为安全的解决方案。它最初由芬兰的一家公司开发，但由于受版权和加密算法的限制，很多人转而使用免费的替代软件OpenSSH。SSH（Secure Shell）是以远程联机服务方式操作服务器时的较为安全的解决方案。它最初由芬兰的一家公司开发，但由于受版权和加密算法的

限制，很多人转而使用免费的替代软件OpenSSH。用户通过SSH可以把所有传输的数据进行加密，使“中间人”的攻击方式不可能实现，而且也能够防止DNS和IP欺骗。它还有一个额外的好处是传输的数据是经过压缩的，可以加快传输的速度。SSH作用广泛，既可以代替Telnet，又可以为FTP、POP，甚至为PPP提供一个安全的“通道”。SSH协议在预设的状态中，提供两个服务器功能：一个是类似Telnet的远程联机使用Shell服务器，即俗称SSH功能；另一个是类似FTP服务的SFTP-Server功能，可提供更安全的FTP服务。SSH的安全验证如何工作呢？主要依靠联机加密技术。从客户端来看，有以下两种安全验证级别：1．基于口令的安全验证（ssh1）只要知道自己的账号和口令，就可以登录到远程主机。所有传输的数据都将被加密，但是不能保证正在连接的服务器就是想要连接的服务器。可能受到“中间人”的攻击。2．基于密匙的安全验证（ssh2）需要依靠密匙，即用户必须为自己创建一对密匙，并把公用密匙放在需要访问的服务器上。如果要连接到SSH服务器上，客户端软件就会向服务器发出请求，请求用密匙进行安全验证。服务器收到请求之后，先在该服务器的home目录下寻找公用密匙，然后把它和发送过来的公用密匙进行比较。如果两个密匙一致，服务器就用公用密匙加密“质询”（challenge），并把它发送给客户端软件。客户端软件收到“质询”后，就可以用私人密匙解密再把它发送给服务器。使用这种方式，用户必须知道自己密匙的口令。与第一种级别相比，这种级别不需要在网络上传送口令，不仅加密所有传送的数据，而且阻止了“中间人”攻击方式。OpenSSH目前存在两个安全遗患：口令、密匙破解（

利用字典文件去解密码）和OpenSSH中可能被安放木马。