利用Telnet远程登录Linux主机的注意事项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__E5_88_A9_E7_94_A8Teln_c103_586633.htm 利用远程登录协议来远程登录并对服务器进行管理，这是服务器管理员最司空见惯的操作了。在Windows操作环境中，系统管理员可能喜欢采用Telnet协议来完成这个任务。但是在Linux操作系统环境中，要利用这个Telnet协议的话，具有一定的困难。因为由于Telnet协议有一定的安全漏洞，所以Linux操作系统默认情况下是采用ssh远程登录协议来代替这个Telnet协议。不过有些系统管理员还是喜欢采用Telnet协议。如要通过Windows客户端来远程管理Linux主机，如果要使用ssh协议的话，还必须去下载这个工具。因为Windows客户端默认情况下只支持Telnet协议，而不支持ssh协议。为了满足这部分系统管理员的需要，笔者今天就谈谈在Linux主机上启用Telnet协议的注意事项。 第一、 手工启动telnet协议。 默认情况下，红帽子Linux操作系统是不会启用Telnet协议。其他版本的Linux操作系统其实也都有类似的限制。这主要是因为Telnet其有一个比较大的安全隐患。即其在数据传输的过程中，用户名、密码、指令都是明文传输的。为此在传输过程中，容易遭受到攻击，如利用嗅探器攻击者可以轻松的获取帐号、密码等敏感信息。为了Linux服务器的安全，建议大家采用ssh协议，而不是Telnet协议。如果一定要采用这个Telnet协议的话，则首先需要在Linux 服务器上启用这个Telnet协议。如果需要启用这个协议的话，则需要利用vi等文本编辑器修改telnet文件。在/etc/xinetd.d下有一个/telnet文件。在这个文件中，有一条记录为disable=no。只需

要把这条记录改为disable=yes即可。注意在修改时，大小写是敏感的。这里是小写的yes，而不是大写。 不过这个文件修改后还不能够及时生效。系统管理员需要重新启动来让这个文件生效。如果不想重新启动的话，则需要执行命令/etc/init.d/xinetd reload命令，强制让系统重新加载设置文件。这个命令执行完成后，操作系统会立即启用telnet服务了。为了服务器的安全考虑，笔者再强调一次，最好不要轻易启动这个服务。如果启动了这个服务的话，那么在用完之后最好能够及时关闭，以确保其安全。或者说，在网络上采用其他的安全措施，如IPSec安全策略等等，来加密网络中传输的数据。跟这些类似的工具结合使用，也可以减少采用Telnet协议带来的安全风险。 第二、 允许root帐号采用Telnet协议远程登录。 即使启用来Telent服务，默认情况下系统管理员仍然不能够利用Telnet协议远程登录操作系统。这主要是因为默认情况下，在红帽子 Linux操作系统中，是不允许root帐户采用Telnet进行远程登录的。而作为系统管理员来说，如果要执行管理任务的话，则大部分情况下都需要特权用户root才能够完成。所以启用了Telnet服务后，还需要允许特权帐户root可以采用这个协议进行远程登录并执行相关的维护操作。 其实Linux操作系统这么设计并不是在为难系统管理员，其也有特殊的考虑。主要是因为采用Telnet协议的时候，利用特权帐户root登录时需要在网络上明文传输特权用户的密码。而root帐户对Linux服务器具有最高的操作权限。为此如果其密码泄露的话，那么就可以让攻击者任意妄为了。所以Linux操作系统设计者在不得已的情况下，采取了这个限制。 如果要允许root帐户远程登录操作系统的话，可以按照下面的方法来操作。

对于root帐户，在操作系统中专门有一个文件/etc/securretty 来限制root帐号可以从哪一个终端来登录。在这个文件中，不仅固定了本地终端，也同时规定了远程终端。在Linux操作系统中，远程终端的代码是 pts。其后面的代码(/0，/1)表示允许登录用户的数量。如果允许同时有多个用户远程登录到操作系统的话，则需要设置多个pts终端。通过这个终端的数量，可以限制同时进行远程登录用户的数量。当用户登录时，到底是采用那个终端则是不一定的。如现在已经有三个用户远程登录到操作系统，此时系统管理员远程登录到操作系统时，则采用的终端号就为pts/4。如果要运行root特权帐户采用Telnet协议远程登录的话，则需要将这些终端加入到这个文件中。这里需要注意的是，如果远程登录的用户比较多时，则需要在这个文件中多加入几个远程终端，即pts/0,pts1等等。否则的话，有其他用户捷足先登了，那么系统管理员就不能够在远程登录了。一般情况下，需要加入两到三个远程终端。不过具体要加入多少，还是需要系统管理员根据企业的实际情况来定。如果企业系统管理员比较多时，或者需要同时远程登录这台Linux服务器进行远程协作等等，那么就需要多启用几个远程端口。以便不时之需。在文件中加入这些端口之后，系统管理员就可以利用root帐户进行远程登录了。注意，如果采用的是ssh远程登录协议的话，不需要进行类似的设置。因为ssh 协议默认情况下其传输的内容是加密的，所以系统允许root帐户进行远程登录。 如果系统管理员觉得这个方式比较麻烦的话，那么还有一种比较简便的方法。即直接将这个文件删除，或者对其进行重命名即可。把文件删除或者重命名，操作系统就找不到相关的设置文件了。此时系

统就会允许root帐户利用所有可用的终端进行登录了。不过显然这么操作，虽然方便了，但是留下了很大的安全隐患。为此，笔者还是建议，如果真的允许root帐户利用Telnet协议进行远程登录的话，还是老老实实的，在上面这个配置文件中加入相关的记录。其实这个配置起来也不是很麻烦，而且这个配置文件修改后即时生效。不需要重新启动或者手工执行命令让强制生效。所以这个配置文件修改起来还是比较简单的。另外需要提醒管理员的是，如果采取配置文件自动备份机制的话，则最好在修改这个配置文件之前，对其进行备份。毕竟最老的“ 鸟 ”也会有失手的时候。因为 Linux操作系统中的配置文件，就好像微软操作系统中的注册表文件。对他们进行修改时，都必须要先进行备份。这个安全措施，即使对Linux系统管理专家来说也仍然是不可少的。 第三、 建立使用ssh协议来替代Telent协议。 其实从功能上来说，telnet协议能够完成的事情，ssh协议也能够完成。但是，在Linux操作系统环境下使用ssh协议，有两方面的优势。首先，ssh协议比telnet协议具有更高的安全性。前者帐号、密码、指令等等在传输的过程中都是加密过的。为此即使攻击者获取这些信息也没有作用。而后者由于在传输过程中以明文传输，为此攻击者可以轻松后去所需要的内容，特别是帐号与口令，从而为下一步攻击做好准备。其次，默认情况下，Linux操作系统只支持ssh协议，而不支持Telnet协议。也就是说，如果想通过Telnet协议远程登录到Linux操作系统的话，就需要向上面介绍的进行一些额外的设置。而如果采用ssh协议的话，想比起来可以避免类似设置的麻烦。 而如果通过Windows客户端来远程管理Linux服务器系统时，若采用ssh协议则有一个障

碍。即在Windows的客户端中，现在还不支持ssh协议。为此如果要通过Windows客户端来管理Linux操作系统(是很多系统管理员所采用的方法)，则必须要下载一个小工具，如putty等等，让在Windows客户端上也可以使用ssh协议。虽然从网上下载工具有一定的麻烦，但是比起这个安全性来说，这还是值得的。为此笔者再次建议系统管理员，要使用ssh协议来远程登录与维护Linuxc操作系统，而不是采用Telnet协议。 