[telnet命令](http://www.cnblogs.com/peida/archive/2013/03/13/2956992.html)

telnet命令通常用来远程登录。telnet程序是基于TELNET协议的远程登录客户端程序。Telnet协议是TCP/IP协议族中的一员，是Internet远程登陆服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的 能力。在终端使用者的电脑上使用telnet程序，用它连接到服务器。终端使用者可以在telnet程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制服务器。要开始一个 telnet会话，必须输入用户名和密码来登录服务器。Telnet是常用的远程控制Web服务器的方法。

但是，telnet因为采用明文传送报文，安全性不好，很多Linux服务器都不开放telnet服务，而改用更安全的ssh方式了。但仍然有很多别的系统可能采用了telnet方式来提供远程登录，因此弄清楚telnet客户端的使用方式仍是很有必要的。

telnet命令还可做别的用途，比如确定远程服务的状态，比如确定远程服务器的某个端口是否能访问。

**1．命令格式：**

telnet[参数][主机]

**2．命令功能：**

执行telnet指令开启终端机阶段作业，并登入远端主机。

**3．命令参数：**

-8 允许使用8位字符资料，包括输入与输出。

-a 尝试自动登入远端系统。

-b<主机别名> 使用别名指定远端主机名称。

-c 不读取用户专属目录里的.telnetrc文件。

-d 启动排错模式。

-e<脱离字符> 设置脱离字符。

-E 滤除脱离字符。

-f 此参数的效果和指定"-F"参数相同。

-F 使用Kerberos V5认证时，加上此参数可把本地主机的认证数据上传到远端主机。

-k<域名> 使用Kerberos认证时，加上此参数让远端主机采用指定的领域名，而非该主机的域名。

-K 不自动登入远端主机。

-l<用户名称> 指定要登入远端主机的用户名称。

-L 允许输出8位字符资料。

-n<记录文件> 指定文件记录相关信息。

-r 使用类似rlogin指令的用户界面。

-S<服务类型> 设置telnet连线所需的IP TOS信息。

-x 假设主机有支持数据加密的功能，就使用它。

-X<认证形态> 关闭指定的认证形态。

**4．使用实例：**

**实例1：远程服务器无法访问**

**命令：**

telnet 192.168.120.206

**输出：**

[root@localhost ~]# telnet 192.168.120.209  
Trying 192.168.120.209...  
telnet: connect to address 192.168.120.209: No route to host  
telnet: Unable to connect to remote host: No route to host  
[root@localhost ~]#

**说明：**

处理这种情况方法：

（1）确认ip地址是否正确？

（2）确认ip地址对应的主机是否已经开机？

（3）如果主机已经启动，确认路由设置是否设置正确？（使用route命令查看）

（4）如果主机已经启动，确认主机上是否开启了telnet服务？（使用netstat命令查看，TCP的23端口是否有LISTEN状态的行）

（5）如果主机已经启动telnet服务，确认防火墙是否放开了23端口的访问？（使用iptables-save查看）

**实例2：**域名无法解析

**命令：**

telnet www.baidu.com

**输出：**

[root@localhost ~]# telnet www.baidu.com  
www.baidu.com/telnet: Temporary failure in name resolution  
[root@localhost ~]#

**说明：**

处理这种情况方法：

（1）确认域名是否正确

（2）确认本机的域名解析有关的设置是否正确（/etc/resolv.conf中nameserver的设置是否正确，如果没有，可以使用nameserver 8.8.8.8）

（3）确认防火墙是否放开了UDP53端口的访问（DNS使用UDP协议，端口53，使用iptables-save查看）

**实例3：**

**命令：**

**输出：**

[root@localhost ~]# telnet 192.168.120.206  
Trying 192.168.120.206...  
telnet: connect to address 192.168.120.206: Connection refused  
telnet: Unable to connect to remote host: Connection refused  
[root@localhost ~]#

**说明：**

处理这种情况：

（1）确认ip地址或者主机名是否正确？

（2）确认端口是否正确，是否默认的23端口

**实例4：启动telnet服务**

**命令：**

service xinetd restart

**输出：**

[复制代码](javascript:void(0);)

[root@localhost ~]# cd /etc/xinetd.d/  
[root@localhost xinetd.d]# ll  
总计 124  
-rw-r--r-- 1 root root 1157 2011-05-31 chargen-dgram  
-rw-r--r-- 1 root root 1159 2011-05-31 chargen-stream  
-rw-r--r-- 1 root root  523 2009-09-04 cvs  
-rw-r--r-- 1 root root 1157 2011-05-31 daytime-dgram  
-rw-r--r-- 1 root root 1159 2011-05-31 daytime-stream  
-rw-r--r-- 1 root root 1157 2011-05-31 discard-dgram  
-rw-r--r-- 1 root root 1159 2011-05-31 discard-stream  
-rw-r--r-- 1 root root 1148 2011-05-31 echo-dgram  
-rw-r--r-- 1 root root 1150 2011-05-31 echo-stream  
-rw-r--r-- 1 root root  323 2004-09-09 eklogin  
-rw-r--r-- 1 root root  347 2005-09-06 ekrb5-telnet  
-rw-r--r-- 1 root root  326 2004-09-09 gssftp  
-rw-r--r-- 1 root root  310 2004-09-09 klogin  
-rw-r--r-- 1 root root  323 2004-09-09 krb5-telnet  
-rw-r--r-- 1 root root  308 2004-09-09 kshell  
-rw-r--r-- 1 root root  317 2004-09-09 rsync  
-rw-r--r-- 1 root root 1212 2011-05-31 tcpmux-server  
-rw-r--r-- 1 root root 1149 2011-05-31 time-dgram  
-rw-r--r-- 1 root root 1150 2011-05-31 time-stream  
[root@localhost xinetd.d]# cat krb5-telnet   
# default: off  
# description: The kerberized telnet server accepts normal telnet sessions, \  
#              but can also use Kerberos 5 authentication.  
service telnet  
{  
        flags           = REUSE  
        socket\_type     = stream          
        wait            = no  
        user            = root  
        server          = /usr/kerberos/sbin/telnetd  
        log\_on\_failure  += USERID  
        disable         = yes  
}  
[root@localhost xinetd.d]#

[复制代码](javascript:void(0);)

**说明：**

**配置参数，通常的配置如下：**

service telnet

{

disable = no #启用

flags = REUSE #socket可重用

socket\_type = stream #连接方式为TCP

wait = no #为每个请求启动一个进程

user = root #启动服务的用户为root

server = /usr/sbin/in.telnetd #要激活的进程

log\_on\_failure += USERID #登录失败时记录登录用户名

}

如果要配置允许登录的客户端列表，加入

only\_from = 192.168.0.2 #只允许192.168.0.2登录

如果要配置禁止登录的客户端列表，加入

no\_access = 192.168.0.{2,3,4} #禁止192.168.0.2、192.168.0.3、192.168.0.4登录

如果要设置开放时段，加入

access\_times = 9:00-12:00 13:00-17:00 # 每天只有这两个时段开放服务（我们的上班时间：P）

如果你有两个IP地址，一个是私网的IP地址如192.168.0.2，一个是公网的IP地址如218.75.74.83，如果你希望用户只能从私网来登录telnet服务，那么加入

bind = 192.168.0.2

各配置项具体的含义和语法可参考xined配置文件属性说明（man xinetd.conf）

配置端口，修改services文件：

# vi /etc/services

找到以下两句

telnet 23/tcp

telnet 23/udp

如果前面有#字符，就去掉它。telnet的默认端口是23，这个端口也是黑客端口扫描的主要对象，因此最好将这个端口修改掉，修改的方法很简单，就是将23这个数字修改掉，改成大一点的数字，比如61123。注意，1024以下的端口号是internet保留的端口号，因此最好不要用，还应该注意不要与其它服务的端口冲突。

启动服务：

service xinetd restart

**实例5：正常telnet**

**命令：**

telnet 192.168.120.204

**输出：**

[复制代码](javascript:void(0);)

[root@andy ~]# telnet 192.168.120.204  
Trying 192.168.120.204...  
Connected to 192.168.120.204 (192.168.120.204).  
Escape character is '^]'.  
  
    localhost (Linux release 2.6.18-274.18.1.el5 #1 SMP Thu Feb 9 12:45:44 EST 2012) (1)  
  
login: root  
Password:   
Login incorrect

[复制代码](javascript:void(0);)

**说明：**

一般情况下不允许root从远程登录，可以先用普通账号登录，然后再用su -切到root用户。