**安装telnet**

telnet是标准的远程登录协议，历史悠久。但是telnet的对话数据没有加密，甚至用户名和密码都是明文显示，这样的服务风险极大。目前大多数系统多已经不会再安装这个服务了，用户需要自己手动安装

1、安装telnet软件，用户可以将telnet的服务器和客户端都安装

|  |
| --- |
| [root@localhost wj]# **rpm -qa | grep telnet**  [root@localhost wj]# **yum install -y telnet-server //telnet服务器端，允许其他电脑连接**  Installed:  telnet-server.i686 1:0.17-48.el6  Complete!  [root@localhost wj]# **yum install -y telnet //telnet客户端，可以连接其他电脑**  Installed:  telnet.i686 1:0.17-48.el6  Complete! |

2、配置telnet，修改配置文件“/etc/xinetd.d/telnet”，将参数disable改为no

|  |
| --- |
| [root@localhost wj]# **gedit /etc/xinetd.d/telnet**  # default: on  # description: The telnet server serves telnet sessions; it uses \  # unencrypted username/password pairs for authentication.  Service telnet  {  flags = REUSE  socket\_type = stream  wait = no  user = root  server = /usr/sbin/in.telnetd  log\_on\_failure += USERID  **disable = no //这个默认是yes，只有改成no才可以启动telnet**  } |

3、修改端口。telnet默认的端口是23，用户可以修改“/etc/services”文件来改变端口。

|  |
| --- |
| [root@localhost wj]# **gedit /etc/service**  **telnet 23/tcp //为了防止被攻击，一般都不会使用23端口。注意这里的23端口要使用tcp和udp两种协议**  **telnet 23/udp** |

4、修改防火墙，打开tcp和udp的23端口

|  |
| --- |
| [root@localhost wj]# **gedit /etc/sysconfig/iptables**  **-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT**  **-A INPUT -m state --state NEW -m udp -p udp --dport 23 -j ACCEPT**  [root@localhost wj]# **service iptables restart**  iptables：将链设置为政策 ACCEPT：filter nat [确定]  iptables：清除防火墙规则： [确定]  iptables：正在卸载模块： [确定]  iptables：应用防火墙规则： [确定]  iptables：载入额外模块：nf\_conntrack\_ftp [确定] |

5、启动telnet

|  |
| --- |
| [root@localhost wj]# **service xinetd restart //telnet依赖xinetd**  停止 xinetd： [确定]  正在启动 xinetd： [确定] |

6、测试，在window端连接telnet。**注意，不要用root用户登录，默认不允许。**

|  |
| --- |
| [root@localhost wj]# **telnet 192.168.0.119**  Trying 192.168.0.119...  Connected to 192.168.0.119.  Escape character is '^]'.  CentOS release 6.5 (Final)  Kernel 2.6.32-431.el6.i686 on an i686  **login: david**  **Password:**  Last login: Thu Aug 16 08:24:19 from 192.168.0.119  already login |

Copyright@david zhytwj2018@163.com