

# Telnet

(noODLe , weazy)

## ***A tutorial on telnet for beginners.***

First of all what is telnet? Telnet is a protocol which is part of the TCP/IP suite. It is quite similar to the UNIX rlogin program. Telnet allows you to control a remote computer from your own one. It is terminal emulation software. In the old days harddrives were humonguous and expensive (i am talking waY back here) and there were no personal computers. To make use of existing computers you had to lease harddrive space and use terminals to operate the system. For developers this was great because computing became lots cheaper. You needed a server and many connections could be made. With telnet u can emulate this type of distributed computing and for example operate a supercomputer from a distance.

TCP/IP works with ports and telnet has one also. It's nr 23. It's has several rfc's. Nr 854 dates back to 1983 and is named telnet protocol specification.

With telnet you can do various things like send mail, log in to irc or proxy and even (though hardly anymore) view and modify websites. There are telnet services available allowing you to search through large databases using telnet. With this you use the remote computer's power so it won't presure your precious resources. Usually help or remotehelp are the commands to use to find out what you can and cannot do. If you can't see what you type in then set echo. Once you made a connection you can use the computer as if it was your own. You use command lines for this. Telnet knows different emulation types. VT-100 is most used. This emulation was used on the video terminals of DEC. There are still VT-100 servers running out there. Scientists use these.

To use telnet you need a client. Windows has telnet built in by default (as does UNIX but that's a different story), but there are third party clients available on the net. You start a telnet session by typing in the command 'telnet server.net 23' where the port number is optional. Since Telnet was based on UNIX (as it is part of TCP/IP which also was based on UNIX) it uses UNIX commands. Basic knowledge would help you here. The port number specifies what services you will use. 23 is the default one. You can log into various services. 80 is the HTTP server for that.

So say you wanted to modify your site from a distance on a leased line. You don't have your fav progs and hardly any time.

```
/* telnet server.net 80 (leave the /*)
```

```
/* GET http://www.server.net/YOURSITE.HTM HTTP/1.1
```

You can use this method to get the output of a cgi-script as well. The simple request doesn't use the HTTP/1.1 (this is the HTTP version running on the server). If you perform a bad request you usually get some info on the server. Use this to find a the correct versions of services running.

To put files to the server u use the PUT command. Telnet is pretty simillar to FTP which is also part of TCP/IP. There are other commands available like POST, which is used to put larger data files to the server, HEAD to get the sites header and DELETE. This one is obvious isn't it.

You can also use telnet to send raw imails. The port to login to is 25.

First you have to identify your self. This geos like this:

```
/* telnet mail.server.net 25
```

```
/* HELO www.you.net
```

When you typed this command you'll get some feedback telling you who and what you logged on to. When you login u may get also some feedback telling you things. :`;

After this you tell the server where the mail is from like this:

```
/* MAIL FROM:you@youradress.net
```

The server will give you feedback again telling you

```
/* ...Sender OK
```

You are accepted. Now for the receiptant

```
/* RCPT TO:yourroommate@hisadress.net
```

again feedback

```
/* ...Receptient OK
```

The server stil does it's duty.....

```
/* DATA
```

After typing this command you'll get the instructions on the proper way to send the mail. Type your mail using the instructions. After you're done sending your mail close the connection using

```
/* QUIT (or END, EXIT, LOGOFF LOGOUT)
```

You can use this to receive your mail as well (if your provider allows you). The POP port is 110.

Telnet to the server on this port. Once there use the following commands.

```
/* USER you@THE_SERVER_GOES_HERE.net
```

```
/* PASS ;type in your password (simple huh.).
```

Once you are accepted as a valid user use the following to list your mail.

```
/* LIST
```

Ports can be configured so they may be different on some systems. Many admins use the default ones though.

Two things come in handy when completely understanding telnet and how it works. They are a basic understanding of TCP/IP and a basic understanding of UNIX commands.

You could use telnet to connect to a proxy and from there on continue your quest. Find a good proxy (use a search engine to locate one) and create an account. Now telnet to the server on the port specified on the website and hang loose. Using a proxy to use the web keeps your identity better hidden. Proxies often use port 8080 or 3128. If you use IE or Netscape you configure them to use a proxy. If you have computer friends maybe they could help you locate one nearby. To learn more about proxies read a tutorial about them. Telnet is part of TCP/IP and with this comes specific built in connection security. This basicly comes down to the three-way-handshake which i will not furtherly discuss in this tut. Terminal emulation was embraced by developers because it is a quick and secure way for remote computing.

Bcause telnet is developed to be quick and reliable you could use it to connect yourself to an irc-server and chat with your buddies without a resource consuming GUI. You may even want to use a proxy to keep the (f)lamers from finding out your ip. To do this you have to know that the irc protocol has it's ports dedicated to 6666:6669. Ports can be configured so you have to know to what port you should connect. The identd runs on port 113. Better use a shell account to connect to IRC servers or a GUI client. Once you are there u can use the usual irc commands. If you have got a good shell (command.com) you can use scripts to automate procedures. To learn more about irc: Request for Comments: 1459 Internet Relay Chat Protocol. mIrc is a pretty good irc-client for nowadays high resource computers if you want to learn this to. Since linux was built on UNIX and linux is free, you should have by now installed this operating system. OK

U can also post to newsgroups if the server allows this. Newsgroups use nntp (rfc 977) over port 119. Use your skills. If you want to get information on a particular system you can use a technique known as port scanning. There are pretty fancy port scanners on the net but to become a guru you will have to know how hits take place. So use port surfing instead. Telnet to the server on various ports to get info on services. This is much more rewarding then using someone else's portscanner. If you want to become a good hacker learn a programming language and write your own. Because TCP/IP is not designed for a specific platform it works much the same on any. TCP/IP uses ports that have certain services.

There are severel interresting ports for trying telnet like 7:echo. This one replies whatever you type in.

13 daytime

15 netstat

37 time time

39 rlp

53 domain  
119 nntp  
443 https

Use your commands to get the requested info. By connecting to different services you get a clear look at the system in use. If you want to exploit a system use the info and go to exploiters.net. If you come across a system you don't know read the ALT.2600.FAQ.

There are also a lot of trojans circulating (like back orifice or netbus). If you know how to use these you can do some rad things but mostly the use of trojans is considered lame. Learn the commands and setup your private backdoor. When you want to attack a system prepare yourself for this. There has been some discussion on the legality of port-scanning/surfing. Many servers log every attempt to connect to it. Be warned.

The expansion of free software towards the windows market gives great tools to set up your own hackerlab. For this you use your computer and one other. Set up a simple network with a server. Configure the server and start hacking.

If you have a root account on a telnet server you can use this to remotely administer the server. There are many ways to get a root account. Remember that if an administrator finds a new root account on his system he will know it has been tampered with. Covering your tracks is fatal if you want to stay uncaught. Telnetting from a PDA is a pretty fancy way to read your mail or post to newsgroups from a distance. Because GSM phones can only transmit upto 9600 bps you might not want to load up the web.

U can use telnet to create a shell account. This allows you to use a good shell even though u use Microsoft OS. Shell accounts vary in the services they have available. To find a good shell account search the net or try freeshell.org. Look for a shell that offers the progs you'dd like to use.