



# Lab 22 Redirector (xinetd and ssh)



## Requirements

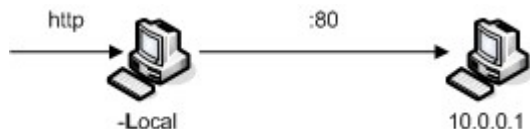
- During the labs: Use connections from SuSE to SuSE or from RedHat to RedHat to prevent version incompatibility.
- A classroom web site. E.g.:  
`echo "<b>My Classroom Site</b>" > index.html`
- A classroom telnet server.
- A firewall would be nice, but not required.
- A partner PC, called *myhome*.

## To Do

1. Redirect the incoming port 80 on your local host to the classroom web site using the Internet super daemon.

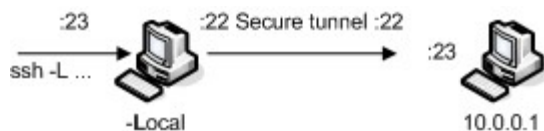
Test the connection to your local port 80 before and after the redirection:

<http://localhost>



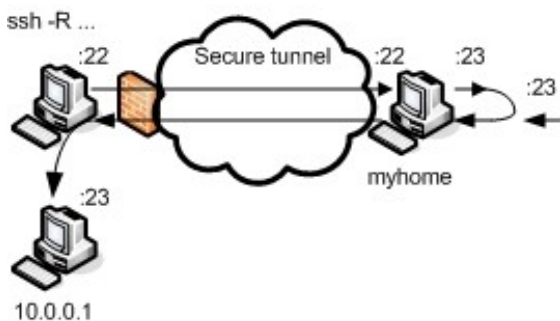
2. Redirect the incoming port 23 on your local host to the classroom telnet daemon using a secure tunnel (ssh).

Test the connection to your local port 23 before and after the redirection: `telnet localhost`



3. Team up with a partner. Redirect the incoming port 23 on your partners host (called *myhome*) to the classroom telnet daemon. Use a secure tunnel (ssh) from your local host, through the optional firewall, to your partners host.

Test the connection on your partners host before and after the redirection: `telnet localhost`



## Quick Reference Objectives to learn

```
(Un)Secure Teleworking      #Redirector options

Test for open (listening) ports
netstat -antp                #Show listening tcp ports on localhost
nmap -sT 172.28.21.[1-254]   #Show exposed Tcp ports on host(s)

Super daemon xinetd        #Use snippet name from /etc/services
vi /etc/xinetd.conf         #Edit general settings
vi /etc/xinetd.d/snippet    #Change settings per snippet
only_from = 172.28.0.0/16 172.27.200.1
no_access = 172.28.24.1    #or: access_times = 9:00-18:00
redirect = 10.0.0.1 80    #Redirect to newtargetip newport
log_type = FILE /var/log/redirector.log
wait = no | yes           #no=tcp, yes=udp
protocol = tcp | dgram    #tcp=tcp, dgram=udp
socket_type = stream      #tcp and udp
/etc/init.d/xinetd restart  #Activate changes
```

```
ssh
#Redirect Local port 23 via ssh to 10.0.0.2:23 using port 22:
ssh -L 23:10.0.0.1:23 -N root@10.0.0.1 &

#Man In The Middle command opens up closed firewall from the outside
#Connect Remote myhome:23 to local network 10.0.0.1:23:
ssh -R 23:10.0.0.1:23 -N root@myhome &
```

## Theory Modules

- LPIC 1 Certification Bible, isbn 0-7645-4772-0
- p. 705-717 Using SSH
  - p. 371-375 Running X and clients remotely
- Downloadable manual([www.novell.com/documentation](http://www.novell.com/documentation))  
SUSE LINUX Enterprise Server – Install. and Admin.
- p. 652-656 SSH – Secure Shell, the Safe Alternative

## Extra References

- [www.tldp.org](http://www.tldp.org)
-