

Connecting to Windows Machines via OpenSSH / Cygwin

Simon Baker
UCL Computer Security Team
11/28/06

Introduction

Recently, several problems have come to light with remote access solutions.

Two of the most popular solutions are VNC and Microsoft Remote Desktop Protocol, known as RDP or rdesktop, and these have both had quite serious flaws, which could lead to a system compromise.

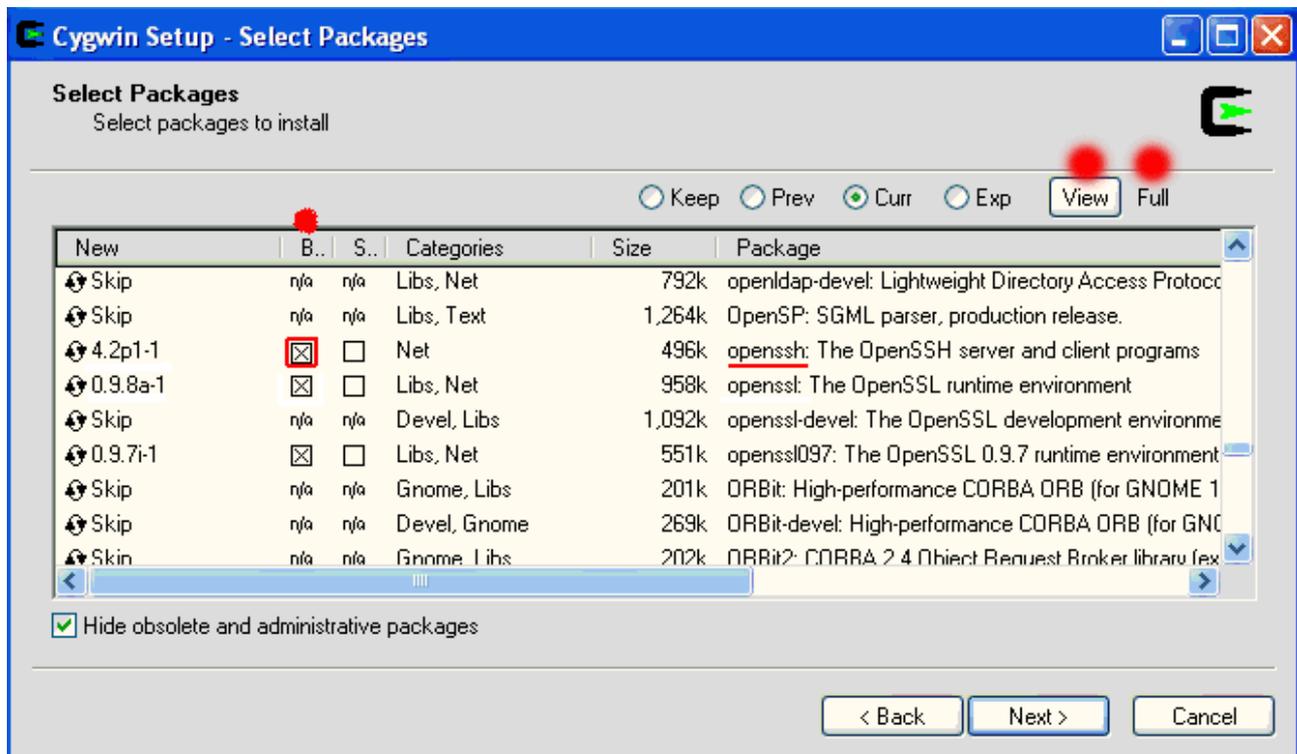
However, by contrast, the OpenSSH software implementation has been reviewed by multiple competent people, and had very few vulnerabilities recently. In this paper, we will look at how to install OpenSSH onto a windows system, and effectively `wrap` access to RDP or VNC servers via a much more secure protocol.

Installing OpenSSH (Server)

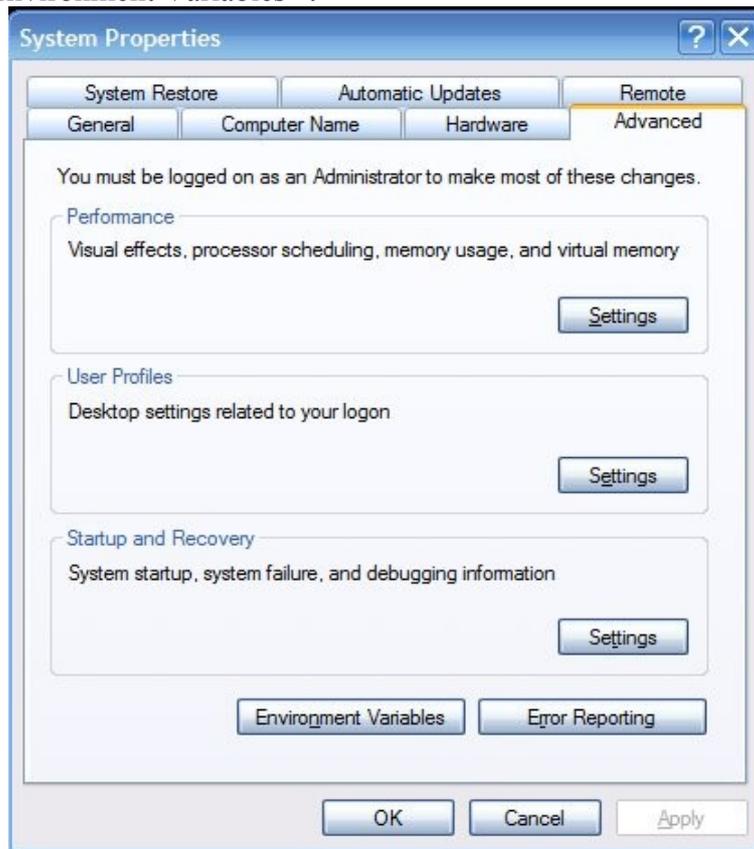
First, install Cygwin from <http://www.cygwin.com/>

The installation instructions for this task are available at <http://www.cygwin.com/cygwin-ug-net/setup-net.html>

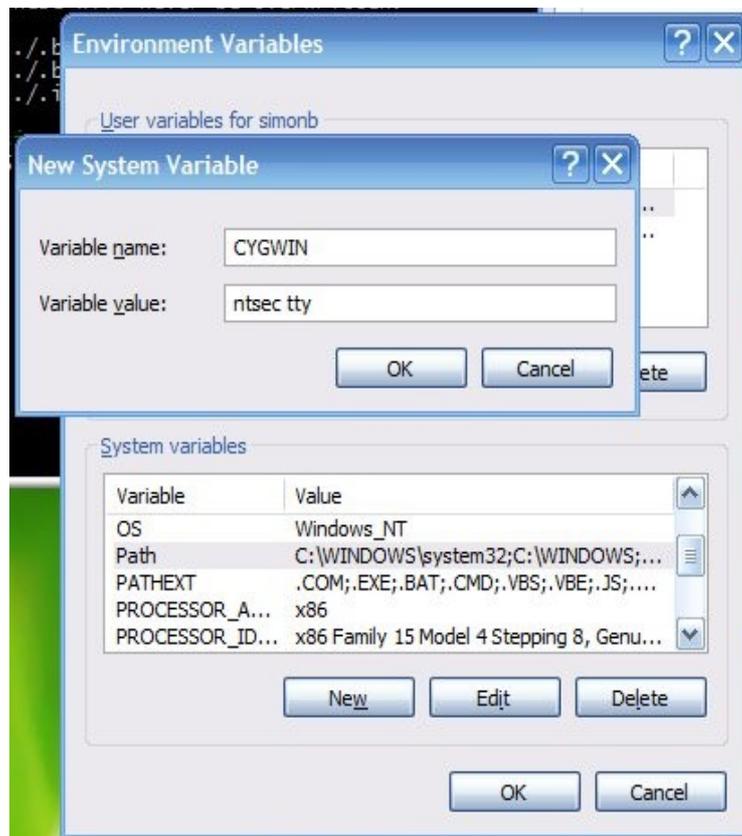
Ensure that you install the “OpenSSH” package, which appears under the “Net” category, or select the “Full” view mode.



Once the installation is complete, we need to edit and add some environment variables. Open control panel, select “System”. Once this has loaded, select the “Advanced” tab, as shown below, and further select “Environment Variables” :



Under the “System Variables” section, click “New” - a “New System Variable” window should load. Enter the information as shown below:

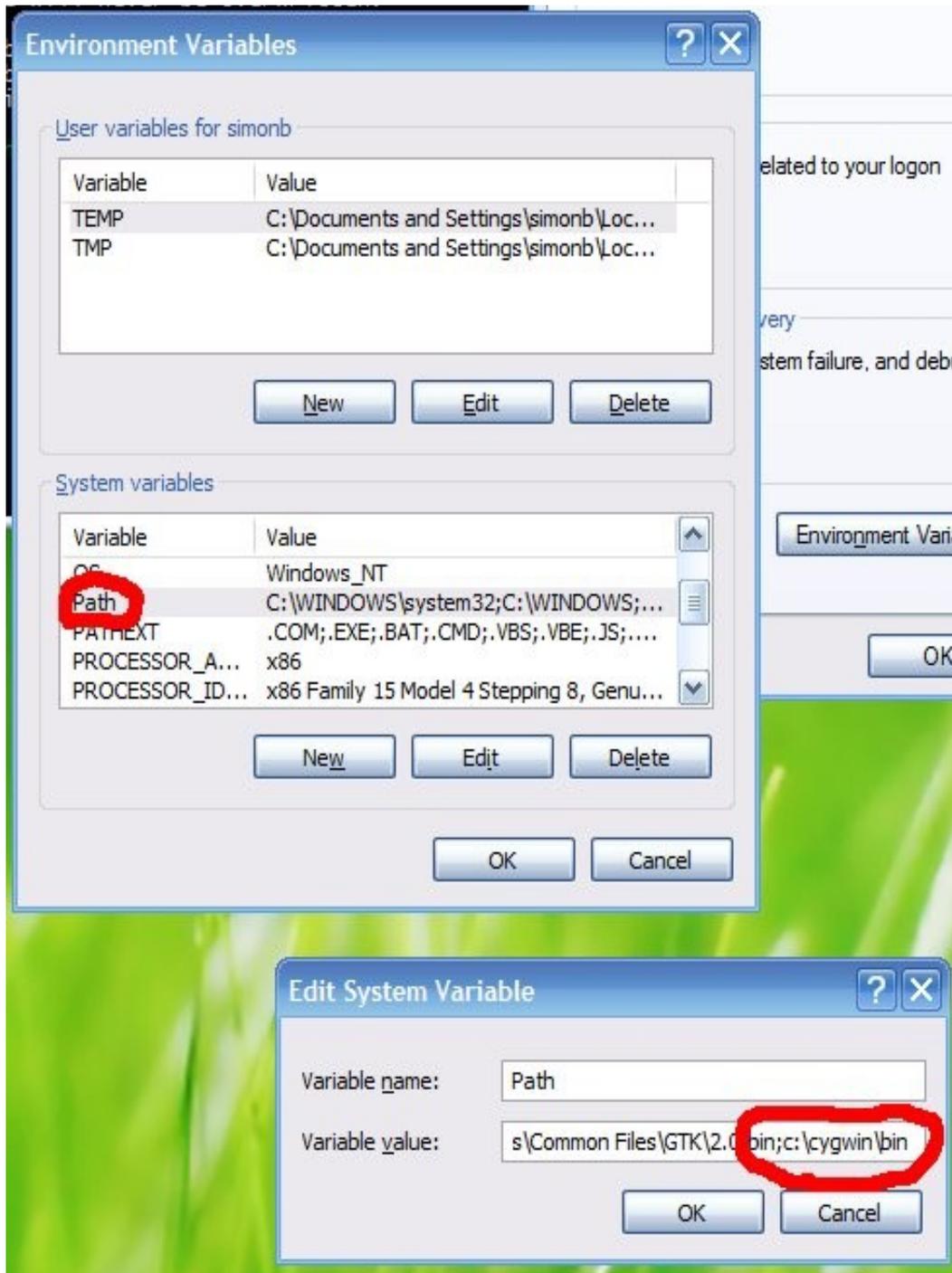


Then click OK.

ntsec is an *environment variable* to instruct cygwin to use Windows' security rules for controlling users' access to files and other operating system facilities.

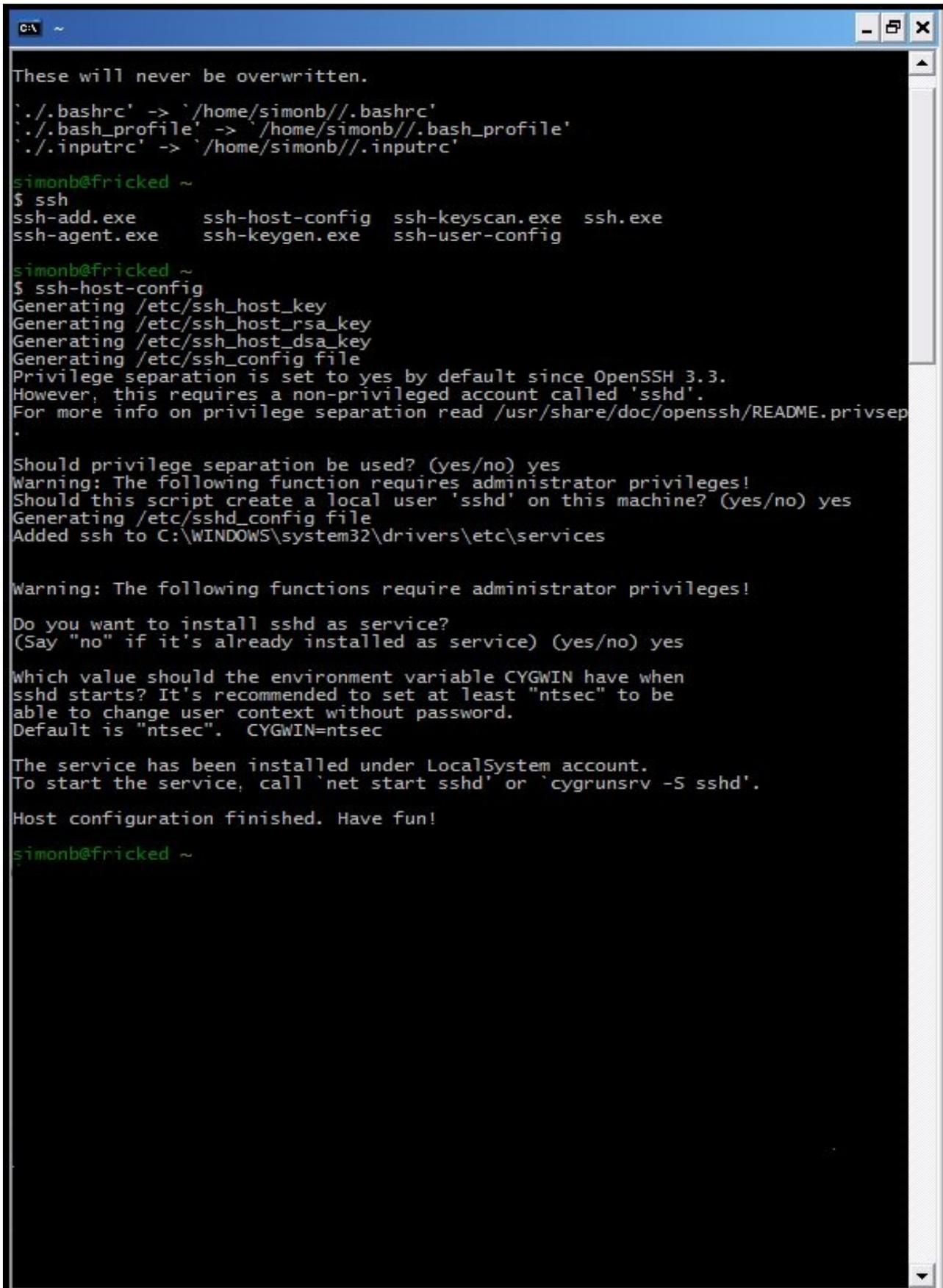
For more information on this setting, please see <http://cygwin.com/cygwin-ug-net/ntsec.html>

Next, select the “Path” variable and click Edit. Append “;c:/cygwin/bin” to this variable as shown below:



Then close all the open windows. The variables should be set correctly.

We can now start Cygwin - Start it via Start->Programs->Cygwin->Cygwin Bash Shell. You should then be presented with a console box. Run the “ssh-host-config” script, as shown in the screen shot below. Use the same answers as shown:



```
C:\ ~
These will never be overwritten.
`./bashrc' -> `/home/simonb//.bashrc'
`./bash_profile' -> `/home/simonb//.bash_profile'
`./inputrc' -> `/home/simonb//.inputrc'

simonb@fricked ~
$ ssh
ssh-add.exe      ssh-host-config  ssh-keyscan.exe  ssh.exe
ssh-agent.exe    ssh-keygen.exe   ssh-user-config

simonb@fricked ~
$ ssh-host-config
Generating /etc/ssh_host_key
Generating /etc/ssh_host_rsa_key
Generating /etc/ssh_host_dsa_key
Generating /etc/ssh_config file
Privilege separation is set to yes by default since OpenSSH 3.3.
However, this requires a non-privileged account called 'sshd'.
For more info on privilege separation read /usr/share/doc/openssh/README.privsep
.

Should privilege separation be used? (yes/no) yes
Warning: The following function requires administrator privileges!
Should this script create a local user 'sshd' on this machine? (yes/no) yes
Generating /etc/sshd_config file
Added ssh to C:\WINDOWS\system32\drivers\etc\services

Warning: The following functions require administrator privileges!

Do you want to install sshd as service?
(Say "no" if it's already installed as service) (yes/no) yes

Which value should the environment variable CYGWIN have when
sshd starts? It's recommended to set at least "ntsec" to be
able to change user context without password.
Default is "ntsec".  CYGWIN=ntsec

The service has been installed under LocalSystem account.
To start the service, call `net start sshd' or `cygrunsrv -S sshd'.

Host configuration finished. Have fun!

simonb@fricked ~
```

Once this has completed, you can start the actual SSH daemon.

This can be achieved by one of three ways. Firstly, you can run “net start sshd” within the Cygwin prompt, or you can run “cygrunsrv.exe -S sshd”. The third way is to simply reboot.

You may however see the following error message if you are using certain security templates:

```
simonb@fricked ~  
$ net start sshd  
The CYGWIN sshd service is starting.  
The CYGWIN sshd service could not be started.
```

The service did not report an error.

More help is available by typing NET HELPMSG 3534.

```
simonb@fricked ~  
$ cygrunsrv.exe -S sshd  
cygrunsrv: Error starting a service: QueryServiceStatus: Win32 error 1062:  
The service has not been started.
```

This is due to permission setting problems with the Cygwin directory. This thread has some helpful advice: <http://erdelynet.com/archive/ssh-l/2001-09/0068.html>

You can check to see if SSH is running, by running “netstat -a” in a cmd.exe or from a Cygwin shell, or use “TCPView” from <http://sysinternals.com>

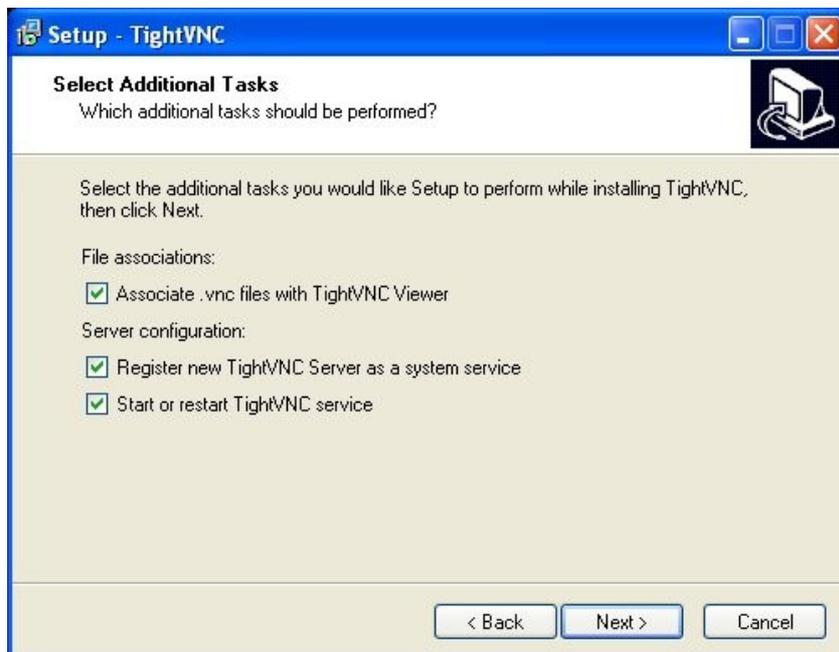
Installation of TightVNC

The TightVNC projects homepage is available at <http://www.tightvnc.com/>

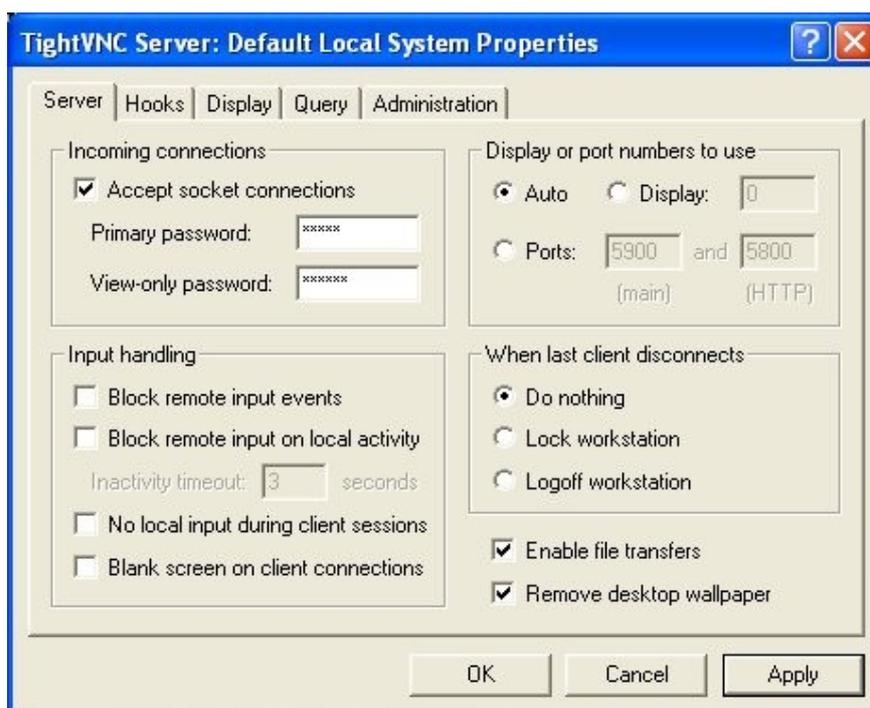
At time of writing, the current installer is available from:

<http://heanet.dl.sourceforge.net/sourceforge/vnc-tight/tightvnc-1.3.8-setup.exe>

Download and run the installer, and under “Additional Tasks” ensure you enable the following options:



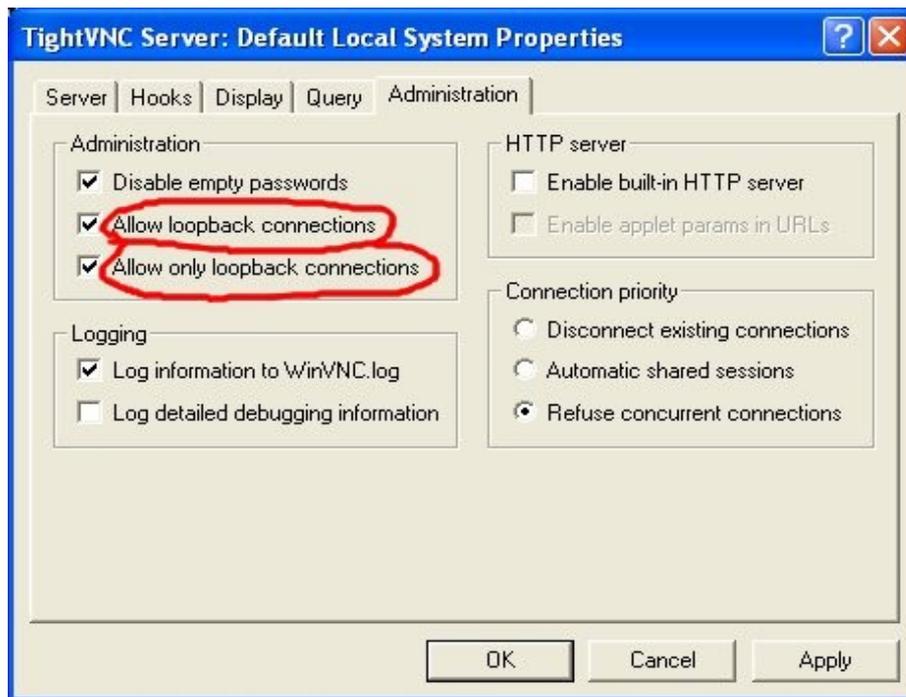
You will then be presented with the actual “Setup” screen. Firstly, enter two distinctly different passwords in the “Primary” and “View-Only” screen, as shown below:



If you want to install TightVNC on a number of computers, and do not want to repeatedly enter the same password on each machine, install TightVNC once and set the password, then copy the registry settings under HKEY_CURRENT_USER\Software\ORL\WinVNC3 to other machines.

The next step is to enable connections via SSH only. Click the “Administration” tab, and enable the “Allow loopback connections” and “Allow only loopback connections”.

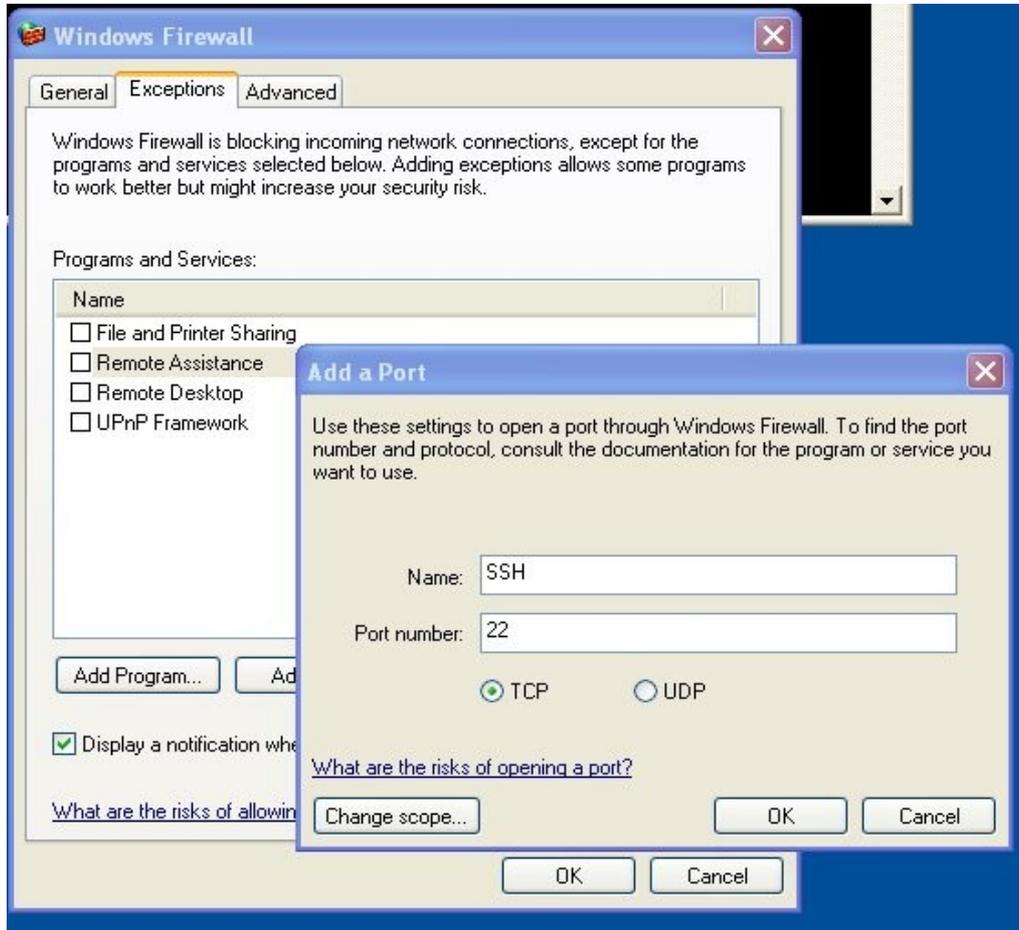
Note that under Windows XP connections will already be firewalled by the inbuilt XP firewall (or whatever other solution you are using, e.g. F-Secure firewall). We will discuss enabling access to **ssh** later via the firewall.



Once this has been completed, click “Apply” then “OK”. The service should be configured and running.

Enabling SSH access via XP Firewall

Open control panel, then select “Windows Firewall”. Once this has loaded, click the “Exceptions” tab, and then click “New”. Enter the appropriate information for the exception, in our case port 22.

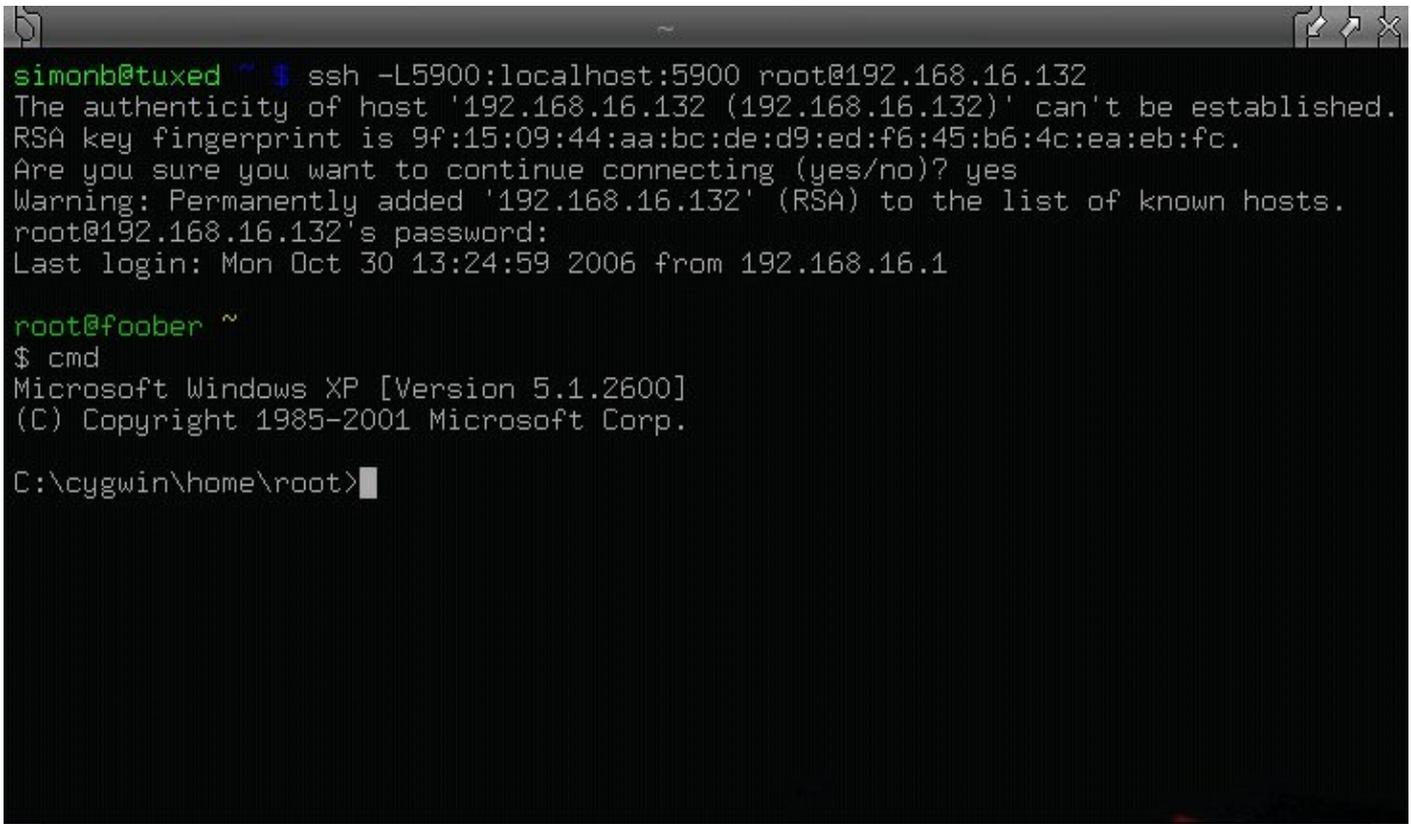


While you are editing the firewall rules, you may as well disable the “Remote Desktop” checkbox, if enabled, as you can now SSH portforward the protocol over SSH. RDP uses port 3389 by default.

SSH'ing in from a UNIX Client

One of the benefits of VNC is that the software will also run on a UNIX system, which means you can actually control and administer Windows machines from a UNIX client.

If you are using the command line SSH, the following shows an example of how to connect:

A terminal window showing an SSH connection. The user 'simonb@tuxed' runs the command 'ssh -L5900:localhost:5900 root@192.168.16.132'. The terminal displays a warning about the host's authenticity, the RSA key fingerprint, and a confirmation to continue. After entering the password, the user is logged in as 'root@foober'. The user then runs the command '\$ cmd', which displays the Windows XP version and copyright information. The prompt then changes to 'C:\cygwin\home\root>'.

```
simonb@tuxed ~ $ ssh -L5900:localhost:5900 root@192.168.16.132
The authenticity of host '192.168.16.132 (192.168.16.132)' can't be established.
RSA key fingerprint is 9f:15:09:44:aa:bc:de:d9:ed:f6:45:b6:4c:ea:eb:fc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.16.132' (RSA) to the list of known hosts.
root@192.168.16.132's password:
Last login: Mon Oct 30 13:24:59 2006 from 192.168.16.1

root@foober ~
$ cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\cygwin\home\root>
```

From there, you simply load up a VNC client on your machine, and tell it to connect to “localhost” or “127.0.0.1”. The connection will automatically be routed down the SSH tunnel to the remote server.

For example, from another Terminal you could run vncviewer:

```
simonb@tuxed ~ $ vncviewer --help
TightVNC viewer version 1.2.9
```

```
Usage: vncviewer [<OPTIONS>] [<HOST>][:<DISPLAY#>]
       vncviewer [<OPTIONS>] [<HOST>][::<PORT#>]
       vncviewer [<OPTIONS>] -listen [<DISPLAY#>]
       vncviewer -help
```

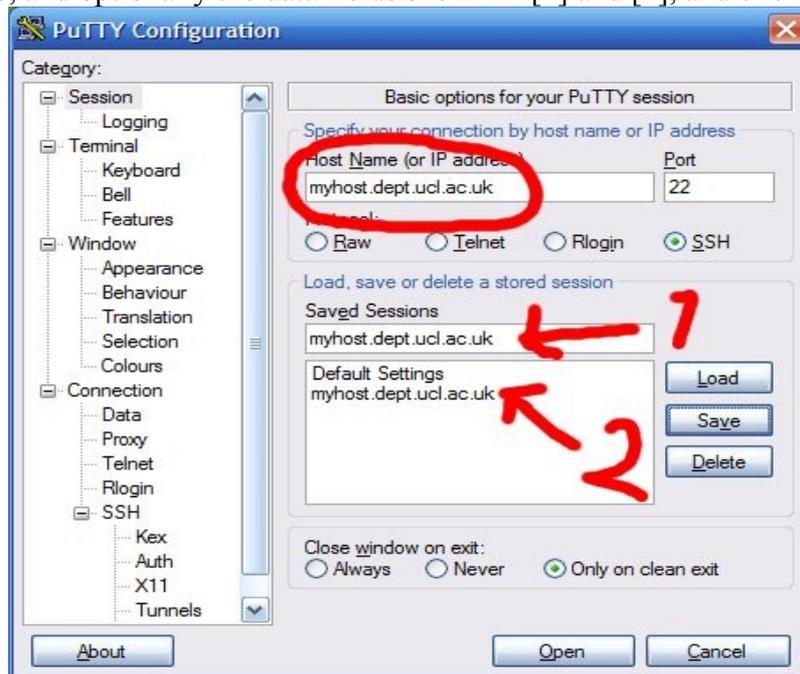
Again, simply use “localhost” as the HOST setting, e.g.
vncviewer localhost

will connect you to the remote host via the SSH tunnel. However, please bear in mind you can only connect to one host at a time, unless you increment the ssh command line, e.g.:
use -L5901:localhost:5900 for example, and then connect your local client to that port.

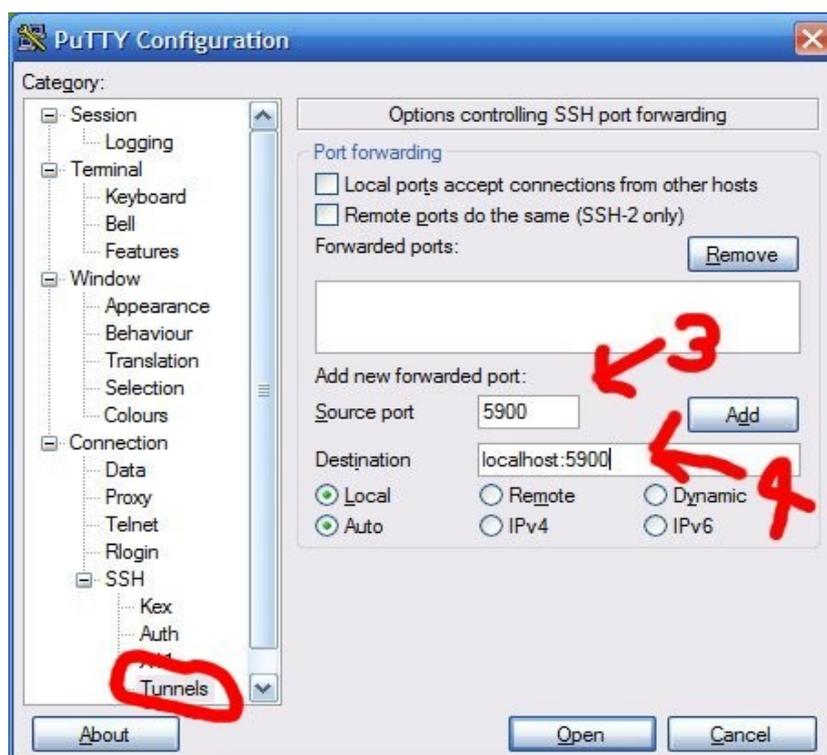
SSH'ing in from a Windows Client

You can use the UNIX method described above from a windows host, assuming it has cygwin installed on it, or there are several other SSH clients available, both commercial and freeware. One of the most popular is called PuTTY, and available from <http://www.chiark.greenend.org.uk/%7esgtham/putty/>

It is quite easy to configure. On the **client** machine, download and install PuTTY (you can use either putty.exe, or the actual installer), and run putty. You will then see a configuration screen ; enter the hostname, and optionally the data fields shown in [1] and [2], and click "Save" :



Then, click "Tunnels" in the left pane, and enter the appropriate information. In the example below, we are forwarding VNC traffic (Port 5900), though this can be anything you like (for example, rdesktop is 3389)

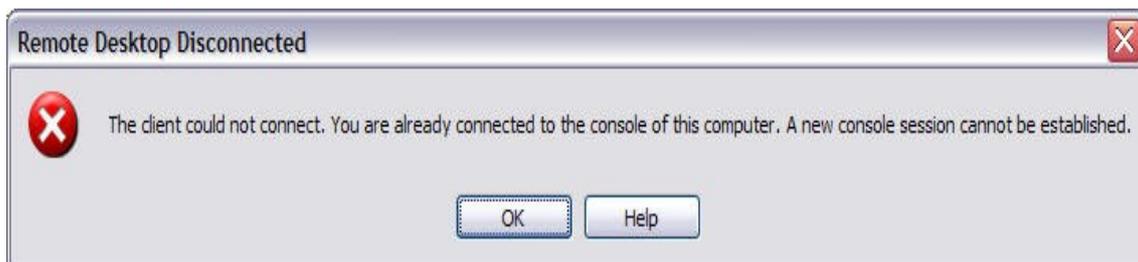


Once you have configured PuTTY, you can then connect to the host in question. Then, you can simply use the VNC client or Rdesktop client installed locally to connect to localhost / 127.0.0.1 .



Problem Solving

If you get “User already logged on” error messages, you need to read:
<http://support.microsoft.com/default.aspx?scid=kb;%5BLN%5D;884020>



References

<http://www.microsoft.com/technet/prodtechnol/winxpro/reskit/c08621675.msp>