Install Secure Shell Server (sshd) on Windows using Cygwin

In this tutorial you will learn to install a Secure Shell Server (also known as sshd or Secure Shell Daemon) on a Windows system using the openssh package and the Cygwin utilities. You will learn how to use the secure shell client to connect to a system running sshd and start a shell. If you were unaware, the shell is the equivalant of the Windows command prompt (cmd.exe). This shell is what you will be interacting with on the system running sshd.

SSH is a suite of client/server based tools used for encrypted communication between two systems. There are several tools included in the suite of SSH tools. The two we are going to use in this tutorial are the following:

1. sshd – The secure shell server software.
2. ssh – The secure shell client software, used to connect to the server.

Why would you want to do this? These tools were built as a secure replacement for telnet. If you still use telnet, then you need to switch to SSH now! Telnet sends information across the network in plain text, including your username and password! Anyone able to sniff your network traffic can see this information and then log in as you.

If you aren't familiar with Cygwin, it is an awesome suite of tools that make many Linux utilities available in the Windows environment. This will allow you to run a BASH shell in your Windows environment! If you aren't familiar with Linux, Cygwin is one way to get started learning some of the basic tools provided with Linux. At some point I'll write a post about why these tools are so awesome and why everyone stuck developing on a Windows system should install them.

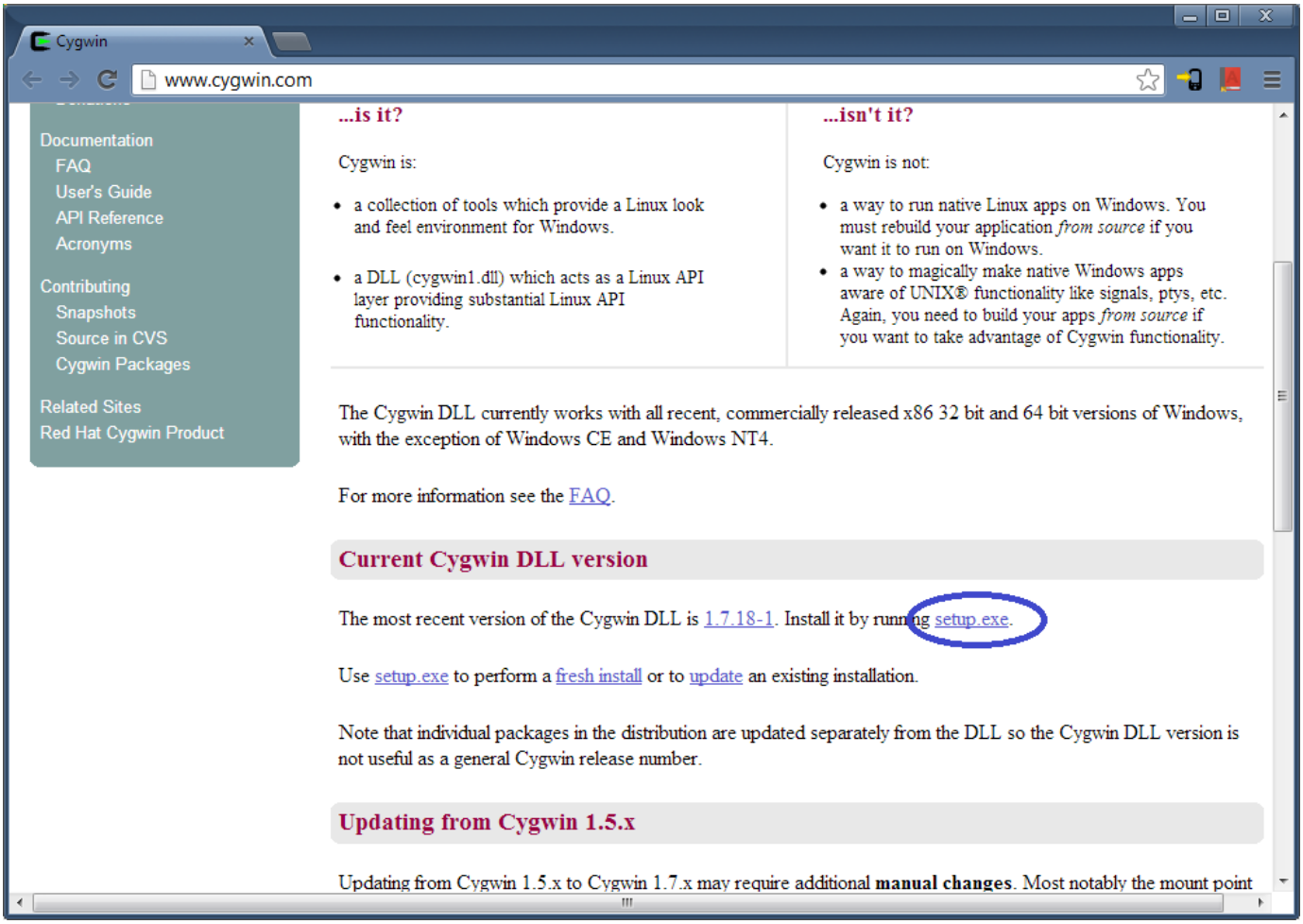
A quick word about security after you install sshd. When you connect to the system running sshd, you will have to supply a username and password (until you learn how to configure keys: next article). The username and password that you will supply needs to correspond with a Windows user account on the system running sshd. That said, make sure every user account on the sshd system has a strong password(passphrase is better).

When you install sshd, you are making port 22 available for connections by anyone, unless you lock it down through a firewall of some sort(which you should). I will repeat myself, make sure every user account on the system has a strong password! Port 22 is the standard SSH port number. There are botnets running on the internet that

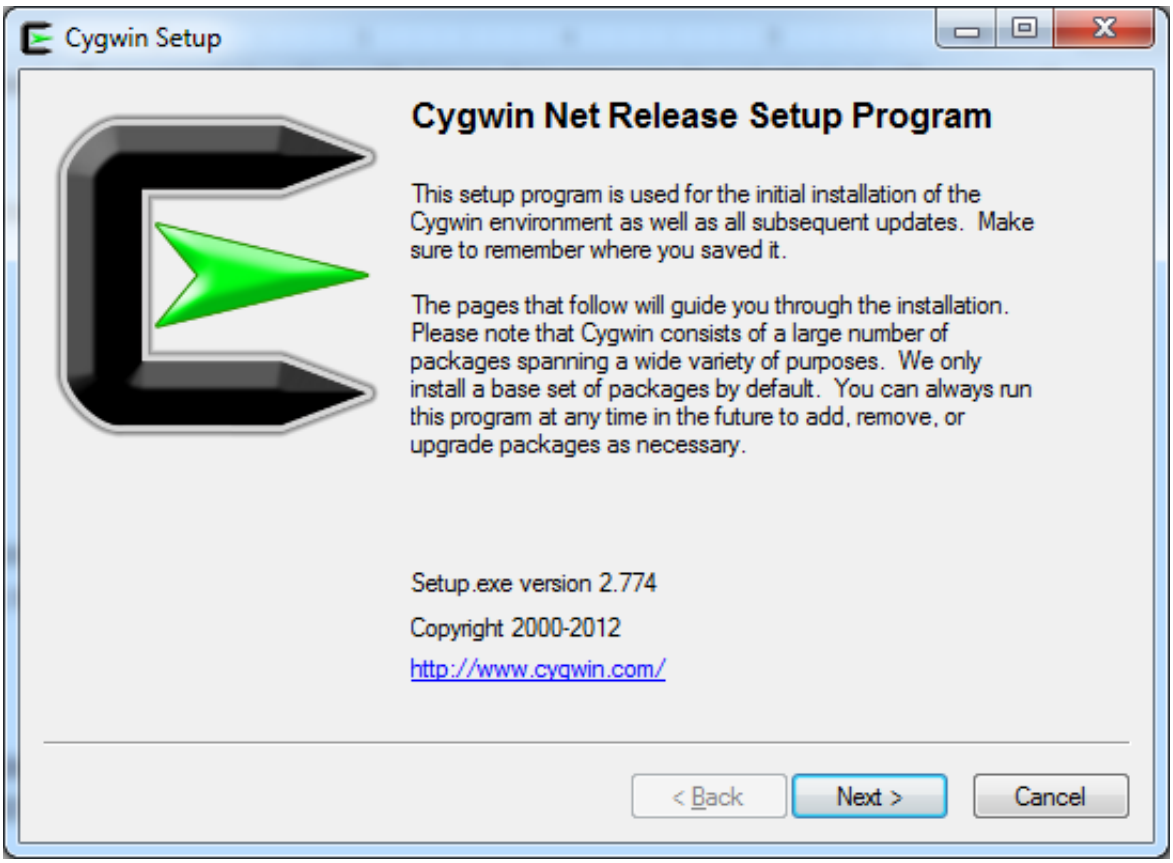
may find your machine with port 22 open. The bots will assume sshd is running on port 22, so don't be suprised if you look at logs and see failed login attempts with simple username/password combinations of root/blank, Administrator/blank, etc… The login attempts are nothing to be alarmed about if you have strong passwords. root is the unix equivalent of the Windows Administrator account.

Installing Cygwin and openssh applications

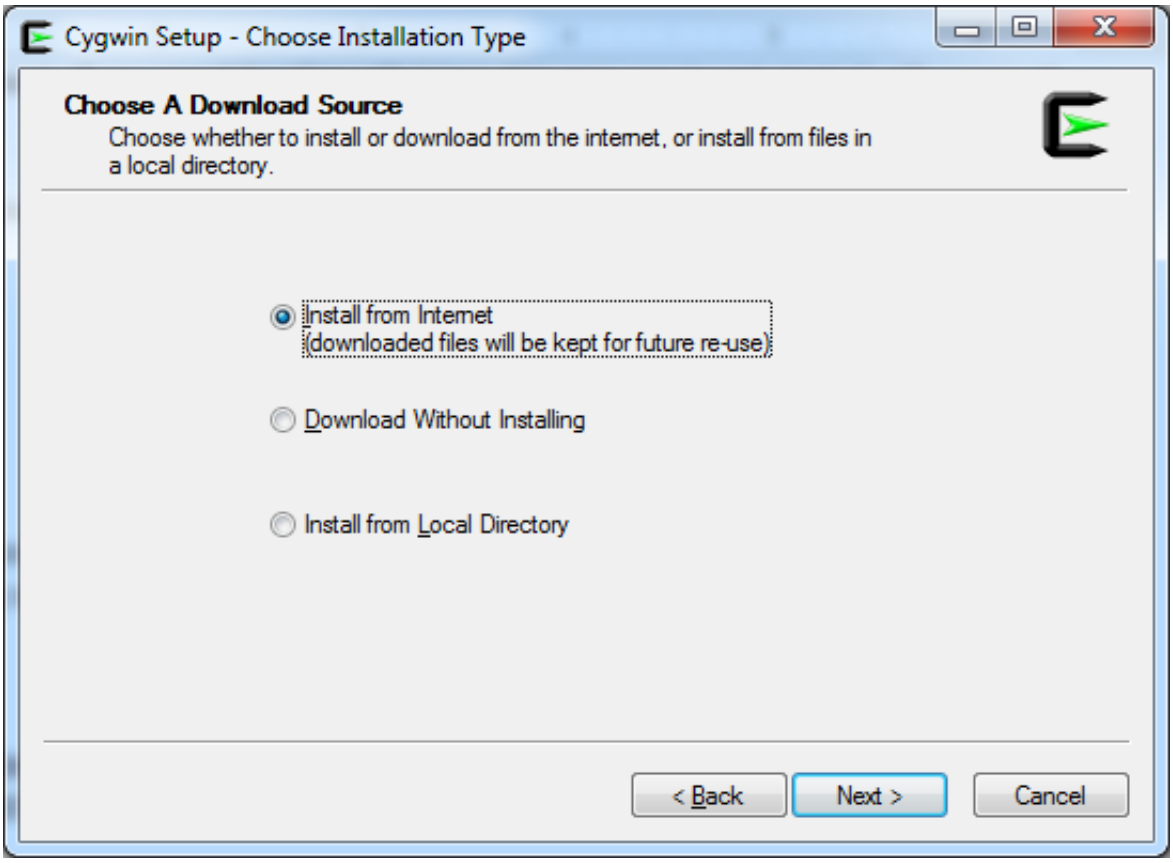
1. First we need to download setup.exe from the Cygwin website.



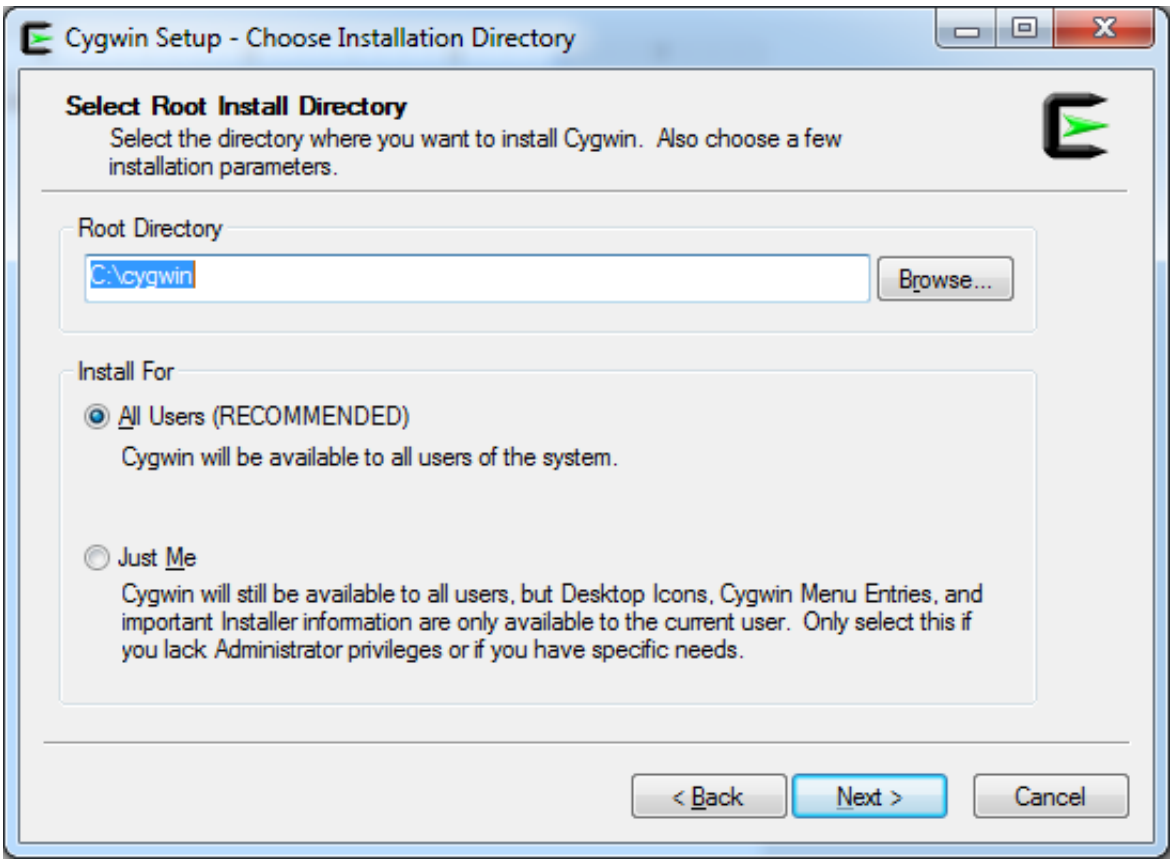
2. Run the setup.exe which you just downloaded.
3. Select next.



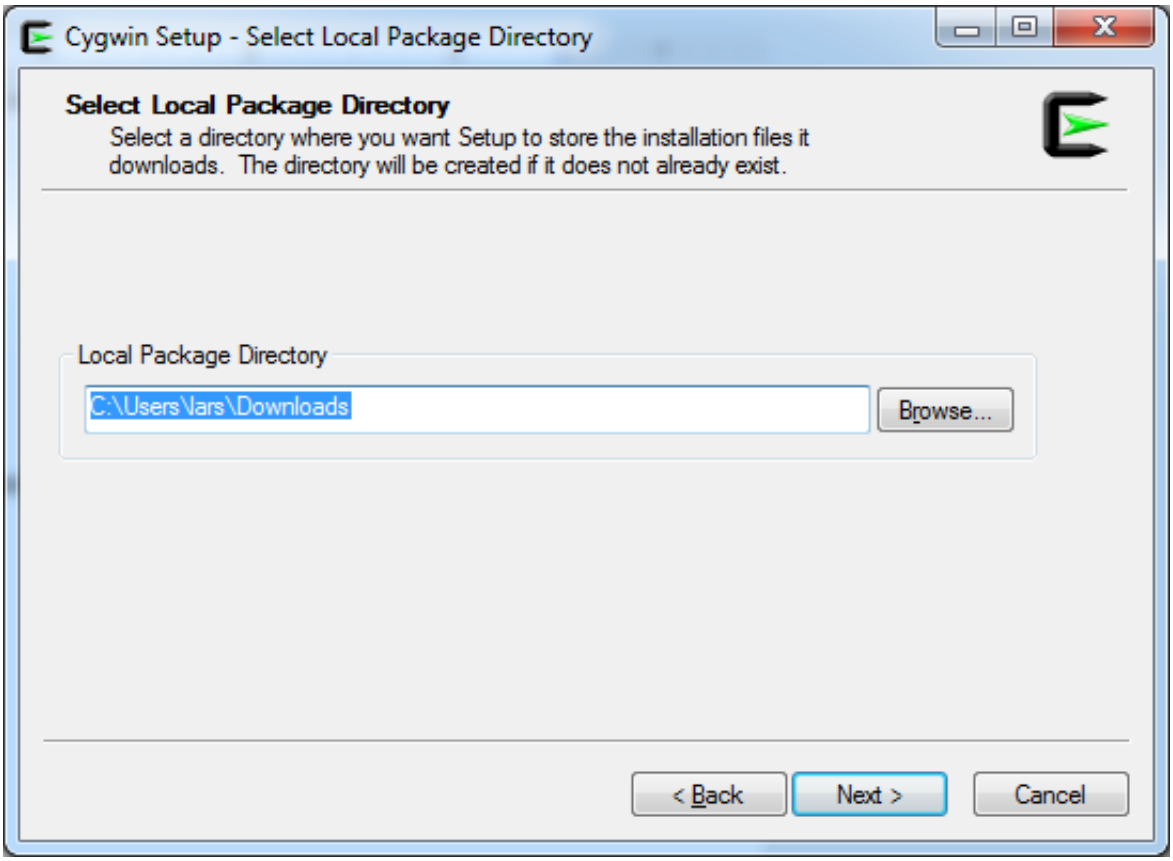
4. Select 'Install from Internet'



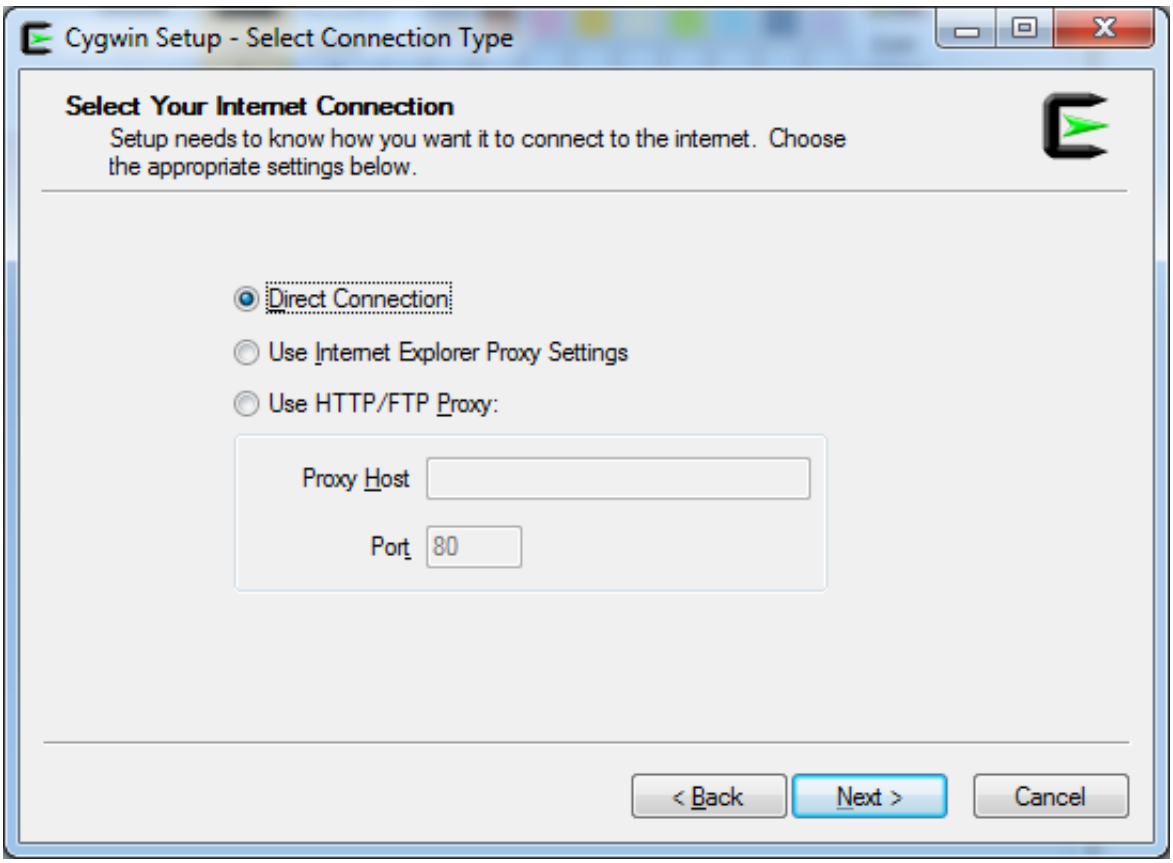
5. Select the root directory of the installation and who is allowed to use it.
    a. (c:\cygwin and 'All Users' should be fine)



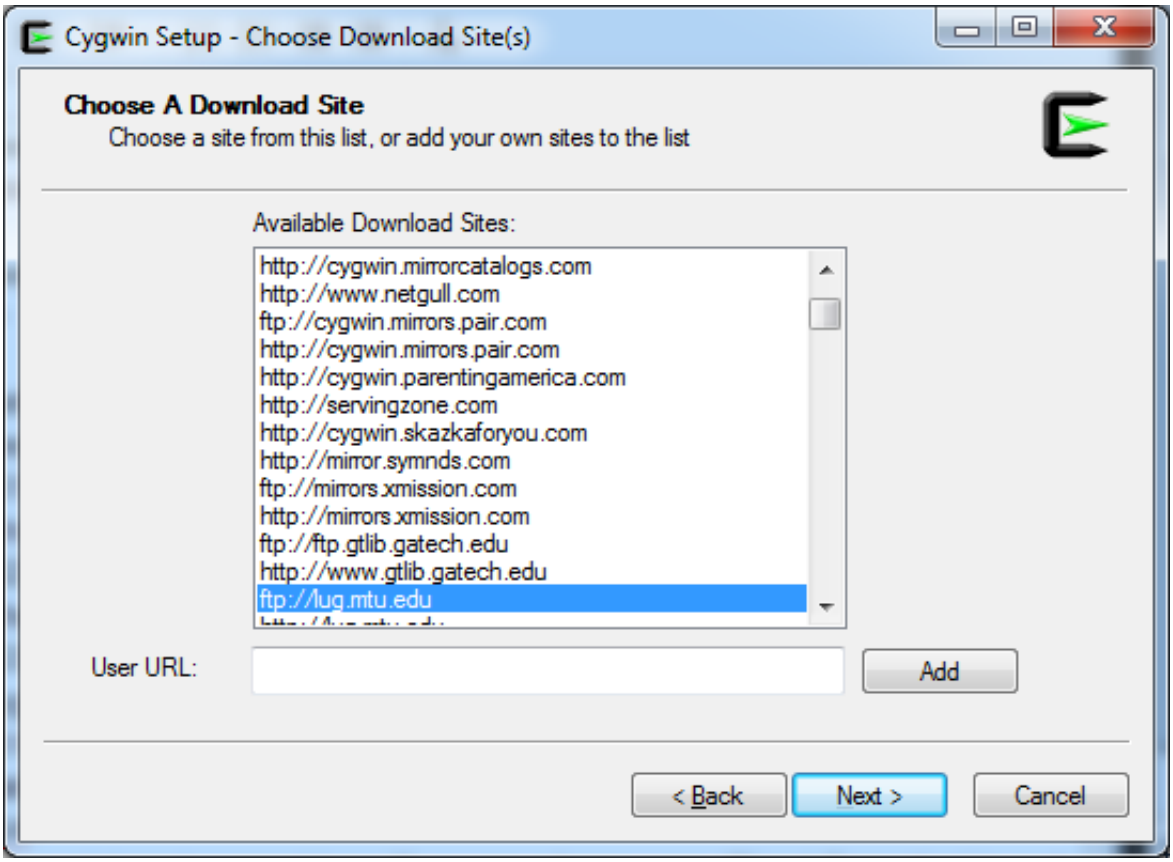
6. Select the 'Local Package Directory'. This location will be used to store downloaded information during the installation process.



7. Select your internet connect type. (If you don't use a proxy, select 'Direct Conection').



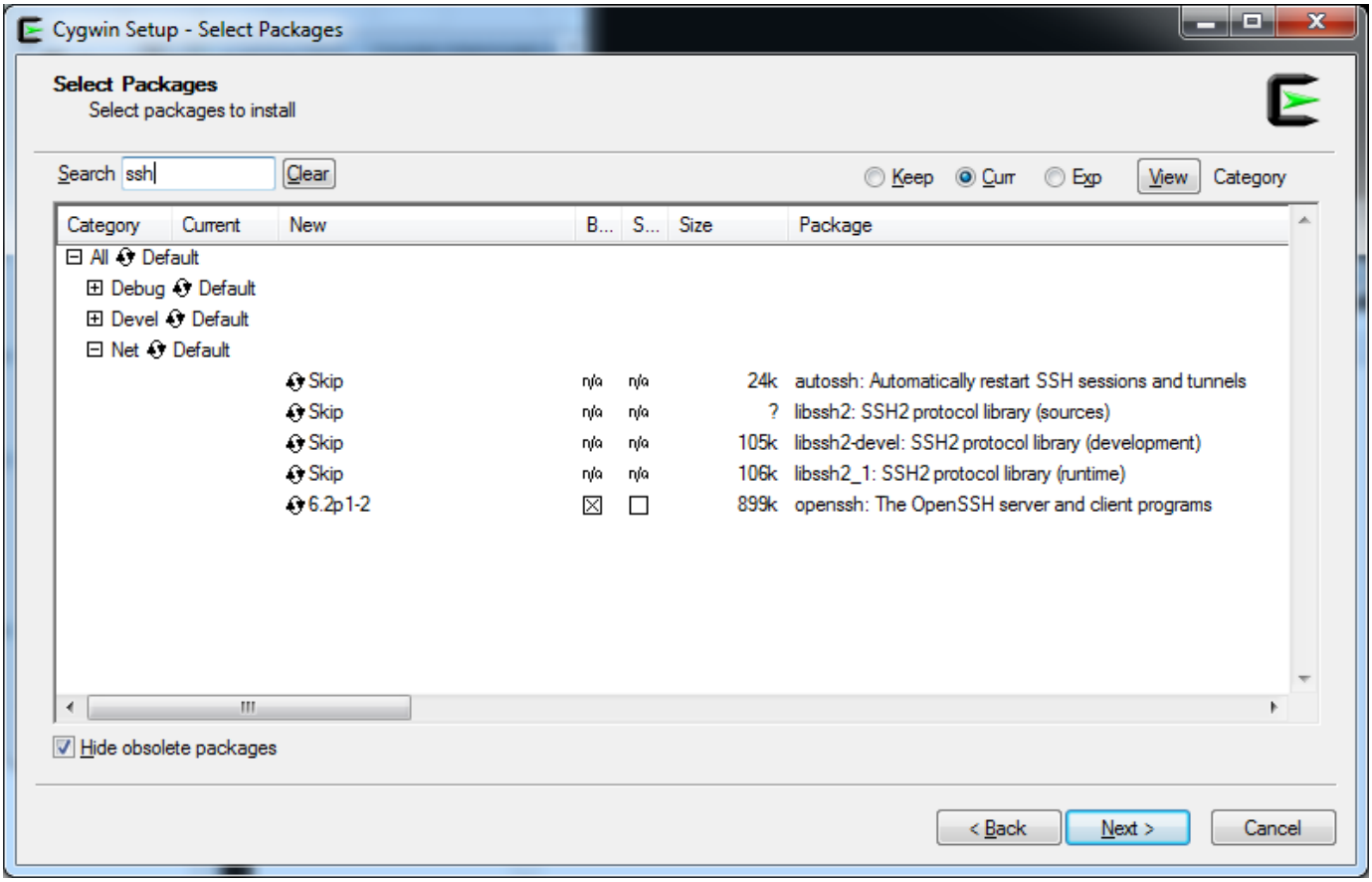
8. Choose a download site. Just pick one.



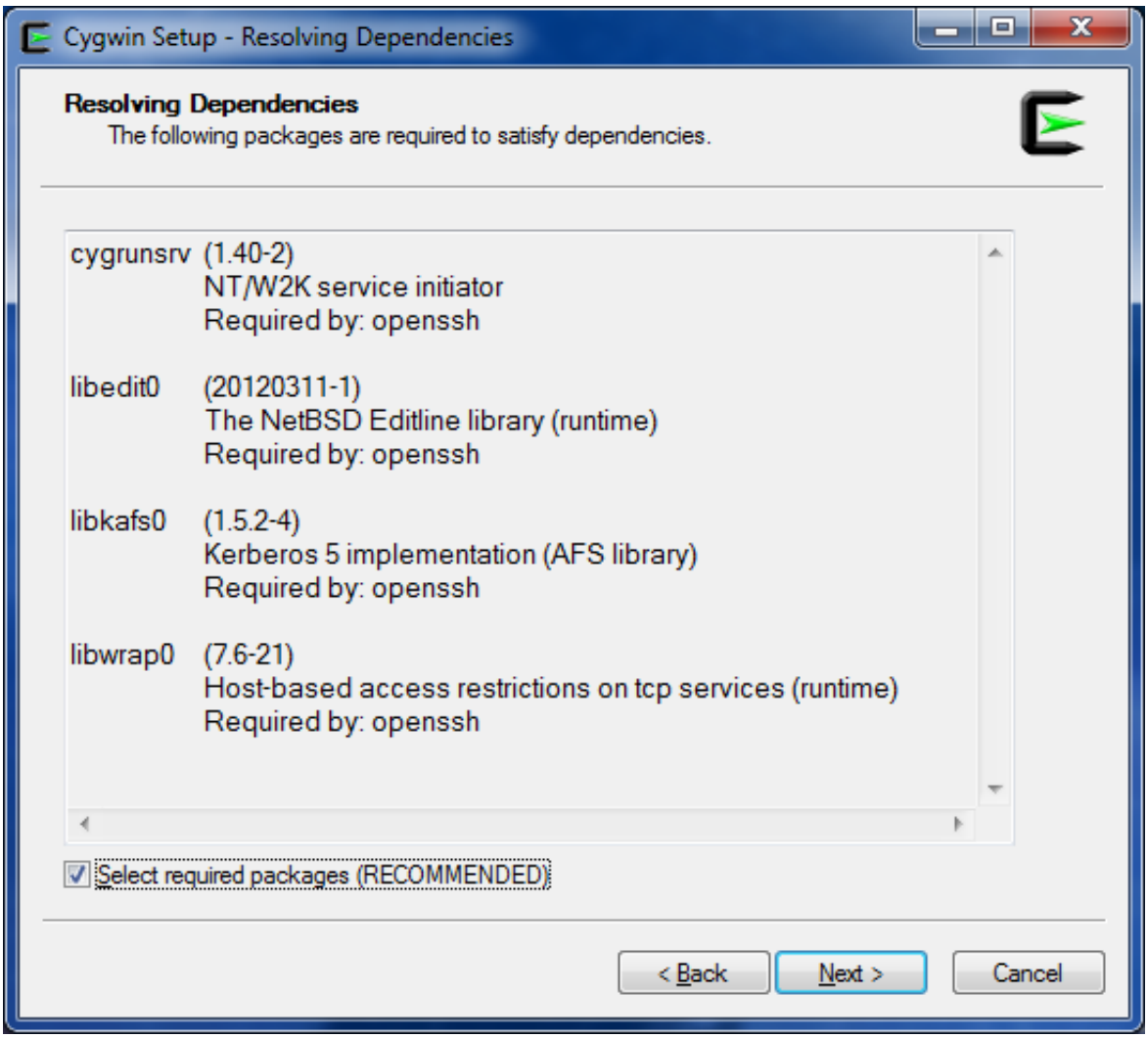
9. Select the openssh package for installation.
    a. In the search field, enter in 'ssh'. The installer will automatically search for matches.
    b. Expand the 'Net' menu
    c. Click (only once!) on the word 'Skip' in the openssh package row. This will cycle it to the next option, which displays the current version. At the time

of writing (5/13/2013) that version is 6.2p1-2

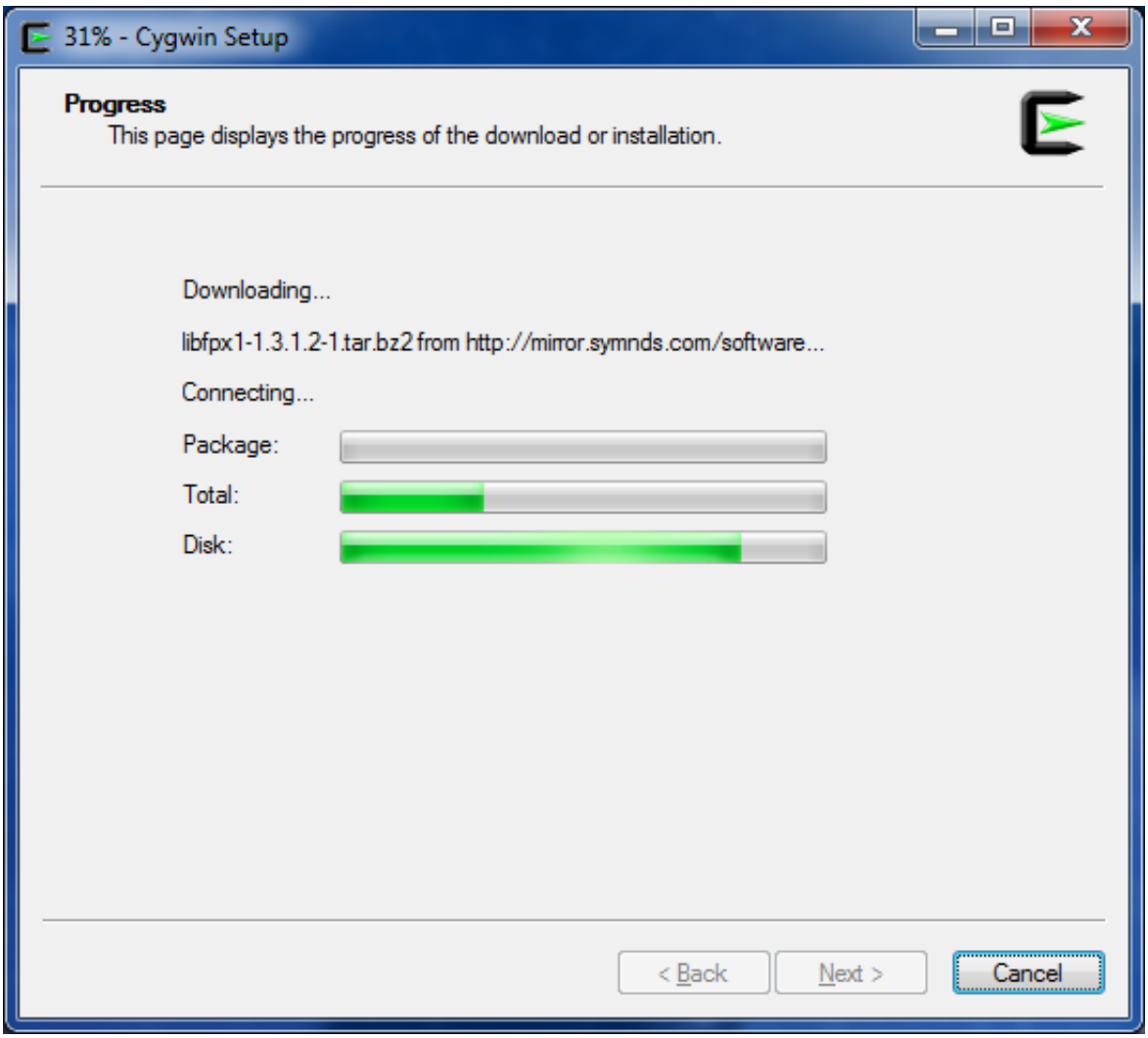
d. Note that this is only installing the openssh binary package. It is not setting up the Secure Shell Server for you. That comes later.



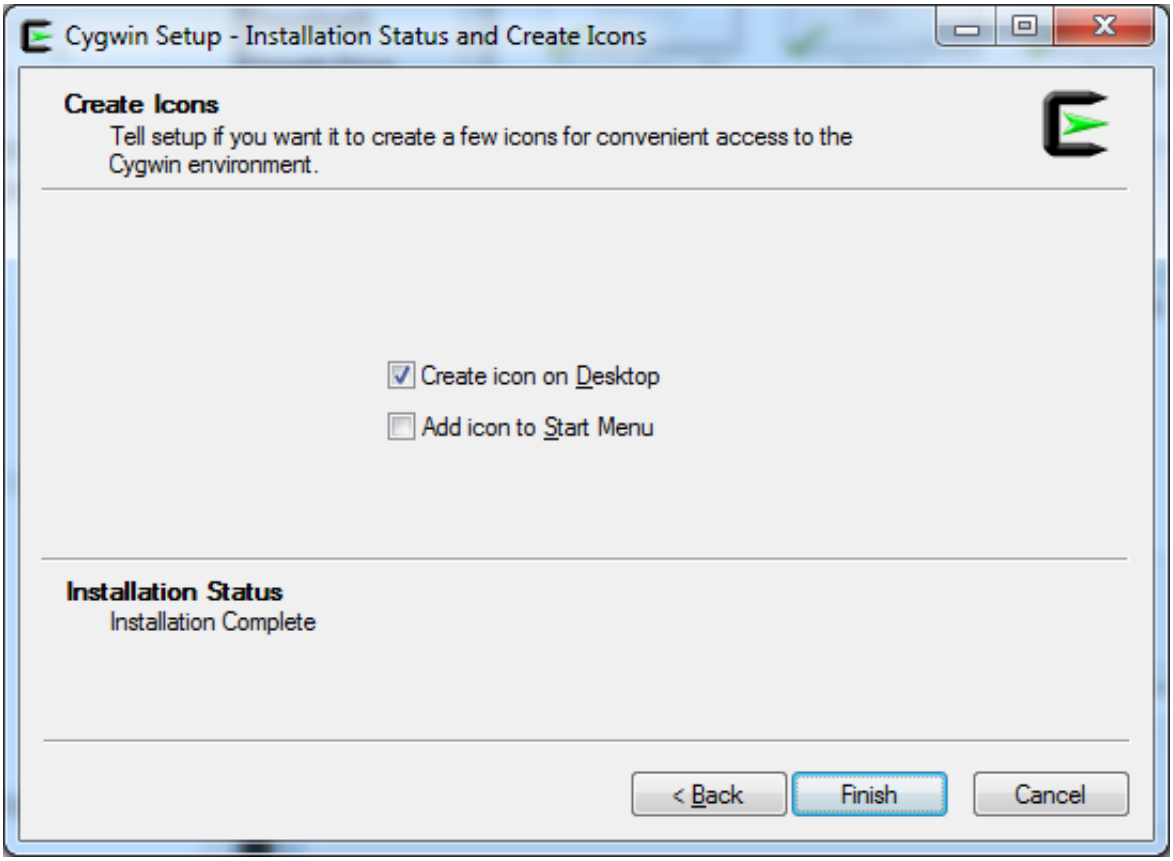
10. The installer will show you a list of openssh dependencies (things it uses). Select next.



11. Let the installer do it's thing… Some people have experienced half hour long installs. If you do, try selecting a different download site.

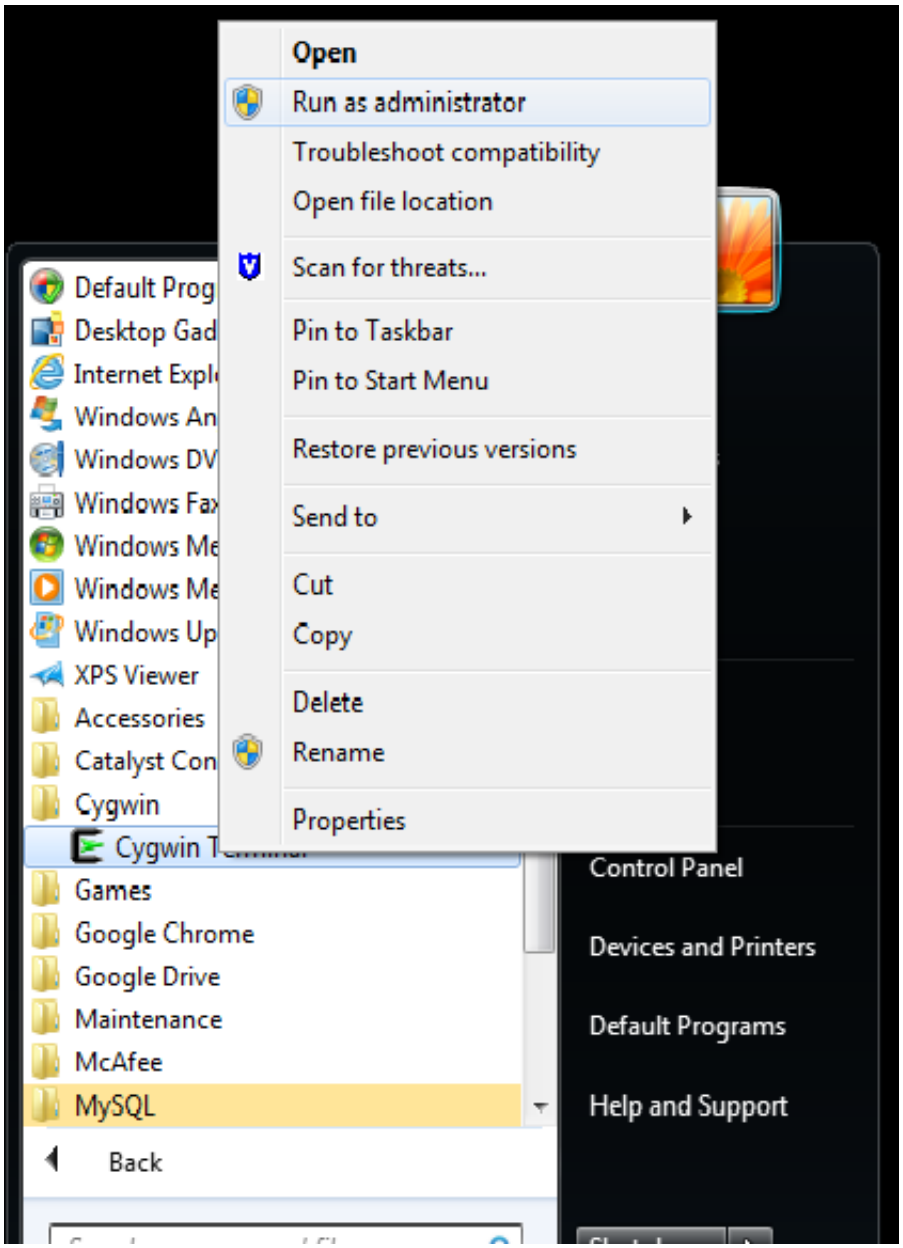


12. Cygwin set up is complete. Click finish.

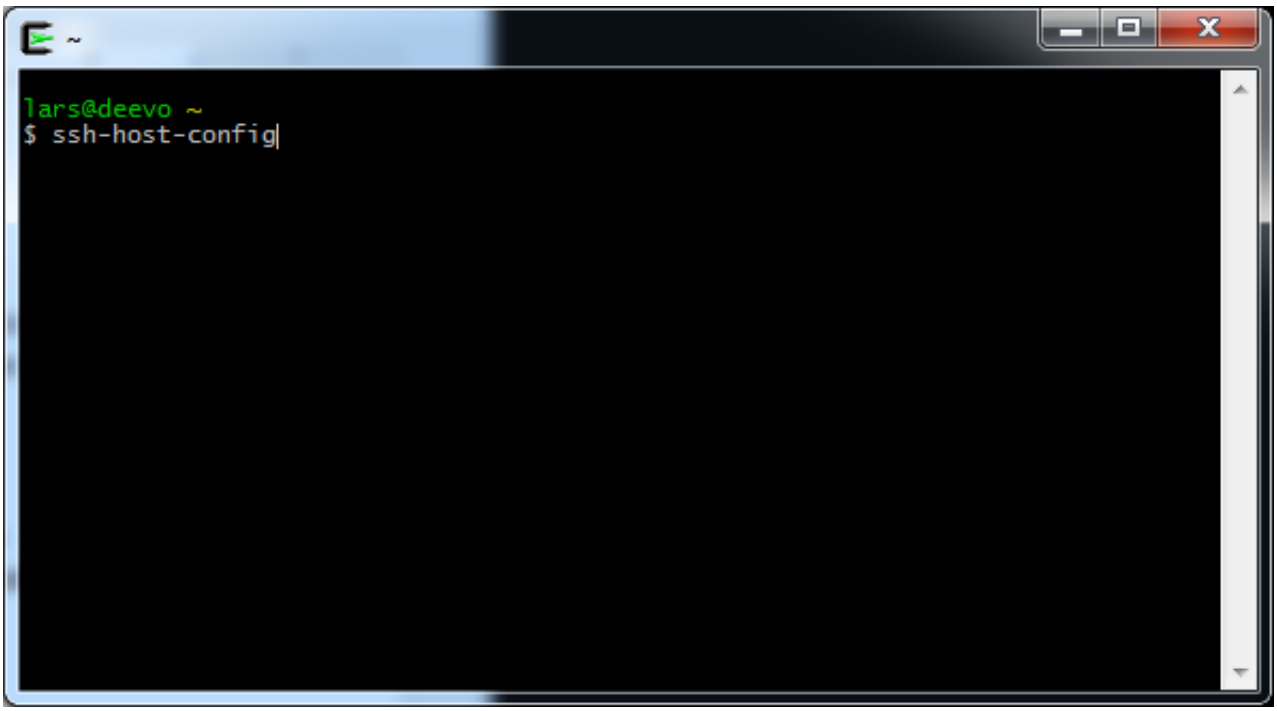


Setting up Secure Shell Server (sshd)

1. Start a Cygwin Terminal as an Administrator. You must run the terminal with administrative access to set up sshd. To start a cygwin terminal with administrative access:
   a. Find the Cygwin Terminal icon in the start menu.
   b. Right click the 'Cygwin Terminal' icon and select 'Run as Administrator'.



2. The Cygwin installer put a script on your system that performs the sshd set up for you. The script exists here: /usr/bin/ssh-host-config
   a. At the prompt, enter in 'ssh-host-config' (without the single quotes, and press enter)



3. You will now either see a warning about not having administrative privileges because you didn't run the terminal as an Administrator, or the script will start generating keys and begin asking you questions. If you see warnings about privileges then you need to close the terminal and run it again with administrative privileges (see above).
4. Here are the answers you will be asked by the script, along with the response you should supply in **bold**Query: Should privilege separation be used? (yes/no) **yes**

   Query: new local account 'sshd'? (yes/no) **yes**

   Query: Do you want to install sshd as a server?

   Query: (Say "no" if it is already install as a service) (yes/no) **yes**

   Query: Enter the value of CYGWIN for the daemon: [] **(DON'T ENTER ANYTHING, PRESS ENTER)**

   Query: Do you want to use a different name? (yes/no) **no**

   Query: Create new privileged user account 'cyg_server'? (yes/no) **yes**

   Query: Please enter the password: **ENTER YOUR PASSWORD HERE**

   Query: Reenter: **RE-ENTER YOUR PASSWORD**

5. Now you should have a Windows service installed named 'CYGWIN sshd',

which is run as the user 'cyg_server'. If you look at the service, you can see it is running the executable 'c:\cygwin\bin\cygrunsrv.exe'. There will be a new Windows account 'Privileged Server'. That's it. That is all there is to getting the Secure Shell Server installed! You can always go back and re-run the script if you need to.

Starting and stopping the sshd server

1. Starting the server
    a. At the command prompt enter 'net start sshd'
    b. You should see the following output:The CYGWIN sshd service is starting.

       The CYGWIN sshd service was started successfully.

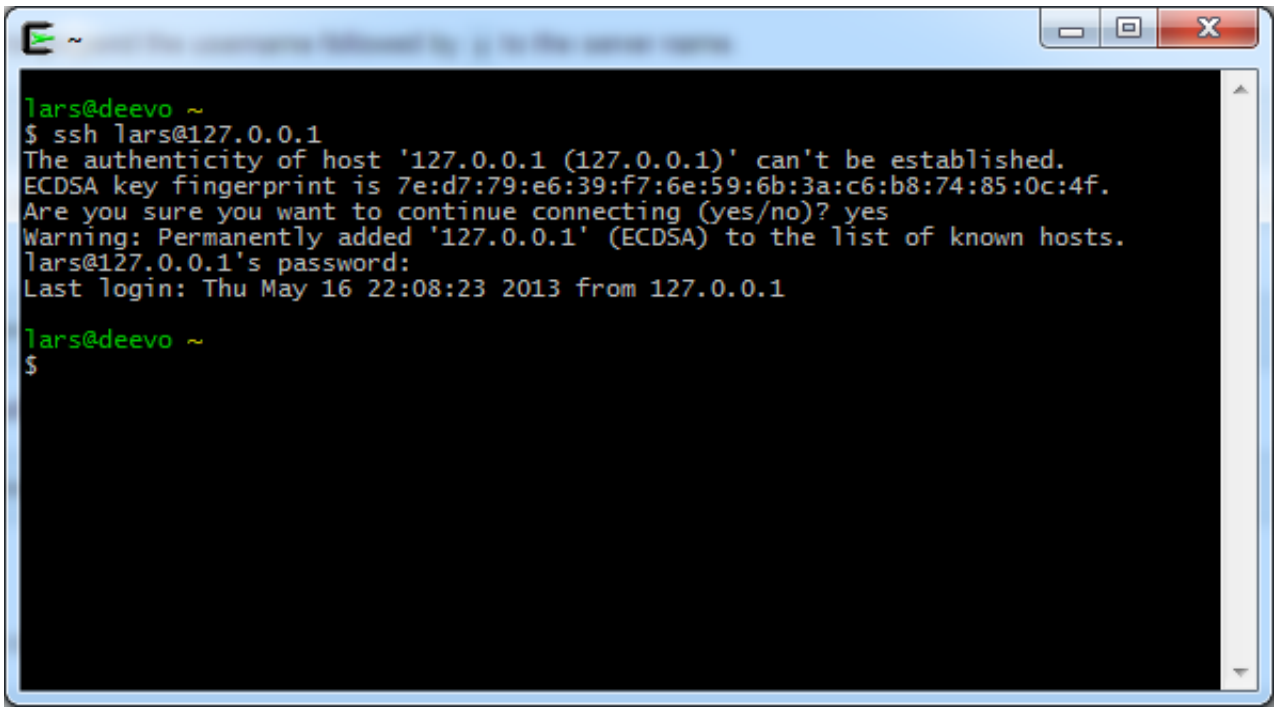
2. Stopping the server
    a. At the command prompt enter 'net stop sshd'
    b. You should see the following output:The CYGWIN sshd service is stopping.

       The CYGWIN sshd service was stopped successfully.

Testing your sshd installation

To connect to an sshd server you can type in the command 'ssh username@ipaddress' where username is the windows username and ipaddress is in dotted-decimal notation.

1. Now we will test our sshd installation.
2. Start a cygwin terminal on the system that sshd is installed on.
3. Enter the following at the command prompt 'ssh username@127.0.0.1' where username is the Windows account username you want to connect as on the system running sshd.
4. You will be presented some information and asked: Are you sure you want to continue connecting (yes/no)?
    a. enter **yes**
5. Enter the pasword for your Windows account.
6. If your connection was successful you should see something similar to this:



Now what?

1. Type 'help' at the command line to see what is offered in the BASH shell.
2. Learn about the BASH shell: https://www.google.com/search?q=learn+the+bash+shell
3. Next time, we will talk about hardening / configuring the sshd installation. When the article is complete, it will be linked to here.

Firewalls

As with all networking software, you need a good understanding of TCP/IP to get everything running properly. If you are only expecting ssh connections from specific systems, you should try to limit incoming connection to those IPs or an IP range. I'm not going to go into detail about configuring your firewall. However, here are the two important pieces of information for setting up the firewall for sshd.

1. sshd default port: 22
2. sshd application will appear to run from the executable c:\cygwin\bin\cygrunsrv.exe

Logs

sshd will write to the windows logs. The souce of the log entry will be from 'sshd'.

Troubleshooting

You may see a connection attempt fail and present a similar error message:

ssh: connect to host 127.0.0.1 port 22: Connection refused

This can happen for at the very least, one of the two following reasons:

1. sshd is not running. In which case you can start the service by entering 'net start sshd'
2. The firewall on the sshd system may be blocking port 22 from your IP address.

More information

1. Cygwin docs: http://cygwin.com/cygwin-ug-net.html
2. OpenSSH: http://www.openssh.org/