Securing Remote Desktop for Windows XP

http://www.mobydisk.com/./techres/securing_remote_desktop.html

Remote Desktop, Un Safely

Many people use the Windows XP Professional remote desktop feature to gain easy access to their home PCs. But opening up a connection to an administrator account on your system is very dangerous. Just by opening the port on my firewall I received several logon attempts, from various countries, within a week. Free tools exist that assist hackers with breaking into Windows Remote Desktop connections. Fortunately there are a few simple steps you can take to protect yourself:

Remote Desktop, Safely

Limit users who can log on remotely

First, only allow certain users remote desktop access. Go to the Control Panel, then system, then the Remote tab.

From there, enable "Allow users to connect remotely to this computer." Then, click "Select Remote Users."
Here, add only the users who you want to be able to log in remotely. If you are super-secure, you can set this to a standard user account, and force yourself to run as a normal user. This is a very difficult way to run Windows since many applications assume the user has Administrator rights, so I leave that decision up to you.

Unfortunately for you, that setting didn't do a thing! You will find that you can still log on as any administrator account. To make things complicated, Microsoft defaults to the least secure setting possible while hiding this fact from the user. You will need to go to another location to change the real list. Click Start - Programs - Administrative Tools - Local Security Policy. If you can't find it, you can also do Start - Run - enter "%SystemRoot%\system32\secpol.msc /s" - Ok.
Under Local Policies - User Rights Assignment, there is a line that says "Allow logon through Terminal Services." And just next to it is "Administrators, Remote Desktop Users." Aha! Too bad it didn't show "Administrators" in the other screen. Double-click this setting and remove "Administrators." If you want an administrator to have access, just add them explicitly through the other screen.

Set an account lockout policy
There are already tools that will use brute-force to guess passwords and log-on remotely. You cannot stop this, but it can be minimized by setting an account lockout policy. If someone tries to guess the password, then after a few guesses they will be locked out for a period of time. This can make hours or days of guessing become centuries. That makes it infeasable to brute-force into your system.

From the same Local Security Policy screen from before, go to Account Policies - Account Lockout Policy.

**Account lockout threshold:** This is the number of failed logon attempts before the user is locked-out. Three is usually sufficient to indicate someone is trying to break in.

**Reset account lockout counter after:** For a typical home system, set this setting to be the same as the **Account Lockout Duration** below.

**Account lockout duration:** This is how long the user will be unable to logon after several failed attempts. Even a few minutes will significantly reduce the possibility of a remote brute-force attack. For a home system, any more than a few minutes can be frustrating. You may come home to find your account is locked-out because of some joker guessing passwords. Adjust the setting to your own tolerance. Setting this value to zero means to lock the account until it is manually unlocked.

To manually unlock an account you must logon as another administrator user (preferably one without remote desktop access). Then go to Start - Programs - Administrative Tools - Computer Management - Local Users and Groups. Click on the individual user and uncheck the "account is disabled" check box. You may then log on as that user.
Require Passwords and 128-Bit Encryption

For compatibility with older, weaker, less-secure clients, Windows XP defaults to allowing minimal or no encryption on remote desktop connections. If you are connecting with older software, upgrade it. If you are connecting with the PocketPC Terminal Services Client, then this setting won't work for you since that client does not support high encryption. :-(

Click Start - Run - "%SystemRoot%\system32\gpedit.msc /s" to get to the Group Policy Editor. I don't know how to get there any easier than that, so you might want to add an icon for it to your Administrative Tools.

You can change the "Set client connection encryption level" from "Not Configured" to "Enabled" and "High Level" to force the client to use 128-bit security. This protects your passwords as well as anything transmitted during your terminal service session.

Enabling "Always prompt client for password upon connection" prevents the remote user from saving the password on the client computer and avoiding the password prompt. Saving passwords is generally a dangerous setting since the password is now on another computer, and because it allows the user to forget it.

**Account Audit Logging**

Under Local Security Policies you can turn on Auditing by checking the success and/or failure of the Audit Account Logon Events and Audit Logon Events Properties. This will allow you to track success or failures of any attempt to logon your computer including access to any shares over the network. Many failures will indicate that that someone is trying to access your computer and is a good time to change or strengthen your passwords.

Go to: /Control Panel/Administrative Tools/ and open the “Local Security Settings” Tool. Select the Local Policies/Audit Policy and then double click on Audit Account Logon Events. Do the same for the Audit Logon Events Policy.
Other things you can do

The Event Viewer logs failed login attempts and account lockouts. You can periodically check this to see if anyone is trying to get in. If your firewall keeps logs (Windows Firewall does) then you can use these to see when someone tries to connect. You can also move the terminal services port from 3389 to another port by changing the registry key at

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

from 3389 to something else. You will then need to specify the port when you connect to your system. Connect with something like "my.computerathome.com:3389" instead of "my.computerathome."

Security Limitations

Remote desktop is encrypted, which makes it more secure than many simplistic VNC implementations. However, Remote Desktop is vulnerable to a man-in-the-middle attack because it does not use a certificate to authenticate the server like SSL/SSH does. That means that if you connect to a your system via remote desktop, there is no guarantee that the conversation is not recorded and your passwords are not guaranteed to be safe, even though the session is encrypted.

Check here for more information on man-in-the-middle attacks.

http://en.wikipedia.org/wiki/Man-in-the-middle

The only surefire way to prevent this is to use SSH tunneling over a VNC connection.

http://www.shebeen.com/vnc_ssh/