Global Information Assurance Certification Paper

Paranoid PC Anywhere

Kris Kistler
MCSE, MCP+I, CCNA, CNA, CCA, A+

If you are like most administrators, sooner or later you end up needing remote access to a server(s) to either fix a problem or finish an install. How to do this without leaving your hosts open to every script kiddie and weekend hacker is the question I hope to answer. The best solution for remote access is obviously to have someone available to initiate the session and not to leave it open 24x7. For some situations, full time access is a requirement. The question is, then "How do I secure my systems from the bad guys?". This paper will deal with host mode configuration on an Windows NT 4 Server or workstation system. We will assume you have taken all the other recommended steps to properly lock down your server from unwanted access by reading the current bulletins, applying the latest service packs and hotfixes, http://www.microsoft.com/technet/security/current.asp , disabling the guest account, renaming the administrator account, removing remote access, applying correct permissions to the registry, etc. and all the other issues commonly addressed in various white papers and checklists. A few good sites for configuration guidelines are:

Microsoft: http://www.microsoft.com/technet/security/tools.asp (free)
Security Focus http://securityfocus.com/focus/microsoft/nt/ntsecure.html (free)
Sans http://www.sans.org/newlook/publications/ntstep.htm (small fee, but also the best imho and has an excellent checklist)

Once these are finished, you are ready to install and configure your PC Anywhere. As always, start with the most currently available version, which at the time of this writing is 9.0. By staying current on software versions, you are assured that the software has had the latest bug and vulnerability fixes (normally). This version provides connectivity from Windows 9x and W2K versions as well as from Windows NT clients. Once we have installed and rebooted. We will want to configure PC Anywhere to run as a service, this can then be configured to start automatically at boot time, if desired. I prefer to enable host mode in network mode, using TCP/IP protocol only. No direct dial up or IPX, this way we can filter and log any access. Any remote administrators that require access must have dedicated isdn that calls into our T1-PRI loop, this is then further filtered by a firewall restricting ip addresses and ports.

We do not currently permit access using PC Anywhere thru our internet firewall, although some sites may decide that the benefits of doing so outweigh the risks. If so, this configuration should help minimize your exposure if the proper filtering is also done both at your firewall and the remote users firewall. All your remote PC Anywhere users have firewalls on their systems too... right?

If you are going to use this across the internet, it makes sense to modify the standard ports that PC Anywhere uses. While the quote "security thru obscurity" is overused, I'll use it again here because it adds an extra layer of protection. By changing the port number, your servers will not scream out that you are running in host mode to the bad guys (gals), or even the person who "accidentally" misconfigures their PC Anywhere client to scan your subnet , just waiting for them to come log in and drive your computer for awhile.

Most people who have used PC Anywhere know that if you don't specify an IP address to connect to, it automatically scans your local subnet and displays any active listening hosts. Many do not know that if you place a 255 in place of the last octet, it will also scan and display listening hosts on remote subnets. OOPS! How Interesting! Many IT departments running IDS systems can tell you that they regularly receive scans at the standard ports. This "feature" can be blocked by telling the host not to answer scan requests. Standard registry editing warnings apply: To disable, set this Registry DWORD value to 0
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System\DisplayHostInList

Standard (default) ports are:

PC ANYWHERE version	TCP (data) port number	UDP port number
2.0	65301	22
7.0	65301	22
7.50, 7.51	65301	22
CE	65301	22
7.52	5631	5632
8.x, 9.x	5631	5632

A more complete description of the default ports and this Registry hack is listed on the Sans GIAC Security site at:
http://www.sans.org/y2k/reports.htm or at Symantec's site
http://service1.symantec.com/SUPPORT/pca.nsf/pfdocs/1998122810210812

This change will not prevent them from attempting login if they know the port number and the IP address. If you change the standard port number, they must also guess the port number before they can attempt a login. If they do a probe or port scan, they will see an open port but not know what it is being used for. If they do a port scan and find the default ports open, they will know immediately that it is PC Anywhere listening in host mode.

Information on changing the default port numbers can be found at Symantec's site:
http://service1.symantec.com/SUPPORT/pca.nsf/docid/1996123152253

Thinking twice now about those blank or weak password accounts, or about renaming the administrator account and setting account lockouts so they don't have unlimited login tries... if not, you should be. Remember the warning above to lock down your hosts first!

Extra Paranoid: You may wish to filter at the host level as well, in Windows NT you can get there by going into your "Control Panel", "Network", "Protocols", "TCP/IP Protocol", "Properties", "Advanced", Click the checkbox marked "Enable Security" and then click the "Configure" button. You should see the picture below. You can then specify the ports you wish to allow traffic on. ** The graphic is for illustration purposes only. Only perform this step if you are sure what you are doing, modifying these parameters could have undesireable effects.**

Ok, we have checked our firewalls, locked down our hosts, installed PC Anywhere, now what? Let's configure the host.

Setting the Host options:

Under the "Be a Host PC" button, Go to the network properties.

Connection Tab: Click the connectivity needed. I use TCP/IP only, this may vary depending on your configuration.

Settings Tab: Run minimized and run as service should be checked. I also like to check the box under Abnormal End of Session to secure by logging off the user, or locking the workstation. This would prevent the machine from being left in an open state in the event of abnormal disconnection. Are your servers in a locked, restricted access room?

Callers Tab: Select windows authentication with windows privileges. Then click add user to add users you wish to grant access to. **DO NOT ADD THE ADMINISTRATORS GROUP**. I repeat for emphasis, **DO NOT ADD THE ADMINISTRATORS GROUP**. This is a common mistake made by even experienced system administrators. If you don't believe me, read the "War Story" below. By adding the administrators group, you can inadvertently open holes for system accounts and automatically created accounts to access your systems remotely. Pick your users specifically and grant them access or create a special "pcanywhere" group and place your users in that group if you have many administrators or a fast turnover of remote users.

Security Options Tab: Encryption Settings. Set this to AT LEAST "pcAnywhere" Encryption and better if you can support it. You should also check to "Deny Lower Encryption Level" so that the client is REQUIRED to connect with an encrypted session. The client connection will also have to select this. Other settings are optional.

Conference Tab: I usually leave this off, unless you have a specific need for it.

Protect Item Tab: Set your password here so no one can change the settings you worked so hard secure.

Logging:

Under the "Tools" "Logging Options" option, you can set the logging parameters you wish. I

suggest using NT Event logging and/or snmp and enabling at minimum all sessions and file transfers. Preferably your NT logs are also forwarded to an external logging server, since anyone having admin remote access to your server would also have the capability to modify or destroy log files. The truly super-paranoid may wish to even record the entire Host session, or do so on a "Honey Pot" machine to see what kind of interesting captures they receive. Remember to check the logs!

Many sites with one administrator or limited number of administrators will also stayed logged in, locking the screen. In the event that someone does login remotely, they must unlock the screen with an administrator account and log off the current user. This should send up a warning flag that someone else logged into your machine. It should also tell you not to leave the machine unattended with an account logged in without the screen locked, even in a secured area.

War Story: I was once asked to do a security check across a WAN connection. They had an Internet firewall in place, but their Security Official was new and unsure of the exposure from the 40,000 plus nodes on their multi-company WAN. The Security Official I was with had to catch a plane in 2 hours and asked me if I could give him a "quick" idea of some vulnerabilities they might be facing on some of their systems.

I just happened to have a copy of ISS Internet Security Scanner handy on my laptop, so I did a zone transfer from their DNS server, found some interesting server names, and ran a scan. After running for about 10 minutes, the scanner came up with a service account that had been obviously misconfigured (probably automatically created and added to the administrators or system group) to have the same password as the account name. This server also showed up with the default port for PC Anywhere open. He asked "What's wrong"? as he heard me chuckle loudly. I said "Let's try something" and fired up my PC Anywhere, logged into the remote server using the service account name and said "Would you like to drive your domain controller for awhile?" The noise from his jaw hitting the table drew a few onlookers from down the hall. I then explained how easy it would be to upload any utility I wanted, view or change user accounts, or even obtain the SAM password file and crack ALL the accounts at my leisure. I think the short demonstration had an effect on him, and I hope it serves as a reminder to you that configuring a server securely isn't near as much work as de-rooting and rebuilding one.

I'll say it one more time. Everybody with me now..... **DO NOT ADD THE ADMINISTRATORS GROUP!**

In conclusion, I'll add that this was done with permission and under the supervision of the target site security personnel for all the brainers that may want to try this at home... You KNOW that you could get into serious trouble for this.

References:

Symantec Corporation Web Site
http://service1.symantec.com/SUPPORT/pca.nsf/docid/1996123152253
http://service1.symantec.com/SUPPORT/pca.nsf/pfdocs/199732093939
http://service1.symantec.com/SUPPORT/pca.nsf/pfdocs/1998122810210812

http://service1.symantec.com/SUPPORT/pca.nsf/pfdocs/1997471006

Sans Global Incident Analysis Center Web Site (GIAC)
http://www.sans.org
http://www.sans.org/y2k/reports.htm
http://www.sans.org/giac.htm

Microsoft Corporation Web Site
http://www.microsoft.com/technet/security/current.asp
http://www.microsoft.com/technet/security/tools.asp