

20 Windows 2003 Command-Line Weapons

Sean Deuby

(Reprinted from WindowsItPro Magazine)

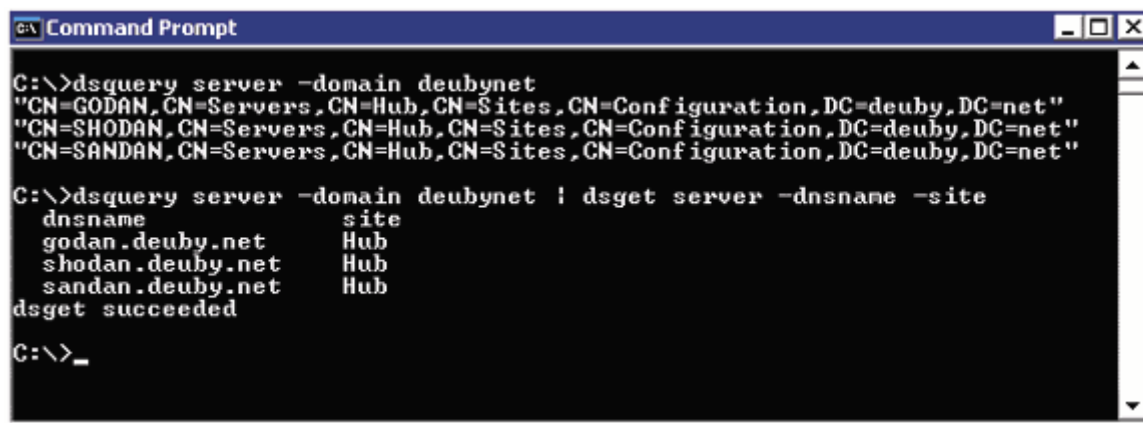
In the Windows realm, command-line utilities never seem to garner the attention that graphic utilities do. Even though command-line tools have experienced a myriad of improvements over the years, you still have to dig around to find them. Not only does Windows Server 2003 boast a wealth of new command-line utilities, but Microsoft has also enhanced a number of mainstay Windows 2000 (and even Windows NT 4.0) tools. In addition, Microsoft has added or enhanced many of the tools at its Download Center.

Indeed, valuable command-line stuff is out there, but it remains scattered and poorly advertised. The sidebar "Get Your Command-Line Utilities Here!" gives you the five premier locations at which you'll find Windows command-line utilities. In the following discussion, I talk about all kinds of tools, from the generally useful to more specific server-troubleshooting and Active Directory (AD)-troubleshooting utilities. I break the discussion down according to the origins of the tools, beginning with the base OS and continuing through Support Tools, the Microsoft Download Center, the Microsoft Windows Server 2003 Resource Kit, and even some third-party resources.

The Base OS

Utilities installed with the OS are the most fundamental of all the tools in this article. Nonetheless, you might not be aware of some of these essential utilities.

Ds- tools. No discussion of Windows 2003 command-line tools would be complete without at least a mention of the Ds- directory service tools—Dsquery, Dsget, Dsadd, Dsmode, Dsmove, and Dsrms—that come with the OS. Dsquery and Dsget, which come with Windows 2003, perform slightly different functions that are confusing at first but complementary when you combine the tools. Dsquery returns lists of AD objects in distinguished name (DN) format by specifying search parameters with a combination of keywords and search filters. Dsget uses the same method to return the attributes of a specific AD object. Dsget also accepts output from Dsquery via the pipe (|) command, allowing Dsget to return only certain attributes or otherwise format the output of a list of objects. Figure 1 shows the output of Dsquery to return all domain controllers (DCs) in the deubynet domain, and also shows the output after the output is run through Dsget to return only the DNS name and site information for each.



```
Command Prompt
C:\>dsquery server -domain deubynet
"CN=GODAN,CN=Servers,CN=Hub,CN=Sites,CN=Configuration,DC=deuby,DC=net"
"CN=SHODAN,CN=Servers,CN=Hub,CN=Sites,CN=Configuration,DC=deuby,DC=net"
"CN=SANDAN,CN=Servers,CN=Hub,CN=Sites,CN=Configuration,DC=deuby,DC=net"

C:\>dsquery server -domain deubynet | dsget server -dnsname -site
dnsname      site
godan.deuby.net      Hub
shodan.deuby.net     Hub
sandan.deuby.net     Hub
dsget succeeded

C:\>_
```

Dsadd (add objects), Dsmode (modify attributes of existing objects), Dsmove (move objects within a domain), and Dsrms (remove objects) have syntax that's similar to that of Dsquery and Dsget.

In deference to the complexity of the AD hierarchy, the first parameter of Dsquery, Dsget, Dsadd, and Dsmode is a keyword that specifies the type of object you're operating on. This parameter avoids the

20 Windows 2003 Command-Line Weapons

Sean Deuby

(Reprinted from WindowsItPro Magazine)

requirement of knowing exactly where in AD the objects reside. For example, with the third-party AdFind tool, an efficient search of sites would set the base DN with which to begin the search to `cn=sites,cn=configuration,cn=yourdomain,cn=com`. With Dsquery, you simply need to specify dsquery sites in the command string. I would argue, however, that to truly understand AD, you need to know the location of these objects. Also, the Ds suite doesn't provide the full range of operations you might need. For example, you can't programmatically manipulate site configuration. When you're comfortable with the Ds tools, step up to AdFind and AdMod, which I discuss in a moment.

Where. Have you ever tried to run a utility, found it wasn't on your current system, but couldn't remember whether it was a resource kit tool, a Support Tools utility, a server-specific command, or a downloaded tool? When I face this situation, I go to the system and run the command

where

where name.extension is the tool's filename. This command tells you the tool's directory location. Better yet, to perform this task on a remote system without leaving your chair, run this command in conjunction with the Sysinternals tool PsExec, which I describe later:

```
psexec \\
%windir%\system32where.exe
```

Support Tools

If the base OS tools are your fundamental utilities, the Support Tools are a close second. Originally intended to help Microsoft support professionals diagnose problems, the Support Tools have become an essential part of any administrator's toolkit and should be installed on all systems.

DcDiag

The Support Tools' DcDiag tool is the first utility you should run if you suspect a DC problem. The tool's basic functionality, without options, is to run 27 tests against a target DC (five more than in Win2K). If you use the /s switch to specify a target DC, you can then use the /a switch to test all DCs in the target DC's site. If doing so doesn't provide a broad enough scope, you can use the /e switch to test all DCs in your forest. (Obviously, in a large forest, you should wait to run the /e switch at an off-peak time.) The /dcpromo switch is a useful new option that tests a member server's configuration for readiness to become a DC. The /dcpromo switch is the only one that doesn't actually work on a DC.

DNSLint

The Support Tools utility DNSLint is a little-known tool that lets you diagnose common DNS problems related to incorrect delegation or incorrect or missing DNS records for a domain. If you choose, DNSLint can traverse the entire domain and all DNS servers within it to check for errors in the DNS structure. As with most of the utilities in this article, DNSLint offers unique options. In many situations in which you have a test (or otherwise internal) domain, you'll want to use the /s DNS server IP address option because it bypasses an Internet lookup of the domain. DNSLint creates an output HTML report called dnslint.htm. If you want text output instead of the default HTML format (perhaps because you want to use a script to process the output), you can specify the /t and /no_open options.

DNSLint reveals its true power, however, when you use the /ad option to run AD DNS tests. The /ad option runs a battery of AD-related queries about proper GUID registrations for the forest's DCs, Start of Authority (SOA) and Name Server (NS) records, and SRV record registration. With this option, you must specify the IP address of a DC that's authoritative for the root domain of the forest. You also

20 Windows 2003 Command-Line Weapons

Sean Deuby

(Reprinted from WindowsItPro Magazine)

have to use the /s option to bypass InterNIC lookup—usually, you'll use the same IP address of the server you're using for the /ad option, so the command will look like

```
dnslint /ad 192.168.1.51 /s 192.168.1.51
```

The option also checks for DNS glue records, which are A records in the root domain that locate the DNS servers that are authoritative for the child domains. If you want to customize DNSLint by specifying certain DNS servers and certain tests, you can use the /ql option. If you add autcreate after /ql, DNSLint will create a sample input file named in-dnslint.txt for you to build on.

Command Prompt Here

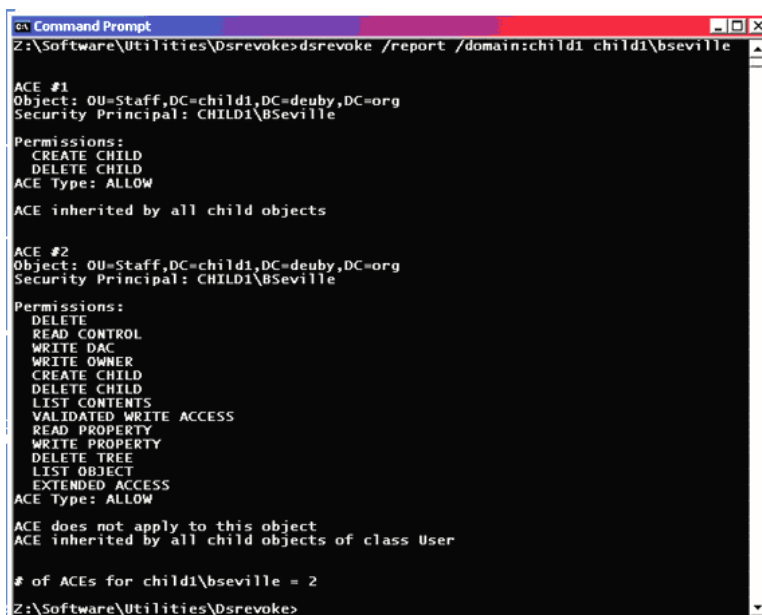
A utility I like to install on all my administrative consoles is Command Prompt Here, a simple tool that you can find among the Microsoft PowerToys for Windows XP. (See the sidebar "Get Your Command-Line Utilities Here!" for download information.) Command Prompt Here adds a context menu item in Windows Explorer that lets you launch a command prompt from whatever folder you've right-clicked on.

Dsrevoke

Have you ever granted permissions to a user or group (say, with the Active Directory Delegation of Control wizard) somewhere in a domain, but now you need to revoke those permissions? Searching through the domain and removing security principals can be tedious. Dsrevoke essentially undoes the actions of the Delegation of Control wizard or its equivalent. You can use

```
dsrevoke /report <security principal>
```

to generate a report of the access control entries (ACEs) that have been set on all domain and OU objects under the domain's root. Suppose the user Barbara Seville has been granted permissions to create, manage, and delete user accounts in the Staff OU. Figure 2 shows the results of Dsrevoke /report for Barbara. To remove her permissions, simply change the /report option to /remove. Dsrevoke will display her permissions, as with /report, then confirm the deletion. Enter Y for Yes to remove her ACEs.



```
Command Prompt
Z:\Software\Utilities\Dsrevoke>dsrevoke /report /domain:child1 child1\bseville

ACE #1
Object: OU=Staff,DC=child1,DC=deuby,DC=org
Security Principal: CHILD1\bseville
Permissions:
  CREATE CHILD
  DELETE CHILD
ACE Type: ALLOW
ACE inherited by all child objects

ACE #2
Object: OU=Staff,DC=child1,DC=deuby,DC=org
Security Principal: CHILD1\bseville
Permissions:
  DELETE
  READ CONTROL
  WRITE DAC
  WRITE OWNER
  CREATE CHILD
  DELETE CHILD
  LIST CONTENTS
  VALIDATED WRITE ACCESS
  READ PROPERTY
  WRITE PROPERTY
  DELETE TREE
  LIST OBJECT
  EXTENDED ACCESS
ACE Type: ALLOW
ACE does not apply to this object
ACE inherited by all child objects of class User

# of ACEs for child1\bseville = 2
Z:\Software\Utilities\Dsrevoke>
```

20 Windows 2003 Command-Line Weapons

Sean Deuby

(Reprinted from WindowsItPro Magazine)

Note that, like the Delegation of Control Wizard, this tool works only for permissions granted on the OU; if you granted permissions explicitly to objects or containers (such as Computers) instead of letting the OU's permissions inherit to the objects, you'll have to remove the permissions on your own. DCGPOFix and Recreatedefpol. Should you encounter severe problems with the default Group Policy Objects (GPOs) in your domain—the default domain policy and the default domain controllers policy—you can use Windows 2003's DCGPOFix or Win2K's Recreatedefpol to restore them to their default state. DCGPOFix can restore the default domain policy (/target:domain), the default domain controllers policy (/target:DC), or both (/target:both).

If you have to use the /target:both option, you'll probably need more than these tools to straighten things out. To prepare yourself for a rough situation in which you've lost one or more GPOs, take advantage of a fringe benefit of Microsoft's Group Policy Management Console (GPMC), which comes with a great set of command-line scripts and the ability to write more of your own. With no extra effort, you can back up and restore individual GPOs or all GPOs in the domain, copy individual GPOs, and generate reports on one GPO or all the GPOs in a domain in the GPMC's familiar settings format. You can even save the entire Group Policy environment—GPOs, settings, links, permissions—to an XML file with a sample script, and restore it with another script.

Readmin

A Microsoft Product Support Services (PSS) mainstay, Readmin is the kitchen sink of replication-troubleshooting tools. This tool has so many commands (59), options, and switches that it needs three levels of Help. The /oldhelp switch displays the original syntax and options, some of which have been replaced by newer commands described in /help. (The original ones still work.) If you don't dig into the syntax, you might find yourself running a less useful version and never know it. For example, every Readmin user seems to first learn about the /showreps switch. It's still there in Windows 2003, but a newer version—/showrepl—has a handy /erroronly option that prevents the necessity of wading through pages of connection-object information to find errors.

The /experthelp switch lets you access undocumented, advanced Readmin options that are dangerously powerful. In fact, the /experthelp switch itself is undocumented. The safeties are off now, so attempt these operations only in a test forest until you're familiar with them. (You get no confirmation dialog boxes that ask, "Do you really want to delete that naming context?")

One useful /experthelp command is /options. This command lets you create a Global Catalog (GC) server with the simple command

```
readmin /options <dcname> +is_gc
```

You can reverse the operation by changing the plus (+) to a minus (-). You can quickly disable replication to a DC with the command

```
readmin /options <dcname>  
+disable_inbound_replication
```

and from a DC with the command

```
readmin /options <dcname>  
+disable_outbound_replication
```

20 Windows 2003 Command-Line Weapons

Sean Deuby

(Reprinted from WindowsItPro Magazine)

Also, you can use the /options switch to check the status of any of these operations, as follows:

```
repadmin /options <dcname>
```

A great new Repadmin command for Windows 2003 is /replsummary. This command provides a quick summary of the replication health of all the DCs in your forest, in a table-like format. The tool runs quickly, even in large forests, and you can add the /erroronly option to limit the output to unhealthy DCs. The /bridgeheads option lists details about bridgehead servers. (With no options, the /replsummary command reports on all bridgeheads in the forest.) The /quersites option lets you determine the site link cost between two or more sites in the forest—helpful functionality for determining the least-cost route in a complicated site topology. Many more Repadmin commands await you, and time spent studying them can be rewarding.

Resource Kit

Unlike the Support Tools, the resource kit tools aren't on the installation media. Although they're slightly less crucial than the native OS utilities and Support Tools, many resource kit tools are so handy that I also recommend installing them on every server.

ADLB

The resource kit's Active Directory Load Balancing (ADLB) tool is new to Windows 2003 because it influences a new behavior in the OS. Win2K designates a single DC in each site as the bridgehead server, which handles the connection objects between its site and the sites that the Knowledge Consistency Checker (KCC) decides it should be connected to. If you have many sites, this situation can lead to a scalability problem: The overhead of being a bridgehead server to a lot of branch office sites can load down a DC. Windows 2003 resolves that problem by permitting all DCs in a site to be bridgehead servers for the directory partitions they host, so multiple DCs can handle the connection-object load. The OS initially makes random selections but unfortunately it never rebalances them.

Therefore, if the DC configuration in a site changes—for example, if you add a newer, more powerful DC—the distribution of intersite connection objects never changes. ADLB examines and rebalances the distribution of intersite connections between DCs in a site. Before you use ADLB, you need to complete your Windows 2003 DC upgrades so that it will operate evenly on all DCs. The tool won't load-balance Win2K DCs.

The simplest way to run ADLB is with the parameters /server:DcName /site:SiteName. The tool will then report on the connection objects for the target site and suggest changes. (The server you specify can be any DC that's a member of the forest.) Note that ADLB will make changes to the bridgehead configuration only when you add the /commit parameter. You can perform all ADLB operations (except /commit) without elevated rights, which makes your bridgehead-balancing investigations a little less cumbersome.

For more advanced fiddling, you can use the /stagger parameter so that ADLB takes control of the intersite replication schedule and staggers the replication interval between the connection objects that a bridgehead server owns. This functionality spreads out the impact of the replication operation on each connection object that would otherwise hit the server all at once. However, once you've used ADLB to take the replication schedule away from the KCC, you'll have to maintain it with ADLB.

ADLB needs a set of rules to work within, and you can modify just about all of them if you deem it necessary. The /maxbridge option specifies the maximum number of connection objects that AD will modify due to bridgehead load-balancing. The /maxperserver option specifies the maximum number

20 Windows 2003 Command-Line Weapons

Sean Deuby

(Reprinted from WindowsItPro Magazine)

of changes to be moved onto a DC at one time so that it won't be overloaded with a sudden increase in connection objects. You can create /preimbalance and /postimbalance reports (only in the newest version) to view inbound replication imbalances before and after balancing occurs. These reports are in comma separated value (CSV) format for easy importing into Microsoft Excel.

ADLB can be a powerful utility for your replication topology, but you need to perform a careful evaluation before you use it. My recommendation is to start by examining your largest sites (i.e., the ones with the largest number of DCs) because they're the most likely to have an imbalance. If you discover an imbalance in the connection-object distribution, don't just assume you need to fix it. Do a performance analysis on the bridgehead server that has the greatest number of connection objects. Is it actually suffering? If it's not, leave it (and the site) alone. Leave the schedule staggering alone unless you really have to modify it. Why make automated operations manual unless you have a good reason?

If you decide that you need to use ADLB to correct your connection-object distribution, run the tool on a schedule determined by your environment. If you're actively modifying your site configuration by deploying DCs, adding or changing site links, creating sites, and so on, consider running ADLB once a day. When you're done with your changes, stop using ADLB.

GPOTool

You probably associate only GUI utilities with Group Policy, but several command-line utilities are available. The resource kit's GPOTool utility checks the health of your GPOs. It reads mandatory and optional directory services properties (e.g., version, friendly name, extension globally unique identifiers GPOTool—GUIDs, and Sysvol data), compares directory services and Sysvol version numbers, and performs other consistency checks.

Third Party

Just because a tool doesn't come from Microsoft doesn't mean it can't help you. In fact, some of the most powerful Windows tools available come from third parties. Here are some must-haves.

AdFind and AdMod

AdFind and AdMod are two powerful, easy-to-use freeware utilities written by Joe Richards. AdFind is a Dsquery-like AD-query utility that offers a wide selection of options beyond those of Dsquery. Besides basic Lightweight Directory Access Protocol (LDAP) search options such as base DN, filter, and scope, the tool gives you every option you can imagine—34 of them!—with which to refine the query or otherwise make AdFind easier to use. Particularly useful is AdFind's ability to provide search statistics, with the use of its four /stats options. These options tell you how efficient your query is and what indexes (if any) it used—information that can teach you how to make better LDAP queries or at least avoid making bad ones.

AdMod is similar to Dsmmod, except it offers far broader powers. One of the nagging problems about Dsmmod is that it lets you modify some, but not all, AD objects. For example, you can't use Dsmmod to create sites, site links, or subnets. AdMod lets you modify anything in AD, and you can use it to make these modifications for large numbers of objects. However, AdMod's power also makes it very dangerous, if you aren't careful. Fortunately, the tool checks with you before it modifies more than x number of objects (10 is the default, but you can alter this number). If you need to modify large numbers of objects, you can use an -unsafe option that disables this notification. As with Dsquery and Dsmmod, you can pipe AdFind's output into AdMod so that the first utility searches for certain objects or attributes and the second makes the changes you desire. You can use this pairing as a powerful scripting tool.

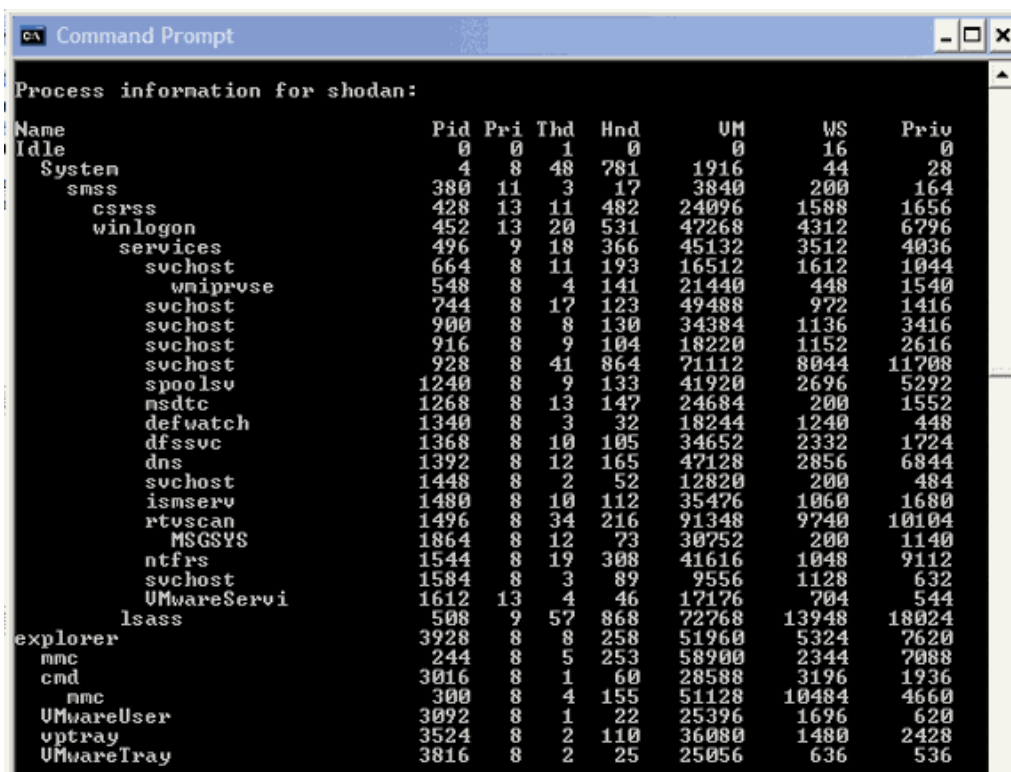
20 Windows 2003 Command-Line Weapons

Sean Deuby

(Reprinted from WindowsItPro Magazine)

PsTools

Sysinternals' PsTools toolset is a collection of command-line administration tools that are useful in many situations. I find PsList, a remote process and memory viewer, particularly handy. What sets it apart from other similar utilities is how deeply it lets you dig into process and memory internals. The tool's -m option shows memory details, the -d option shows thread details, and the -t option shows the process tree, as Figure 3 shows. The process tree is handy for determining what processes run under other processes (e.g., the services process). You can run it with an automatic refresh so that it functions like a remote task manager (by using the -s option), and you can focus on a process name or PID only. By combining these options, you can zoom in on a process that might be causing a memory leak and monitor its memory usage, or you can watch a remote process's user and kernel time to see whether it's executing or hung.



```
Process information for shodan:
```

Name	Pid	Pri	Thd	Hnd	UM	WS	Priv
Idle	0	0	1	0	0	16	0
System	4	8	48	781	1916	44	28
smss	380	11	3	17	3840	200	164
csrss	428	13	11	482	24096	1588	1656
winlogon	452	13	20	531	47268	4312	6796
services	496	9	18	366	45132	3512	4036
svchost	664	8	11	193	16512	1612	1044
wnipruse	548	8	4	141	21440	448	1540
svchost	744	8	17	123	49488	972	1416
svchost	900	8	8	130	34384	1136	3416
svchost	916	8	9	104	18220	1152	2616
svchost	928	8	41	864	71112	8044	11708
spoolsv	1240	8	9	133	41920	2696	5292
msdtc	1268	8	13	147	24684	200	1552
defwatch	1340	8	3	32	18244	1240	448
dfssvc	1368	8	10	105	34652	2332	1724
dns	1392	8	12	165	47128	2856	6844
svchost	1448	8	2	52	12820	200	484
ismserv	1480	8	10	112	35476	1060	1680
rtuscan	1496	8	34	216	91348	9740	10104
MSGSYS	1864	8	12	73	30752	200	1140
ntfrs	1544	8	19	308	41616	1048	9112
svchost	1584	8	3	89	9556	1128	632
UMwareServi	1612	13	4	46	17176	704	544
lsass	508	9	57	868	72768	13948	18024
explorer	3928	8	8	258	51960	5324	7620
nmc	244	8	5	253	58900	2344	7088
cmd	3016	8	1	60	28588	3196	1936
nmc	300	8	4	155	51128	10484	4660
UMwareUser	3092	8	1	22	25396	1696	620
optray	3524	8	2	110	36080	1480	2428
UMwareTray	3816	8	2	25	25056	636	536

Another handy tool in the PsTools toolset is PsExec, which lets you execute processes on a remote machine as if you're logged on to it. This functionality is quite useful for the many utilities that don't work remotely. For example, if you've ever needed to call a colleague at a distant location, but you weren't sure of the time at his or her office, you can query the time on a server in the user's time zone with the command

```
psexec \\<computer> net time
```

Figure 4 shows the command's results. If you aren't sure what command you need to use, or if you want to enter multiple commands, simply enter

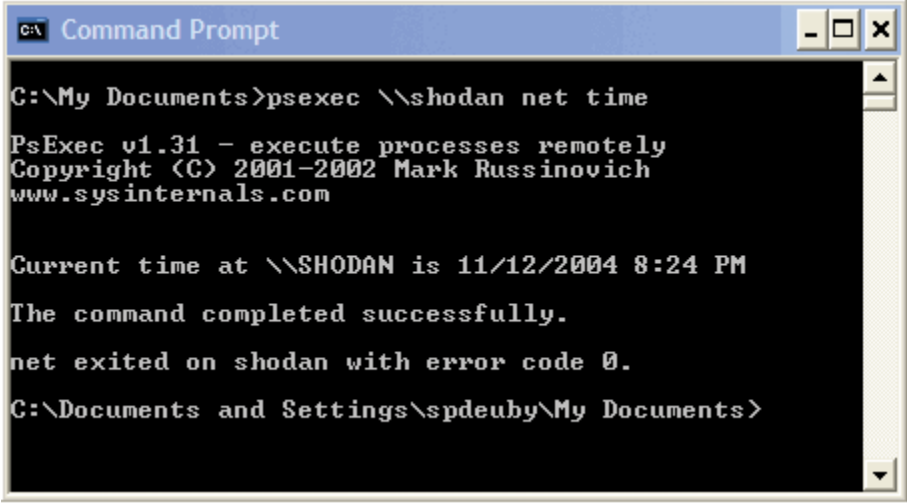
```
psexec \\<computer> cmd.exe
```

20 Windows 2003 Command-Line Weapons

Sean Deuby

(Reprinted from WindowsItPro Magazine)

to launch the command interpreter on the remote computer, and suddenly it appears as though you're in a command prompt at the console. Enter Exit to quit the remote session. For more information about PsTools, see "PsExec," July 2004, InstantDoc ID 42919.



```
c:\ Command Prompt

C:\My Documents>psexec \\shodan net time

PsExec v1.31 - execute processes remotely
Copyright (C) 2001-2002 Mark Russinovich
www.sysinternals.com

Current time at \\SHODAN is 11/12/2004 8:24 PM

The command completed successfully.

net exited on shodan with error code 0.

C:\Documents and Settings\spdeuby\My Documents>
```