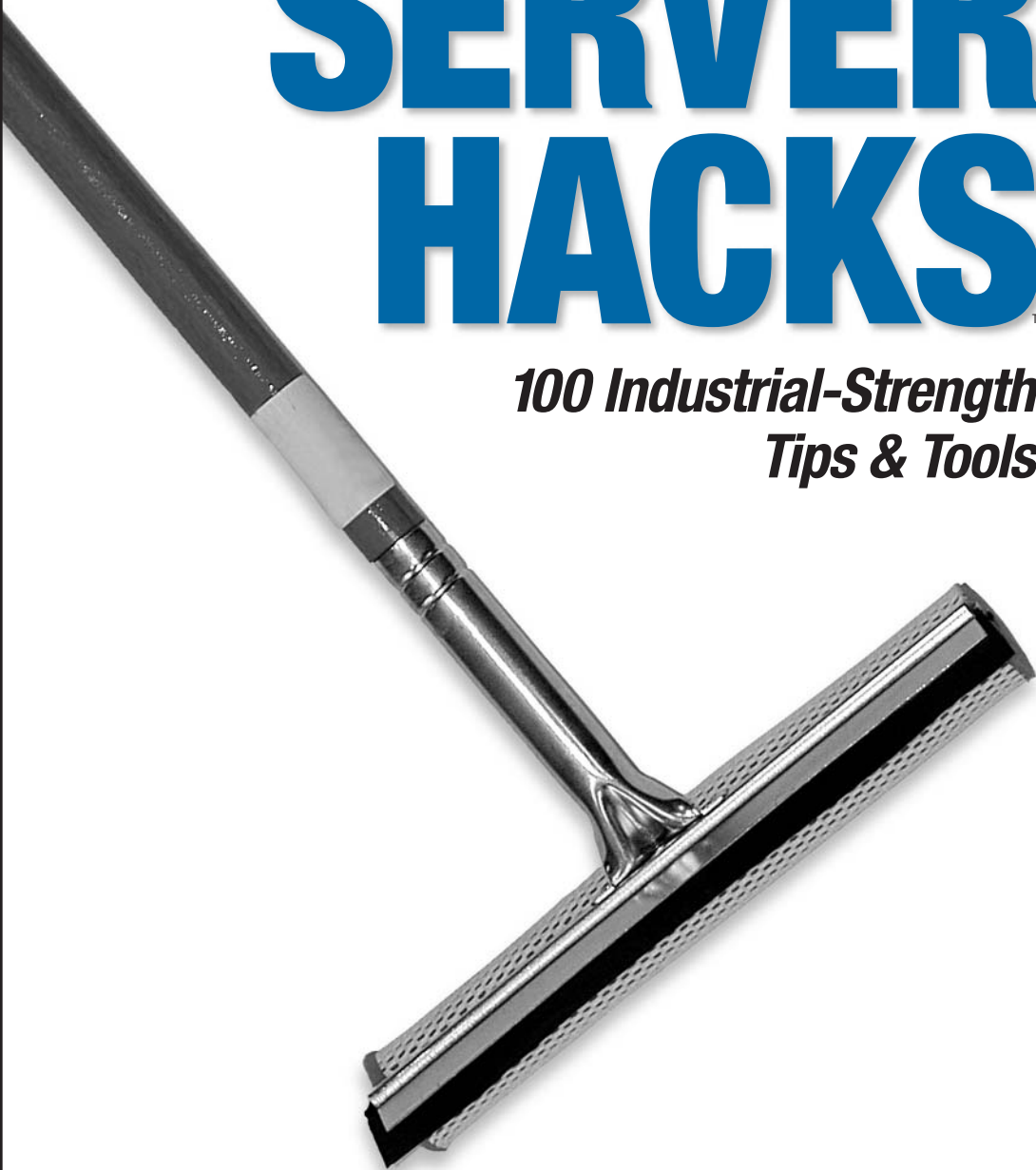


WINDOWS SERVER HACKS™

*100 Industrial-Strength
Tips & Tools*



O'REILLY®

Mitch Tulloch

HACK
#28

Get User Account Information

Need to find information about user accounts on a machine? Use this handy script to do it fast.

This script lets you quickly query a Windows 2000 (or later) machine to determine what user accounts are present, whether local accounts in the SAM database or domain accounts in Active Directory. It will output a list of accounts, giving the following information for each account:

- Username of user
- Full name of user
- Account lockout status
- Whether the user is allowed to change the password
- Whether the account is nonexpiring or not

The Code

To use the script, simply type it into Notepad (with Word Wrap turned off) and save it with a *.vbs* extension as *GetAccountInfo.vbs*:

```

ComputerName = localhost

winmgmt1 = "winmgmts:{impersonationLevel=impersonate}!//"& ComputerName & ""

Set UserSet = GetObject( winmgmt1 ).InstancesOf ("Win32_UserAccount")

for each User in UserSet
WScript.Echo "======"
WScript.Echo "Information for " & User.Name
WScript.Echo "The full username for the specified computer is: " & _
User.FullName
WScript.Echo "Account Locked? " & User.Lockout
WScript.Echo "Password can be changed?: " & User.PasswordChangeable
WScript.Echo "Password is expirable: " & User.PasswordExpires
WScript.Echo "======"
Next

```

Running the Hack

Here's some typical output when the script is run locally on a Windows 2000 domain controller. To avoid getting the series of dialog boxes that would appear if you ran the script using *Wscript.exe*, use *Cscript.exe* to run it from the command-line instead:

```

C:\>cscript.exe C:\MyScripts\GetAccountInfo.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

```

```
=====
Information for Administrator
The full username for the specified computer is:
Account Locked? False
Password can be changed?: True
Password is expirable: False
=====
=====
Information for Guest
The full username for the specified computer is:
Account Locked? False
Password can be changed?: False
Password is expirable: False
=====
=====
Information for jsmith
The full username for the specified computer is: Jane Smith
Account Locked? False
Password can be changed?: True
Password is expirable: False
=====
=====
Information for bsmith
The full username for the specified computer is: Bob Smith
Account Locked? False
Password can be changed?: True
Password is expirable: True
=====
```

The output continues for the remaining accounts on the system.

Hacking the Hack

You can easily modify the script to get user information from a remote computer instead of from the local computer on which the script is running. This is useful when you want to run the script from an administrator workstation instead of interactively on a domain controller.

Simply change this line:

```
ComputerName = localhost
```

to this:

```
ComputerName = InputBox("Enter the name of the computer you wish to query")
```

The script will prompt you with a dialog box (see Figure 3-3) for the name of the remote computer whose accounts you want to query. You can specify the NetBIOS name, DNS name, or IP address of the remote machine, as long as your currently logged-on account has administrative privileges on the remote machine.

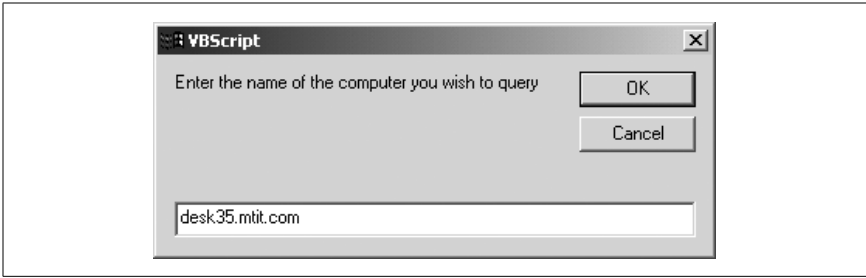


Figure 3-3. Querying user account information on a remote computer

—Rod Trent