

F1 Solutions November 2004



::REM

Hello All,

It's hard to believe the holidays are fast approaching. Unfortunately, that doesn't always mean a holiday from work. In fact for some readers, I know that the holidays can be the busiest time of the year for IT work.



This month we continue our mini-tutorial on netdom and explore how the tool can create trusts and verify secure channels. Netdom is such a critical and powerful tool that I'll be back next month to wrap up the discussion.

On the bookshelf this month is a new Exchange 2003 book. Personally, I don't think you can have enough high-quality reference books. Even though there will be some overlap, different authors bring different experiences and approaches to the subject and this month's title is no exception.

Finally, we wrap up as usual with a quick and dirty script to dump group membership. You can dump local or domain groups depending on the server you connect to. This is a must-have for any sort of network or security audit.

I hope you are finding these newsletters informative and worth your time. If so, I have another project in the works that I trust will interest you, especially if you finish each newsletter hungry for more. I hope to have some sort of announcement in the next newsletter and on the web site.

As always, I appreciate your continued support and welcome all comments, suggestions and feedback at jhicks@jdhitsolutions.com.

~Jeff

Security Watch

A Secure Wireless Network Is Possible

Wireless networks can be secure if you use the right technologies. To add a secure wireless network to an existing Windows network, all you need to do is install one or more 802.1x-compliant wireless Access Points (APs) and one computer running Windows Server 2003. [Read More.](#)



Testing and Reporting in 3 Key Areas Can Lead to Better Security

As I've expressed in previous articles I strongly believe that management can do a lot to reduce information security risks... [Read More](#)

Security News Briefs

Have you had enough phishing yet? The Anti-Phishing Working Group recently released a report that offers insight into phishing attacks and trends, and apparently the piranha are still swarming... [Read More](#)

Volume 1, Issue 9

November 2004

Special points of interest:

- Security Watch
- Learn Exchange 2003
- Netdom Part 2
- Dump Group Members

Inside this issue:

Web Crawling	2
IT Bookshelf	2
Tech Tutor	3
10 Minute Scripts	4

Security Watch - cont'd.

Improving Resiliency with Windows XP SP2

New features in Windows XP Service Pack 2 (SP2) help mitigate several security scenarios. [Read More](#)

Learn About Office 2003 Service Pack 1

Office 2003 Service Pack 1, which provides the latest updates to Microsoft Office 2003, contains significant security enhancements. [Read More](#)

Windows XP SP2 Requires MSBA Update

Users of Windows XP SP2 using the Microsoft Baseline

Security Analyzer will need an update. [Read More](#)

RECENT SECURITY ALERTS

AS OF September 17

- AOL (1)
- Microsoft (3)
- Oracle (2)
- Red Hat (27)
- Sun (11)
- SuSE (9)

[Read More](#)

This issue of *Security Watch* is being brought to you by JDH Information Technology Solutions

Each *Security Watch* eNewsletter is produced independently by the Windows IT Pro Custom Media Group and is distributed by various Microsoft security partners. Each eNewsletter contains up-to-date information about security strategies, technologies, and alerts.

Malware Threat Watch

Normal Elevated High Critical

Remember, if you can see the Internet, the Internet can see you!

“Here’s a bit of advice for those of you planning IT budgets. For the next five to 10 years, set aside 10 percent to comply with new government regulations, both from the United States and from other governments in your major markets. .”

—[InfoWorld](#)

Web Crawling - GPAnswers.com

Jeremy Moskowitz is one of the industry’s best known experts on Group Policy. So it should come as no surprise that he has a web site devoted to all things Group Policy. In addition to a full discussion forum there are template and script downloads, webinars, book samples and a free newsletter. If you have any of his recent Group Policy books on your shelf you will find errata and updates in the community Room. Finally, you can also arrange specialized, instructor-led training on Group Policy with Jeremy personally.

The site has only been around for a year and appears to be slowly growing. For example, the FAQ section is short and others completely under development. Yet I expect this to remain a consistently high source of information on Group Policy.

GPAnswers is a service of Moskowitz, Inc. Visit the site at <http://www.gpanswers.com> to learn more.

(if you have a site recommendation , let me know! I’m always interested in high-value sites that may be off the beaten path)

Learning Exchange 2003

This month’s title is the latest offering from Windows expert Bill Boswell. [Learning Exchange 2003](#) is unlike other technical titles. It is not a recitation of menu choices and features, but rather a concise primer on how to **use** Exchange 2003. Even though the book is written assuming no previous Exchange experience, even seasons Exchange administrators will learn at least one new thing about how Exchange really works.

I was fortunate enough to review this book while still in manuscript form and am very excited by the finished product. Excellent illustrations and a warm style that make what could be dry technical content, interesting and fun. The book can be read from start to finish for a great story, or jump from chapter to chapter to bone up on the latest features of Exchange 2003.

I urge you to take a look at this title at your favorite bookseller or online at <http://www.awprofessional.com/title/032122874X>



Tech Tutor – NetDom Part 2

This month we'll continue our exploration of netdom. I previously said you needed to install it, and that is probably not true. Netdom is now a part of Windows 2000 and 2003. You might only need to get a copy if you are running Windows NT or XP. There are different versions depending on your OS. What's nice about netdom is that you can execute commands from your workstation, specifying administrative credentials as needed. Last month we saw how to use netdom to join a computer to a domain. Next we'll see how to use netdom to work with trusts and secure channels.

Let's first start by using netdom to verify a secure channel already exists between a member computer and a domain. I ran the following command from the domain controller to check the connection to an XP workstation.

```
C:\>netdom verify godot /domain:matrix.local
The secure channel from GODOT to the domain MATRIX.LOCAL has been
verified. The connection is with the machine
\\TRINITY.MATRIX.LOCAL.
The command completed successfully.
```

If run the command but aren't logged in with administrative credentials on the target computer, in this case Godot, you can specify them. If I wanted to run the same command from a 3rd workstation logged in with regular user credentials, I would type the command:

```
netdom verify godot /domain:matrix.local /
UserO:matrix\administrator /PasswordO:P@ssw0rd
```

If the channel was not verified, I could have tried resetting it with netdom like this:

```
Netdom reset godot /domain:matrix.local
```

Again, I could use UserO and PasswordO parameters to specify administrative credentials. If you prefer not displaying an administrative password clear text, you can substitute an asterisk (*) in which case you will be prompted for the password and nothing will be displayed on the screen.

Even though Active Directory Domains and Trusts makes it very easy to establish two way trusts, there are times when a command line approach is easier. Using a command line can also sometimes give you more information if things aren't working as expected. Assuming you have name resolution handled between the two domains, you can easily and quickly create a two way trust like this:

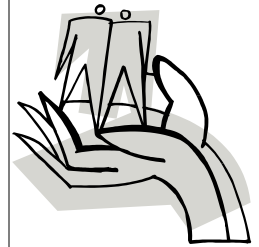
```
Netdom trust matrix /domain:Win2kDom /
UserD:\win2kdom\administrator /PasswordD:P@$2kdom
/UserO:matrix\administrator /PasswordO:P@ssw0rd /PasswordT:Trust-
Password /Add /TwoWay
```

If you would like to verify the trust you would then type:

```
Netdom trust matrix /domain:Win2kDom /UserD:\win2kdom\administrator
/PasswordD:P@$2kdom /UserO:matrix\administrator /
PasswordO:P@ssw0rd /Verify
```

Finally, if you wanted to get rid of the trust, you can use the /Remove switch in place of /Verify.

I hope you'll warm up your test network and try some netdom commands out for yourself. Next month we'll wrap up our mini-series on netdom and learn how to use it to tell us what is happening on our network.



“Like dreams,
statistics are a
form of wish
fulfillment.”

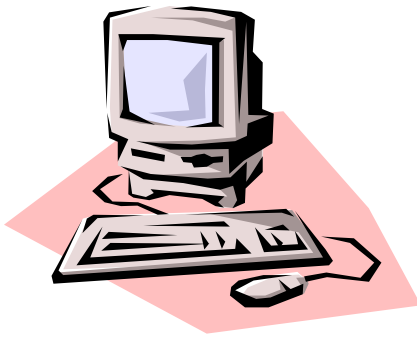
- Jean
Baudrillard

JDH Information Technology Solutions

4233 Lafayette Road
Jamesville, NY 13078

Phone: (315) 256-7023
Fax: (315) 295-2534
E-mail: jhicks@jdhitsolutions.com

WE'RE ON THE WEB AT
HTTP://
WWW.JDHITSOLUTIONS.COM



If you wish to no longer receive this newsletter, please send an email to:

newsletters@jdhitsolutions.com

Use a subject line of Unsubscribe.

This newsletter was created with
Microsoft Publisher 2003

Copyright 2004 All Rights Reserved
JDH Information Technology Solutions, Inc.

All trademark names are property of their
respective owners

Disclaimer:

All code and script samples are provided
'as is' with no warranty, either expressed
or implied.

Use at your own risk and test thoroughly in
a non-production environment.

Mission Statement

Our mission is to provide outstanding information technology consulting services and solutions to our clients utilizing a value-oriented approach. We recognize that most information technology projects are goal not hour driven. Our aim is to leverage technology to solve our clients' business challenges in the most cost-effective manner possible. We succeed when they succeed.

10 Minute Scripts

Part of any network audit should include group membership review at both the domain level and locally on mission-critical servers. This month's quick script dumps group members and their class to the screen. The script uses ADSI to make a connection to the group then enumerates all members and class (i.e. user or computer). The WinNT provider works on NT, Windows 2000, Windows XP and Windows 2003 so you can audit local or domain-based groups. This script will query the user's domain for the specified group. As written you should use Cscript as each group member is echoed to the screen.

You might want to enhance the script to allow passing the group name as a parameter, read from a text list of groups, loop through and process nested groups, and/or write results to a text file or web page.

```
'DumpGroup.vbs
On Error Resume Next
Dim oGrp, oArgs, WshNetwork, wshell
Set wshell=CreateObject("wscript.shell")
set WshNetwork=CreateObject("WScript.Network")

strGrpName=InputBox("Enter the name of the group to dump. You
quotes around names with spaces.", "Group Info", CHR(34) &
"Domain Admins" & Chr(34))

Set oGrp = GetObject("WinNT://" & WshNetwork.UserDomain & "/" &
strGrpName & ",group")

icount=0

set memberlist=oGrp.Members
for each member in memberlist
'display member name and class, such as user or computer
wscript.echo member.Name & "," & member.Class
icount=icount+1

Next

strMsg="Counted " & icount & " members of " & WshNet-
work.UserDomain & "\" & strGrpName

wshell.Popup strMsg,10,"Group Info",0+64

wscript.quit

'EOF
```