

Re: UDP Ports, closing Win2K Server (No IIS)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-08/0810.html>

From: Karl Levinson [x y] mvp (levinson_k_at_despammed.com)

Date: 08/21/03

Date: Thu, 21 Aug 2003 07:12:47 -0400

What's listening on UDP 995? Could be you've been hacked. There's a widespread worm going around called Sobig.F that listens on UDP 99x [995 through 999]. The worm spreads via email but some antivirus vendors report it may also spread silently across Windows network shares too. Update your antivirus?

<http://www.sarc.com/avcenter/venc/data/w32.sobig.f@mm.html>

<http://securityadmin.info/faq.htm#hacked>

Closing ports is a two step process: shut down the listening processes and also use a firewall. Both are highly recommended. I would really advise against using IPSec as a firewall, and blocking just one or two ports here or there really doesn't improve your security very much, you want to block all by default except for those needed. Also, learning how to do port filtering on a live web server is a good way to get hacked. If you do get hacked and you have no firewall and just IPSec, you've got no logs to show where the attack came from, because IPSec has no logging. Big drawback. There are a number of free firewalls out there:

<http://securityadmin.info/faq.htm#closeport>

<http://securityadmin.info/faq.htm#firewall>

<http://securityadmin.info/faq.htm#harden>

"Craig Gillette" <craig@accessorystore.com> wrote in message news:059301c36789\$545cbc50\$a601280a@phx.gbl...

- > *I am managing a Win2K Server, no IIS. I want to start*
- > *closing ports to help prevent worm attacks.*
- > *How do I do this? Do I need IIS?*
- > *I was thinking of using IPSec? Is this correct?*
- > *I wanted to block inbound traffic on port 995, for*
- > *example, and I was going to use this syntax:*
- >
- > *ipsecpol -w REG -p "Block UDP 995 Filter" -r "Block*
- > *Inbound UDP 995 Rule" -f *=0:995:UDP -n BLOCK -x*
- >
- > *Does this look correct? Is there another or a better way?*
- >

microsoft.public.inetserver.iis.security: Re: UDP Ports, closing Win2K Server (No IIS)

>