

microsoft.public.win2000.security: Re: Hacker "scanned" my webserver

Re: Hacker "scanned" my webserver

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-05/0607.html>

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

Date: 05/11/04

Date: Tue, 11 May 2004 06:32:08 -0400

That's not exactly a scan, that's a compromise.

<http://securityadmin.info/faq.asp#ftpfolders>

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

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

I suspect the folders were made undeletable using the Posix subsystem, which you can remove. Sounds like you're not running URLScan and IIS Lockdown, free from www.microsoft.com/technet/security. That plus the URLs above would probably have prevented this. And are you installing all the latest patches for Windows, IIS, etc. from <http://windowsupdate.microsoft.com> or from www.microsoft.com/technet/security/current.aspx shortly after new ones are released?

What we still don't know is which vulnerability was used to hack your system. Do you have FTP server services enabled, and if you did, did you change the permissions so that the anonymous user [e.g. IUSR] does not have both read and write permissions to any folder? Can you disable FTP services and/or change the permissions?

If this was an IIS web server vulnerability, check the web server logs, although some attacks like buffer overflows or non-web vulnerabilities won't show up there:

<http://securityadmin.info/faq.asp#iislogs2>

<http://securityadmin.info/faq.asp#iislogs>

"Dr. Bob" <anonymous@discussions.microsoft.com> wrote in message news:26D4BAB4-96C2-43F4-AC40-0485BC860BD1@microsoft.com...

> *I have a Win2K webserver running IIS that was "scanned" by a hacker. I now have files/folders with non-printing characters in their names. When I try to delete them, I get "file not found" or "cannot read from source file or disk" errors. Any way to fix this problem? Also, what can I do to keep this from happening again? Thanks for your help.*

> *Bob*

Re: Hacker "scanned" my webserver