

## Re: Security Scan on IIS shows files and folders

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-08/2916.html>

---

**From:** karl [x y] ([jamescagney90210@excite.com](mailto:jamescagney90210@excite.com))

**Date:** 08/15/02

From: "karl [x y]" <[jamescagney90210@excite.com](mailto:jamescagney90210@excite.com)>

Date: Wed, 14 Aug 2002 21:51:02 -0400

"Don Wood" <[don@iemployee.com](mailto:don@iemployee.com)> wrote in message  
news:d0fbf0ed.0208141300.74752155@posting.google.com...

> *HELP!*

>

> *Recently our comapny had a Professional Security Scan done one of our  
> production web sites. We are running Windows 2000 SP2 (with all  
> up-to-date patches), IIS 5.*

>

> *When they conducted the security scan, they told us we had many files  
> with ".old or.bak" extensions. They also viewed the contents of a  
> folder called "\_test" on the site (off the wwwroot).*

>

> *My question, since they will not tell us, is; How are they viewing  
> these files????*

>

> *How can they see folders "\_xxxx" and files with "old" extensions on  
> the Hard Drive.*

I guess it's too late for this now, but if you paid for this security scan, I would recommend confirming beforehand that the scan includes recommendations as to how to fix the problems they found. I can't imagine how a scan like this would be useful without receiving recommendations following the scan.

I recommend checking your IIS web logs. Everything they did is probably in those logs, including the URLs they used. From this you can guess about what exploit they used, or whether they used an automated script to guess hundreds of file and folder names through brute force.

If you don't have NTFS permissions blocking access to those files, anyone who can guess the name of the files and folders can view them. It could be that they just guessed about the name of the files and pulled them up. For example, if your web site has a page called default.asp or index.htm, then perhaps they tried to access default.old or index.bak Renaming .ASP files to .Old or .Bak is a serious problem as the attacker gets to see your .ASP code, the code in the file is displayed as plain text instead of being

microsoft.public.inetserver.iis.security: Re: Security Scan on IIS shows files and folders

processed server-side. Once they see the code in your .ASP file, they may have seen any links, includes or other pointers to other files and folders that are in your code, so that they can then bring those folders up. It's a good idea to name other code-containing files such as your include files to be named .ASP as well, for the same reason. It's probably also a good idea to remove any files, folder and code that is considered test or backup and not production from the production server.

Without additional information, it's not necessarily true that these people have been able to penetrate your server; they've only shown that they've been able to do some initial information gathering. Re-evaluating NTFS file permissions, removing old or test code and renaming files to .ASP is a start.

I guess you know that installing all the patches is only part of what you need to do; if you haven't already, you also need to configure IIS and Windows correctly, using IISlockdown with URLscan and/or the checklists for securing IIS and windows at [www.microsoft.com/security](http://www.microsoft.com/security). It's also a good idea to search google for such checklists from other non-microsoft sources, such as the NSA guides linked at [www.cisecurity.org](http://www.cisecurity.org)

I might recommend reading Hacking Exposed 3rd edition and/or Incident Response. Whatever method they used or whatever exploits you haven't yet closed may well be described in there.