

[Full-Disclosure] w32.frethem.k@mm and good reading

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2002-07/0500.html>

From: Nathan Fain (full-disclosure@lists.netsys.com)

Date: 07/16/02

From: full-disclosure@lists.netsys.com (Nathan Fain)

Date: Tue, 16 Jul 2002 13:28:05 +0300

This method of obfuscation applies If you are only protecting a static website that doesnt deal with any security critical data (credit info, shopping, etc.) and defacement of your site is a primary concern. Script kiddies deface websites (with few exceptions). Script kiddies run OS fingerprint scan's or other scans to find their target. Yes, script kiddies will be quite fooled by this method. Otherwise you are only obfuscating your own perception of security. IP stacks are secure in their own right (i haven't heard of anyone gaining remote access by exploiting the IP stack). And this is about all you change keeping with an older OS itself.

The idea of keeping older versions of services you required (ie Apache) has little application as well. It applies to the concern of stability.

Once **proven** stable (left to your own interpretation) one should switch to the later version. Reason being that at some point the developers will stop looking at code in older version all together. So even if you have the oldest version of apache with the latest patches available for it, you will likely have wide vulnerabilities in functions that are used in the code or underling libraries. And in such a scenario, while you might have stopped script kiddies, you have left the door wide open for anyone determined to get in your system.

The article applies to those whose primary concern is perhaps defacement alone

> *By Robin Miller, NewsForge.com*

>

>> *Posted: 06/06/2002 at 12:10 GMT*

>> *[724.gif] Here's an interesting way to secure an Internet-connected computer against intruders: Make sure the operating system and software it runs are so old that current hacking tools won't work on it. This was suggested by Brian Aker, one of the programmers who works on Linux.com, NewsForge, Slashdot, and other OSDN sites; he runs several servers of his own that host a number of small non-profit sites in the Seattle area. "I have one box still*