

## Re: Unix vs. Windows Security

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-02/0321.html>

---

**From:** Gideon Lenkey ([glenkey@spam\\_this.org](mailto:glenkey@spam_this.org))

**Date:** 02/12/02

From: Gideon Lenkey <[glenkey@spam\\_this.org](mailto:glenkey@spam_this.org)>

Date: Tue, 12 Feb 2002 12:56:49 GMT

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

I wasn't going to touch this one with a ten foot pole, however, some good points have been made as well as some bad ones, so I'll add my two cents in.

First of all the question is really vague. What are you trying to secure? Better overall for what purpose? I'll answer the question on the following assumptions. a) No real distinction between server and desktop, and b) security will mean Internet security.

There are some core issues at the heart of the UNIX vs. Windows security debate. UNIX is an older more mature operating system that was designed with networking 'built in'. It was designed for easy collaboration between users. Windows evolved from a code base that never even dreamed of having more than one user or network connectivity beyond a small lan. Neither were ever designed to be secure. Security came later for both of them and both can be made relatively secure.

In my opinion, the problem is that when you take an OS product out of the box and use it as advertised on the Internet, you'll probably get hacked and quickly. You don't have to be a 'clueless admin'. My mom shouldn't have to be an 'admin' to buy a commercial computer and hook it up to a phone line to use the Internet. Windows come from the vendor completely bent over, as in dropped the soap in the shower, greased up ready for action. UNIX does too. The same thing will happen to you if you install Solaris (7) or Red Hat 6.x default (as most home users do). I know Red Hat 7.x has fixed this problem, I don't know about Solaris 8. The point is, vendors turn on every bell and whistle by default to make it easy for the end user. Easy is the opposite of secure in my book.

Another contributing factor is Microsoft's attempt to push into the server market. From their point of view what a NOC really needs is more mice and an talking animated paper clip. They realized that their marketing efforts would out-pace their training and education programs so

they 'dumbed' the product down so that, according to them, anyone could administer it. Remember 'zero' admin? That didn't work so well, and resulted in record numbers of mis-configured machines. Machines that got hacked AND THE OWNERS WERE THE LAST TO NOTICE!

UNIX, on the other hand, is more difficult to manage and generally intimidating to the inexperienced. Which is not a bad thing. UNIX, in general, is more professionally managed. At least in a commercial environment. Even professionals get lazy though and a small slip-up in the UNIX environment can leave you wide open to attack.

To sum it up, both of the OS's you've asked about can be made 'secure' enough for use on the Internet. Both will experience vulnerabilities that require vendor patches. For 'better overall' from a security standpoint, my pick is UNIX (openBSD for servers, Red Hat Linux or Solaris for desktop). I like the flexibility it offers. Enough flexibility to overcome it's shortcomings. With Windows, you have to wait for either Microsoft or a vendor to solve your problems for you or take up one of those damned pointy clicky programming environments and that just takes all the fun out of it!

Anyway, I hope this helps.

--Gideon

| InfoTech Associates, Inc. | glenkey(@)infotech-nj(\*)com |

On 9 Feb 2002, Colin wrote:

> *I would like your opinion on the merits/faults of Unix compared to  
> Windows in respect to security. What are the specific issues that  
> differentiate them? Which is the better overall?*

>

> *Thanks.*

> *Colin*

>

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.6 (SunOS)

Comment: For info see <http://www.gnupg.org>

iD8DBQE8aRLJH1ef35JVa+wRAs3/AJ9QMKEkaqTCN+FIDAUwe7UTBOvjZACfSWQP

lm0ONFiVzNL33XJ28aI6KDI=

=YsLE

-----END PGP SIGNATURE-----

- 
- **Next message:** [Valdis Kletnieks: "Re: checking for all known viruses vs. fixing the system"](#)
  - **Previous message:** [Philip J. Koenig: "Re: Microsoft finally acknowledges the security drumbeats"](#)
  - **In reply to:** [Colin: "Unix vs. Windows Security"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)