

## RE: [Full-Disclosure] RE: Linux (in)security

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-10/1385.html>

---

*From:* Arcturus (*arcturus\_at\_secrev.net*)

*Date:* 10/22/03

To: <support@mmicman.com>, "Thomas Binder" <full-disclosure@arago.de>, <full-disclosure@lists.n  
Date: Wed, 22 Oct 2003 16:10:53 -0400

Ahh,

True, true, but:

For those of us who secure Microsoft Systems and Networks for fun and profit, we understand the vulnerabilities just as you do for your linux/unix systems. We simply use alternate approaches to security.

In lieu of securing the actual box, we put a firewall (running linux/unix) in front of it. Then, we use a simple approach of "that which is not expressly allowed, is expressly denied" in our policies, and voila. Secured.

Now OF COURSE, I am over simplifying, it wouldn't matter what type of system was behind the firewall if the rules were not tight enough, but, the simple fact still remains: The majority of the world's corporations are using Microsoft for their platform of choice, so, we are simply changing with the times...

Just for the record, this was written in Outlook, and sent out via a secured system, that happens to run a Microsoft OS.

I would completely agree with Edward, "It's not the OS, it's the operator"

Just my 2¢, YMMV.

Arcturus.

-----Original Message-----

From: full-disclosure-admin@lists.netsys.com

[mailto:full-disclosure-admin@lists.netsys.com] On Behalf Of Edward W. Ray

Sent: Wednesday, October 22, 2003 1:16 PM

To: 'Thomas Binder'; full-disclosure@lists.netsys.com

Subject: RE: [Full-Disclosure] RE: Linux (in)security

There seems to be this tendency in every market the have the product with the most widgets at the least cost. Security vendors are out there selling

Full-Disclosure: RE: [Full-Disclosure] RE: Linux (in)security

a "one size fits all" solution to all of your security problems these days.

I have never heard of a Linux vendor saying that Linux is "secure out of the box." Maybe Openwall or Engarde Linux, but most distos need to be made secure by the user.

Linux is the hands of someone with no interest or regard for security is the same as Windows or any other OS in the hands of the same clueless individual. The main difference between the Linux and Unix variants (i.e. BSD, Solaris, HP-UX) is that they have already learned their lesson regarding buffer overflows and kernel hardening and allowed the user more control in securing their systems. M\$ has not, and that is unfortunate.

Edward W. Ray

-----Original Message-----

From: full-disclosure-admin@lists.netsys.com

[mailto:full-disclosure-admin@lists.netsys.com] On Behalf Of Thomas Binder

Sent: Wednesday, October 22, 2003 8:39 AM

To: full-disclosure@lists.netsys.com

Subject: Re: [Full-Disclosure] RE: Linux (in)security

Hi!

On Wed, Oct 22, 2003 at 09:12:12AM -0500, Schmehl, Paul L wrote:

> *Now, lest you get your hopes up and think it's possible to change the*

> *world, read this:*

>

> <http://www.ukauthority.com/articles/story898.asp>

>

> *After reading this, I had a good cry and then took some aspirin.*

> :-(

Of course, what they do not (and most likely cannot) mention is how many of the passwords entered were just random keystrokes instead of a real world password.

In fact, I tend to advise people not to completely refuse giving their password / PIN / etc. when asked for by someone, but to reluctantly "disclose" something completely wrong. This way, the attacker might think he's won and – depending on the attacked system – effectively locks the account he wants to break into.

Ciao

Thomas

--

It is better to never have tried anything than to have tried something and failed.

- motto of jerks, weenies and losers everywhere

---

RE: [Full-Disclosure] RE: Linux (in)security

Full-Disclosure: RE: [Full-Disclosure] RE: Linux (in)security

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

---

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

---

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>