

Re: firewall securing outgoing traffic?

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-02/0186.html>

From: Alexander (aldem-news@news.aldem.net)

Date: 02/05/02

From: "Alexander" <aldem-news@news.aldem.net>

Date: Tue, 5 Feb 2002 08:28:37 +0100

"Dimitri Maziuk" <dima@127.0.0.1> wrote:

- > *Keep in mind that there aren't any trojan programs for Linux*
- > *to speak of: 1) OS security makes it hard for them to do*
- > *real damage (you must run the trojan as root, otherwise it*
- > *won't be able to access the important stuff),*

Hmm... "OS security"? Which one? :) Novice users, and most home users run their system as root anyway, so... Or how can you explain thousand of owned/hacked Linux systems around the world?

- > *chances of success are higher. This is oversimplifying quite a*
- > *bit, but the point is, trojans and viruses are not a very big*
- > *problem on Linux ATM.*

Really? See note above. A lot of hacked Linux boxes.

- > *Secondly, a program can e.g. lie to ZA about its name. So*
- > *setting up firewall rules on per-program basis is not all*
- > *that foolproof, either.*

Aha... Lie... Embed into kernel, modify it, etc... Trojan OS, eh? :)
Well. It can be done on misconfigure (or not configured) system, but if you know what to do, on WinNT/2K/XP it just cannot happen (forget about W95/98/ME – this is DOS with GUI).

- > *Sorry, Unix/Linux philosophy is that your brain works much better*
- > *than any code, so you're supposed to use it.*

That's common sense, and (IMHO) has nothing to do with Linux/UNIX :)
If you can use your brain – it will work everywhere, isn't?

OTOH, clerks and pizza-boys (who do work with computers) are not supposed to go so far – to understand how computers work and why. They just use it.
You don't need to know what is inside if you can use it (cars, for instance).

comp.os.linux.security: Re: firewall securing outgoing traffic?

> *The downside is that there's a steep learning curve, esp. in the beginning.*
OTGH, it
> *really *does* work better than a computer program.*

But slower as well. You can't know everything – so it won't work better for everyone. That's why we have doctors, for instance – because not everyone can help himself :)

/AI

- ***Next message:*** Alexander: "Re: crypted file system 2.4 ?"
- ***Previous message:*** Cedric Blancher: "Re: --state ESTABLISHED.RELATED (was: Re: POP-before-SMTP/log2db/RH 6.2/Sendmail 8.11/Cyrus-SASL)"
- ***Maybe in reply to:*** Zaphod Beeblebrox: "Re: firewall securing outgoing traffic?"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]