

Re: [fw-wiz] Securing a Linux Firewall

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2002-07/0281.html>

From: Stephen P. Berry (spb@meshuggeneh.net)

Date: 07/30/02

To: "R. DuFresne" <dufresne@sysinfo.com>
From: "Stephen P. Berry" <spb@meshuggeneh.net>
Date: Tue Jul 30 19:58:01 2002

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

Hash: SHA1

R. DuFresne writes:

>> *-It ain't really what you want to do. Nobody really wants to allow
>> just any damn thing to happen on their networks.*

>*This is very dependent and in many cases untrue. Too often the business
>model is to allow far too much; the CEO wants to read e-mail off another
>site, management wants to use IM/ICQ/etc, different business groups want
>to play with whiteboarding in netmeeting, the list goes on...*

This is true, but it also does not contradict the point I was making.
A default deny plus a whole bunch of silly explicit allows is still (in
almost all cases) better than a default allow plus a couple explicit
denies. If nothing else, crafting the individual `allow' rules forces
the administrator to have at least a rudimentary understanding of what's
going on---a mildly concussed tarsier can set up the default allow[0].

Of course, I would also add that handling CEO requests---in ways other
than blindly obeying them---is part of how a security administrator earns
their pay, but that's another argument[1].

>*Far too many organizations do not have a properly defined, if they have at
>all "acceptable use policy", concerns relating to such are common
>questions to this and the firewall list. Few organizations that try to
>impliment an "acceptable use policy" have the balls to enforce it.*

[deletia]

>*We're still in perimeter mode, individual host security, on the inside and
>often on the DMZ's is lacking, and often just totally non-existent.*

I'm not sure what you're trying to get at here. Yes, lots of networks,
organisations, and administrators are broken/stupid/mismanaged/whatever.

Firewall-Wizards: Re: [fw-wiz] Securing a Linux Firewall

I'm talking about best practise. The fact that a lot of people Get It Wrong isn't an argument against using minimal OS installs as best practise.

If you're making some other point that I'm just being too obtuse to catch, let me know[2].

*>What Gaspar and others are trying to convey, this works well with single
>boxen nad or minimal setups, but scales poorly when dealing withmass
>pushouts of various differening OS builds on a larger perspective.*

[deletia]

*>And yet maintaining that level of known good bare minimum over upgrades
>and version releases, let alone patch fixes and such can be a tasking
>issue. On a small scale, for single systems it's a no-brainer, but,
>getting this to scale is another matter altogether.*

I couldn't disagree more.

No matter what your HR department tells you, your lusers are not all unique and beautiful like snowflakes. And there's no reason their machines should be, either. If they –are– (the machines, that is), I'd like to hear what your disaster recovery scheme looks like. Let's say a meteor flattens your datacenter and you've got to restore everything from backup. If your machines were all (or mostly) standard builds plus data, the recovery process will be a pain, but it's all meat 'n taters system administration. If each of your machines is unique, then the recovery process (if successful) will be an event of theological significance.

As for upgrades and patches...well, you are upgrading and patching your systems anyway, right? To my mind, having your machines installed from a `known' distribution source makes this sort of maintenance easier. Keeping track of a dozen or so standard installs is easier than keeping track of 5000 unique hand-rolled installs. I'd even go so far as to suggest that if you're not already doing some sort of version control on this sort of thing you're committing a GCE, but that's another separate argument.

For that matter, if the patches and updates are reasonably evenly distributed among all the available packages, then having fewer packages installed implies that you'll have to do fewer updates and patches.

I really think y'all are making too much of the presumed difficulty of maintaining minimal installs. There's an initial investment in setting everything up that is perhaps greater (in terms of skullsweat if not in keystrokes), but from there on it's always been a Big Win in my experience—in terms of security, but also in terms of maintainability. When you have to cope with upgrades, version migrations, patches and that sort of thing, keep in mind that you don't have to redo everything from scratch—you're just dealing with the deltas, and then only if

Firewall-Wizards: Re: [fw-wiz] Securing a Linux Firewall

they apply to the widgets that are a part of your minimal install. This sort of thing is always a pain –regardless– of what your typical machine looks like, and I just don't see how having a bare bones system makes it more painful. It certainly hasn't been in my experience.

I'm assuming that we all started out installing more or less default OS installs when we were wee sysadminlings. From there, some of us seem to have migrated to advocating pared-down, bare bones installs. Anyone gone that way, preferably in a large environment, then decide to go back to their original methods?

--spb

- 0 The implicit assumption here is that given a choice between having your perimeter security handled by administrators with at least a rudimentary understanding of what's going on and having it handled by mildly concussed tariers, you'll take opposable thumbs and large forebrains every time...this being firewall-wizards rather than firewall-tarsiidae. Your Mileage, of course, May Vary.
- 1 And I don't mean just saying `no'. Educating lusers (and in particular The Mgmt.), offering alternatives, and providing a meaningful analysis of risks is part of what security administrators get paid for. If your network is doing something that you think it shouldn't be doing, blaming the CEO is just a lame excuse.
- 2 I'm frequently obtuse, only occasionally acute, and sometimes right.

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

Version: GnuPG v1.0.7 (OpenBSD)

iD8DBQE9RyQNG3kIaxeRZl8RAhS5AJ0Snk13lna683C9OBGOy4j9zgsKSQCdHa3m
/Fj89Gj4Tw6DbboK+sBUdQc=
=5XH5

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