

Re: Fw: Re[2]: FW: Linux server as it own firewall

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2001-09/0100.html>

From: Scott Gifford (sgifford@tir.com)

Date: 09/16/01

To: Jeff Schaller <schaller@freeshell.org>
Subject: Re: Fw: Re[2]: FW: Linux server as it own firewall
From: Scott Gifford <sgifford@tir.com>
Date: 16 Sep 2001 05:36:11 -0400
Message-ID: <lybskb5vg4.fsf@gfn.org>

Jeff Schaller <schaller@freeshell.org> writes:

- > *On 13 Sep 2001, Scott Gifford wrote:*
- >
- > > *The O'Reilly security book (sorry, don't remember the name;*
- > > *it's got a safe on the front) had some ideas for running a*
- > > *UNIX off of read-only media. The tricky problems are where to*
- > > *put logfiles (configure it to use remote syslog or a printer),*
- > > *PID files (no easy solution), etc. Depending on what you hope*
- > > *to accomplish, you may also need to make sure your kernel*
- > > *doesn't support any memory or network-based filesystems, such*
- > > *as a ramdisk or tmpfs, since that would be another place to*
- > > *put executables.*
- >
- > *(The book is Practical Unix and Internet Security by Simson and*
- > *Garfinkel)*
- >
- > *My work-in-progress plan for a floppy-based firewall has the*
- > *following ideas:*
- >
- > *1. no unnecessary files. a minimal set to begin with, and several*
- > *are removed after booting.*
- > *2. floppy disk is physically read-only*
- > *3. files that shouldn't change (most of them) are set immutable.*
- > *the chattr program does not exist on the system.*

It's probably not quite as simple as removing the chattr() program; there are other ways to get the equivalent ioctl() to run. The simplest would be to use perl's syscall() or ioctl() functions, if perl was available, but there are probably other ways. You would need to be extremely careful with the set of tools you allowed to be able to really prevent users from making this system call.

- > *4. no logging.*

SecurityFocus Linux: Re: Fw: Re[2]: FW: Linux server as it own

That makes monitoring the system pretty hard...Maybe remote syslog would be a good option?

- > 5. *temporary files are avoided as much as possible. temp space*
- > *is created with a ramdisk of less than 1 megabyte, mounted*
- > *nosuid,noexec.*

If a user gets root on the system, what prevents them from running:
mount -o remount,suid,exec /tmp

(or wherever the ramdisk is mounted) and then putting nasty files there? Or, for that matter, mounting another ramdisk elsewhere and putting things there?

And if the assumption is that a user won't get root on the system, why not just make everything owned by root and mode 755?

For similar reasons, you would want to make sure that no extra filesystems, like tmpfs, nfs, smbfs, loopback filesystems, or anything else that doesn't require a physical disk are not compiled in.

Still, good ideas. If you know or can find solutions to these problems, this would be very useful.

-----ScottG.

-
- **Previous message:** Scott Gifford: "Re: Clever firewall rules"
 - **Maybe in reply to:** James Puckett: "Linux server as it own firewall"
 - **Next in thread:** Jeff Schaller: "Re: Fw: Re[2]: FW: Linux server as it own firewall"
 - **Reply:** Jeff Schaller: "Re: Fw: Re[2]: FW: Linux server as it own firewall"
 - **Messages sorted by:** [date] [thread] [subject] [author] [attachment]