

Re: Deny local socket/port binding on server.

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2003-01/0442.html>

From: QuestionGuy (screw@spam.bots)

Date: 01/18/03

From: QuestionGuy <screw@spam.bots>
Date: Fri, 17 Jan 2003 18:55:48 -0800

Tim Haynes wrote:

>

...

>

> *You're looking for the GRSecurity patches. Specifically, the options for
> restricting certain groups from establishing client and/or server sockets:*

>

> *| zsh/scr, 10:38PM / # grep sock /etc/group*

> *| socknone:x:999*

> *| socknocli:x:998:gateway*

> *| socknosrv:x:997:apache*

> |

> *| CONFIG_GRKERNSEC_SOCKET_ALL_GID=998*

> *| CONFIG_GRKERNSEC_SOCKET_CLIENT_GID=997*

> *| CONFIG_GRKERNSEC_SOCKET_SERVER_GID=996*

>

Thanks Tim. That's what I'm looking for. I installed this patch already, but I likely didn't choose the correct options.

And in response to the other poster, for the record, I believe there's plenty of reasons to limit this on a server. Saying "If you can't trust users on your system, don't allow any" is a completely ridiculous. After all, that's like saying if you shadow passwords and have it set for only root to have read access on the shadow file, that if you can't trust your users...

I have policies stating they can't run such services, but that's not going to stop someone from doing that, now is it?! This prevents people from being able to do a variety of things. I.e., the only way to stop a DoS attack, is to make the server at the other end that is the source, to not be able to be a source.

I can surely terminate an account that violates the TOS, but if they've

comp.os.linux.security: Re: Deny local socket/port binding on server.

opened up a service to listen on a port to allow people a means to perhaps circumvent something or to do something annoying or abusive, it's sort of already too late. I just like having a means to limit things. It's only one small step and certainly doesn't make the system secure in itself, but it's one more thing that makes my job as an administrator easier and it makes the system better protected.

Overall, I'm not worried that user's can do this, but I'd like for them to not be able to. It's not a security issue if they can, anymore than if a user has shell access, for example, I am aware of that, but that while they have shell access, they can't do certain things they ought not do. Not to confuse my inquiry with meaning I think this is a solution to a problem, or to secure the system, but that it's just one step of many to make things more controlled. Thanks again, Tim, I'll check this and compile the kernel again with the proper options.