

Re: The -g and -R options

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2002-12/0281.html>

From: Richard E. Silverman (slade@shore.net)

Date: 12/21/02

From: slade@shore.net (Richard E. Silverman)

Date: 21 Dec 2002 05:56:40 -0500

>>>> "C" == Cylurian <fsromero@hotmail.com> writes:

C> if I type ssh -L 5003:time.csudl.edu:5003 -N jro@time.csudh.edu

C> I know that what ever comes out from the user to the server will be

C> secure, but is that also true when the data goes from the server to

C> the user?

This is ambiguous; I will assume you're talking about data passing over an instance of the port-forwarding tunnel here. Anyway, since the tunnelling is entirely symmetric, whatever you "know" about one direction will also be true of the other. Since in this case both the unprotected legs of the tunnel are loopback connections, one would usually say they are secure, in the sense that it can't easily be monitored. What makes you think the situation would be different depending on direction of data flow?

C> If the tunnel is secure both ways, then what are the -g and -R

C> options for?

This is an odd question, since neither -g nor -R serve to increase security. As documented, -g allows non-loopback connections to the forwarded port, so that one leg might *not* be secure. -R reverses the direction of connection establishment for instances of the tunnel: the SSH server forwards the port, rather than the client.

--

Richard Silverman
slade@shore.net