

Re: PermitRootLogin=yes versus su

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-01/0523.html>

From: Sebastian Hans (hanss@in.tum.de)

Date: 01/27/03

From: Sebastian Hans <hanss@in.tum.de>

Date: Mon, 27 Jan 2003 11:22:34 +0000 (UTC)

Bill Lewis Clark <wclark@eden.rutgers.edu> wrote:

- > *A long-standing pet peeve of mine is the nearly universal belief that*
- > *remote root logins via SSH are somehow less secure than connecting as*
- > *a regular user and using su to become root.*
- >
- > *Back in the days before strong encryption, when remote access was done*
- > *via telnet or rlogin, it made perfect sense to restrict root logins.*
- > *In situations where remote root access was absolutely necessary, su*
- > *was a reasonable alternative.*
- >
- > *However, we now have SSH. Given the option of securely logging into a*
- > *machine as root, I don't see the advantage of using su in this*
- > *capacity, any longer. In fact, I see several disadvantages.*
- >
- > *Logging in directly as root via SSH only leaves the remote account and*
- > *SSH protocols as vulnerabilities.*
- >
- > *Logging in as a regular user via SSH, then using su to become root,*
- > *leaves the remote account, SSH protocols, local regular user account,*
- > *and su binary all as potential vulnerabilities.*
- >
- > *I don't see how adding more points of vulnerability is an improvement.*
- > *I know that the su method made sense before SSH, but why is it still*
- > *considered standard practice? Is it simply inertia?*

In addition to all the other comments:

The su binary isn't /just/ an additional point of vulnerability in any case. To exploit su I would have to gain access as the regular user in the first place. If you protect the login of the regular user the same way as you would protect root's, su adds another layer of security – it doesn't take one away.

Just my 2¢.
seb