

Re: Strange command histories in hacked shell history

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-12/0035.html>

From: Scott Gerhardt (scott_at_g-it.ca)

Date: 12/18/04

Date: Fri, 17 Dec 2004 21:21:51 -0600

To: bv@wjv.com

- > *I understand that after using Unix for about 2 decades.*
- > *However in FreeBSD a user is supposed to be in the wheel group [if*
- > *it exists] to be able to su to root.*
- >
- > *But if a person who is not in wheel su's to a user who is in wheel,*
- > *then they can su to root – as the system sees them as the other*
- > *user. This means that the 'wheel' security really is nothing more*
- > *than a 2 password method to get to root.*
- >
- > *If the EUID of the original invoker is checked, even if they su'ed*
- > *to a person in wheel, then they should not be able to su to root.*
- >
- > *I'm asking why is this permitted, or alternatively why is putting a*
- > *user in the wheel group supposed to make things secure, when in*
- > *reality it just makes it seem more secure – as there is only one*
- > *more password to crack.*
- >

This makes no sense. If you can su to a user in the wheel group as an unprivileged user you need to know the users password and you also need to know roots password to su to root. This seems pretty secure to me.

If you want to be more secure than this then use sudo.

--

Scott

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"