

Re: Default permissions of /home/user..

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-10/0055.html>

From: Chuck Swiger (cswiger_at_mac.com)

Date: 10/24/04

Date: Sun, 24 Oct 2004 17:33:45 -0400
To: Jesper Wallin <jesper@hackunite.net>

Jesper Wallin wrote:

> *Sure, this works nice.. but yet, I did have to modify /usr/sbin/adduser .. Also, some of*
> *you said it's bad having a homedir chmod 700, how come? Let's say I use the account for*
> *coding, IRC perhaps, mail, etc.. none of those things require more access than 700?*

If you want to set up a highly secure user-account, using permissions of 700 is reasonable. However, it may not be sufficient, which is why chroot() and jails are available to create more restricted environments. One creates a "bind" user and chroot()s named to run inside /var/named, for example.

You also should think about the umask being used. Historically, the default umask was 022. You seem to want something like 027 or 077.

> *All I can think of is public_html which need o+x so nobody and/or www can access that*
> *directory.. I know, FreeBSD isn't Linux but most Linux systems run the same programs*
> *such as postfix, mysql, apache, openssh, etc.. and I know some distributions (like*
> *gentoo for example) which chmod it to 700 by default.. :)*

FreeBSD would prefer you to set up a group for each user, with GID == UID. This lets you use a umask of 002, and be able to share write access with other people who are in the same group. This is not significant to the owner of the file, who has user-mode access as well, but it lets the admin create new groups for a project, and users can chgrp files they want to share from their personal GID to the project GID.

--

-Chuck

frebsd-security@frebsd.org mailing list

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

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