

Re: Chroot environment for ssh

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2002-08/11357.html>

From: Wincent Colaiuta (wincentcolaiuta@mac.com)

Date: 08/20/02

Date: Tue, 20 Aug 2002 08:35:46 +0930
To: Philip Paeps <philip@paeps.cx>
From: Wincent Colaiuta <wincentcolaiuta@mac.com>

El Thursday, 15 August, 2002, a las 11:13 PM, Philip Paeps escribió:

> *I'm in the process of setting up a form of fileserver, and I'd like for*
> *my*
> *users to be able to work only in their home directories, not anywhere*
> *else. I*
> *would like to use SSH for the connections, as opposed to FTP, but I*
> *don't want*
> *users to be able to log into an interactive shell (only SCP/SFTP) and I*
> *don't*
> *want them to 'escape' out of their home directories.*

Use ssh2 from the ports collection:
`cd /usr/ports/security/ssh2 && make install`

In `/usr/local/etc/ssh2/sshd2_config` set the `ChRootGroups` and `ChRootUsers` directives to chroot the group(s) and/or user(s) that are to have `ChRooted` access.

Turn off the default ssh (OpenSSH) by setting in `/etc/rc.conf`:
`sshd_enable="NO"`

Start the new ssh:
`/usr/local/etc/rc.d/sshd.sh start`

When you create the user's account, make sure the shell is set to `/bin/nologin` or something similar.

With this setup, they can `sftp` in and are chroot to the home dir, and they can't get a shell when they connect via ssh.

In my opinion, OpenSSH should have this feature. We are told not to use `ftp` because of clear-text passwords, so we have to use `ssh/sftp`, but when we do that we can no longer chroot people to their home dirs! And if we're not careful, we end up giving them a login shell. Using `ssh2` from the ports gets around this limitation, but just check the licence

FreeBSD-Security: Re: Chroot environment for ssh

before you install to make sure that you qualify (otherwise it's not free).

Cheers :-)

Wincent

To Unsubscribe: send mail to majordomo@FreeBSD.org with "unsubscribe freebsd-security" in the body of the message