

weird ssh problem under OS X 10.3.6

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-11/0187.html>

From: Mike Zulauf (mazulauf_at_met.utah.edu)

Date: 11/26/04

Date: Fri, 26 Nov 2004 11:55:27 -0800

Hi all,

I've recently experienced an unusual problem with ssh (openssh) on both of my OS X machines (G4 iMac and G4 PowerBook). I recently applied an Apple Security Update and also an upgrade to openssh by way of fink. The problem occurs whether I use the fink version or the Apple supplied version, so my best guess is that Apple may have changed some config files (used by both) that may affect my particular setup.

Anyway, what happens is that when I try to initiate an ssh connection between my machines, or even from one machine to itself, I get the following message (for example):

```
% ssh localhost
ssh_exchange_identification: Connection closed by remote host
```

If I examine /var/log/system.log, I see the following entries:

```
Nov 26 11:45:34 iMac xinetd[305]: START: ssh pid=24267 from=:1
Nov 26 11:45:34 iMac sshd[24267]: fatal: Missing privilege separation
directory:
/var/empty
```

OK, that looks suggestive. So, I issue this command:

```
% sudo mkdir /var/empty
```

After this, I can use ssh, but I don't know if this is the best solution, or if the correct permissions are set for /var/empty. In addition, now I get the following sorts of messages in the system.log when I log out:

```
Nov 26 11:51:05 iMac sshd[28308]: error: BSM audit: solaris_audit_record
failed
to write "sshd logout " record: Operation not supported
```

So, any thoughts why this happened (to both of my Macs), whether this is the best solution, if there are any additional problems, anything else I

comp.security.ssh: weird ssh problem under OS X 10.3.6

should do, etc?

Thanks,
Mike

--
Mike Zulauf
mazulauf@met.utah.edu