

## OpenSSH root forced command?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2002-03/0619.html>

---

**From:** Joseph Gosselin ([gnostic@rcn.com](mailto:gnostic@rcn.com))

**Date:** 03/28/02

From: Joseph Gosselin <[gnostic@rcn.com](mailto:gnostic@rcn.com)>

Date: 28 Mar 2002 05:56:03 GMT

Hello, I am experiencing some relatively difficult issues with OpenSSH on two Redhat 7.1 boxen. What I would like to do, is set up a system whereby we can tell our clients to just create a file in `.ssh/authorized_keys` for root, which will contain the `command="..."` syntax option followed by a key for our root user, so that we can run backup operations without a password, and without having to ask the client to change the `'sshd'` config file and HUP the daemon. According to the manpage (or at least how I read it), you can run root commands even with `PermitRootLogin` set to `'no'` in the `'sshd_config'` file, so long as you specify the specific command to run in the key syntax in root's `.ssh/authorized_keys` file. Unfortunately in my experience this has not been the case. On multiple machines across many architectures (though I am only currently concerned with Linux), this system will simply not work with `PermitRootLogin` set to `"no"`, although it works fine with that parameter set to `"yes"` (though it kind of defeats the purpose that way). I've searched for hours on Google for someone with this info, but have not found anything – I apologize if I'm being a nuisance.

Oddly enough, the error which stops me from running this forced command appears to occur on the client side, instead of the server side, as per the following snippet:

```
debug1: Remote: Forced command: /bin/date
debug1: Received RSA challenge from server.
debug1: Sending response to host key RSA challenge.
debug1: Remote: RSA authentication accepted.
debug1: RSA authentication refused.
```

I read this as saying that the Remote machine (the server) has accepted my authentication, but that the client is reading this as a denial for some reason. I have added to the end of this post the full triple-verbosity output of my ssh command to the server. I sincerely thank you for your aid.

(ps: I've tried this with SSH version 2 as well – the problem remains exactly the same)

## comp.security.ssh: OpenSSH root forced command?

```
# ssh -v -v -v -l root@server /bin/date
OpenSSH_3.1p1, SSH protocols 1.5/2.0, OpenSSL 0x0090600f
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Applying options for *
debug1: Rhosts Authentication disabled, originating port will not be
trusted.
debug1: restore_uid
debug1: ssh_connect: getuid 0 geteuid 0 anon 1
debug1: Connecting to eagle.bu.edu [128.197.20.26] port 22.
debug1: temporarily_use_uid: 0/0 (e=0)
debug1: restore_uid
debug1: temporarily_use_uid: 0/0 (e=0)
debug1: restore_uid
debug1: Connection established.
debug1: identity file /root/.ssh/identity type 0
debug1: Remote protocol version 1.99, remote software version
OpenSSH_2.9p2
debug1: match: OpenSSH_2.9p2 pat OpenSSH*
debug1: Local version string SSH-1.5-OpenSSH_3.1p1
debug1: Waiting for server public key.
debug1: Received server public key (768 bits) and host key (1024 bits).
debug3: check_host_in_hostfile: filename /root/.ssh/known_hosts2
debug3: check_host_in_hostfile: filename /etc/ssh/ssh_known_hosts2
debug3: check_host_in_hostfile: filename /root/.ssh/known_hosts2
debug3: check_host_in_hostfile: filename /etc/ssh/ssh_known_hosts2
debug3: check_host_in_hostfile: filename /root/.ssh/known_hosts
debug3: check_host_in_hostfile: match line 1
debug3: check_host_in_hostfile: filename /root/.ssh/known_hosts
debug3: check_host_in_hostfile: match line 1
debug1: Host 'eagle.bu.edu' is known and matches the RSA1 host key.
debug1: Found key in /root/.ssh/known_hosts:1
debug1: Encryption type: 3des
debug1: Sent encrypted session key.
debug1: cipher_init: set keylen (16 -> 32)
debug1: cipher_init: set keylen (16 -> 32)
debug1: Installing crc compensation attack detector.
debug1: Received encrypted confirmation.
debug1: Trying RSA authentication with key '/root/.ssh/identity'
debug1: Remote: Forced command: /bin/date
debug1: Received RSA challenge from server.
debug1: Sending response to host key RSA challenge.
debug1: Remote: RSA authentication accepted.
debug1: RSA authentication refused.
debug1: Doing challenge response authentication.
debug1: No challenge.
debug1: Doing password authentication.
```

---

- ***Next message:*** [Peter Boosten: "Re: scp logged anywhere? \(ftp-like logs\)"](#)
- ***Previous message:*** [Nico Kadel-Garcia: "Re: Tunnelling via SSL anonymously to connect to remote host\(s\)"](#)

comp.security.ssh: OpenSSH root forced command?

- *Messages sorted by:* [ date ] [ thread ] [ subject ] [ author ] [ attachment ]