

## Re: X11 forwarding after su'ing

**Source:** [http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure\\_Shell/2003-06/0038.html](http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2003-06/0038.html)

---

**From:** Haan, de, Jan ([Jan.de.Haan\\_at\\_Essent.nl](mailto:Jan.de.Haan_at_Essent.nl))

**Date:** 06/06/03

To: [secureshell@securityfocus.com](mailto:secureshell@securityfocus.com)

Date: Fri, 6 Jun 2003 13:33:44 +0200

> > 3. why not use `ssh -X -l <thootheruserIwantedsudo?> <thehost>?`

> *Maybe, because -l root ain't that nice?*

> *Philipp*

Sorry for referring so late to a (securityfocus) post, but the Subject has been nagging me for the last month ;-) Problem was how to keep your DISPLAY, xauth and security (no 'ssh root@host' over the net) when changing users remotely (especially to root with su/sudo)

Comments please on the security side of this 'solution' and the proposed feature request.

Solved it by running two sshd's, one started with "`sshd -f sshd1_config`" with

```
"ListenAddress <hostname on ethx>"
```

```
"PermitRootLogin no"
```

```
"PidFile /var/run/ssh1.pid" <== That one bit me  
... in the ass a few times ;-)
```

```
...
```

And another started with "`sshd -f sshd2_config`"

```
"ListenAddress dummy0"
```

```
"PermitRootLogin yes"
```

```
"PidFile /var/run/ssh2.pid"
```

dummy0 is the hostname of the ip address on a loopbackadapter (Debian/GNU/Linux /etc/modules, dummy; HP-UX/Sun ifconfig lo0:1; winx msloopback adapter) which is not visible on the outside (disabled in routing) Only one extra address/subnet (/30 ?) is needed for an unlimited number of hosts since it can be identical on all because it is not routed.

Access can be gained in two ways: generating two keys that you both load in your ssh-agent or by adding your identity.pub to the authorized\_keys2 of the second remote user.

## SecurityFocus Secure Shell: Re: X11 forwarding after su'ing

Proof of concept:

```
user1@host1:/home/user1 >ssh -X host2
Linux host2 2.4.18-686 #1 Sun Apr 14 11:32:47 EST 2002 i686 unknown
Last login: Fri Jun 6 08:44:00 2003 from host1
user1@host2:~$ ssh -X root@dummy0
Linux host2 2.4.18-686 #1 Sun Apr 14 11:32:47 EST 2002 i686 unknown
Last login: Fri Jun 6 11:25:25 2003 from dummy0
root@host2:/root >echo $DISPLAY
localhost:11.0
root@host2:/root >
```

and

```
user1@host1:/home/user1 >ssh -X -f host2 'ssh -X -f root@dummy0
/usr/bin/X11/xterm'
```

works too.

Feature request

This kludge (2 daemons) would not have to be used if the possibility existed of

using a combined "AllowUsers" and "ListenAddress" parameter (ACL's ?) for instance:

ACL

```
[allow|deny],[dns|host|ipaddress|range[:port]],[user|group],[dns|host|ipaddress|range[:port]]
```

```
ACL allow, hostname, root, dummy0
```

```
ACL deny, *, !root, dummy0
```

```
ACL allow, *, !root, *
```

```
ACL deny, *, *, * (sorry, Cisco heritage showing ;-) )
```

Sincerely,

Jan.