

## Re: Auditing

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2002-02/7846.html>

---

**From:** Eli Dart ([dart@nersc.gov](mailto:dart@nersc.gov))

**Date:** 02/06/02

To: Paulo Fragoso <[paulo@nlink.com.br](mailto:paulo@nlink.com.br)>

Date: Tue, 05 Feb 2002 16:48:40 -0800

From: Eli Dart <[dart@nersc.gov](mailto:dart@nersc.gov)>

I don't know all the details involving your particular incident, but at one time there was a bug in PC-Anywhere that caused it to listen on UDP port 22 (they didn't put their port number in network byte order as I remember).

I still see scanners looking for UDP port 22 every once in a while (script kiddies looking for poorly configured PC-Anywhere instances).

So, this could be unrelated to your incident, and just be some random script kiddie. In general, if you turn on log\_in\_vain on a box that is directly connected to the Internet, you'll see a lot of random cruft....

--eli

In reply to Paulo Fragoso <[paulo@nlink.com.br](mailto:paulo@nlink.com.br)> :

> *Hi,*

>

> *We have a client which was using 4.2-RELEASE and telnetd enabled. In that*

> *machine was running an ircd installed and started by a hacker, probaly*

> *exploiting telnetd hole.*

>

> *We have instaled 4.5-RELEASE using another HD and log\_vain="YES" in the*

> *rc.conf. Some time after that upgrade, someone try to connect in this*

> *machine:*

>

> *Connection attempt to UDP mmm.mmm.mmm.mmm:22 from hhh.hhh.hhh.hhh:1384*

>

> *How can we found in the old system all mechanism to enable remotely ircd*

> *or backdoor? Are there any rootkit which it has a backdoor at UDP port 22?*

>

> *Paulo.*

>

>

> *To Unsubscribe: send mail to [majordomo@FreeBSD.org](mailto:majordomo@FreeBSD.org)*

Re: Auditing

FreeBSD-Security: Re: Auditing

> with *"unsubscribe freebsd-security"* in the body of the message

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

---

- application/pgp-signature attachment: stored