

Dubious ifconfig / tcpdump behaviour

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-02/0071.html>

From: Stefano Busti (*teppic11_at_yahoo.co.uk*)

Date: 02/12/04

Date: Thu, 12 Feb 2004 18:49:49 +0000 (GMT)
To: freebsd-security@freebsd.org

Hi, I have a FreeBSD 4.8 box connected to the net which until recently hasn't had any problems. Today DNS lookups mysteriously stopped working (the box has tinydns & dnscache installed to handle dns requests).

I noticed some strange things while checking the problem with tcpdump. Tcpdump appears not to show any traffic whatsoever on either my external interface or internal lan interface, this despite the fact I was successfully pinging hosts over both interfaces from a different console while checking the traffic. I do get notified about promiscuous mode being enabled and disabled as normal, and a message at the end saying that packets were successfully received by the kernel. I just don't see the actual packets. Tcpdump had always worked fine before, and still works normally on the loopback interface.

Also I seem to be unable to disable either of the affected interfaces with ifconfig, whereas in the past I never had a problem doing this. Requests to bring either interface down are silently ignored.

Does anyone have an idea what the cause could be? Have I overlooked some obvious configuration issue, or might tcpdump, ifconfig or any system routines they call have been compromised? Sadly I hadn't installed an intrusion detector such as tripwire previously, and system logs don't `_appear_` to show evidence of any compromise.

BT Yahoo! Broadband – Free modem offer, sign up online today and save £80 <http://btyahoo.yahoo.co.uk>

freebsd-security@freebsd.org mailing list

FreeBSD–Security: Dubious ifconfig / tcpdump behaviour

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"