

Re: Hacked or not appendice

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-06/0029.html>

From: Alex Povolotsky (*tarkhil_at_webmail.sub.ru*)

Date: 06/12/04

Date: Sat, 12 Jun 2004 17:45:29 +0400

To: freebsd-security@freebsd.org

On Sat, 12 Jun 2004 13:03:07 +0000

Thordur Ivar <thib@mi.is> wrote:

TI> I have on a CD a number of binaries (sources actually) (e.g. ls,
TI> find, grep, awk, sed, locate e.t.c.) and when I believe that a
TI> machine has been cracked I remove the network cable from that
TI> machine and mount the cdrom build the sources and start looking. If
TI> I need something in that process I put it on my USB memstick from a
TI> 'trusted machine' and move it by hand over.

When I was unable to do the same thing, I've recompiled md5 tool from freshly fetched sources and used it to test utilities. I don't beleive in attacker catching thr build process transparently...

--

Alex.

freebsd-security@freebsd.org mailing list

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

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