

Re: sequences in the auth.log

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-08/0044.html>

From: Nikolay Pavlov (*quetzal_at_roks.biz*)

Date: 08/18/04

Date: Wed, 18 Aug 2004 12:54:21 +0300

To: Justin <freebsd@alt-network.com>

Hi, Justin

On Tuesday, 17 August 2004 at 23:01:28 –0500, Justin wrote:

> *I'm seeing the same thing in my log. It makes me think it is a virus because*
> *test, guest, and admin are not normal unix users.*

And I'm too. But I think that this is a some kind of Linux worm.

The first record in my auth.log dated on Jul 23 01:48:30

Nmap identificates all hosts (already more than ten) in my auth.log as

"Linux 2.4.0 – 2.5.20, Linux 2.4.20 (Itanium), Linux 2.4.20 – 2.4.22 w/grsecurity.org patch"

Best regards,

Nikolay Pavlov.

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"