Re: newbie with www user security problem

Source: http://www.derkeiler.com/Mailing−Lists/FreeBSD−Security/2005−08/0008.html

---

From: Yann Golanski (*yann_at_kierun.org*)
Date: 08/11/05

```
Date: Thu, 11 Aug 2005 16:50:23 +0100
To: Ken Hawkins <ken@rosewoodblues.com>
```

Quoth Ken Hawkins on Thu, Aug 11, 2005 at 11:32:44 −0400
> The box is secure that much i have found out. the only problems have
> been with this email spamming. nothing in the tmp dirs out of the
> ordinary and no missing files running scripts etc. I have changed
*> everyone passwords on the box. *'d the www password, ensured there is*
> no shell with the www user, etc.

Have you run chkrootkit on it?

> i am in the process of upgrading the ports now and there are problems
> (of course). the ports seem to have been mangled as the listing in /
> var/db/ports does not match what i KNOW is running on the box. The
> person i have inherited this from manually deleted from the /var/db/
> ports to get some of the applications to re−install! gotta love that!

ICK! Make sure you database is fine otherwise, you'll get into no end
of trouble.

> well here i come port fix hell! This is a production box and can't be
> taken off line as of this moment so i am going to have to attempt on
> the fly fixing / upgrading of the ports. i would love to wipe it but
> it is just not a possibility right now.

Oh dear. How about living it as is −− minus the spam emailer −− and
rebuilding another one to replace it?

```
−−
yann@kierun.org                 −=*=−                      www.kierun.org
    PGP:   009D 7287 C4A7 FD4F 1680  06E4 F751 7006 9DE2 6318
```

- application/pgp−signature attachment: stored