

## Re: theo

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2002-01/7733.html>

---

**From:** f.johan.beisser ([jan@caustic.org](mailto:jan@caustic.org))

**Date:** 01/26/02

Date: Fri, 25 Jan 2002 15:20:19 -0800 (PST)  
From: "f.johan.beisser" <[jan@caustic.org](mailto:jan@caustic.org)>  
To: Robert Simmons <[rsimmons@wlcg.com](mailto:rsimmons@wlcg.com)>

On Fri, 25 Jan 2002, Robert Simmons wrote:

> -----BEGIN PGP SIGNED MESSAGE-----  
> Hash: RIPEMD160  
>  
> Lets say someone has a machine they don't have console access to, but they  
> know that the OS comes back every time they reboot the fucker.  
>  
> The kernel is on the old hard drive, with the swap garbage. The brand  
> spanking new OS is mirrored on a twed. How can I tell that the core  
> team's brand spanking newly de scriptkiddified kernel is the one that  
> boots? dmesg?

generally, i can tell via an `ls -al /kernel`, and checking the timestamp.  
failing that, i can look at the output from `uname`:

FreeBSD pogo.caustic.org 4.4-STABLE FreeBSD 4.4-STABLE #1: Wed Nov 14  
11:14:38 PST 2001 [root@pogo.caustic.org](mailto:root@pogo.caustic.org):/usr/src/sys/compile/POGO i386

and looking at that alone, i can tell (i tend to rebuild the kernel once  
each major change/kernel level patch. so, in this case, the timestamp on  
the `uname` output (Wed Nov 14 11:14:38 PST 2001) tells me that this is the  
kernel i build ages ago.

should i do more frequent rebuilds, the string "FreeBSD 4.4-STABLE #1"  
would tell me which build number of the kernel (since building POGO's  
first kernel) i have.

if what you're refrencing is the specific kernel loaded by the loader,  
unless you change it at boot time (`unload kernel`, `load <altkernel>`, `boot`),  
it will default to `/kernel`.

> BTW, there isn't a floppy installed, nor a CD\_ROM.

that's fine, you can change the device that the kernel is loaded from if  
you really wish too.

FreeBSD-Security: Re: theo

> *Also, you win, you people get the prize for the most security alerts in  
> one year. :)*

thanks. i tend to be glad to see so many security alerts. makes me feel like someone is finding, and fixing, problems in the OS. "Security is not a product, it is a process" and all that jazz.

btw, anyone know who said that? i'm inclined to think it's bruce schneier.

-----/ f. johan beisser /-----+-----

[http://caustic.org/~jan\\_jan@caustic.org](http://caustic.org/~jan_jan@caustic.org)

"John Ashcroft is really just the reanimated corpse  
of J. Edgar Hoover." -- Tim Triche

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