

## Re: Renaming root account

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-03/0003.html>

---

**From:** Ed Stover (*estover\_at\_nativenerds.com*)

**Date:** 03/03/05

To: [freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org)

Date: Thu, 03 Mar 2005 01:42:32 -0700

This response is a bit off of what you asked but I will just toss this out there.

I generally protect my machines from the root user but utilizing chflags and kernel secure levels. That way if an attacker were to gain root access they wouldn't be able to change files... On my firewalls I modify rc.conf to boot to secure level 2 ,then I lock down /bin /sbin /etc /usr/local/etc with chflags schg while still in secure level 0 then reboot. Upon the restart you have a very secure machine that is protected from root user. In secure level two, even root cannot change those files flagged immutable. The only way to change those files would be to have physical access to the machine and modify rc.conf in single user mode and then reboot change the flags back from immutable and then modify the files. That is a bit too secure to be user friendly. I am just a getRdun type of person, you could lock down certain files and leave the five passwd files alone so users could change their passwords but generally attackers try to add themselves an account right away. What application would you be using the server for? Most H4X0RZ attacks I have seen where they have gained shell access are stumped when it comes to file flags and kernel secure levels.

On Thu, 2005-03-03 at 08:03 +0000, Craig Edwards wrote:

```
> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
> Hi everyone,
>
> One quick question: Is it safe and/or sensible to rename the root
> account, so that the only uid 0 user on a system is something different
> to root? I can see how this would be effective against external
> attackers who have no knowledge of the internals of the system as they
> would spend pointless hours trying to crack a user which doesnt exist,
> however to internal users they could always just cat /etc/passwd and see
> that root has been renamed. So firstly, is this possible, and security
> wise is it of any real use? Can anyone think of any apps it would break
> that assume that the uid 0 user is called root and don't just address
> the user by its uid?
>
> Thanks,
```

FreeBSD–Security: Re: Renaming root account

> *Craig Edwards*  
>  
> ---  
> *WinBot IRC client developer: <http://www.winbot.co.uk>*  
> *ChatSpike – The users network: <http://www.chatspike.net>*  
> *InspIRCd – Modular IRC server: <http://www.inspircd.org>*  
> *Online RPG Developer: <http://www.ssod.org>*  
> ---  
> -----BEGIN PGP SIGNATURE-----  
> Version: GnuPG v1.2.5 (MingW32)  
>  
> *iD8DBQFCJsTf0k42Wxli/BARAp2DAJ9dp1eu2IL41pfp/4ZFP9kS2KuMdgCeI20k*  
> *w1Jt+uriEmWM+wmhEFxH+vw=*  
> =vGhO  
> -----END PGP SIGNATURE-----  
>  
> \_\_\_\_\_  
> *frebsd–security@frebsd.org mailing list*  
> *<http://lists.frebsd.org/mailman/listinfo/frebsd–security>*  
> *To unsubscribe, send any mail to "frebsd–security–unsubscribe@frebsd.org"*

\_\_\_\_\_  
frebsd–security@frebsd.org mailing list  
<http://lists.frebsd.org/mailman/listinfo/frebsd–security>  
To unsubscribe, send any mail to "frebsd–security–unsubscribe@frebsd.org"