Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Wed, 21 Nov 2007 06:01:58 GMT
View Forum Message <> Reply to Message

I would note that you cannot make process "hidden" from userspace. It can be done from kernel-space only, i.e. by using loadable kernel modules.
However nobody inside VE have such permissions, nobody is able to load any kernel modules from inside VE, only HW-node admin is able to do it.

Therefore "hidden" proccesses detected inside VE is not mean that your VE has been hacked. All that yo can do is just report to HW-node admin and he can check your "hidden" pids.

However you can make some checks inside VE too. Usually "virtual" pids visible inside VE = "system" Pid + 1024 (i.e bit 10 is used to mark pid as Virtual). Therefore if you found "hidden" pid with this number, it makes sense to search according "virtual" pid inside VE.

Of course we'll make "system" pids to be more "invisible" inside VE -- to prevent chkrootkit's false alerts.

Thank you,
Vasily Averin