Subject: Re: Hidden process for init (PID 1)?
Posted by signal11 on Wed, 17 Dec 2008 09:36:01 GMT
View Forum Message <> Reply to Message

maratrus wrote on Mon, 15 December 2008 11:22Hi,

There are no hidden processes in OpenVZ. Please, describe in more detail what do you have in mind?

Quote:
But as far as I understand, every process in the container is a process on the host, usually with a fixed offset in PID.

You cannot rely on this fact. It could be true for a lot of examples but this is not the rule and could be broken down for example after VE will be migrated.

Within the container, you can detect both PIDs for a process, the one for the host process and the one in the VE PID namespace. But within the VE, ps, top, or other standard tools only list the PID in the VE PID namespace. Thus for all practical purposes, for an observer within the VE the host PIDs appear as hidden processes.

This is problematic because: if you want to check from within the container whether your 'ps' has been replaced by a rootkit to hide processes, you need to identify legitimate PIDs that represent host processes corresponding to PIDs in your VE PID namespace.

Insofar the 'offset by 1024' is nice, and as long as it works in the VE I'm concerned with, I don't have a problem with the fact that it might not be true always and everywhere.

The only problem I have, and what my question was about, is whether I have to expect that there will be one host PID (which in my guess would correspond to init in the VE) that will not follow the 'offset by 1024' rule.