Subject: Hidden process for init (PID 1)?
Posted by signal11 on Mon, 15 Dec 2008 09:05:17 GMT
View Forum Message <> Reply to Message

I'm trying to detect hidden processes within a container (no, you don't need a kernel module to hide a process.. trojan ps and top go a long way already).

I'm aware that OpenVZ already has a hidden process for every visible process in the container, and that there's an offset of 1024 in PID between hidden and visible processes, which allows to identify the legitimate hidden OpenVZ processes.

However, there remains one unaccounted hidden process (i.e. no visible process at hidden PID + 1024). On the other hand there's no obvious hidden process candidate for init (PID 1). Is it safe to presume that the unaccounted hidden process is the one corresponding to PID 1?