Subject: Re: "hidden processes" in OpenVZ
Posted by vaverin on Wed, 21 Nov 2007 12:53:57 GMT

View Forum Message <> Reply to Message

As you know each process has a directory on proc filesystem:
/proc/<pid>/...

Usually /proc/<pid> are visible by any filesystem system calls. "Hidden" pids are not visible directly -- for example readdir() system call does not show it. However some other system calls still can use this pid: for exmaple you can change directory to "hidden" or something else. (I would note -- it is not usual "cd" shell command, but syscall chdir() used by chkproc).

Procfs -- is virtual filesystem, its content created by kernel an the fly and even root is not able to change its content. On the other hand root is able to load some kernel modules that will change kernel code and by this way will be able to change proc output too. Some rootkits uses this ability and changes kernel code to make itself invisible.

That's why chkrootkit tries detect these "invisible" processes by using some unusual ways. Such "hidden" processes really looks suspect.

Unfortunately our "system" pids are visible inside VE for some system call, chkrootkit is able to detect it and report about suspected pids.

However nobody inside VE hav permissions to load kernel modules, and therefore any rootkits inside VE are not able to make the processes "hidden".

thank you,
Vasily Averin