Subject: OpenVZ and rootkits

Posted by curtis_isparks on Fri, 27 May 2011 18:11:55 GMT

View Forum Message <> Reply to Message

Because OpenVZ does not have a hypervisor layer (where guests run their own kernel), it does make me wonder about security. Does it still provide protection for the HN against most rootkits that might be run inside a container? In other words, do rootkits that have no knowledge that they are being run inside a container also cause problems for the HN? Are there rootkits that are built specifically to break out of OpenVZ containers?

Thanks,

Curtis

Subject: Re: OpenVZ and rootkits

Posted by curtis_isparks on Sat, 28 May 2011 23:51:28 GMT

View Forum Message <> Reply to Message

Lots of views on this posting, but it seems nobody knows the status of OpenVZ in regards to whether putting clients inside an OpenVZ container offers any protection against a hacker actually getting root access to the host node?

Why am I asking this? Well, it's a lot easier to rebuild a container than it is to completely reinstall a machine that has been hacked. But, am I fooling myself that by putting customers inside a container that I'm reducing the chances of a hacker actually getting access to the physical machine?

Subject: Re: OpenVZ and rootkits

Posted by dzimi on Sun, 29 May 2011 11:44:51 GMT

View Forum Message <> Reply to Message

Argh!! (You cannot use links until you have posted more than 10 messages.)

openvz.livejournal.com/37305.html

read it. OWL patches would like to help you

Subject: Re: OpenVZ and rootkits

Posted by curtis_isparks on Fri, 03 Jun 2011 18:14:05 GMT

View Forum Message <> Reply to Message

dzimi wrote on Sun, 29 May 2011 07:44Argh!! (You cannot use links until you have posted more than 10 messages.)

openvz.livejournal.com/37305.html

read it. OWL patches would like to help you

Thanks for the suggestion, dzimi. It looks, however, that to use OWL, it acts as the host node OS, and I'm using Proxmox as my host OS.

Oh well, I am going to try asking this question another way, since this thread did not draw much response.

Curtis