Subject: Breaking Out of Openvz.
Posted by hello-world on Thu, 02 Oct 2008 04:55:25 GMT
View Forum Message <> Reply to Message

We have a couple of demo servers running inside openvz vps. The version is: 2.6.18-53.1.19.el5.028stab053.14

One of our demo servers was 'hacked'. As in, somebody got into the root of this demo vps. (which was not unexpected at all), but what happened next, i am trying to figure out.

Now, looking through this guy's .bash_history INSIDE the vps, i found that he created a large 150MB image file, and then ran losetup on it.

I searched for "openvz losetup vulnerability" and even "openvz losetup", but it didn't turn up anything. There were also some commands where he downloaded the code from ftp4.netbsd.us.netbsd.org and compiled some code. Again a search with the keywords didn't return anything.

I am attaching the 2 bash_histories with this: One is run in his home directory logged in as user joki.

And the other he ran as root:

Can someone look through the file and tell me if any of those actions he did can lead to him breaking out of openvz and into the main node on kernel 2.6.18-53.1.19.el5.028stab053.14.

I couldn't find anything suspicious on the node, but that's partly because, i am not 100% sure of what's the exact situation when a person breaks out of a vps.

So this is a generic question too: How do i determine if someone has broken out of his vps? Is there some logs or traces that such a person will leave?

Will he be executing the node's shell as root? i couldn't find any suspicious .bash_history anywhere on the node.

Thanks a lot for any help.

File Attachments

1) joki-bash-history, downloaded 1035 times
2) root-bash-history, downloaded 1010 times