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 802 times
2) root-bash-history, downloaded 780 times

Subject: Re: Breaking Out of Openvz.
Posted by hello-world on Thu, 02 Oct 2008 16:21:18 GMT
View Forum Message <> Reply to Message

OK, some general comments about the guy who got in. One thing about him is that he is no master of subtlety. His behavior inside the demo server can only be described as being that of a bull in a china shop, and he has pretty much left his paw prints everywhere.

He didn't even care to delete the .bash_history, nor did he even trim the last log. I found around 18 logins into the VPS in a 5 hour period.

So if he did break out of openvz, and got into the node, the complete lack of any trace of activity is absolutely not purposeful, since we have seen by his activity inside the VPS, he completely lacks the idea of being stealthy.

Subject: Re: Breaking Out of Openvz.
Posted by hello-world on Thu, 02 Oct 2008 17:37:22 GMT
View Forum Message <> Reply to Message

joki	pts/0	Tue Sep 30 07:34 - 08:03 (00:28)	ptc-gw.ptc.com
root	pts/0	Tue Sep 30 07:33 - 07:34 (00:00)	ptc-gw.ptc.com
joki	pts/1	Tue Sep 30 05:14 - 05:15 (00:00)	ptc-gw.ptc.com
joki	pts/6	Tue Sep 30 04:49 - 05:10 (00:20)	ptc-gw.ptc.com
joki	pts/5	Tue Sep 30 04:49 - 05:15 (00:26)	ptc-gw.ptc.com
joki	pts/4	Tue Sep 30 04:46 - 05:13 (00:27)	ptc-gw.ptc.com
joki	pts/2	Tue Sep 30 04:23 - 05:06 (00:43)	ptc-gw.ptc.com
joki	pts/1	Tue Sep 30 03:16 - 04:51 (01:35)	ptc-gw.ptc.com
root	pts/1	Tue Sep 30 03:16 - 03:16 (00:00)	ptc-gw.ptc.com
joki	pts/1	Tue Sep 30 03:16 - 03:16 (00:00)	ptc-gw.ptc.com
joki	pts/1	Tue Sep 30 03:15 - 03:16 (00:00)	ptc-gw.ptc.com
root	pts/1	Tue Sep 30 03:10 - 03:15 (00:04)	ptc-gw.ptc.com
joki	pts/1	Tue Sep 30 03:09 - 03:10 (00:01)	ptc-gw.ptc.com
joki	pts/0	Tue Sep 30 02:30 - 06:44 (04:13)	ptc-gw.ptc.com
root	pts/0	Tue Sep 30 02:29 - 02:30 (00:00)	ptc-gw.ptc.com
joki	pts/0	Mon Sep 29 16:45 - 16:54 (00:09)	cpc2-oxfd10-0-0-cust53.oxfd.cable.ntl.com
joki	pts/1	Mon Sep 29 16:06 - 16:54 (00:47)	cpc2-oxfd10-0-0-cust53.oxfd.cable.ntl.com
joki	pts/0	Mon Sep 29 16:02 - 16:40 (00:37)	cpc2-oxfd10-0-0-cust53.oxfd.cable.ntl.com
root	pts/0	Mon Sep 29 16:01 - 16:02 (00:00)	cpc2-oxfd10-0-0-cust53.oxfd.cable.ntl.com
root	pts/0	Mon Sep 29 16:01 - 16:01 (00:00)	cpc2-oxfd10-0-0-cust53.oxfd.cable.ntl.com
root	pts/0	Mon Sep 29 16:01 - 16:01 (00:00)	cpc2-oxfd10-0-0-cust53.oxfd.cable.ntl.com
root	pts/2	Mon Sep 29 10:19 - 11:43 (01:24)	ptc-gw.ptc.com
joki	pts/0	Mon Sep 29 09:47 - 11:44 (01:57)	ptc-gw.ptc.com
joki	pts/1	Mon Sep 29 09:40 - 11:43 (02:02)	ptc-gw.ptc.com

```
joki     pts/0        Mon Sep 29 08:38 - 09:43  (01:05)     ptc-gw.ptc.com
joki     pts/0        Mon Sep 29 08:37 - 08:38  (00:00)     ptc-gw.ptc.com
joki     pts/0        Mon Sep 29 08:36 - 08:37  (00:01)     ptc-gw.ptc.com
joki     pts/0        Mon Sep 29 08:35 - 08:36  (00:01)     ptc-gw.ptc.com
joki     pts/0        Mon Sep 29 08:34 - 08:35  (00:00)     ptc-gw.ptc.com
root     pts/0        Mon Sep 29 08:34 - 08:34  (00:00)     ptc-gw.ptc.com
joki     pts/0        Mon Sep 29 08:33 - 08:33  (00:00)     ptc-gw.ptc.com
root     pts/0        Mon Sep 29 08:30 - 08:33  (00:02)     ptc-gw.ptc.com
```

The above is the last log access by this person inside the demo VPS.

Subject: Re: Breaking Out of Openvz.
Posted by Sigkill on Sat, 18 Jun 2011 22:15:49 GMT
View Forum Message <> Reply to Message

Probably he is getting out of memory errors when trying to compile stuff so he wants to use swapon to give himself more memory, he is not trying to break out.

Altough it nowadays exists several break-out-of-openvz versions of ordinary local kernel exploits...
