Subject: See connections from other VE's in netstat
Posted by ceelian on Mon, 21 Dec 2009 12:26:15 GMT
View Forum Message <> Reply to Message

Hi,

When i run netstat -tapn i can see the connections of ip's from other VE's on the same hardware node.
In the netstat column Local Adress (inside the VE) there are the "neigbour" VE ips beside mine. I think there only should be connections from my VE IP not from the others too.

Is that a feature or a security critical bug.

How can i disable that, or is it neccessary?

Devices in VE's are venet Devices.

Thx.

Subject: Re: See connections from other VE's in netstat
Posted by kir on Mon, 21 Dec 2009 12:40:36 GMT
View Forum Message <> Reply to Message

What kernel is it? Please provide output of
uname -a
cat /proc/vz/version

Subject: Re: See connections from other VE's in netstat
Posted by ceelian on Mon, 21 Dec 2009 12:45:50 GMT
View Forum Message <> Reply to Message

Hi,

uname -a
Linux testhn2 2.6.26-2-openvz-amd64 #1 SMP Wed Aug 19 23:15:49 UTC 2009 x86_64 GNU/Linux

cat /proc/vz/version
036test001

The HN is a Ubuntu Jaunty System with the Debian OpenVZ Kernel (Ubuntu has AFAIK no OpenVZ Kernel officially supported). The vzctl comes from the official Ubuntu Jaunty APT-Repository. I wonder why the version is "...test...". I thought Ubuntu Jaunty ships with a stable vzctl.

Regards,
ceelian

Subject: Re: See connections from other VE's in netstat
Posted by ceelian on Tue, 29 Dec 2009 17:15:03 GMT
View Forum Message <> Reply to Message

After some research i found out that it might be the capability NET_ADMIN:on which causes this effect.

Can anyone agree with this or is it impossible that the NET_ADMIN can cause this effect?

Anyway if I use NET_ADMIN:on, which must be set for OpenVPN to work properly, can Containers interfere in an "Attacking way" due to this setting? I mean can anyone break in someones other container due to that option turned on? Or is the worst thing that can happen that a neighbors container can sniff the network traffic?

thx,
ceelian

Subject: Re: See connections from other VE's in netstat
Posted by hfb9 on Thu, 31 Dec 2009 22:16:52 GMT
View Forum Message <> Reply to Message

We are now seeing this behavior on:

2.6.26-2-openvz-amd64

Which is the latest OpenVZ Kernel in the Debian Lenny stable repositories.

Does this mean packet sniffing between virtual servers on the same hardware is now possible?