Subject: hidden iptables in containers
Posted by cgm00 on Fri, 24 Apr 2009 06:52:17 GMT
View Forum Message <> Reply to Message

Hello
Is it posible to create iptables rules in hwnode that are not seen
inside containers related with -m owner . Basically I do not want
that if some1 gets root inside a CT to be able to alter/see
any iptables rules (you can not use -m owner with FORWARD)
Or are there plans to implement such feature?

Subject: Re: hidden iptables in containers
Posted by maratrus on Fri, 24 Apr 2009 12:45:44 GMT
View Forum Message <> Reply to Message

Hello,

could you possibly provide the precise command that needs to be invoked on the HN so that we'll be able to see the rule on the HN and inside VE simultaneously?

Subject: Re: hidden iptables in containers
Posted by cgm00 on Fri, 24 Apr 2009 13:32:40 GMT
View Forum Message <> Reply to Message

Lets say this command

#iptables -A OUTPUT -m owner --uid-owner 0 -j ACCEPT

Subject: Re: hidden iptables in containers
Posted by maratrus on Mon, 27 Apr 2009 07:59:43 GMT
View Forum Message <> Reply to Message

Hi,

uname -a
Linux test 2.6.18-92.1.18.el5.028stab060.2 #1 SMP Tue Jan 13 12:18:59 MSK 2009 i686 i686 i386 GNU/Linux

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            owner UID matchroot
# vzctl exec 101 iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Please, specify your kernel. I cannot reproduce the issue. The provided rule was aplied on the HN (and iptables -L command showed that it appeared in OUTPUT chain), but there was nothing inside VE.

Subject: Re: hidden iptables in containers
Posted by cgm00 on Mon, 27 Apr 2009 08:37:00 GMT
View Forum Message <> Reply to Message

I did not said this is a bug. I asked if is posible to see
iptables ONLY from hwnode(for CT), this would be a great security feature.

Subject: Re: hidden iptables in containers
Posted by maratrus on Mon, 27 Apr 2009 08:43:12 GMT
View Forum Message <> Reply to Message

Hi,

Quote:
I asked if is posible to see iptables ONLY from hwnode(for CT)

Of course, it shouldn't be possible.
If you manage to observe such behavior - it's a secure bug and it have to be filed to bugzilla.