Subject: scapy filters / tcpdump
Posted by gorzilla on Tue, 15 May 2012 13:24:38 GMT
View Forum Message <> Reply to Message

I'm trying to use scapy to capture raw data packets on my vps but I'm getting unexpected results and I'd like to know if this a problem with openvz.

At first I thought it was a configuration error on my part but I've tried quite a few of the different operating systems my host offers and the error persists regardless. The tool works as it's supposed to when I tried to reproduce the error in VirtualBox. Doing the work in a virtual machine would be fine, but my project involves DNS resolution.

Scapy does packet sniffing/manipulation. The filtering relies on tcpdump, however when run on its own, tcpdump runs properly with filtering working as expected.

I've tried using different filters such as 'tcp' or 'port 80' but none of them give any results. Scapy is definitely able to see the traffic however, since without a filter the traffic is recorded properly (and can be sorted out programmatically after the fact).

Scapy docs:
hxxp://www.secdev.org/projects/scapy/doc/usage.html#sniffing

My testing process:
[for operating systems with python > 2.6]
wget scapy.net
sh ./scapy
scapy

x=sniff(filter='icmp', count=1)
[should stop as soon as it sniffs an icmp packet but instead runs indefinitely and nothing is captured]

[in another terminal]
ping google.com

It could well be a bug in scapy but Google gives no relevant results and I'm at a loss. Any help you could offer would be greatly appreciated.