Subject: Snort can't capture packets on venet0:0 interface
Posted by ivani on Tue, 05 Apr 2011 16:44:53 GMT

Hi folks.

I just joined in this forum... I'm newbie with Snort running in virtual machines and I have a doubt.

I've googled many sites, lists, but I'm lost about a weird error.
I've installed and configured the snort 2.9.4 but I can't start it.

This is my interface:

venet0:0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet addr:XXX.XXX.XXX.XXX P-t-P:XXX.XXX.XXX.XXX Bcast:XXX.XXX.XXX.XXX
Mask:255.255.255.255
        UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1

I did a test with snort:

snort -vv -i venet0:0
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "venet0:0".
Decoding Linux SLL

        --== Initialization Complete ==--

  ,,_   -*> Snort! <*-
 o")~   Version 2.9.0.4 IPv6 GRE (Build 110)
  ""   By Martin Roesch & The Snort Team:
        Copyright (C) 1998-2011 Sourcefire, Inc., et al.
        Using libpcap version 1.1.1
        Using PCRE version: 6.6 06-Feb-2006
        Using ZLIB version: 1.2.3

Commencing packet processing (pid=5776)
Can't acquire (-1) - cooked-mode frame doesn't have room for sll header!

And the snort can't start.

I don't know which kind of Linux is running on the parent host.
I've installed the CentOS 5.5, and this is output of uname:

uname -a

Linux snortlab 2.6.18-194.8.1.el5.028stab070.5 #1 SMP Fri Sep 17 19:10:36 MSD 2010 i686 i686 i386 GNU/Linux

Someone can help me?

Thank in advance.

Regards,

Ivani