Suricata - Bug #3

pcap_dispatch blocks on exit if no traffic is seen.

11/10/2009 11:12 AM - Will Metcalf

Status:	Closed		
Priority:	Low		
Assignee:			
Category:			
Target version:			
Affected Versions:		**Difficulty:**	
Effort:		**Label:**	

Description

If the engine is sent a signal to exit in pcap live mode, pcap_dispatch will block until a packet is received.

See the threads below. We can overcome this by setting the pcap
handle to non-blocking but cpu utilization increases a ton. Not that big of an issue but here are some threads explaining it and possible solutions.

http://www.mail-archive.com/tcpdump-workers@lists.tcpdump.org/msg02491.html
http://seclists.org/tcpdump/2009/q1/171

History

#1 - 11/10/2009 11:51 AM - Victor Julien

The non blocking solution is probably not interesting for performance reasons. The other option is to look at pcap_breakloop but that needs to be called by the pcap thread(s) itself then. Low priority issue.

#2 - 12/30/2009 07:44 AM - Victor Julien

- Target version changed from 0.8.0 to TBD

#3 - 08/18/2011 08:46 AM - Eric Leblond

I'm not able to reproduce it. Maybe we could close it ?

#4 - 08/23/2011 10:07 AM - Will Metcalf

- Status changed from New to Closed

- % Done changed from 0 to 100

afaik this was a libpcap 0.9.x bug. closing.

#5 - 01/13/2012 06:21 AM - Victor Julien

- Assignee deleted (OISF Dev)

- Target version deleted (TBD)