I am attempting to compile suricata-5.0.1 with pfring enabled but the configuration script reports an error over pfring library version lesser than version 6. I've install libpcap from pf_ring/userland

```
checking pcap.h usability... yes
checking pcap.h presence... yes
checking for pcap.h... yes
checking for pcap.h... (cached) yes
checking pcap/libpcap.h usability... yes
checking pcap/libpcap.h presence... yes
checking for pcap/libpcap.h... yes
checking pcap/bpf.h usability... yes
checking pcap/bpf.h presence... yes
checking for pcap/bpf.h... yes
checking for PCAP... no
checking for pcap_open_live in -lpcap... yes
checking for pcap_activate in -lpcap... yes
checking for pcap-config... /usr/local/bin/pcap-config
checking for pcap_set_buffer_size in -lpcap... yes
checking for pfring_open in -lpfring... yes

ERROR! --enable-pfring was passed but the library version is < 6, go get it from http://www.ntop.org/products/pf_ring/
```

My system -

```
Linux linux-1vv0 4.12.14-1p151.28.36-default #1 SMP Fri Dec 6 13:50:27 UTC 2019 (8f4a495) x86_64 x86_64 x86_64 GNU/Linux
```

Configure arguments -

```
./configure --prefix=/usr/local --sysconfdir=/usr/local/etc --localstatedir=/var --includedir=/usr/local --enable-python --enable-gccprotect --enable-gccprofile --enable-profiling --enable-debug --enable-afl --enable-unittests --enable-profiling --enable-profiling-locks --enable-pfring --with-libpfring-includes=/usr/local/include --with-libpfring-libraries=/usr/local/lib64 --with-libpcap-includes=/usr/local/include/pcap --with-libpcap-libraries=/usr/local/lib64 --enable-luajit --enable-geoip --enable-hiredis --enable-unittests --enable-af-packet --enable-prelude --enable-netmap --with-netmap-includes=/usr/local/include/net --enable-non-bundled-htp --with-libhtp-includes=/usr/local/include --with-libhtp-libraries=/usr/local/lib --enable-nflog --with-libnetfilter_log-includes=/usr/include/libnetfilter_log --with-libnetfilter_log-libraries=/usr/lib64 --enable-nfqueue --with-libnetfilter_queue-includes=/usr/include/libnetfilter_queue --with-libnetfilter_queue-libraries=/usr/lib64
```

```
1. modinfo pf_ring
   filename: /lib/modules/4.12.14-1p151.28.36-default/updates/pf_ring.ko
   alias: net-pf-27
   version: 7.5.0
   description: Packet capture acceleration and analysis
   author: ntop.org
   license: GPL
   suserelease: openSUSE Leap 15.1
   srcversion: 75A292B9B1771B425C1A677
```
depends:
retpoline: Y
vermagic: 4.12.14-lp151.28.36-default SMP mod_unload modversions
depends:
Parm: min_num_slots: Min number of ring slots (uint)
Parm: perfect_rules_hash_size: Perfect rules hash size (uint)
Parm: enable_tx_capture: Set to 1 to capture outgoing packets (uint)
Parm: enable_frag_coherence: Set to 1 to handle fragments (flow coherence) in clusters (uint)
Parm: enable_ip_defrag: Set to 1 to enable IP defragmentation (only rx traffic is defragmented) (uint)
Parm: quick_mode: Set to 1 to run at full speed but with up to one socket per interface (uint)
Parm: force_ring_lock: Set to 1 to force ring locking (automatically enable with rss) (uint)
Parm: enable_debug: Set to 1 to enable PF_RING debug tracing into the syslog, 2 for more verbosity (uint)
Parm: transparent_mode: (deprecated) (uint)

I am enclosing config.log

The error appears on line 3389 -

/usr/local/include/pfring.h:60:10: fatal error: linux/pf_ring.h: No such file or directory
The header file is present -

# ls -l /usr/local/include/pfring.h
-rw-r--r-- 1 root root 56044 Dec 14 03:00 /usr/local/include/pfring.h

History
#1 - 12/14/2019 04:07 PM - David Peters

David Peters wrote:

I am attempting to compile suricata-5.0.1 with pf ring enabled but the configuration script reports an error over pf ring library version lesser than version 6. I've install libpcap from pf_ring/userland

[...]

My system -

Linux linux-1vv0 4.12.14-lp151.28.36-default #1 SMP Fri Dec 6 13:50:27 UTC 2019 (8f4a495) x86_64 x86_64 x86_64 GNU/Linux

Configure arguments -

[...]

pf_ring version - PF_RING v.7.5.0

1. modinfo pf_ring
   alias: net-pf-27
   version: 7.5.0
   description: Packet capture acceleration and analysis
   author: ntop.org
   license: GPL
   suserelease: openSUSE Leap 15.1
   srcversion: 75A292B9B1771B425C1A677
   depends:
   retpoline: Y
   vermagic: 4.12.14-lp151.28.36-default SMP mod_unload modversions
Parm: min_num_slots: Min number of ring slots (uint)
Parm: perfect_rules_hash_size: Perfect rules hash size (uint)
Parm: enable_tx_capture: Set to 1 to capture outgoing packets (uint)
Parm: enable_frag_coherence: Set to 1 to handle fragments (flow coherence) in clusters (uint)
Parm: enable_ip_defrag: Set to 1 to enable IP defragmentation (only rx traffic is defragmented) (uint)
Parm: quick_mode: Set to 1 to run at full speed but with up to one socket per interface (uint)
Parm: force_ring_lock: Set to 1 to force ring locking (automatically enable with rss) (uint)
Parm: enable_debug: Set to 1 to enable PF_RING debug tracing into the syslog, 2 for more verbosity (uint)
Parm: transparent_mode: (deprecated) (uint)

I am enclosing config.log

The error appears on line 3389 -

06/13/2020
The header file is present -

This issue is fixed, I recompiled pfring and it installed pfring.h in /usr/include/linux. Sorry for the bother.

#2 - 12/14/2019 06:16 PM - Victor Julien
- Tracker changed from Bug to Support
- Status changed from New to Closed
- Effort deleted (medium)
- Difficulty deleted (medium)

Files
config.log  140 KB  12/14/2019  David Peters