Suricata - Bug #3873

NET_RAW capability dropped for NFQ mode when uid/gid is specified

08/10/2020 06:01 PM - Steven Tang

Status: New
Priority: Normal
Assignee: 
Category: 
Target version: 
Affected Versions: 5.0.3
Difficulty: low
Effort: low
Label:

Description
When using suricata with any uid/gid specified and nfq mode, the following code is run. As a result, NET_RAW capability is dropped. 
https://github.com/OISF/suricata/blob/fa2b46cdc3f539a31e917c3b63ede70309bcc0b0/src/util-privs.c#L78

However, when a reject rule is executed, libnet_init gets called via below code path and fails the worker thread.
https://github.com/OISF/suricata/blob/ac491c6e8da9982e4ff6de743de916666a4b16/src/respond-reject-libnet11.c#L109

Please add NET_RAW to the capabilities for NFQ mode as well if libnet is to be used.

Log snippet:
2020-08-10T14:22.84197991Z