How to fix tcpdump error with file permission denied

Author : Dan Nanni

Categories : Networking

Tagged as : apparmortcpdump

Question: When I run `tcpdump` with "-r" option to read from a packet dump file, I am getting an error from `tcpdump` saying that "file permission denied". I am getting this error even when I run `tcpdump` with root privilege. How can I fix this error?

If this problem happens on Ubuntu, it is possible that AppArmor (Ubuntu's access control system) may be interfering with `tcpdump` when it attempts to read from a packet dump.

To verify this behavior:

```
$ sudo cat /var/log/syslog | grep denied
```

```
  Jan  7 10:48:50 server kernel: [1706354.881017] type=1400 audit(1389109730.21
7:14): apparmor="DENIED" operation="open" parent=26733 profile="/usr/sbin/tcpdu
mp" name="/home/dev/packet.dump" pid=26734 comm="tcpdump" requested_mask="r" de
nied_mask="r" fsuid=0 ouid=1001
```

To avoid this problem, you can disable the restrictive AppArmor profile for `tcpdump` temporarily as follows.

```
$ sudo apparmor_parser -R /etc/apparmor.d/usr.sbin.tcpdump
```

If you want to disable the AppArmor profile permanently across reboots, refer to this tutorial.