Secure and Dependable Systems Module: CO-566
Constructor University Date: 2023-03-17
Dr. Jürgen Schönwälder **Due: 2023-03-24**

Problem Sheet #6

Problem 6.1: *denial of service protection using network packet filters* (3+3+4 = 10 points)

You are providing a web service on the IPv4 address 192.0.2.1. You want to achieve a high degree of availability of the service and hence you monitor the system's CPU load and the traffic received by the system. To solve this problem sheet, you will have to learn about the Linux framework for packet filtering and classification called nftables. Official documentation can be found on the netfilter project web site.

a) On day one, you observe a significant increase of the network traffic reaching the server. A packet sniffer reveals that the traffic is a large number of TCP SYN packets to the TCP ports 80 and 443 originating from the IPv4 addresses 198.51.100.7, 198.51.100.14, 203.0.113.21, and 203.0.113.28.

   You decide to resolve the problem by blocking all traffic from these IPv4 addresses (and you accept that this may include some legitimate traffic). Write nftables packet filter rules that block traffic from these addresses.

b) On day two, you observe a significant increase of the network traffic reaching the server but this time, the packet sniffer reveals that the traffic is coming from many different IPv4 addresses. The packets still are TCP SYN packets to the TCP ports 80 and 443.

   You decide to change to adapt your packet filtering strategy. Instead of filtering specific source addresses, you decide to limit the number of connection attempts to 60 SYN packets per second. Write nftables packet filter rules that rate limit traffic to your web service.

c) One day three, you are notified that many users have problems to reach your web service at prime times. It turns out that the limit is too strict.

   You decide to change the global limit to a limit per IPv4 address. Write nftables packet filter rules that rate limit traffic to your web service by source IPv4 address.

You may want to use virtual machines and the `hping3` tool to test whether your filter rules work.