Homework 4

1. Conduct an experiment presenting the effectiveness of SYN cookies:
   a. Disable SYN cookies (`# sysctl -w net.ipv4.tcp_syncookies = 0`), run a SYN Flooding attack against your system and describe how the system behaves (you can use e.g., `netstat`).
   b. Repeat the experiment with SYN cookies enabled (`# sysctl -w net.ipv4.tcp_syncookies = 1`).
   c. Compare and report the obtained results.

   (Note, that a SYN flooding attack has to target an open TCP port.)

2. Read about the DNSSEC Root Key rollover.
   a. Why this process is unsuccessful?
   b. If you could redesign DNSSEC from scratch, how would you handle key rollovers?

   Resources:
   https://www.icann.org/resources/pages/ksk-rollover
   https://blog.cloudflare.com/its-hard-to-change-the-keys-to-the-internet-and-it-involves-destroying-hsms
   https://www.csoonline.com/article/3223951/internet/dnssec-key-signing-key-rollover-are-you-ready.html

3. From the Alexa top 1 million sites [1] select **randomly** 200 domains.
   a. Show the selected domains (sorted in the lexicographic order).
   b. For each domain check whether it supports SSL/TLS (port 443 – make sure you do **not** scan for multiple ports!), DNSSEC, DANE, and CAA. Report the obtained results and attach logs demonstrating the queries and responses.

   [1] http://s3.amazonaws.com/alexa-static/top-1m.csv.zip
   Resources:
   https://arxiv.org/pdf/1702.05311.pdf