<u>SYN FloodExercise = Grading Key</u>

Please note that in this exercise you are given all the tests that the checkers will perform, including the expected results and a file with the results you need to receive.

| Test | Desired result | Grade |
|---|---|---|
| Software runs | The software doesn't hang or crash | 100 |
| IP address quality | All 51 suspicious IP addresses in the attached `filteredAttackersList` file | Minus 2 points for each missing address |
| Number of suspicious IP addresses | Between 50-150 | Minus 2 points for every deviation from the range |
| False alarms. The attacked network has an IP address range; check that none of them are identified as an attacker | No IP addresses are flagged from the attacked network | Minus 20 points |
| The detection algorithm is based on at least three of the following parameters:<br>1. Using the SYN flag<br>2. Use the ACK flag<br>3. Packet sending rate<br>4. Target IP address range<br>5. Source IP address range<br>6. Another creative idea that works | The algorithm includes at least three parameters from the list | Minus 20 if the algorithm is not documented. **No resubmission allowed!** |