Assignment 4 (Due Mar 27th)

Both security experts and attackers study network traffic to search for vulnerabilities. In this Lab, you will examine a network traffic trace, commonly known as a "pcap" file, to identify suspicious behaviors, e.g., *port scanning*.

Port scanning is a technique used by attackers to find vulnerable hosts that have services listening on certain ports. In a SYN scan attack, the scanner sends TCP SYN packets and wait replies from hosts that send back SYN+ACK packets. Since most hosts are not prepared to receive connections on any given port, during a port scan, a much smaller number of hosts will respond with SYN+ACK packets than originally received SYN packets. By observing this phenomenon in a trace file, you can identify source addresses that may be launching a port scan.

You are asked to develop a Java program, e.g., scannerfinder.java, which analyzes a pcap file in order to detect possible SYN scans. You might want to use a library for packet manipulation and dissection, e.g., jNetPcap. The jNetPcap library is available at https://sourceforge.net/projects/jnetpcap or https://github.com/ruedigergad/clj-net-pcap (the original jnetpcap.com page is down for unknown reason). You can find more information about parsing a .pcap file via https://javatutotial.net/tag/jnetpcap (there are quite a few such pages on Google). Your program will take the pcap file to be analyzed as a command-line parameter, e.g.,

```
java scannerfinder ./capture.pcap
```

The output of your program should be the set of IP addresses (one per line) that sent more than 3 times as many SYN packets as the number of SYN+ACK packets they received. A sample .pcap file captured from a real network can be downloaded from D2L (under Assignment 4). This trace file is provided by the LBNL/ICSI Enterprise Tracing Project. For this input, part of your program's output should look like (order of IP addresses could be different):

```
128.3.23.5
128.3.164.249
128.3.23.158
```

Submit your solution, the scannerfinder.java file as well as the output.txt file, on D2L and put your names in the comment section of both files. You could assume that jNetPcap library is available on the grader's computer.